Modul 1

Membandingkan Fungsi Jaringan Model OSI

- Bandingkan dan Kontraskan Lapisan Model OSI
  Pendahuluan: Bandingkan dan Kontraskan Lapisan Model OSI
  Jaringan dibangun di atas standar dan model umum yang menjelaskan bagaimana perangkat dan protokol saling terhubung. Dalam topik ini, Anda akan mengidentifikasi bagaimana implementasi dan dukungan sistem ini mengacu pada model referensi umum yang penting: model Open Systems Interconnection (OSI). Model OSI memecah proses komunikasi data menjadi lapisan-lapisan diskrit. Mampu mengidentifikasi lapisan OSI dan membandingkan fungsi perangkat dan protokol yang bekerja di setiap lapisan akan membantu Anda menerapkan dan memecahkan masalah jaringan.

- Model Interkoneksi Sistem Terbuka
  Jaringan adalah dua atau lebih sistem komputer yang dihubungkan oleh media transmisi dan berbagi satu atau lebih protokol yang memungkinkan mereka untuk bertukar data. Anda dapat memikirkan jaringan apa pun dalam hal node dan tautan. Node adalah perangkat yang mengirim, menerima, dan meneruskan data dan tautan adalah jalur komunikasi di antara mereka.

  Organisasi Internasional untuk Standardisasi (ISO) mengembangkan model referensi Open Systems Interconnection (OSI) (iso.org/standard/20269.html) untuk mempromosikan pemahaman tentang bagaimana komponen dalam sistem jaringan bekerja. Ini dilakukan dengan memisahkan fungsi komponen perangkat keras dan perangkat lunak menjadi tujuh lapisan terpisah. Setiap lapisan melakukan kelompok tugas yang berbeda yang diperlukan untuk komunikasi jaringan.



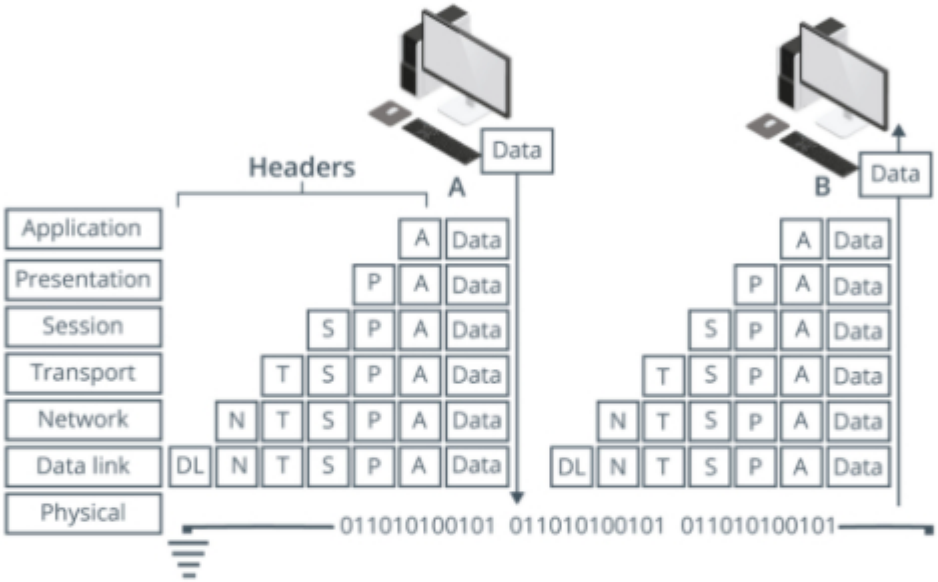
Model OSI.

Meskipun tidak semua sistem jaringan menerapkan lapisan menggunakan struktur yang tepat ini, mereka semua mengimplementasikan setiap tugas dalam beberapa cara. Model OSI bukanlah standar atau spesifikasi; itu berfungsi sebagai pedoman fungsional untuk merancang protokol jaringan, perangkat lunak, dan peralatan dan untuk pemecahan masalah jaringan.

Tips: Untuk mengingat tujuh lapisan, gunakan **mnemonic** berikut: **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing.

- Enkapsulasi dan Dekapsulasi Data
  Protokol jaringan adalah seperangkat aturan untuk bertukar data dalam format terstruktur. Sebuah protokol jaringan memiliki dua fungsi utama:
  - Addressing-Mendeskripsikan kemana pesan data harus pergi. Pada setiap lapisan, ada mekanisme yang berbeda untuk mengidentifikasi node dan aturan bagaimana mereka dapat mengirim dan menerima pesan.
  - Enkapsulasi-Menjelaskan bagaimana pesan data harus dikemas untuk transmisi. Enkapsulasi seperti amplop untuk surat, dengan perbedaan bahwa setiap lapisan membutuhkan amplopnya sendiri. Di setiap lapisan, protokol menambahkan bidang di header ke data (payload) apa pun yang diterimanya dari aplikasi atau protokol lain.

Sebuah jaringan akan melibatkan penggunaan banyak protokol yang berbeda yang beroperasi pada lapisan yang berbeda dari model OSI. Pada setiap lapisan, agar dua node dapat berkomunikasi, mereka harus menjalankan protokol yang sama. Protokol yang berjalan pada setiap lapisan berkomunikasi dengan lapisan yang setara (atau rekan) pada node lain. Komunikasi antara node pada lapisan yang sama digambarkan sebagai interaksi lapisan yang sama. Untuk mengirim atau menerima komunikasi, pada setiap node, setiap lapisan menyediakan layanan untuk lapisan di atasnya dan menggunakan layanan lapisan di bawahnya. Ini disebut sebagai interaksi lapisan yang berdekatan.



Enkapsulasi dan dekapsulasi. (Gambar © 123RF.com.)

Ketika sebuah pesan dikirim dari satu node ke node lain, ia berjalan menuruni tumpukan lapisan pada node pengirim, mencapai node penerima menggunakan media transmisi, dan kemudian melewati tumpukan pada node itu. Pada setiap level (kecuali lapisan fisik), node pengirim menambahkan header ke muatan data, membentuk “potongan” data yang disebut *protocol data unit* (PDU). Ini adalah proses enkapsulasi.

Misalnya, pada node pengirim, data dihasilkan oleh aplikasi, seperti HyperText Transfer Protocol (HTTP), yang akan menyertakan header aplikasinya sendiri. Pada lapisan transport, header Transport Control Protocol (TCP) ditambahkan ke data aplikasi ini. Pada lapisan jaringan, segmen TCP dibungkus dalam header Internet Protocol (IP). Paket IP dienkapsulasi dalam bingkai Ethernet di lapisan data link, kemudian aliran bit yang membentuk bingkai ditransmisikan melalui jaringan di lapisan fisik sebagai sinyal listrik termodulasi.

Node penerima melakukan proses sebaliknya, disebut sebagai dekapsulasi. Ini menerima aliran bit yang tiba di lapisan fisik dan menerjemahkan bingkai Ethernet. Itu mengekstrak paket IP dari bingkai ini dan menyelesaikan informasi di header IP, kemudian melakukan hal yang sama untuk TCP dan header aplikasi, akhirnya mengekstraksi data aplikasi HTTP untuk diproses oleh program perangkat lunak, seperti browser web atau server web.

Lapisan 1-*Physical*

Lapisan *physical* (PHY) dari model OSI (lapisan 1) bertanggung jawab untuk transmisi dan penerimaan sinyal yang mewakili bit data dari satu node ke node lain. Berbagai jenis media transmisi dapat diklasifikasikan sebagai kabel atau nirkabel:

- Kabel -Sebuah konduktor sinyal fisik disediakan antara dua node. Contohnya termasuk jenis kabel seperti kabel tembaga atau serat optik. Media kabel juga dapat digambarkan sebagai media yang dibatasi.
- Nirkabel -Menggunakan ruang kosong antar node, seperti radio microwave. Media nirkabel juga dapat digambarkan sebagai media tak terbatas.

Lapisan *physical* menentukan berikut ini:

- *Physical topology* -Tata letak node dan link seperti yang ditetapkan oleh media transmisi. Area jaringan yang lebih besar disebut segmen. Sebuah jaringan biasanya dibagi menjadi beberapa segmen untuk mengatasi pembatasan fisik dari media jaringan yang digunakan, untuk meningkatkan kinerja, atau untuk meningkatkan keamanan. Pada lapisan Fisik, segmen adalah tempat semua node berbagi akses ke media yang sama.
- *Physical interface* - Spesifikasi mekanis untuk media jaringan, seperti spesifikasi kabel, konektor media dan detail pin-out (jumlah dan fungsi berbagai pin dalam konektor jaringan), atau spesifikasi radio transceiver.
- Proses pengiriman dan penerimaan sinyal melalui media jaringan, termasuk skema modulasi dan pengaturan waktu/sinkronisasi.

Perangkat yang beroperasi pada lapisan *physical* meliputi:

- **Transceiver** -Bagian dari antarmuka jaringan yang mengirim dan menerima sinyal melalui media jaringan.
- **Repeater** -Sebuah perangkat yang memperkuat sinyal elektronik untuk memperpanjang jarak maksimum yang diijinkan untuk jenis media.
- **Hub** -Sebuah repeater multiport, digunakan sebagai titik pusat koneksi untuk node.
- **Konverter media** -Perangkat yang mengubah satu jenis pensinyalan media ke yang lain.

- **Modem** -Perangkat yang melakukan beberapa jenis modulasi dan demodulasi sinyal, seperti mengirim data digital melalui saluran analog.

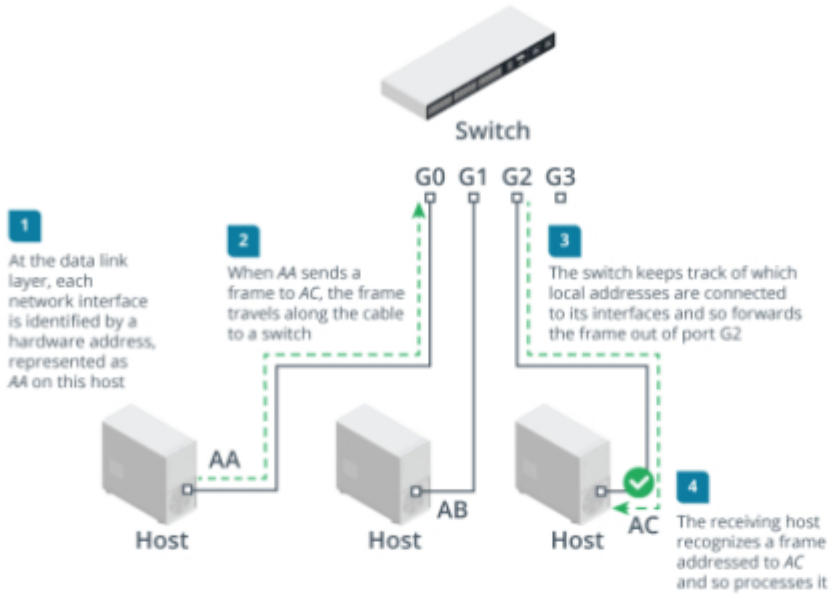
Lapisan 2-Data Link

Lapisan data link (lapisan 2) bertanggung jawab untuk mentransfer data antar node pada segmen logis yang sama. Pada lapisan Data Link, segmen adalah segmen di mana semua node dapat mengirim lalu lintas ke satu sama lain menggunakan alamat perangkat keras, terlepas dari apakah mereka berbagi akses ke media yang sama. Segmen lapisan 2 mungkin mencakup beberapa segmen fisik. Ini disebut sebagai topologi logis.

Relatif sedikit jaringan yang didasarkan pada menghubungkan host secara langsung bersama-sama. Daripada membuat host membangun hubungan langsung satu sama lain, setiap host terhubung ke node pusat, seperti switch atau titik akses nirkabel. Node pusat menyediakan fungsi penerusan, menerima komunikasi dari satu node dan mengirimkannya ke node lain. Alamat antarmuka dalam segmen lapisan 2 yang sama digambarkan sebagai alamat lokal atau alamat perangkat keras.

Node yang mengirim dan menerima informasi disebut sebagai sistem akhir atau sebagai node host. Jenis node ini termasuk komputer, laptop, server, telepon Voice over IP (VoIP), smartphone, dan printer. Sebuah node yang hanya menyediakan fungsi penerusan disebut sebagai sistem perantara atau node infrastruktur.

Lapisan data link mengatur aliran bit yang datang dari lapisan fisik ke dalam unit terstruktur yang disebut frame. Setiap frame berisi paket lapisan jaringan sebagai muatannya. Lapisan data link menambahkan informasi kontrol ke payload dalam bentuk bidang header. Bidang ini mencakup alamat perangkat keras sumber dan tujuan, ditambah pemeriksaan kesalahan dasar untuk menguji apakah bingkai diterima utuh.



Komunikasi pada lapisan 2 model OSI. (Gambar © 123RF.com)

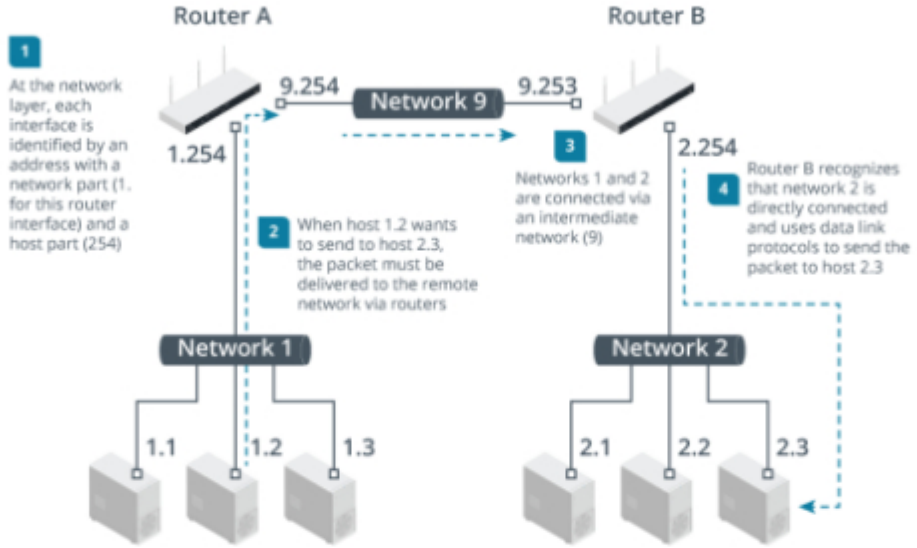
Perangkat yang beroperasi pada lapisan data link meliputi:

- ***Network adapter or network interface card*** (NIC) - Sebuah NIC bergabung dengan host sistem akhir ke media jaringan (kabel atau nirkabel) dan memungkinkannya untuk berkomunikasi melalui jaringan dengan merakit dan membongkar bingkai.
- ***Bridge*** -Jembatan adalah jenis sistem perantara yang menggabungkan segmen jaringan fisik sambil meminimalkan pengurangan kinerja karena memiliki lebih banyak node pada jaringan yang sama. Sebuah jembatan memiliki beberapa port, yang masing-masing berfungsi sebagai antarmuka jaringan.
- ***Switch*** -Jenis jembatan tingkat lanjut dengan banyak port. Switch menciptakan hubungan antara sejumlah besar node dengan lebih efisien.
- ***Wireless access point*** (AP) -Sebuah AP memungkinkan node dengan kartu jaringan nirkabel untuk berkomunikasi dan menciptakan jembatan antara jaringan nirkabel dan yang kabel.

Lapisan 3-Network

Lapisan jaringan (lapisan 3) bertanggung jawab untuk memindahkan data di sekitar jaringan jaringan, yang dikenal sebagai internetwork atau Internet. Sementara lapisan data link mampu meneruskan data dengan menggunakan alamat perangkat keras dalam satu segmen, lapisan jaringan memindahkan informasi di sekitar

internetwork dengan menggunakan jaringan logis dan ID host. Jaringannya seringkali heterogen; yaitu, mereka menggunakan berbagai media lapisan fisik dan protokol tautan data. Alat utama yang bekerja pada layer 3 adalah router.



Komunikasi pada lapisan 3 model OSI. (Gambar © 123RF.com)

Lapisan network meneruskan informasi antar jaringan dengan memeriksa *network-layer address* tujuan atau *logical network address*. Paket diteruskan, router demi router (atau hop demi hop), melalui internetwork ke jaringan target. Setelah mencapai jaringan tujuan, alamat perangkat keras dapat digunakan untuk mengirimkan paket ke node target.

Konvensi umum adalah untuk menggambarkan PDU yang dikemas pada *network layer as packets or datagrams*, dan pesan yang dikemas pada lapisan *data link layer as frames*. Namun, paket sering digunakan untuk menggambarkan PDU pada lapisan mana pun.

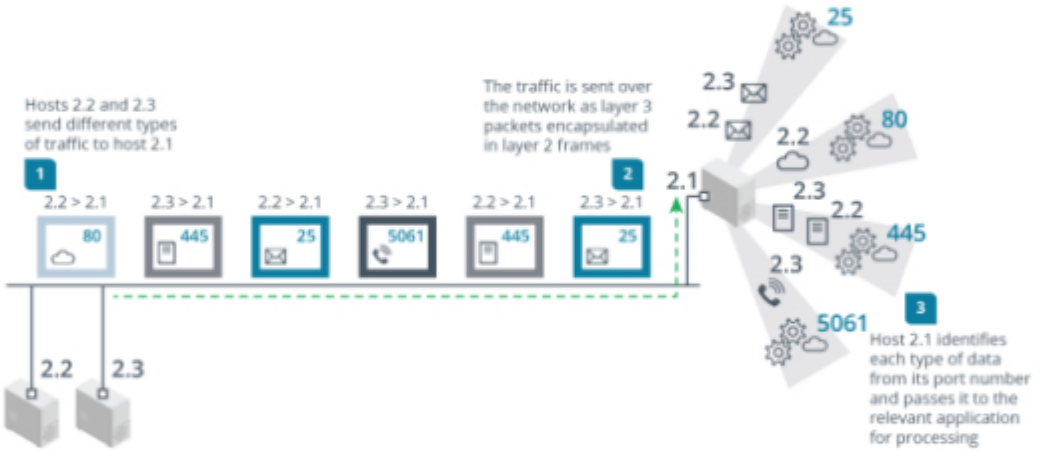
Biasanya penting untuk lalu lintas yang lewat di antara jaringan untuk disaring. Firewall dasar beroperasi pada lapisan 3 untuk menegakkan *access control list* (ACL). ACL jaringan adalah daftar alamat dan jenis lalu lintas yang diizinkan atau diblokir.

Lapisan 4-Transport

Tiga lapisan pertama dari model OSI terutama berkaitan dengan *moving frames and datagrams* antara node dan jaringan. Pada lapisan transport juga dikenal sebagai

end-to-end atau host-to-host *layer-the content of the packets becomes significant.*. Setiap host pada jaringan akan berkomunikasi dengan banyak host lain menggunakan berbagai jenis data jaringan. Salah satu fungsi dari lapisan transport adalah untuk mengidentifikasi setiap jenis aplikasi jaringan dengan memberikan nomor port. Misalnya, data yang diminta dari aplikasi web HTTP dapat diidentifikasi sebagai port 80, sedangkan data yang dikirim ke server email dapat diidentifikasi sebagai port 25.

Pada lapisan transport, pada host pengirim, data dari lapisan atas dikemas sebagai rangkaian PDU lapisan 4, disebut sebagai segmen. Setiap segmen ditandai dengan nomor port aplikasi. Segmen tersebut kemudian diteruskan ke lapisan jaringan untuk pengiriman. Banyak host yang berbeda dapat mengirimkan beberapa HTTP dan paket email secara bersamaan. Ini digandakan menggunakan nomor port bersama dengan alamat jaringan sumber dan tujuan ke tautan yang sama.



Komunikasi pada lapisan 4 (transportasi) dari model OSI. (Gambar © 123RF.com)

Pada lapisan *network* dan *data link*, nomor port diabaikan-ini menjadi bagian dari muatan data dan tidak terlihat oleh router dan sakelar yang mengimplementasikan fungsi pengalamatan dan penerusan lapisan ini. Di host penerima, setiap segmen didekapsulasi, diidentifikasi dengan nomor portnya, dan diteruskan ke handler yang relevan di lapisan *application*. Dengan kata lain, arus lalu lintas de-multiplexed.

Lapisan transport juga dapat mengimplementasikan mekanisme pengiriman data yang andal, jika aplikasi memerlukannya. Pengiriman yang andal berarti bahwa setiap paket yang hilang atau rusak akan dikirim ulang.

Perangkat yang bekerja di lapisan transport termasuk sakelar multilayer-biasanya berfungsi sebagai penyeimbang beban-dan banyak jenis peralatan keamanan, seperti firewall yang lebih canggih dan intrusion detection systems (IDS).

Upper Layers

Upper layers model OSI kurang jelas terkait dengan protokol dunia nyata yang berbeda. Lapisan ini mengumpulkan berbagai fungsi yang menyediakan antarmuka yang berguna antara aplikasi perangkat lunak dan *transport layer*.

Layer 5-Session

Sebagian besar protokol aplikasi memerlukan pertukaran beberapa pesan antara klien dan server. Pertukaran urutan pesan seperti ini disebut sesi atau dialog. Lapisan *session* (lapisan 5) mewakili fungsi yang mengelola proses pembuatan dialog, mengelola transfer data, dan kemudian mengakhiri (atau meruntuhkan) sesi.

Layer 6-Presentation

Layer presentasi (layer 6) mengubah data antara format yang diperlukan untuk jaringan dan format yang diperlukan untuk aplikasi. Misalnya, lapisan presentasi digunakan untuk konversi kumpulan karakter, seperti antara Kode Standar Amerika untuk Pertukaran Informasi (ASCII) dan Unicode. Lapisan presentasi juga dapat dipahami sebagai pendukung kompresi dan enkripsi data. Namun, dalam istilah praktis, fungsi-fungsi ini sering diimplementasikan oleh perangkat enkripsi dan protokol yang berjalan di lapisan bawah tumpukan atau hanya di dalam lapisan aplikasi yang homogen.

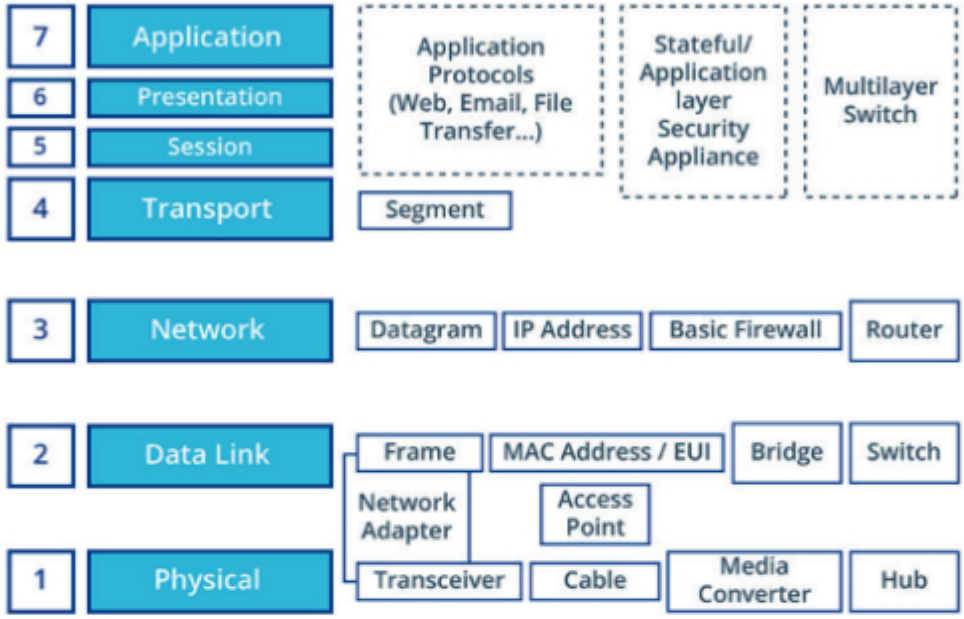
Layer 7-Application

Layer application (layer 7) berada di atas tumpukan OSI. Protokol lapisan aplikasi tidak merangkum protokol lain atau menyediakan layanan ke protokol apa pun. Protokol lapisan aplikasi menyediakan antarmuka untuk program perangkat lunak pada host jaringan yang telah membentuk saluran komunikasi melalui protokol tingkat yang lebih rendah untuk bertukar data.

Secara lebih luas, protokol lapisan atas menyediakan sebagian besar layanan yang membuat jaringan berguna, bukan hanya fungsional, termasuk penelusuran web, email dan komunikasi, pencarian direktori, pencetakan jarak jauh, dan layanan basis data.

Ringkasan Model OSI

Gambar berikut merangkum model OSI, daftar PDU di setiap lapisan, bersama dengan jenis perangkat yang bekerja di setiap lapisan.



Perangkat dan konsep direpresentasikan pada lapisan model OSI yang relevan.

Configure SOHO Networks

Introduction: Configure SOHO Networks

Model OSI melibatkan cukup banyak abstraksi. Sebagai contoh praktis, ada baiknya memeriksa bagaimana jaringan dasar diimplementasikan. Dalam topik ini, Anda akan mempelajari opsi koneksi dan konfigurasi untuk komponen dalam router small office/home office (SOHO) biasa.

Router SOHO

Jaringan dengan ukuran berbeda diklasifikasikan dengan cara yang berbeda. Sebuah jaringan di satu lokasi sering digambarkan sebagai jaringan area lokal (LAN). Definisi ini mencakup banyak ukuran jaringan yang berbeda dengan fungsi dan kemampuan yang sangat bervariasi. Ini dapat mencakup jaringan perumahan dengan beberapa komputer, dan jaringan perusahaan dengan ratusan server dan ribuan workstation.

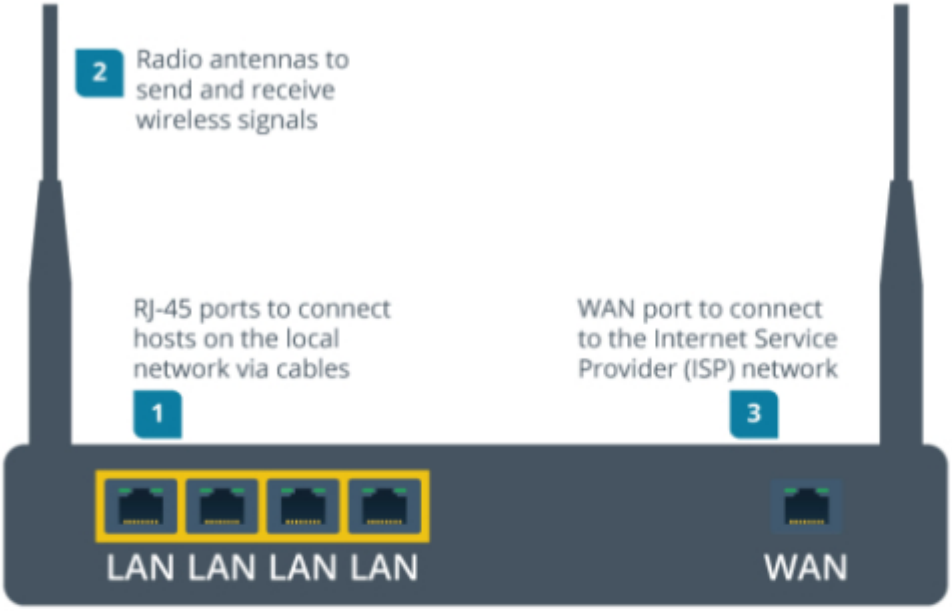
Small office/home office (SOHO) adalah kategori LAN dengan sejumlah kecil host komputasi yang biasanya mengandalkan satu alat terintegrasi untuk konektivitas lokal dan Internet.

Jaringan seperti Internet yang terletak di wilayah geografis yang berbeda tetapi dengan tautan bersama disebut jaringan area luas (WAN). Sistem perantara yang memberi daya pada jaringan SOHO biasanya digambarkan sebagai router SOHO karena salah satu fungsi utamanya adalah meneruskan lalu lintas antara LAN dan WAN. Namun, perutean sebenarnya hanyalah salah satu fungsinya. Kita dapat menggunakan model OSI untuk menganalisis masing-masing secara bergantian.

Physical Layer Functions

Mulai dari lapisan 1, router SOHO menyediakan koneksi fisik berikut:

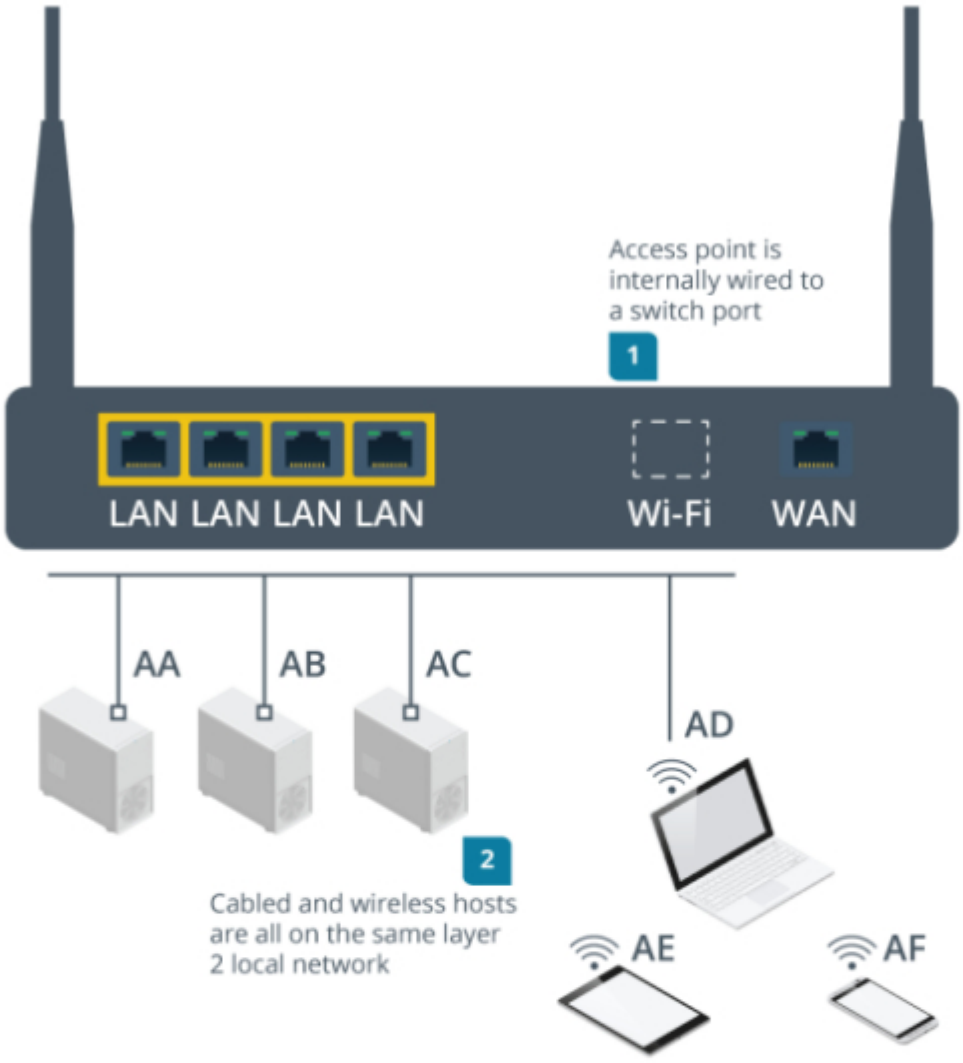
- Sejumlah port RJ-45 (biasanya empat) untuk terhubung ke jaringan kabel lokal. Ini biasanya diberi label sebagai port LAN.
- Antena radio untuk mengirim dan menerima sinyal nirkabel.
- Jenis modem (biasanya kabel atau saluran pelanggan digital) untuk terhubung ke jaringan Penyedia Layanan Internet (ISP). Ini biasanya diberi label sebagai port WAN. Pada contoh dalam diagram, antarmuka adalah port RJ-45 lain, yang dirancang untuk terhubung ke serat ke layanan Internet lokal menggunakan teknologi Ethernet yang sama dengan jaringan lokal. Pada router SOHO lainnya, mungkin ada jenis modem WAN yang berbeda, seperti port RJ-11 untuk terhubung ke layanan digital subscriber line (DSL).



Opsi konektivitas lapisan fisik pada router SOHO.

Pada lapisan 2, router SOHO mengimplementasikan fungsi berikut untuk menggunakan adaptor lapisan fisiknya:

- Sakelar Ethernet - jack RJ-45 dihubungkan secara internal oleh sakelar Ethernet.
- Titik akses nirkabel -antena radio menerapkan beberapa versi standar Wi-Fi. Titik akses berfungsi sebagai hub nirkabel, memungkinkan stasiun (PC, tablet, smartphone, dan printer) membentuk jaringan nirkabel. Titik akses juga disambungkan ke sakelar Ethernet melalui port internal. Ini membentuk jembatan antara segmen kabel dan nirkabel, menciptakan jaringan lokal logis tunggal.

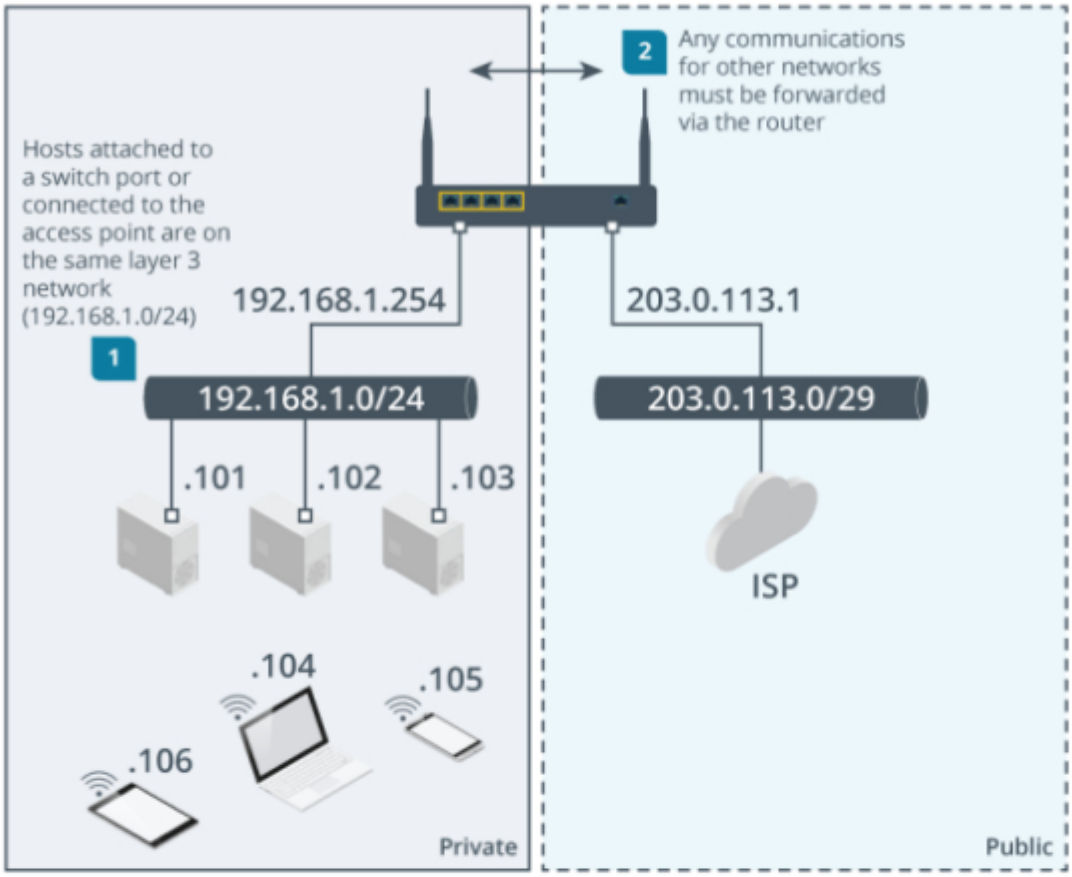


Segmen jaringan lokal lapisan data link. (Gambar © 123RF.com)

Pada lapisan ini, setiap antarmuka host diidentifikasi oleh alamat kontrol akses media (MAC).

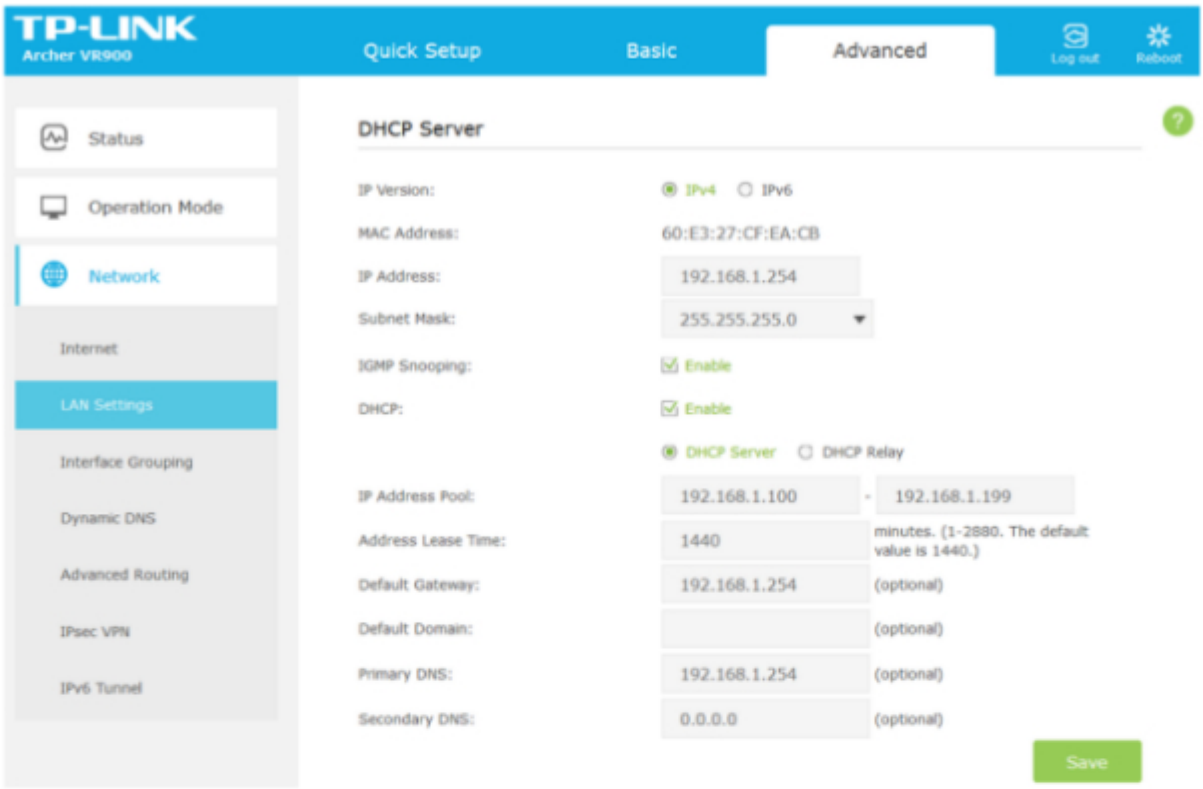
Network Layer Functions

Pada lapisan 3, lapisan jaringan, bagian perutean dari router SOHO membuat keputusan penerusan antara jaringan pribadi lokal dan Internet publik. Zona ini dibedakan berdasarkan alamat protokol internet (IP). Jaringan lokal menggunakan rentang alamat IP pribadi, seperti 192.168.1.0/24. Router SOHO itu sendiri diidentifikasi dengan alamat dalam kisaran ini, seperti 192.168.1.1 atau 192.168.1.254 .



Segmen pribadi dan publik lapisan jaringan. (Gambar © 123RF.com)

Router menjalankan server protokol konfigurasi host dinamis (DHCP) untuk mengalokasikan alamat unik ke setiap host yang terhubung melalui port Ethernet atau melalui titik akses nirkabel. Alamat yang diberikan ke klien menggunakan tiga oktet pertama yang sama dengan alamat router: 192.168.1. Oktet terakhir dapat berupa nilai dari 1 hingga 254, tidak termasuk nilai mana pun yang digunakan oleh router.



Mengkonfigurasi alamat LAN menggunakan DHCP pada router nirkabel. (Tangkapan layar milik TP-Link Technologies Co., Ltd.)

Antarmuka WAN router SOHO dialokasikan alamat IP publik, katakanlah 203.0.113.1, oleh penyedia layanan internet. Ketika sebuah host di jaringan lokal mencoba mengakses alamat IP yang valid di luar rentang 192.168.1.0/24, router meneruskan paket itu melalui antarmuka WAN dan mengarahkan balasan apa pun kembali ke host di LAN.



Mengonfigurasi antarmuka WAN (internet) pada router nirkabel. Parameter ini disediakan oleh ISP. Banyak layanan ISP menggunakan DHCP untuk mengalokasikan alamat WAN dinamis, tetapi beberapa menawarkan pengalamatan statis. (Tangkapan layar milik TP-Link Technologies Co., Ltd.)

Transport and Application Layer and Security Functions

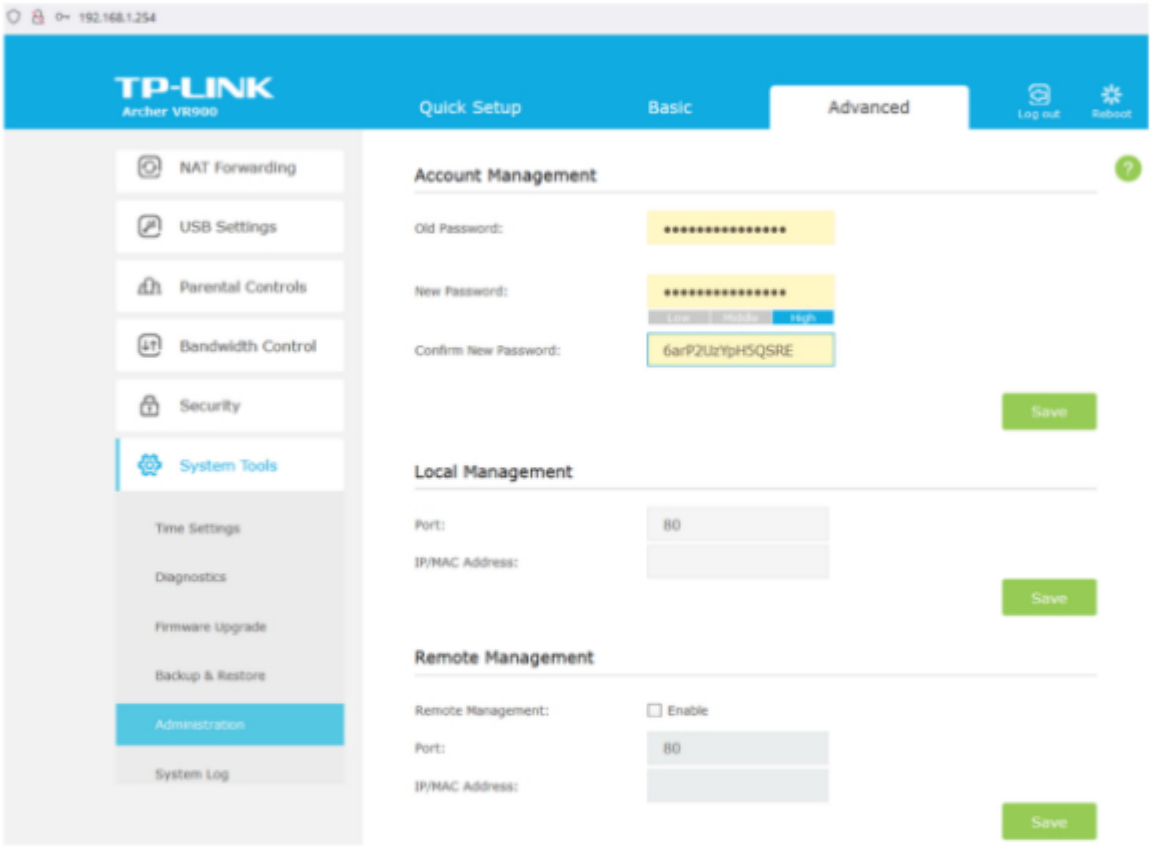
Tidak ada lapisan model OSI terpisah untuk keamanan. Sebaliknya, masalah keamanan dapat muncul dan solusi diperlukan di setiap lapisan. Keamanan jaringan pada dasarnya adalah masalah mengizinkan atau mencegah perangkat, pengguna, dan layanan (aplikasi) menggunakan jaringan. Antarmuka WAN adalah perimeter jaringan. Router SOHO dapat menerapkan aturan penyaringan untuk lalu lintas yang dikirim antara zona publik dan pribadi, menerapkan firewall. Firewall dapat dikonfigurasi untuk memblokir lalu lintas berdasarkan alamat IP sumber atau tujuan dan juga pada jenis aplikasi.

Pada lapisan 4, setiap aplikasi diidentifikasi dengan nomor port, seperti 80 untuk lalu lintas web protokol transfer hypertext (HTTP) atau 25 untuk lalu lintas email Simple Mail Transfer Protocol (SMTP).

Firewall di router dapat dikonfigurasi dengan aturan yang menentukan perilaku untuk setiap port. Misalnya, komputer di jaringan mungkin menggunakan protokol blok pesan server (SMB) untuk berbagi file. Host di Internet tidak akan dapat mengakses file bersama ini, sehingga port SMB akan diblokir secara default pada antarmuka WAN tetapi diizinkan pada antarmuka LAN dan WLAN.

Setiap host dapat terhubung ke port RJ-45 pada router dan bergabung dengan jaringan. Jaringan nirkabel biasanya dilindungi oleh sistem enkripsi yang mengharuskan setiap stasiun dikonfigurasi dengan kunci berbasis frasa sandi untuk bergabung dengan jaringan.

Akses ke antarmuka manajemen router dan pengaturan konfigurasinya dilindungi oleh frasa sandi akun administratif. Karena router terhubung ke Internet, sangat penting untuk mengonfigurasi frasa sandi yang kuat.



Mengonfigurasi antarmuka manajemen pada perute nirkabel. (Tangkapan layar milik TP-Link Technologies Co., Ltd.)

Internet

Antarmuka WAN dari router menghubungkan jaringan SOHO ke Internet.

The Public Switched Telephone Network

Sebagian besar akses Internet pelanggan SOHO difasilitasi melalui jaringan telepon umum (PSTN). Router SOHO digambarkan sebagai peralatan tempat pelanggan (CPE). Lebih luas lagi, ini adalah peralatan terminasi dan perutean yang ditempatkan di lokasi

pelanggan. Beberapa dari peralatan ini mungkin dimiliki atau disewa dari perusahaan telekomunikasi (atau telco); beberapa mungkin dimiliki oleh pelanggan.

CPE terhubung melalui modem dan port WAN ke loop lokal. Ini adalah pemasangan kabel dari tempat pelanggan ke bursa lokal. Titik di mana pemasangan kabel telekomunikasi memasuki tempat pelanggan disebut sebagai titik demarkasi (sering disingkat menjadi demarc).

Internet Service Providers

Infrastruktur utama Internet terdiri dari saluran bandwidth tinggi yang menghubungkan Internet eXchange Points (IXPs). Dalam pusat data IXP, ISP membangun hubungan antara jaringan mereka, menggunakan pengaturan transit dan peering untuk membawa lalu lintas ke dan dari bagian internet yang tidak mereka miliki secara fisik. Ada hierarki berjenjang dari ISP yang mencerminkan sejauh mana mereka bergantung pada pengaturan transit dengan ISP lain.

Internet Standards

Meskipun tidak ada satu organisasi pun yang memiliki Internet atau teknologinya, beberapa organisasi bertanggung jawab atas pengembangan internet dan menyetujui standar dan protokol umum.

- **Internet Assigned Numbers Authority (IANA)** (iana.org) -mengelola alokasi alamat IP dan pemeliharaan ruang domain tingkat atas. IANA saat ini dijalankan oleh Internet Corporation for Assigned Names and Numbers (ICANN). IANA mengalokasikan alamat ke pendaftar regional yang kemudian mengalokasikannya ke pendaftar lokal atau ISP. Registri regional adalah Asia/Pasifik (APNIC), Amerika Utara dan Afrika Selatan (ARIN), Amerika Latin (LACNIC), dan Eropa, Afrika Utara, Asia Tengah, dan Timur Tengah (RIPE NCC).
- **Internet Engineering Task Force** (IETF) (ietf.org) -berfokus pada solusi untuk masalah Internet dan penerapan standar baru, diterbitkan sebagai Requests for Comments (RFCs). Beberapa RFC menggambarkan layanan jaringan atau protokol dan implementasinya, sementara yang lain meringkas kebijakan. RFC yang lebih lama tidak pernah diperbarui. Jika perubahan diperlukan, RFC baru diterbitkan dengan nomor baru. Tidak semua RFC menggambarkan standar. Beberapa ditunjuk sebagai informasi, sementara yang lain eksperimental. Repositori resmi untuk RFC ada di rfc-editor.org .

Referensi ke RFC dalam kursus ini adalah untuk informasi Anda jika Anda ingin membaca lebih lanjut. Anda tidak perlu mempelajarinya untuk ujian sertifikasi.

Model OSI memiliki definisi yang lebih ketat dari lapisan Sesi, Presentasi, dan Aplikasi daripada tipikal protokol aktual yang digunakan pada jaringan. Model Internet

(tools.ietf.org/html/rfc1122) menggunakan hierarki empat lapisan yang lebih sederhana, dengan lapisan tautan mewakili lapisan OSI 1 dan 2, lapisan 3 disebut sebagai lapisan Internet, lapisan Transport yang memetakan kira-kira ke lapisan 4 dan 5, dan lapisan Aplikasi yang sesuai dengan lapisan 6 dan 7.

Hexadecimal Notation

Untuk menafsirkan alamat jaringan, Anda harus memahami konsep sistem penomoran dasar. Untuk memulai dengan yang akrab; penomoran desimal juga disebut sebagai basis 10. Basis 10 berarti bahwa setiap digit dapat memiliki satu dari sepuluh nilai yang mungkin (0 hingga 9). Sebuah angka yang ditempatkan di sebelah kiri angka lain memiliki 10 kali nilai angka di sebelah kanan. Misalnya, angka 255 dapat ditulis sebagai berikut:

(2x10x10)+(5x10)+5

Biner adalah basis 2, jadi digit pada posisi tertentu hanya dapat memiliki satu dari dua nilai (0 atau 1), dan setiap posisi tempat adalah pangkat 2. Nilai biner 11111111 dapat dikonversi ke nilai desimal 255 dengan jumlah berikut:

(1x2x2x2x2x2x2x2)+(1x2x2x2x2x2x2)+(1x2x2x2x2x2)+(1x2x2x2x2)+(1x2x2x2)+(1x2x2)+(1x2)+1

Seperti yang Anda lihat, dibutuhkan 8 digit biner untuk mewakili nilai desimal hingga 255. Jumlah bit ini disebut byte atau oktet. Empat angka desimal di alamat IP WAN router SOHO 203.0.113.1 adalah oktet.

Sementara komputer memproses semuanya dalam biner, nilainya menghasilkan string yang sangat panjang jika harus ditulis atau dimasukkan ke dalam dialog konfigurasi. Notasi heksadesimal (atau hex) adalah cara yang nyaman untuk merujuk pada urutan byte yang panjang yang digunakan dalam beberapa jenis alamat jaringan lainnya. Hex adalah basis 16 dengan nilai yang mungkin dari setiap digit yang diwakili oleh angka 0 sampai 9 dan karakter A, B, C, D, E, dan F.

Gunakan tabel berikut untuk membantu mengonversi antara nilai desimal, biner, dan heksadesimal.

Decimal	Hexadecimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110

Decimal	Hexadecimal	Binary
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Seperti yang Anda lihat dari tabel, setiap digit hex berbaris rapi dengan empat digit biner (gigit). Setiap byte atau oktet dapat dinyatakan sebagai dua digit hex. Misalnya, nilai desimal 255 adalah FF dalam heksa. Ini terkadang ditulis sebagai 0xFF untuk kejelasan.

Modul 2

Menyebarkan kabel ethernet

- Ringkas Standar Ethernet
  Pendahuluan: Ringkasan Standar Ethernet
  Dalam topik ini, Anda akan mengidentifikasi komponen yang digunakan dalam implementasi jaringan Ethernet. Ethernet mendominasi pasar produk LAN kabel. Popularitasnya sebagian besar didasarkan pada kemudahan instalasi dan kemampuan untuk ditingkatkan. Jaringan besar dan kecil menggunakan teknologi Ethernet untuk menyediakan layanan *backbone* dan *end-user*. Karena penyebaran Ethernet yang luas saat ini, Anda pasti akan diminta untuk mengelola dan memecahkan masalah jaringan Ethernet.

- TRANSMISI DATA JARINGAN
  Semua sinyal jaringan menggunakan radiasi elektromagnetik dari satu jenis atau lainnya. Radiasi elektromagnetik berarti transmisi sinyal sebagai arus listrik, cahaya inframerah, atau gelombang radio. Radiasi elektromagnetik membentuk gelombang pembawa dengan *bandwidth* atau rentang frekuensi tertentu. Sinyal ditransmisikan melalui gelombang dengan skema modulasi dan pengkodean. Salah satu contoh pengkodean adalah transisi antara keadaan tegangan rendah dan tinggi dalam rangkaian listrik, memanfaatkan karakteristik gelombang yang disebut amplitudo. Perubahan tegangan ini dapat mengkodekan informasi digital-satu dan nol atau bit. Semakin banyak bandwidth yang tersedia di media, semakin besar jumlah data yang dapat dikodekan.

  Tips: Definisi sempit *bandwidth* adalah rentang frekuensi yang diukur dalam siklus per detik atau Hertz (Hz), tetapi istilah ini sangat banyak digunakan dalam jaringan data yang berarti jumlah data yang dapat ditransfer, diukur kelipatan bit per detik (bps) . Metode pengkodean berarti bahwa, misalnya, sinyal dengan bandwidth frekuensi 100 MHz dapat mentransfer lebih dari 100 Mbps.

  - Kabel Tembaga
    Kabel tembaga digunakan untuk mengirimkan sinyal listrik. Kabel antara dua node menciptakan sirkuit listrik tegangan rendah antara antarmuka pada node. Ada dua jenis utama kabel tembaga: *twisted pair* dan *coaxial* (membujuk). Kabel tembaga mengalami redaman tinggi, yang berarti bahwa sinyal dengan cepat kehilangan kekuatan pada tautan yang panjang. Kabel pasangan terpilin dinilai sesuai standar Cat.

  - Kabel serat optik
    Kabel serat optik membawa radiasi frekuensi sangat tinggi di bagian cahaya inframerah dari spektrum elektromagnetik. Sinyal cahaya juga tidak rentan terhadap gangguan atau kebisingan dari sumber lain dan kurang terpengaruh oleh redaman. Akibatnya, kabel serat optik mendukung bandwidth yang lebih

tinggi melalui tautan yang lebih panjang daripada kabel tembaga. Pengkabelan serat optik dibagi menjadi tipe *Single Mode* (SMF) dan *MultiMode* (MMF), dan MMF dikategorikan menurut sebutan Mode Optik (OM1, OM2, OM3, dan OM4).

- STANDAR ETHERNET
  Selama bertahun-tahun, banyak protokol, standar, dan produk telah dikembangkan untuk mengimplementasikan fungsi lapisan fisik dan data link dari model OSI. Yang paling penting adalah standar Ethernet 802.3 *Institute of Electrical and Electronics Engineers* (IEEE) (ieee802.org/3).

  Standar Ethernet memberikan jaminan bahwa pemasangan kabel jaringan akan memenuhi persyaratan bandwidth aplikasi. Standar menentukan kecepatan bit yang harus dicapai pada berbagai jenis media hingga batasan jarak yang didukung. Spesifikasi media Ethernet ini diberi nama menggunakan konvensi tiga bagian, yang sering disebut sebagai xBASE-y. Ini menjelaskan:

  - Kecepatan bit dalam megabit per detik (Mbps) atau gigabit per detik (Gbps).
  - Modus sinyal (*baseband* atau *broadband*). Semua jenis Ethernet arus utama menggunakan transmisi pita dasar, jadi Anda hanya akan melihat spesifikasi dalam bentuk xBASE-y.
  - Sebuah penunjuk untuk jenis media.

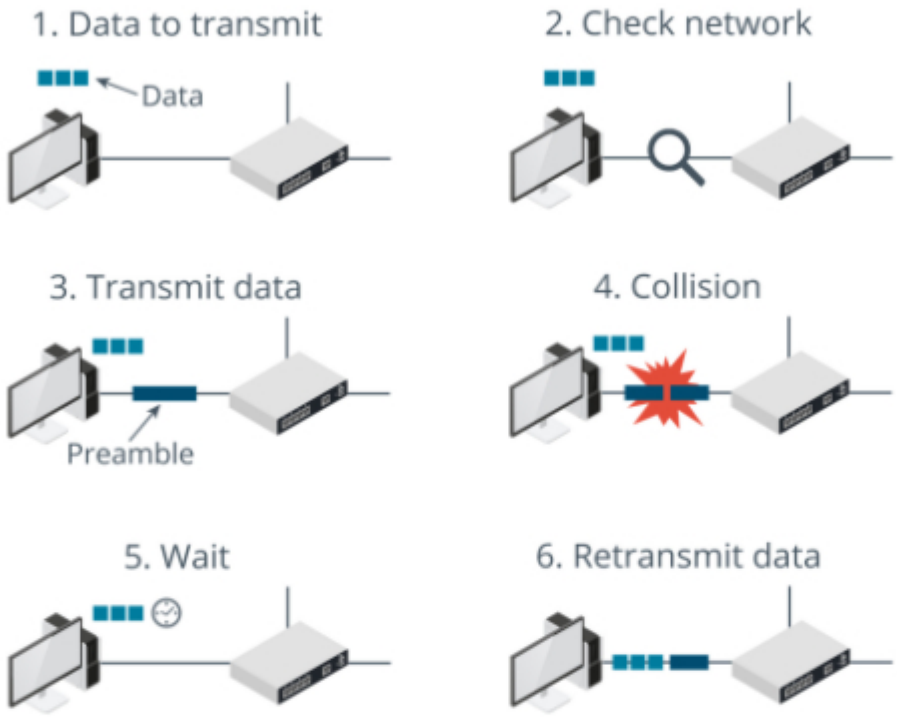
  Misalnya, 10BASE-T menunjukkan implementasi awal yang bekerja pada 10 Mbps (10), menggunakan sinyal pita dasar (BASE), dan berjalan di atas kabel tembaga pasangan terpilin (-T).

- KONTROL AKSES MEDIA DAN DOMAIN TABRAKAN
  Ethernet adalah jaringan area akses ganda, yang berarti bahwa kapasitas komunikasi yang tersedia dibagi antara node yang terhubung ke media yang sama. *Media access control* (MAC) mengacu pada metode yang digunakan teknologi jaringan untuk menentukan kapan node dapat berkomunikasi pada media bersama dan untuk menangani kemungkinan masalah, seperti dua perangkat yang mencoba berkomunikasi secara bersamaan.

  Ethernet menggunakan sistem MAC berbasis pertentangan. Setiap node jaringan yang terhubung ke media yang sama berada dalam domain tabrakan yang sama. Ketika dua node mengirimkan pada saat yang sama, sinyal dikatakan bertabrakan dan tidak ada sinyal yang dapat mencapai tujuannya. Ini berarti bahwa mereka harus dikirim ulang, mengurangi bandwidth yang tersedia. Tabrakan menjadi lebih sering karena lebih banyak node ditambahkan, dan akibatnya kecepatan data efektif berkurang.

  Protokol Ethernet yang mengatur pertikaian dan akses media disebut *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD). Tabrakan adalah keadaan ketika sinyal hadir pada saluran transmisi dan penerimaan antarmuka secara bersamaan. Saat

mendeteksi tabrakan, node menyiarkan sinyal kemacetan. Setiap node yang mencoba untuk menggunakan media kemudian menunggu periode acak (*backoff*) sebelum mencoba untuk mengirimkan lagi.



Metode akses media CSMA/CD. (Images © 123RF.com.)

Mekanisme deteksi tabrakan berarti bahwa hanya transmisi *half-duplex* yang dimungkinkan. Ini berarti bahwa sebuah node dapat mengirim atau menerima, tetapi tidak dapat melakukan keduanya secara bersamaan.

Dalam topologi pengkabelan 10BASE-T, setiap node disambungkan ke hub Ethernet. Hub mengulangi sinyal yang masuk ke setiap node yang terhubung. Akibatnya, setiap host yang terhubung ke hub yang sama berada dalam domain tabrakan yang sama. Standar 10BASE-T berasal dari tahun 1990. Anda sangat tidak mungkin menemukannya dikerahkan ke jaringan mana pun.

- STANDAR GIGABIT ETHERNET

Gigabit Ethernet dibangun berdasarkan standar yang ditentukan untuk Ethernet dan Fast Ethernet untuk menerapkan kecepatan 1000 Mbps (1 Gbps). Melalui kabel tembaga, Gigabit Ethernet ditetapkan sebagai 1000BASE-T, bekerja pada Cat 5e atau lebih baik. Gigabit Ethernet tidak mendukung hub; itu diimplementasikan hanya dengan menggunakan sakelar. Jarak maksimum 100 m (328 kaki) berlaku untuk pemasangan kabel antara node dan port switch, atau antara dua port switch.

Gigabit Ethernet adalah pilihan utama untuk instalasi baru jaringan akses; yaitu,

pemasangan kabel untuk menghubungkan workstation klien ke jaringan lokal. Keputusan utama adalah apakah akan menggunakan kabel tembaga atau serat optik. Fiber memberikan potensi upgrade yang lebih baik di masa depan, sementara kabel tembaga lebih murah untuk dipasang dan jauh lebih banyak host yang dipasang dengan kartu jaringan yang mendukung tembaga daripada serat pendukung.

10 Gigabit Ethernet (10 GbE) mengalikan kecepatan nominal Gigabit Ethernet dengan faktor 10. Karena frekuensi yang lebih tinggi diperlukan, 10 GbE hanya dapat berjalan pada jarak yang dikurangi melalui pasangan terpilin tanpa pelindung. Pengoperasian yang lebih lama membutuhkan kategori kabel yang lebih tinggi dengan beberapa jenis pelindung. Ada juga spesifikasi untuk operasi 40 Gbps:

Specification	Cable	Maximum Distance
10GBASE-T	UTP (Cat 6) F/UTP (Cat 6A) S/FTP (Cat 7)	55 m (180 feet) 100 m (328 feet) 100 m (328 feet)
40GBASE-T	S/FTP (Cat 8)	30 m (100 feet)

Ethernet 10/40 GbE tidak digunakan di banyak jaringan akses, karena biaya adaptor jaringan yang kompatibel dengan 10/40 GbE dan modul transceiver switch tinggi. Ini dapat digunakan di mana bisnis perusahaan membutuhkan transfer data bandwidth yang sangat tinggi, seperti produksi TV dan film.

- Ringkas Jenis Kabel Tembaga
  Pendahuluan: Ringkas Jenis Kabel Tembaga
  Kabel *twisted pair* kabel tembaga adalah pilihan paling populer untuk jaringan akses di kantor. Anda cenderung bekerja dengan media jaringan ini setiap hari sebagai bagian dari tugas Anda sebagai profesional jaringan. Memahami karakteristik *twisted pair* akan memungkinkan Anda untuk menginstal dan melayani jaringan Anda dengan benar.

- Pertimbangan Kabel Twisted Pair Tanpa Pelindung
  Twisted pair adalah jenis kabel tembaga yang telah banyak digunakan untuk sistem telepon dan jaringan data. Sepasang kabel berinsulasi yang dipilin bersama membentuk pasangan seimbang. Pasangan membawa sinyal yang sama tetapi dengan polaritas yang berbeda; satu kawat positif, dan yang lainnya negatif. Hal ini memungkinkan penerima untuk membedakan sinyal dari kebisingan lebih kuat. Kabel dilengkapi dengan jaket luar isolasi.



Kabel pasangan terpilin-Setiap pasangan berkode warna dipelintir pada kecepatan yang berbeda untuk mengurangi interferensi. (Image by Thuansak Srilao © 123RF.com.)

Pasangan dipelintir pada tingkat yang berbeda untuk mengurangi interferensi eksternal dan crosstalk. Crosstalk adalah fenomena di mana satu pasangan menyebabkan gangguan pada pasangan lain sebagai akibat dari kedekatan mereka.

Twisted pair dapat menggunakan kabel konduktor padat atau terdampar. Pengkabelan padat menggunakan satu kawat tebal per konduktor dan digunakan untuk kabel yang berjalan di belakang dinding atau melalui saluran. Pengkabelan terdampar menggunakan kabel filamen tipis yang dililitkan satu sama lain dan digunakan untuk membuat kabel patch fleksibel untuk menghubungkan komputer ke port dinding dan mengalihkan port ke port panel patch. Ketebalan kawat tembaga diukur menggunakan *American Wire Gauge* (AWG). Meningkatkan angka AWG mewakili kawat yang lebih tipis. Kabel solid menggunakan 22 hingga 24 AWG yang lebih tebal, sedangkan kabel terdampar yang digunakan untuk kabel patch sering kali 26 AWG. Atenuasi kawat terdampar lebih tinggi dari kawat padat, sehingga tidak dapat digunakan untuk jarak yang jauh.

Kebanyakan kabel twisted pair yang digunakan di jaringan kantor adalah *unshielded twisted pair* (UTP). Bangunan modern sering kali dibanjiri kabel menggunakan kabel UTP. Ini melibatkan kabel yang diletakkan ke setiap lokasi di gedung yang mungkin perlu untuk mendukung telepon atau komputer.

- Pertimbangan Kabel Twisted Pair Terlindung dan Disaring
  Kabel terlindung kurang rentan terhadap interferensi dan crosstalk. Jenis kabel ini diperlukan untuk beberapa standar Ethernet dan mungkin juga merupakan persyaratan di lingkungan dengan tingkat interferensi yang tinggi.

  Kabel berpelindung dapat disebut secara umum sebagai *shielded twisted pair* (STP), tetapi sebenarnya ada beberapa jenis pelindung:

Kabel yang disaring memiliki satu pelindung foil luar tipis di sekitar semua pasangan. Kabel yang disaring biasanya disebut sebagai *screened twisted pair* (ScTP) atau *foiled/unshielded twisted pair* (F/UTP), atau terkadang *foiled twisted pair* (FTP).

Perkabelan berpelindung penuh memiliki sekat luar yang dikepang dan pasangan berpelindung foil dan disebut sebagai pasangan terpilin terlindung/berfoil (S/FTP). Ada juga varian dengan pelindung luar foil (F/FTP).

Kabel STP lama mungkin rumit untuk dipasang, karena memerlukan pengikatan setiap elemen ke ground secara manual, tetapi solusi F/UTP dan S/FTP modern (menggunakan kabel, konektor, dan panel patch yang sesuai) mengurangi kerumitan ini dengan menggabungkan bonding dalam desain setiap elemen.

Tips: Menggunakan kabel tersaring atau berpelindung berarti Anda juga harus menggunakan konektor tersaring/terlindung. Elemen kabel yang disaring/terlindung tidak boleh dicampur dengan elemen yang tidak disekat/tidak dilindungi.

- STANDAR KABEL CAT
  American National Standards Institute (ANSI) dan *Telecommunications Industry Association* (TIA)/Electronic Industries Alliance (EIA) telah membuat kategori standar kabel untuk twisted pair untuk menyederhanakan pemilihan kabel berkualitas yang sesuai. Kategori ini, bersama dengan aspek lain dari praktik terbaik perkabelan telekomunikasi, didefinisikan dalam Standar Pengkabelan Telekomunikasi Gedung Komersial ANSI/TIA/EIA 568 (tiaonline.org/standard/tia-568). Standar serupa juga dipertahankan oleh ISO (ISO/IEC 11801), yang mengacu pada kategori komponen dan kelas tautan permanen (termasuk kabel dan terminasi).

Cat/Class	Cable Type	Network Application	Max. Distance	Frequency	Connector
3	UTP	10BASE-T	100 m (328 ft)	16 MHz	RJ-45
5	UTP	100BASE-TX	100 m (328 ft)	100 MHz	RJ-45
5e (Class D)	UTP or F/UTP	1000BASE-T	100 m (328 ft)	100 MHz	RJ-45
6 (Class E)	UTP, F/UTP, or U/FTP	1000BASE-T	100 m (328 ft)	250 MHz	RJ-45
		10GBASE-T	55 m (180 ft)		
6a (Class Ea)	UTP, F/UTP, U/FTP, or S/FTP	10GBASE-T	100 m (328 ft)	500 MHz	RJ-45
7 (Class F)	S/FTP or F/FTP	10GBASE-Tv	100 m (328 ft)	600 MHz	GG45/TERA
8/8.1 (Class I)	U/FTP or F/UTP	40GBASE-T	30 m (100 ft)	2000 MHz	RJ-45
8.2 (Class II)	F/FTP or S/FTP	40GBASE-T	30 m (100 ft)	2000 MHz	GG45/TERA

Berikut adalah beberapa detail tentang kategori yang digunakan untuk media jaringan:

- Kabel Cat 5 tidak lagi tersedia. Cat 5e diuji pada frekuensi hingga 100 MHz (seperti Cat 5) tetapi untuk spesifikasi keseluruhan yang lebih tinggi untuk atenuasi dan crosstalk, yang berarti bahwa kabel dinilai untuk menangani throughput Gigabit Ethernet. Cat 5e masih akan menjadi pilihan yang dapat diterima untuk menyediakan tautan jaringan untuk stasiun kerja.

  Tips: Untuk 1000BASE-T, Cat 5 juga dapat diterima (jika dipasang dengan benar), tetapi kabel Cat 5 tidak lagi tersedia secara komersial. Tidak seperti Ethernet dan Fast Ethernet, Gigabit Ethernet menggunakan keempat pasangan untuk transmisi dan dengan demikian lebih sensitif terhadap crosstalk antara pasangan kabel.

- Cat 6 dapat mendukung 10 Gbps tetapi pada jarak yang lebih pendek-nominalnya 55 m, tetapi seringkali lebih sedikit jika kabel dibundel bersama-sama.

- Cat 6A adalah kabel spesifikasi yang ditingkatkan yang dapat mendukung 10 Gbps lebih dari 100 m. Kabel Cat 6A lebih besar daripada Cat 5e, dan persyaratan pemasangan lebih ketat, sehingga pemasangannya di dalam jalur yang dirancang untuk kabel lama dapat menimbulkan masalah. Standar TIA/EIA merekomendasikan Cat 6A direkomendasikan untuk digunakan di fasilitas perawatan kesehatan, dengan instalasi *Power over Ethernet* (PoE) 802.3bt, dan untuk koneksi horizontal ke titik akses nirkabel.

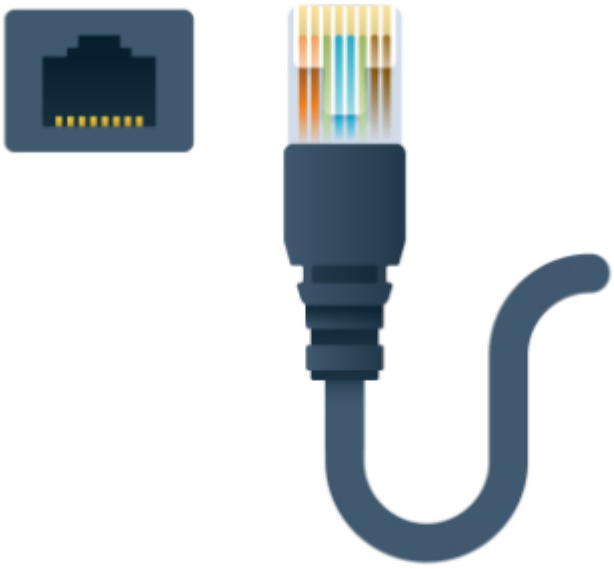
- Kabel Cat 7 selalu memiliki tipe tersaring/terlindung dan memiliki rating untuk aplikasi 10GbE hingga 100 m (328 kaki). Cat 7 tidak dikenali oleh TIA/EIA tetapi muncul dalam standar pemasangan kabel yang dibuat oleh ISO (ISO/IEC 11801). Itu harus diakhiri dengan konektor GG45 atau TERA daripada konektor RJ-45 standar.

  Tips: Pengkabelan bukan satu-satunya bagian dari sistem pengkabelan yang harus dinilai dengan kategori yang sesuai. Untuk aplikasi jaringan yang lebih cepat (Gigabit Ethernet dan yang lebih baik), kinerja konektor menjadi semakin kritis. Misalnya, jika Anda memasang kabel Cat 6A, Anda juga harus memasang panel tambalan Cat 6A, pelat dinding, dan konektor.

- Cat 8 dimaksudkan untuk digunakan di pusat data hanya untuk jalur kabel tambalan pendek yang membuat sambungan atas rak antara peralatan yang berdekatan. ISO mendefinisikan dua varian; 8.1 (Kelas I) setara dengan TIA/EAI Cat 8 dan menggunakan konektor RJ-45 sedangkan 8.2 (Kelas II) harus menggunakan pelindung luar atau saringan dan konektor GG-45 atau TERA.

- JENIS KONEKTOR PASANGAN TWISTED
  Kabel tembaga pasangan terpilin menggunakan konektor Registered Jack (RJ) untuk antarmuka fisik. Ada banyak jenis konektor RJ, yang diidentifikasi dengan angka (dan terkadang huruf). Beberapa secara fisik berbeda, sementara yang lain identik tetapi berbeda untuk aplikasi yang berbeda.

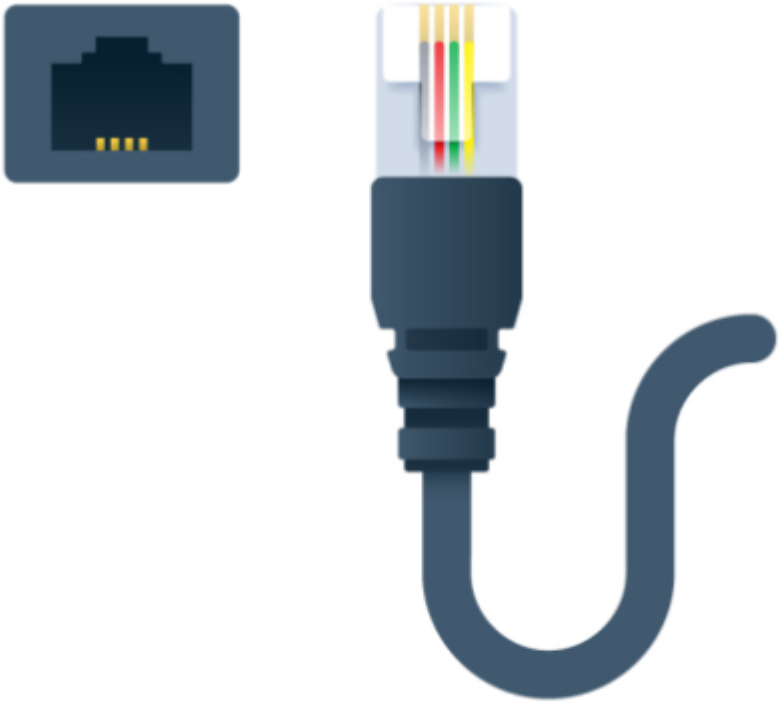
  - Konektor RJ-45
    Konektor RJ-45 digunakan dengan kabel 4-pasangan (8-kawat). Konektor juga disebut sebagai 8P8C, singkatan dari 8-posisi/8-kontak. Ini berarti bahwa kedelapan posisi kabel "potensial" dilengkapi dengan kontak, sehingga semuanya dapat membawa sinyal jika diperlukan. RJ-45 digunakan untuk kabel twisted pair Ethernet.



Soket dan colokan RJ-45. (Image © 123RF.com.)

Tips: Colokan RJ-45 memiliki klip penahan plastik. Ini biasanya dilindungi oleh boot karet. Jenis konstruksi kabel ini juga disebut snagless.

- Konektor RJ-11
  Konektor RJ-11 yang lebih kecil digunakan dengan UTP 2 atau 3 pasang. Ada ruang untuk enam kabel, tetapi empat kabel tengah paling sering digunakan. Biasanya, pasangan terdalam, yang disambungkan ke pin 3 dan 4, membawa nada panggil dan sirkuit suara. Ini juga disebut kabel Tip dan Ring setelah kabel telepon yang lebih tua dihubungkan. Pasangan lainnya biasanya tidak digunakan tetapi dapat digunakan untuk sirkuit sekunder. Konektor RJ-11 digunakan untuk sistem telepon-misalnya, untuk menghubungkan modem ke soket telepon.



Soket dan colokan RJ-11. (Image © 123RF.com.)

Konektor RJ-11 hanya memiliki dua kontak (6P2C). Untuk menggunakan lebih banyak pasangan, jack dapat disambungkan sebagai RJ-14 (6P4C) atau RJ-25 (6P6C).

- Standar Pemutusan Tembaga
  Setiap konduktor dalam kabel data 4-pasangan diberi kode warna. Setiap pasangan diberi warna (Biru, Oranye, Hijau, atau Coklat). Konduktor pertama di setiap pasangan memiliki isolator yang didominasi putih dengan strip warna; konduktor kedua memiliki isolator dengan warna solid. Standar ANSI/TIA/EIA 568 mendefinisikan dua metode untuk mengakhiri konektor Ethernet: T568A dan T568B. Pengkabelan untuk kedua standar ditunjukkan pada gambar berikut.



Diagram pengkabelan T568A dan T568B. (Images © 123RF.com.)

Di T568A, pasangan hijau dihubungkan ke pin 1 dan 2 dan pasangan oranye ditransfer ke pin 3 dan 6. Di T568B, pasangan ini bertukar tempat, jadi oranye diakhiri ke pin 1 dan 2 dan hijau ke 3 dan 6. Organisasi harus mencoba untuk menghindari penggunaan campuran dua standar. T568A diamanatkan oleh pemerintah AS dan oleh standar kabel perumahan (TIA 570), tetapi T568B mungkin lebih banyak digunakan dari keduanya.

Pin	Wire Color (T568A)	Wire Color (T568B)	10/100 Mbps	1/10/40 Gbps
1	Green/White	Orange/White	Tx+	BixA+
2	Green	Orange	Tx-	BixA-
3	Orange/White	Green/White	Rx+	BixB+
4	Blue	Blue		BixB-
5	Blue/White	Blue/White		BixC+
6	Orange	Green	Rx-	BixC-
7	Brown/White	Brown/White		BixD+
8	Brown	Brown		BixD-

Tips: Cat 7 dan Cat 8 sangat sensitif terhadap kebisingan sehingga kabel sekunder di setiap pasangan berwarna putih solid tanpa garis, karena proses pewarnaan mengurangi efektivitas insulasi.

- Kabel dengan peringkat Pleno dan Riser
  Keputusan pertimbangan kabel dasar mencakup kategori, unshielded versus shielded, dan penggunaan yang tepat dari kabel solid versus stranded. Pertimbangan lain adalah bagaimana pemasangan kabel harus sesuai dengan peraturan bangunan nasional atau lokal.

  Ruang pleno adalah ruang kosong di gedung yang dirancang untuk membawa *heating, ventilation, and air conditioning* (HVAC). Ruang pleno biasanya berupa langit-langit palsu, meskipun dapat juga dibangun sebagai lantai yang ditinggikan. Karena mempermudah pemasangan, ruang ini juga telah digunakan untuk kabel komunikasi di beberapa desain bangunan. Ruang pleno adalah saluran yang efektif untuk api, karena ada banyak aliran udara dan tidak ada sekat bakar (seperti dinding atau pintu). Jika ruang pleno digunakan untuk pemanasan, mungkin juga ada suhu yang lebih tinggi. Oleh karena itu, peraturan bangunan mengharuskan penggunaan kabel pleno tahan api di ruang tersebut. Kabel pleno tidak boleh mengeluarkan asap dalam jumlah besar saat dibakar, padam sendiri, dan memenuhi standar keselamatan kebakaran ketat lainnya.

  Pengkabelan tujuan umum (nonplenum) menggunakan jaket dan insulasi PVC (polivinil klorida). Kabel berperingkat pleno menggunakan PVC yang dirawat atau Fluorinated Ethylene Polymer (FEP). Hal ini dapat membuat kabel kurang fleksibel, tetapi bahan yang berbeda yang digunakan tidak berpengaruh pada bandwidth. Kabel data yang diberi peringkat pleno berdasarkan *US National Electrical Cod*e (NEC) ditandai CMP/MMP. Kabel tujuan umum ditandai CMG/MMG atau CM/MP.

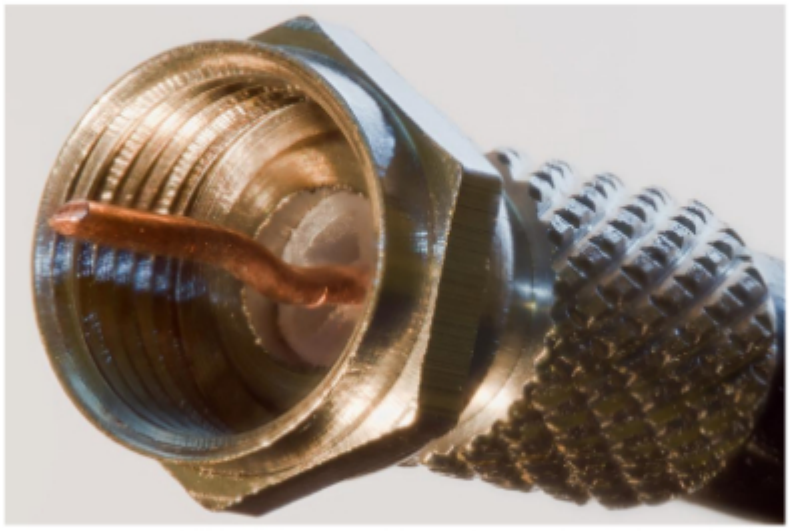
  Kabel yang melewati antara dua lantai disebut sebagai riser. Saluran untuk pemasangan kabel riser harus dihentikan dari kebakaran. Ini berarti bahwa api tidak dapat menyebar melalui lubang yang dibuat oleh saluran. Pengkabelan riser (di saluran atau di ruang seperti poros pengangkat) juga harus sesuai dengan standar keselamatan kebakaran yang sesuai. Ini mirip dengan persyaratan untuk ruang pleno tetapi tidak seketat itu. Kabel data yang diberi peringkat riser di bawah NEC ditandai CMR/MPR.

- Kabel dan Konektor Coaxial dan Twinaxial
  Kabel koaksial (atau coax) terbuat dari dua konduktor yang berbagi sumbu yang sama, maka namanya ("co" dan "ax"). Konduktor inti kabel terbuat dari kawat tembaga (padat atau terdampar) dan ditutup oleh isolasi plastik (dielektrik). Sebuah wire mesh (konduktor kedua), yang berfungsi baik sebagai pelindung dari EMI dan sebagai tanah, mengelilingi bahan isolasi. Selubung plastik yang kuat melindungi kabel.



Kabel coax. (Image by destinacigdem © 123RF.com.)

Kabel coax dikategorikan menggunakan standar Radio Grade (RG), yang mewakili ketebalan konduktor inti dan impedansi karakteristik kabel. RG-6 adalah kabel 18 AWG dengan impedansi 75 ohm yang biasanya digunakan sebagai kabel drop untuk Cable Access TV (CATV) dan modem kabel broadband. Untuk aplikasi ini, coax biasanya diakhiri menggunakan konektor tipe-F, yang diamankan dengan memasang sekrup pada tempatnya.



konektor tipe F. (Image created by Colin and reproduced under the Creative Commons Attribution ShareAlike 3.0 license.)

Twinaxial (atau twinax) mirip dengan coax tetapi berisi dua konduktor dalam. Twinax digunakan untuk interkoneksi pusat data 10 GbE (secara tidak resmi disebut sebagai 10GBASE-CR) dan 40 GbE (40GBASE-CR4) hingga sekitar 5 meter untuk jenis kabel pasif dan 10 meter untuk jenis kabel aktif. Twinax untuk 10/40 GbE diakhiri menggunakan SFP+ *Direct Attach Copper* (DAC) dan transceiver QSFP+ DAC.



Pemasangan kabel twinax Tembaga Langsung (DAC) dengan terminasi SFP+. (Image created by Labsy and reproduced under the Creative Commons Attribution ShareAlike 4.0 license.)

- Ringkas Jenis Kabel Serat Optik

  Pendahuluan: Ringkas Jenis Kabel Serat Optik

  Media serat optik dapat mendukung bandwidth yang lebih tinggi pada jarak yang lebih jauh daripada kawat tembaga. Keunggulan ini menjadikannya pilihan populer untuk jaringan telekomunikasi jarak jauh dan untuk jaringan berkecepatan tinggi yang andal di dalam pusat data. Memahami karakteristik media serat optik akan membantu Anda untuk mendukung instalasi dan peningkatan yang ada.

- PERTIMBANGAN KABEL SERAT OPTIK

  Sinyal listrik yang dibawa melalui kawat tembaga dapat mengalami interferensi dan redaman. Pensinyalan serat optik menggunakan pulsa cahaya inframerah, yang tidak rentan terhadap interferensi, tidak dapat dengan mudah dicegat, dan lebih sedikit mengalami atenuasi. Akibatnya, pemasangan kabel serat optik mendukung bandwidth yang lebih tinggi melalui kabel yang lebih panjang (yang dapat diukur dalam kilometer, bukan meter).

  Serat optik tunggal dibangun dari tiga elemen:

  - ***Core*** menyediakan jalur transmisi untuk sinyal cahaya (waveguide).

  - ***Cladding*** memantulkan sinyal kembali ke pandu gelombang seefisien mungkin sehingga sinyal cahaya berjalan di sepanjang pandu gelombang dengan beberapa pantulan internal. Inti dan kelongsong dapat dibuat dari kaca atau plastik. Cladding diterapkan sebagai lapisan tipis yang mengelilingi inti. Meskipun terbuat dari bahan yang sama, kelongsong memiliki indeks bias yang berbeda

terhadap inti. Efeknya adalah menciptakan batas yang menyebabkan cahaya memantul kembali ke inti, memfasilitasi proses refleksi internal total yang memandu sinyal cahaya melalui inti.

- ***Buffer*** adalah lapisan plastik pelindung. Ini mungkin konfigurasi ketat atau longgar, dengan format longgar menggunakan beberapa bentuk pelumas antara untai dan selubung.

Dalam mode operasi dasar, setiap untai serat optik hanya dapat mentransfer cahaya dalam satu arah pada satu waktu. Oleh karena itu, banyak serat sering digabungkan dalam kabel untuk memungkinkan transmisi dan penerimaan sinyal secara simultan atau untuk menyediakan tautan untuk beberapa aplikasi.

Ada banyak desain dan bahan jaket luar yang berbeda yang cocok untuk berbagai instalasi (dalam ruangan/pleno, luar ruangan, bawah tanah, bawah laut, dan sebagainya). Untaian Kevlar (Aramid) dan terkadang batang fiberglass (anggota kekuatan) sering digunakan untuk melindungi serat dari tekukan atau kerutan yang berlebihan saat "menarik" kabel untuk memasangnya. Untuk aplikasi luar ruangan yang terbuka, pelindung baja (baju besi) dapat ditambahkan untuk mencegah hewan pengerat menggerogoti kabel.

- SERAT MODE TUNGGAL DAN SERAT MULTIMODE
  Kabel serat optik ditentukan menggunakan mode, komposisi (kaca/plastik), dan ukuran inti/kelongsong; misalnya, 8,3 mikron inti/125 microcladding kaca mode tunggal atau 62,5 mikron inti/125 microcladding plastik multimode. Kabel serat optik terbagi dalam dua kategori besar: *single mode* and *multimode*.

  - ***Single Mode Fiber*** (SMF) memiliki inti kecil (8 hingga 10 mikron) dan panjang gelombang yang panjang, sinyal cahaya inframerah dekat (1310 nm atau 1550 nm), yang dihasilkan oleh laser. Kabel mode tunggal mendukung kecepatan data hingga 100 Gbps dan kabel berjalan beberapa kilometer, tergantung pada kualitas kabel dan optik. Ada dua kelas kabel SMF; OS1 dirancang untuk penggunaan di dalam ruangan, sedangkan OS2 untuk penggunaan di luar ruangan.

  - ***Multimode Fiber*** (MMF) memiliki inti yang lebih besar (62,5 atau 50 mikron) dan panjang gelombang cahaya yang lebih pendek (850 nm atau 1300 nm) yang ditransmisikan dalam beberapa gelombang dengan panjang yang bervariasi. MMF menggunakan optik yang lebih murah dan akibatnya lebih murah untuk digunakan daripada SMF. Namun, itu tidak mendukung kecepatan pensinyalan tinggi atau jarak jauh seperti mode tunggal dan lebih cocok untuk LAN daripada WAN.

Tips: Transceiver optik untuk SMF sekarang hanya sedikit lebih mahal daripada untuk MMF. Akibatnya, SMF sering digunakan untuk aplikasi jarak dekat di pusat data, serta untuk tautan jarak jauh. SMF masih hadir dengan sedikit harga premium, tetapi memberikan dukungan yang lebih baik untuk standar Ethernet 40 Gbps dan 100 Gbps.

MMF dinilai menurut kategori Optical Multimode (OM), yang ditentukan dalam standar ISO/IEC 11801:

- Kabel OM1/OM2-62,5-mikron adalah OM1, sedangkan kabel awal 50-mikron adalah OM2. OM1 dan OM2 terutama dinilai untuk aplikasi hingga 1 Gbps dan menggunakan pemancar LED.

- OM3/OM4-ini juga merupakan kabel 50 mikron, tetapi diproduksi secara berbeda, dirancang untuk digunakan dengan Laser Pemancar Permukaan Vertikal-rongga 850 nm (VCSEL), juga disebut sebagai MMF yang dioptimalkan laser (LOMMF). VCSEL tidak sekuat laser solid-state yang digunakan untuk SMF, tetapi mendukung modulasi yang lebih tinggi (mentransmisikan pulsa cahaya dengan cepat) daripada optik berbasis LED.

- Jenis Konektor Serat Optik
  Konektor serat optik tersedia dalam berbagai faktor bentuk. Beberapa jenis lebih populer untuk multimode dan beberapa untuk mode tunggal.

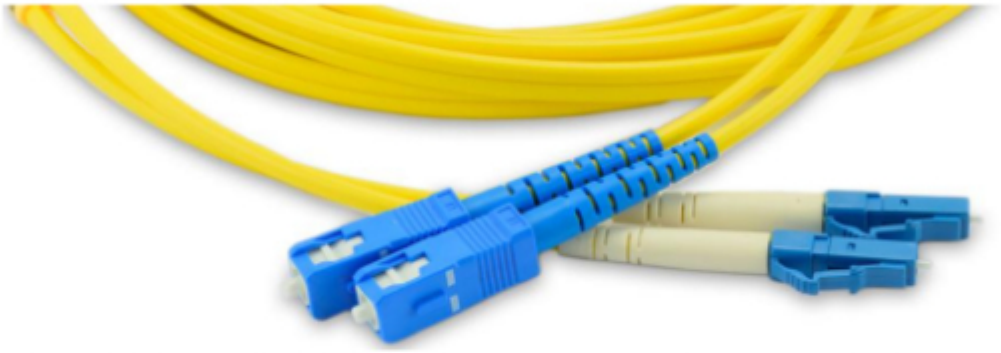
- ***Straight Tip***
  Straight Tip (ST) adalah konektor gaya bayonet awal yang menggunakan mekanisme penguncian push-and-twist. ST sebagian besar digunakan untuk jaringan multimode, tetapi tidak lagi digunakan secara luas untuk instalasi Ethernet.



Dua konektor ST. (Image by Aleh Datskevich © 123RF.com.)

- ***The Subscriber Connector***
  Subscriber Connector (SC) adalah desain push/pull, memungkinkan penyisipan dan pelepasan sederhana. Ini dapat digunakan untuk mode tunggal atau multimode. Ini biasanya digunakan untuk Gigabit Ethernet.

- ***Local Connector***
  The Local Connector (LC) adalah konektor faktor bentuk kecil dengan desain dorong/tarik tab. LC mirip dengan SC, tetapi ukuran yang lebih kecil memungkinkan kepadatan port yang lebih tinggi. LC adalah faktor bentuk yang diadopsi secara luas untuk Gigabit Ethernet dan 10/40 GbE.



Kabel patch dengan konektor format SC dupleks (kiri) dan konektor LC (kanan). (Image by YANAWUT SUNTORNKIJ © 123RF.com.)

- ***Mechanical Transfer Registered Jack***
  Mechanical Transfer Registered Jack (MTRJ) adalah konektor dupleks faktor bentuk kecil dengan desain snap-in yang digunakan untuk jaringan multimode.



MTRJ connector. (Image by Aleh Datskevich © 123RF.com.)

- Standar Fiber Ethernet
  Standar Ethernet melalui serat menetapkan penggunaan berbagai jenis kabel untuk operasi 100 Mbps, 1 Gbps, dan 10 Gbps. Ada varian untuk optik panjang gelombang panjang, diperlukan untuk transmisi jarak jauh, dan optik panjang gelombang pendek.

Specification	Optics	Cable	Maximum Distance	Connectors
100BASE-FX	1300 nm	MMF (OM1) MMF (OM2)	2 km (1.2 miles)	ST, SC, MT-RJ
100BASE-SX	850 nm	MMF (OM1) MMF (OM2)	550 m (1804 feet)	ST, SC, LC
1000BASE-SX	850 nm	MMF (OM1)	275 m (902 feet)	ST, SC, LC, MT-RJ
		MMF (OM2) MMF (OM3)	550 m (1804 feet)	
1000BASE-LX	1300 nm 1310 nm	MMF (OM1/OM2/OM3) SMF (OS1/OS2)	550 m (1804 feet) 5 km (3.1 miles)	SC, LC
10GBASE-SR	850 nm	MMF (OM1)	33 m (108 feet)	SC, LC
		MMF (OM2)	82 m (269 feet)	
		MMF (OM3)	300 m (984 feet)	
		MMF (OM4)	400 m (1312 feet)	
10GBASE-LR	1310 nm	SMF (OS1/OS2)	10 km (6.2 miles)	SC, LC

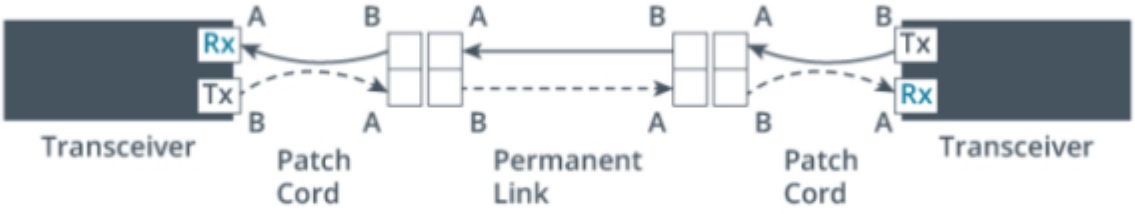
Fiber sering digunakan untuk kabel backbone di jaringan kantor dan untuk workstation dengan kebutuhan bandwidth yang tinggi, seperti video editing. Aplikasi utama 10 GbE (dan lebih baik) adalah:

Meningkatkan bandwidth untuk interkoneksi server dan backbone jaringan, terutama di pusat data dan untuk *storage area networks* (SAN). Mengganti jaringan data publik switch yang ada berdasarkan teknologi eksklusif dengan switch Ethernet yang lebih sederhana (Metro Ethernet).

- INSTALASI KABEL SERAT OPTIK
  Serat optik dapat dipasang pada topologi yang sama dengan kabel tembaga menggunakan bingkai distribusi dan sakelar. Kabel jarak jauh biasanya diletakkan sebagai batang atau cincin dengan repeater atau amplifier di antara segmen kabel untuk memperkuat sinyal.

Biasanya, untai dipasang berpasangan (dupleks) di setiap perangkat, dengan satu untai untuk mengirim (Tx) dan satu untai untuk menerima (Rx).

- Kabel Patch Serat Optik
  Kabel patch untuk serat optik dapat dilengkapi dengan konektor yang sama di setiap ujungnya (LC-LC, misalnya) atau campuran konektor (LC-SC, misalnya). Kabel patch dupleks harus menjaga polaritas yang benar, sehingga port Tx pada pemancar terhubung ke port Rx pada penerima dan sebaliknya. Standar pemasangan kabel TIA/EIA menetapkan kabel patch A ke B ke orientasi port. Setiap elemen pada link harus melakukan crossover, dan elemen harus berjumlah ganjil, seperti dua patch cord dan link permanen (tiga elemen).



Polaritas kabel serat patch.

Sebagian besar konektor diberi kunci untuk mencegah penyisipan yang salah, tetapi jika ragu, pengukur daya optik dapat digunakan untuk menentukan apakah sinyal optik diterima dari serat tertentu.

Tips: Sinyal optik yang ditransmisikan terlihat sebagai bintik putih terang saat dilihat melalui kamera ponsel cerdas. Ini dapat digunakan untuk mengidentifikasi adaptor mana pada antarmuka optik yang mentransmisikan dan kabel serat patch mana yang menerima sinyal dari ujung kabel yang lain.

- Jenis Penyelesaian
  Inti dari konektor serat optik adalah ferrule keramik atau plastik yang menahan untaian kaca dan memastikan penerimaan sinyal cahaya secara terus menerus. Ujung ferrule dapat diselesaikan dalam salah satu dari tiga format:

  - ***Physical Contact*** (PC)- Muka konektor dan ujung serat dipoles sehingga sedikit melengkung dan lebih pas satu sama lain, mengurangi kehilangan pengembalian (gangguan yang disebabkan oleh cahaya yang dipantulkan kembali ke bawah serat).

  - ***Ultra Physical Contact*** (UPC)-Ini berarti kabel dan konektor dipoles ke standar yang lebih tinggi dibandingkan dengan PC.

  - ***Angled Physical Contact*** (APC)-Wajah miring untuk koneksi yang lebih erat dan kinerja pengembalian kerugian yang lebih baik. APC tidak dapat dicampur dengan PC atau UPC. Konektor ini biasanya digunakan ketika serat digunakan

untuk membawa sinyal analog, seperti pada jaringan *Cable Access TV* (CATV). Mereka juga semakin banyak digunakan untuk transmisi jarak jauh dan untuk Jaringan Optik Pasif (PON), seperti yang digunakan untuk mengimplementasikan Fiber to the x (FTTx) beberapa jaringan pelanggan.

Tingkat Pemasangan Kabel Fiber Optik Keyakinan Anda Tinggi Sedang Rendah Lanjut Kategori Topik 2C: Meringkas Jenis Kabel Fiber Optik PEMASANGAN KABEL FIBER OPTIC

Serat optik dapat dipasang pada topologi yang sama dengan kabel tembaga menggunakan bingkai distribusi dan sakelar. Kabel jarak jauh biasanya diletakkan sebagai batang atau cincin dengan repeater atau amplifier di antara segmen kabel untuk memperkuat sinyal.

Biasanya, untai dipasang berpasangan (dupleks) di setiap perangkat, dengan satu untai untuk mengirim (Tx) dan satu untai untuk menerima (Rx).

Kabel Patch Serat Optik Kabel patch untuk serat optik dapat dilengkapi dengan konektor yang sama di setiap ujungnya (LC-LC, misalnya) atau campuran konektor (LC-SC, misalnya). Kabel patch dupleks harus menjaga polaritas yang benar, sehingga port Tx pada pemancar terhubung ke port Rx pada penerima dan sebaliknya. Standar pemasangan kabel TIA/EIA menetapkan kabel patch A ke B ke orientasi port. Setiap elemen pada link harus melakukan crossover, dan elemen harus berjumlah ganjil, seperti dua patch cord dan link permanen (tiga elemen).

- Polaritas kabel serat patch.
Sebagian besar konektor diberi kunci untuk mencegah penyisipan yang salah, tetapi jika ragu, pengukur daya optik dapat digunakan untuk menentukan apakah sinyal optik diterima dari serat tertentu.

Sinyal optik yang ditransmisikan terlihat sebagai bintik putih terang saat dilihat melalui kamera smartphone. Ini dapat digunakan untuk mengidentifikasi adaptor mana pada antarmuka optik yang mentransmisikan dan kabel serat patch mana yang menerima sinyal dari ujung kabel yang lain.

Jenis Finishing Inti dari konektor serat optik adalah ferrule keramik atau plastik yang menahan untaian kaca dan memastikan penerimaan sinyal cahaya secara terus menerus. Ujung ferrule dapat diselesaikan dalam salah satu dari tiga format:

Physical Contact (PC)- Muka konektor dan ujung serat dipoles sehingga sedikit melengkung dan lebih pas satu sama lain, mengurangi kehilangan pengembalian (gangguan yang disebabkan oleh cahaya yang dipantulkan kembali ke bawah serat). *Ultra Physical Contact* (UPC)-Ini berarti kabel dan konektor dipoles ke standar yang lebih tinggi dibandingkan dengan PC. Angled Physical Contact (APC)-Wajah miring

untuk koneksi yang lebih erat dan kinerja pengembalian kerugian yang lebih baik. APC tidak dapat dicampur dengan PC atau UPC. Konektor ini biasanya digunakan ketika serat digunakan untuk membawa sinyal analog, seperti pada jaringan *Cable Access TV* (CATV). Mereka juga semakin banyak digunakan untuk transmisi jarak jauh dan untuk *Passive Optical Networks* (PON), seperti yang digunakan untuk mengimplementasikan *Fiber to the x* (FTTx) beberapa jaringan pelanggan. Penting untuk mencocokkan jenis penyelesaian saat Anda memilih jenis konektor. Penyelesaian APC seringkali tidak didukung oleh panel patch, transceiver, dan port switch yang dirancang untuk Ethernet.

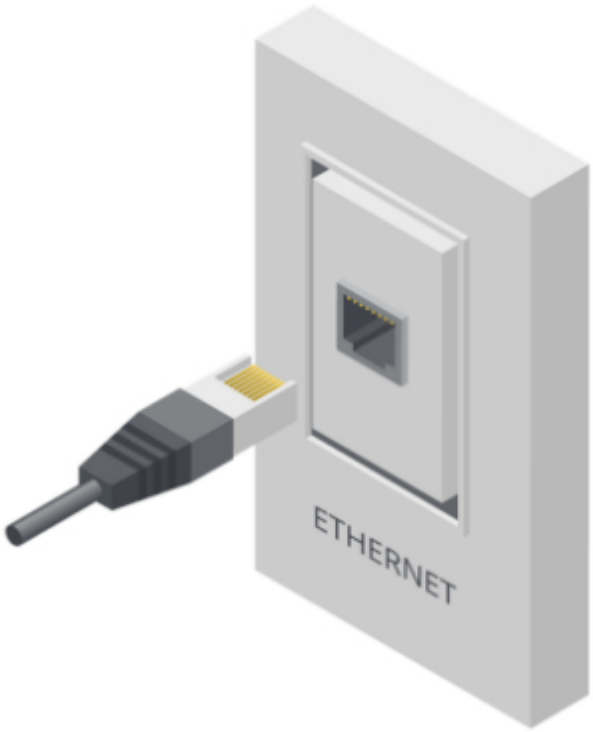
Jika terdapat banyak untaian dalam satu kabel, untaian tersebut diberi kode warna (TIA/EIA 598) untuk membedakannya. Juga, menurut konvensi, jaket kabel dan konektor menggunakan kode warna berikut:

Type	Jacket Color	Connector Color
OM1	Orange	Beige
OM2	Orange	Black
OM3/OM4	Aqua	Aqua
SMF PC/UPC	Yellow	Blue
SMF APC	Yellow	Green

- Menyebarkan Kabel Ethernet
  Pendahuluan: Menerapkan Kabel Ethernet
  Industri jaringan telah mengembangkan model standar untuk menerapkan sistem kabel terstruktur. Model ini dapat beradaptasi dengan jaringan kecil dan besar. Dalam topik ini, Anda akan mempelajari bagaimana sistem distribusi dapat menyediakan akses jaringan di seluruh bangunan atau lokasi.

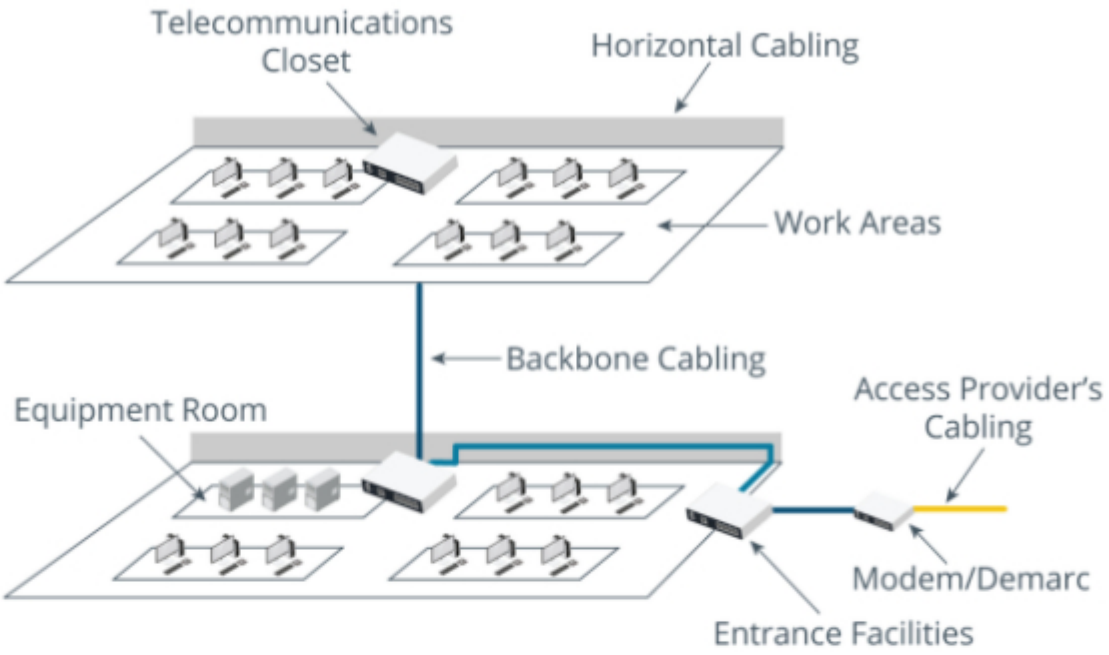
- Sistem Pengkabelan Terstruktur
  Jaringan kabel untuk akses klien di gedung perkantoran akan menggunakan skema pengkabelan terstruktur, seperti yang ditetapkan dalam Standar Pengkabelan Telekomunikasi Gedung Komersial ANSI/TIA/EIA 568. ANSI/TIA/EIA 568 mengidentifikasi subsistem berikut dalam sistem kabel terstruktur:

  - **Area Kerja**-Ruang di mana peralatan pengguna berada dan terhubung ke jaringan, biasanya melalui port dinding.



Pelat dinding modular. (Image by Nikolai Lebedev © 123RF.com.)

- ***Horizontal Cabling***-Menghubungkan area kerja pengguna ke cross-connect horizontal terdekat. Cross-connect juga dapat disebut sebagai kerangka distribusi. Kabel horizontal disebut demikian karena biasanya terdiri dari kabel untuk satu lantai dan terdiri dari kabel yang berjalan secara horizontal melalui saluran dinding atau ruang langit-langit.



Komponen distribusi kabel. (Images © 123RF.com.)

- ***Backbone Cabling***-Menghubungkan horizontal cross-connect (HCC) ke cross-connect utama (opsional melalui intermediet cross-connect). Ini juga dapat digambarkan sebagai sambungan silang vertikal, karena kabel tulang punggung lebih cenderung naik dan turun di antara lantai.

- **Ruang Telekomunikasi**-Rumah-rumah yang saling terhubung secara horizontal. Pada dasarnya, ini adalah titik terminasi untuk kabel horizontal bersama dengan koneksi ke kabel backbone. Ruang peralatan mirip dengan ruang telekomunikasi tetapi berisi penghubung silang utama atau perantara. Ruang peralatan juga cenderung menampung peralatan "kompleks", seperti sakelar, router, dan modem.

- ***Entrance Facilities/Demarc***-Jenis khusus ruang peralatan yang menandai titik di mana pemasangan kabel eksternal (di luar pabrik) disambungkan dengan kabel internal (tempat). Ini diperlukan untuk bergabung dengan jaringan penyedia akses dan untuk komunikasi antar gedung. Titik demarkasi adalah di mana jaringan penyedia akses berakhir dan jaringan organisasi dimulai.

- Manajemen Kabel
  Teknik dan alat manajemen kabel memastikan bahwa pemasangan kabel dapat diandalkan dan mudah dirawat. Kabel tembaga diakhiri menggunakan kerangka distribusi atau blok punchdown. Blok punchdown terdiri dari sejumlah besar terminal koneksi isolasi-perpindahan (IDC). IDC berisi kontak yang memotong isolasi dari kawat dan menahannya di tempatnya. Desain ini memungkinkan

sejumlah besar kabel diterminasi dalam ruang kecil. Beberapa blok punchdown dan format IDC yang berbeda telah digunakan untuk telekomunikasi dan kabel data.

- **66 Blok**
  Blok 66 adalah kerangka distribusi gaya lama yang digunakan untuk mengakhiri pemasangan kabel telepon dan aplikasi data lama (pra-Cat 5). Blok 66 terdiri dari 50 baris 4 terminal IDC. Kabel 25-pasangan dari penyedia akses diakhiri di satu sisi blok. Di sisi lain blok, terminal mengakhiri kabel dari PBX. Sebuah jumper (klip penghubung) dipasang di dua terminal tengah untuk menyelesaikan koneksi.

  Tips: *Private branch exchange* (PBX) adalah sistem telepon yang melayani ekstensi lokal sebuah kantor.

- **110 Blok**
  Blok 110 (dikembangkan oleh AT-and-T) adalah jenis kerangka distribusi yang mendukung operasi 100 MHz (Cat 5) dan lebih baik. Blok kabel 110 diatur secara horizontal daripada vertikal, menawarkan kepadatan yang lebih baik daripada blok 66. Ada juga lebih banyak ruang untuk memberi label pada konektor dan setiap kolom konektor diberi kode warna, membuat manajemen lebih sederhana. Pasangan kabel yang masuk diumpankan ke saluran di blok kabel, kemudian blok konektor atau wafer dipasang untuk menghentikan kabel yang masuk. Pasangan kabel keluar kemudian dilubangi ke terminal pada blok konektor untuk menyelesaikan rangkaian.

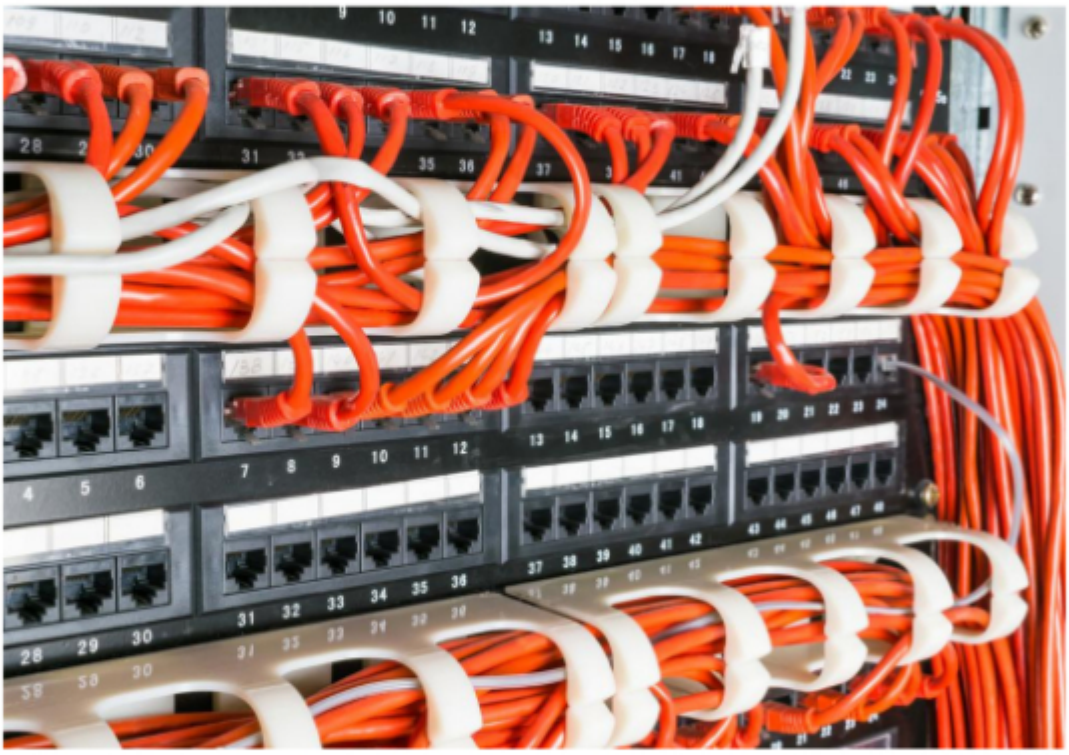
- **Bingkai Distribusi BIX dan Krone**
  Di mana blok 110 menggunakan desain dua bagian di mana blok wafer dipasang di atas blok utama, format bersaing BIX dan Krone menggunakan satu modul. 110 blok dan blok BIX (dikembangkan oleh Nortel) yang umum di Amerika Utara, sementara beberapa vendor Eropa sering lebih memilih Krone. Selain perbedaan dalam desain blok, IDC dimiringkan secara berbeda di setiap format, sehingga memerlukan bilah pemutusan yang berbeda untuk digunakan guna memastikan koneksi yang andal.

- **Panel Patch / Teluk Patch**
  Dalam jaringan data, banyak pemindahan, penambahan, dan perubahan (MAC) akan memerlukan pengkabelan ulang. Untuk menyederhanakan MAC, patch panel atau patch bay adalah jenis blok distribusi dengan IDC di satu sisi dan port modular RJ-45 yang telah dihentikan di sisi lain. Hal ini memungkinkan koneksi masuk dan keluar untuk dikonfigurasi ulang dengan mengubah koneksi kabel patch, yang jauh lebih sederhana daripada mengulang blok punchdown.



IDC di bagian belakang panel patch. (Image by plus69 © 123RF.com.)

Pengkabelan terstruktur (berjalan dari area kerja atau membentuk tulang punggung) diakhiri di bagian belakang panel patch pada IDC. Kabel patch RJ-45 digunakan untuk menghubungkan port ke port jaringan lain, biasanya port switch yang ditempatkan di rak yang sama. Ini sangat menyederhanakan koneksi kabel dan merupakan jenis distribusi kabel yang paling umum dipasang di mana koneksi perlu sering diubah.



Panel tambalan dengan port RJ-45 prakabel. (Image by Svetlana Kurochkina © 123RF.com.)

- Alat dan Teknik Pengkabelan
  Memasang kabel tetap dari bulk spool disebut sebagai kabel penarik karena kabel harus ditarik dengan hati-hati dari lemari telekomunikasi ke area kerja. Kabel biasanya dirutekan melalui saluran atau ruang dinding, menghindari tikungan yang berlebihan dan kedekatan dengan kabel daya listrik dan perlengkapannya, seperti lampu neon, karena ini dapat menyebabkan interferensi. Jangkauan kabel tetap utama dapat mencapai 90 m

(295 kaki). Kabel patch kawat terdampar (antara PC dan port dinding) dan jumper (kabel kawat terdampar tanpa konektor yang digunakan pada sambungan silang) masing-masing dapat mencapai 5 m (16 kaki) dan tidak lebih dari 10 m (33 kaki) dalam panjang keseluruhan. Hal ini karena redaman kabel stranded lebih tinggi dari kabel solid.

Mulai dari panel tambalan, beri label ujung kabel dengan ID jack yang sesuai, lalu jalankan ke area kerja. Ini juga disebut sebagai jatuh, karena dalam kebanyakan kasus Anda akan menjatuhkan kabel dari ruang langit-langit melalui rongga dinding. Jika beberapa kabel menuju ke tempat yang kira-kira sama, Anda dapat menggabungkannya dan menariknya menjadi satu. Biarkan cukup longgar di kedua ujungnya (loop layanan) untuk membuat koneksi dan untuk mengakomodasi koneksi ulang atau perubahan di masa mendatang, potong kabel, dan beri label ujung lainnya dengan ID yang sesuai. Gunting listrik (snips) dirancang untuk memotong kawat tembaga dan pengupasan isolasi dan jaket kabel. Atau, ada alat pengupas kabel khusus yang memiliki bilah yang dapat diganti untuk berbagai jenis kabel data. Pisau pemotong kabel harus dibulatkan untuk mempertahankan geometri kawat. Alat pengupasan harus memiliki diameter yang benar untuk mencetak jaket kabel tanpa merusak kabel insulasi. Pemotong tugas berat diperlukan untuk kabel lapis baja.

- Alat Penghentian
  Kabel tetap diakhiri menggunakan alat punchdown. Alat ini memperbaiki konduktor menjadi IDC. Ada format IDC yang berbeda (66, 110, BIX, dan Krone), dan ini memerlukan blade yang berbeda. Banyak alat punchdown memiliki bilah yang dapat diganti. Pisau dua sisi; satu sisi mendorong kabel ke terminal sementara sisi lain memotong kelebihannya. Pastikan bilah bertanda "potong" diarahkan dengan benar untuk memotong kelebihan kawat.

  Atau, alat blok mengakhiri sekelompok konektor dalam satu tindakan. Untuk panel format 110, ada empat blok posisi (cocok untuk mengakhiri pemasangan kabel data 4-pasangan) dan lima blok posisi (untuk kabel telepon 25-pasangan).

  Kabel patch dibuat menggunakan crimper kabel. Alat ini memperbaiki steker ke kabel. Alat ini khusus untuk jenis konektor dan kabel, meskipun beberapa mungkin memiliki cetakan modular untuk mendukung berbagai jenis colokan RJ.



Menambahkan terminal RJ-45 ke kabel jaringan menggunakan alat punchdown. (Image by dero2084 © 123RF.com.)

Tips: Anda harus melepaskan ujung pasangan kabel dan menempatkannya ke dalam konektor mati dalam urutan yang benar untuk konfigurasi kabel (T568A atau T568B) yang ingin Anda gunakan. Namun, Anda tidak boleh terlalu banyak menggulung kabel. Cat 6 menuntut dalam hal ini dan membutuhkan tidak lebih dari 0,375" (1 cm) pelepasan.

Untuk kabel berpelindung dan tersaring, pemutusan harus dilakukan pada IDC berpelindung atau colokan modular. Pada IDC, klip logam yang ditempatkan di atas foil terbuka atau pelindung yang dikepang mengikat kabel ke rumahan. Steker modular berpelindung memiliki rumah logam dan tidak diakhiri menggunakan crimper standar. Ada beberapa desain yang berbeda, tetapi semuanya mengikuti prinsip menghubungkan pelindung kabel ke strip ikatan.

- Panel Distribusi Serat dan Penyambungan Fusion
  Sebuah bangunan modern atau perbaikan mungkin menggantikan kabel tembaga dengan kabel serat optik. Namun, tautan terstruktur dipasang dengan cara yang mirip dengan pemasangan kabel tembaga, karena menyambungkan kembali kabel serat optik secara terus-menerus berisiko mengalami kerusakan dan keausan, dan Anda tidak ingin harus mengganti jalur kabel melalui saluran. Kabel permanen dijalankan melalui saluran ke port dinding di ujung akses klien dan panel distribusi serat di ujung saklar. Kabel patch serat digunakan untuk melengkapi tautan dari port dinding ke NIC dan dari panel patch ke port saklar.



Panel distribusi serat. (Image by Aleh Datskevich © 123RF.com.)

Menggunakan konektor memang mengurangi kinerja kabel secara keseluruhan. Setiap konektor akan "membebani" sejumlah kerugian penyisipan (biasanya dianggarkan sebagai 0,5 dB) dan kerugian refleksi. Akibatnya, dalam beberapa keadaan mungkin lebih baik untuk menyambungkan dua kabel bersama-sama, baik untuk memperbaiki kerusakan atau untuk memperpanjang kabel. Kabel dapat disambung secara mekanis menggunakan kotak sambungan perekat yang berisi cairan pencocokan indeks yang memastikan jalur kontinu antara dua untai serat. Penyambung fusi mencapai sambungan yang lebih permanen dengan kehilangan penyisipan yang lebih rendah (>=0,1 dB). Mesin penyambungan fusi melakukan penyelarasan yang tepat antara dua untaian dan kemudian menyatukannya secara permanen menggunakan las busur. Sebuah fusion splicer adalah instrumen presisi tinggi dan harus tetap bersih dan dipelihara mengikuti pedoman pabrik.

Penyambungan juga dapat digunakan untuk memasang kuncir (segmen kabel dengan konektor yang dipasang pabrik di satu ujung saja) atau ke terminal ke konektor (menyambung konektor SC atau LC yang disiapkan pabrik ke kabel masuk). Kabel atau kuncir yang disambung harus dilindungi dengan penutup khusus dan ditopang oleh baki sambungan. Konektor untuk penyambungan yang diakhiri bidang tidak memerlukan baki dan penutup pelindung terpasang ke dalam konektor.

- *Transceiver*
  Sebuah jaringan mungkin melibatkan penggunaan beberapa jenis kabel. Ketika ini terjadi, peralatan saklar dan router harus dapat menghentikan jenis kabel dan konektor yang berbeda, dan perangkat harus mengkonversi dari satu jenis media ke jenis media lainnya. Sakelar dan router perusahaan tersedia dengan transceiver/konverter media *hot-swappable* modular untuk berbagai jenis koneksi kabel patch serat optik.

  Tips: Ada juga modul transceiver untuk pemasangan kabel kawat tembaga.

  Secara historis, modul transceiver didasarkan pada faktor bentuk *Gigabit Interface Converter* (GBIC), yang menggunakan port SC dan dirancang (seperti namanya) untuk Gigabit Ethernet. GBIC sangat besar dan sebagian besar telah digantikan oleh *Small Form Factor Pluggable* (SFP), juga dikenal sebagai mini-GBIC.

- SFP/SFP+
  SFP menggunakan konektor LC dan juga dirancang untuk Gigabit Ethernet. *Enhanced SFP* (SFP+) adalah spesifikasi yang diperbarui untuk mendukung 10 GbE tetapi masih menggunakan faktor bentuk LC. Ada modul berbeda untuk mendukung berbagai standar Ethernet dan jenis mode serat (10GBASE-SR versus 10GBASE-LR, misalnya). Akibatnya, transceiver dirancang untuk mendukung panjang gelombang tertentu. Transceiver harus dipasang sebagai pasangan yang cocok.



  Beralih dengan transceiver serat SFP hot-pluggable. (Image by Zdenek Maly © 123RF.com.)

  Tips: Anda akan sering melihat istilah MSA dalam hubungannya dengan transceiver modular. *Multi-Source Agreement* (MSA) dimaksudkan untuk memastikan bahwa transceiver dari satu vendor kompatibel dengan modul switch/router dari vendor lain.

- QSFP/QSFP+
  Quad small form-factor pluggable (QSFP) adalah faktor bentuk transceiver yang mendukung tautan 4 x 1 Gbps, biasanya digabungkan ke satu saluran 4 Gbps. Enhanced quad small form-factor pluggable (QSFP+) dirancang untuk mendukung 40 GbE dengan menyediakan tautan 4 x 10 Gbps. QSFP+ biasanya digunakan dengan serat paralel dan terminasi multi-serat push-on (MPO). Kabel pita tulang punggung MPO mengikat 12 untai atau lebih dengan terminator kompak tunggal (semua kabel diproduksi dan tidak dapat diterminasi di lapangan). Saat digunakan dengan QSFP+, empat untai mengirimkan tautan 40 Gbps dupleks penuh, empat untai menerima, dan empat untai lainnya tidak digunakan.

  QSFP+ juga dapat digunakan dengan standar Ethernet Wavelength Division Multiplexing (WDM).

- Multiplexing Divisi Panjang Gelombang
  SFP/SFP+ biasa (atau "abu-abu") adalah antarmuka dupleks dengan satu port pengirim dan satu port penerima yang memerlukan dua untai serat. Setiap untai adalah saluran tunggal. *Wavelength Division Multiplexing* (WDM) adalah cara menggunakan untai untuk mengirim dan/atau menerima lebih dari satu saluran pada satu waktu.

- Multiplexing Divisi Panjang Gelombang Dua Arah
  Transceiver dua arah (BiDi) mendukung pengiriman dan penerimaan sinyal melalui untaian serat yang sama. Ini menggunakan WDM untuk mentransmisikan sinyal Tx dan Rx melalui panjang gelombang yang sedikit bergeser, seperti 1310 nm untuk Tx dan 1490 nm untuk Rx. Transceiver BiDi harus dipasang dalam pasangan yang berlawanan, sehingga transceiver hilir harus menggunakan 1490 nm untuk Tx dan 1310 untuk Rx. Tautan multiplexing divisi panjang gelombang dua arah (WDM) didokumentasikan dalam standar Ethernet (1000BASE-BX dan 10GBASE-BX).

- Multiplexing Divisi Panjang Gelombang Kasar dan Padat
  Coarse Wavelength Division Multiplexing (CWDM) mendukung hingga 16 panjang gelombang dan biasanya digunakan untuk menyebarkan empat atau delapan saluran dua arah melalui untaian serat tunggal. Dense Wavelength Division Multiplexing (DWDM) menyediakan lebih banyak saluran (20, 40, 80, atau 160). Ini berarti ada jarak yang jauh lebih sedikit antara setiap saluran dan membutuhkan laser yang lebih presisi dan mahal. Transceiver CWDM dan DWDM mendukung tautan Ethernet multi-saluran 1 G, 10 G, dan 40 G. Seperti halnya BiDi, transceiver harus dipasang dalam pasangan yang berlawanan untuk setiap saluran.

  Dalam topologi WDM point-to-point, setiap transceiver disambungkan ke *multiplexer/demultiplexer* (mux/demux). Untai serat tunggal dijalankan ke mux/demux di situs lain. Atau, perangkat yang disebut *optical add/drop multiplexer* (OADM) dapat menyisipkan dan menghapus sinyal untuk saluran panjang gelombang tertentu pada topologi cincin.

Modul 3

Menyebarkan Peralihan Ethernet

PENGANTAR PELAJARAN

Pengkabelan menetapkan hubungan antara node di jaringan, tetapi setiap node juga memerlukan antarmuka jaringan. Tidak banyak jaringan yang dibuat dengan menghubungkan secara langsung setiap sistem akhir ke setiap sistem lokal lainnya. Pengkabelan dan biaya dukungan dikurangi dengan menggunakan sistem perantara untuk membangun jaringan lokal. Sistem perantara ini digunakan sebagai peralatan jaringan seperti hub, jembatan, dan sakelar. Menginstal dan mengkonfigurasi, perangkat ini akan menjadi tugas rutin Anda selama karir Anda di administrasi jaringan.

TUJUAN PELAJARAN

Dalam pelajaran ini, Anda akan:

- Menyebarkan perangkat jaringan.
- Menjelaskan antarmuka jaringan.
- Terapkan fitur peralihan Ethernet umum.

Menyebarkan Perangkat Jaringan

Pendahuluan: Menyebarkan Perangkat Jaringan

Sebagian besar jaringan menggunakan sistem perantara untuk mengurangi biaya dan kerumitan pemasangan kabel. Dalam topik ini, Anda akan merangkum fungsi berbagai perangkat konektivitas yang bekerja pada lapisan fisik dan tautan data.

- **Repeater dan Konverter Media**

  Redaman sinyal yang melewati kabel tembaga atau serat memberlakukan batasan jarak pada tautan. Tautan di mana panjang kabel melebihi batasan jarak mungkin tidak mencapai kecepatan yang diperlukan atau mungkin tidak dapat diandalkan. Sebuah repeater mengatasi batasan jarak dengan meningkatkan sinyal di beberapa titik sepanjang kabel berjalan. Sebuah repeater bekerja pada lapisan fisik (Layer 1) dari model OSI dan transparan sehubungan dengan sisa infrastruktur jaringan (tautan diperlakukan sebagai satu panjang kabel). Pengulang selalu diberi daya dan mewakili satu titik kegagalan untuk tautan. Repeater tersedia untuk sambungan tembaga dan serat, dengan yang terakhir juga digambarkan sebagai optical-electrical-optical (OEO) repeater.

Di mana repeater menghubungkan dua segmen kabel dari jenis yang sama, konverter media digunakan untuk transisi dari satu jenis kabel ke jenis lainnya. Konverter media juga bekerja pada lapisan Fisik model OSI. Mereka dapat disuplai sebagai peralatan yang berdiri sendiri atau peralatan yang dipasang di rak. Konversi media berikut adalah tipikal:

- ☐ **Single mode fiber to twisted pair** : Konverter bertenaga ini mengubah sinyal cahaya dari kabel SMF menjadi sinyal listrik yang dibawa melalui jaringan Ethernet kabel tembaga dan sebaliknya.
- ☐ **Multimode fiber to twisted pair** : Model konverter media yang berbeda diperlukan untuk mengubah sinyal cahaya yang dibawa melalui media MMF.



Single mode fiber to UTP media converter. (Image by ironstealth © 123RF.com.)

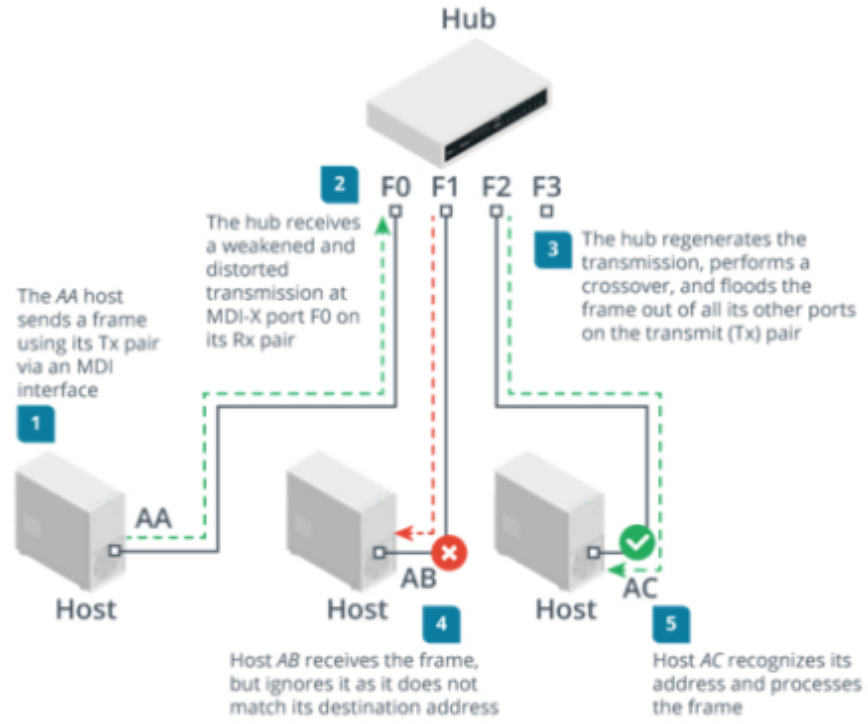
- ☐ **Single mode to multimode fiber** : Perangkat pasif (unpowered) ini mengkonversi antara dua jenis kabel serat.

- **Hubs**

Sebagian besar jaringan Ethernet diimplementasikan sehingga setiap node sistem akhir dihubungkan ke sistem perantara pusat. Pada tipe awal Ethernet, fungsi ini dilakukan oleh hub. Sementara hub tidak lagi digunakan secara luas sebagai peralatan mandiri, penting untuk memahami fungsi dasar yang mereka lakukan.

Hub bertindak seperti repeater multiport sehingga setiap port menerima transmisi yang dikirim dari port lain. Sebagai repeater, hub hanya bekerja pada layer Physical. Secara elektrik, segmen jaringan masih terlihat seperti satu kabel panjang. Akibatnya, setiap port hub adalah bagian dari area akses media bersama yang sama dan dalam domain tabrakan yang sama. Semua antarmuka node adalah half-duplex, menggunakan protokol CSMA/CD, dan bandwidth media (10 Mbps atau 100 Mbps) dibagi antara semua node.

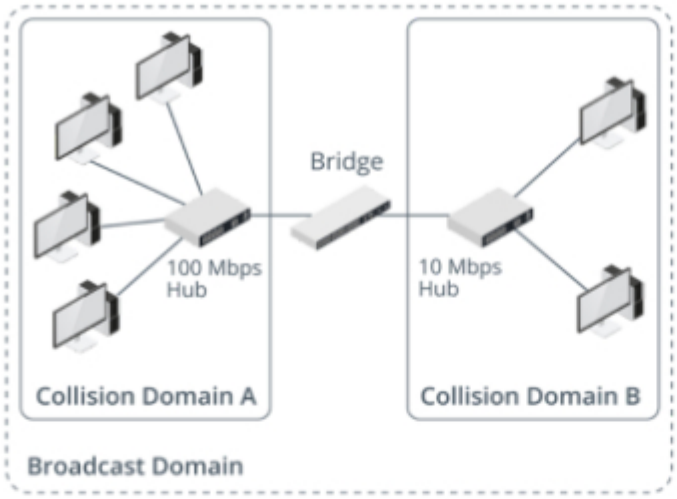
Ketika Ethernet disambungkan dengan hub, perlu ada cara untuk membedakan antarmuka pada sistem akhir (host komputasi) dengan antarmuka pada sistem perantara (hub). Antarmuka sistem akhir disebut sebagai antarmuka tergantung menengah (MDI); antarmuka pada hub disebut sebagai crossover MDI (MDI-X). Ini berarti bahwa kabel pengirim (Tx) pada host terhubung ke kabel penerima (Rx) pada hub.



Hub-based Ethernet communications. (Images © 123RF.com.)

- **Bridges**

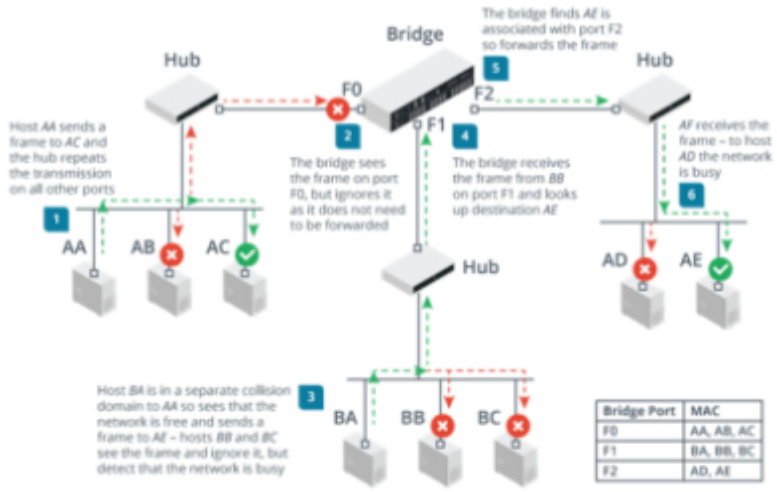
Sebuah jembatan Ethernet bekerja pada lapisan data link (lapisan 2) untuk membangun segmen jaringan fisik yang terpisah sambil menjaga semua node dalam jaringan logis yang sama. Ini mengurangi jumlah tabrakan yang disebabkan oleh terlalu banyak node yang bersaing untuk mendapatkan akses.



Collision and broadcast domains. (Images © 123RF.com.)

Gambar ini menunjukkan bagaimana sebuah jembatan menciptakan domain tumbukan yang terpisah. Setiap hub adalah area media akses bersama. Node yang terhubung ke hub berbagi bandwidth yang tersedia - Ethernet 100 Mbps untuk domain A dan Ethernet 10 Mbps untuk domain B - karena hanya satu node dalam setiap domain tabrakan yang dapat berkomunikasi pada satu waktu. Bridge mengisolasi segmen-segmen ini satu sama lain, sehingga node di domain B tidak melambat atau bersaing dengan node di domain A. Bridge memungkinkan node untuk berkomunikasi dengan domain tabrakan lainnya, dengan hanya meneruskan lalu lintas yang sesuai. Ini menciptakan jaringan logis tunggal, yang disebut sebagai domain broadcast layer 2.

Jembatan Ethernet membangun tabel alamat MAC di memori untuk melacak alamat mana yang terkait dengan port mana. Ketika jembatan diinisialisasi, tabel penghubung kosong, tetapi informasi terus ditambahkan saat jembatan mendengarkan segmen yang terhubung. Entri dihapus dari tabel setelah periode tertentu untuk memastikan informasi tetap terkini.



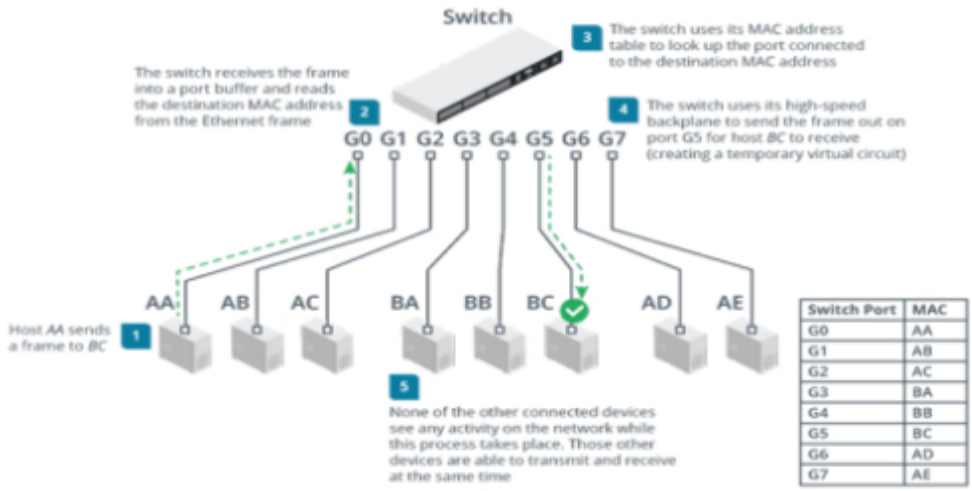
Collision and broadcast domains. (Images © 123RF.com.)

Jika tidak ada catatan alamat perangkat keras atau frame adalah broadcast atau multicast, maka bridge membanjiri frame ke semua segmen kecuali segmen sumber (acting like a hub).

- **Sakelar Lapisan 2 (Layer 2 Switches)**

Masalah yang diciptakan oleh pertengkaran dapat diselesaikan dengan lebih lengkap dengan berpindah dari sistem Ethernet bersama ke Ethernet yang diaktifkan. Hub dan jembatan diganti dengan sakelar. Gigabit Ethernet dan Ethernet 10 GbE tidak dapat digunakan tanpa menggunakan sakelar.

Switch Ethernet layer 2 melakukan fungsi yang sama seperti bridge, tetapi dengan cara yang lebih terperinci dan untuk lebih banyak port daripada yang didukung oleh bridge. Setiap port switch adalah domain tabrakan yang terpisah. Akibatnya, switch membuat link point-to-point antara dua node jaringan. Ini disebut sebagai mikrosegmentasi.



Switch operation. (Images © 123RF.com.)

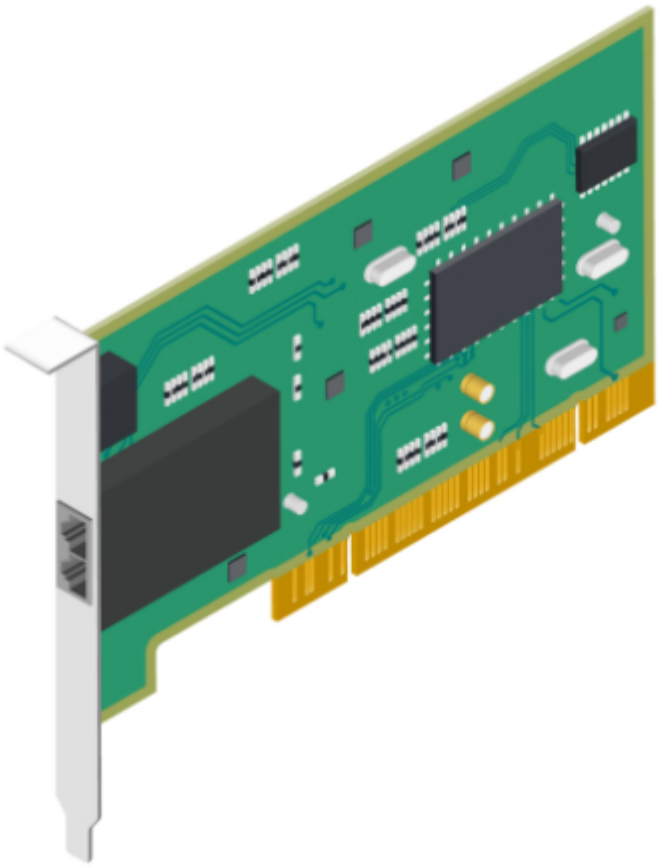
Jelaskan Antarmuka Jaringan

Pendahuluan: Jelaskan Antarmuka Jaringan

Antarmuka jaringan adalah sarana dimana sebuah node terhubung ke media dan bertukar data dengan host jaringan lainnya. Sebagai teknisi jaringan, Anda akan sering terlibat dalam pemasangan, konfigurasi, dan pemecahan masalah antarmuka jaringan. Anda juga harus dapat menangkap dan menganalisis lalu lintas jaringan, menggunakan packet sniffer.

- **INETWORK INTERFACE CARDS**

Komponen transceiver yang bertanggung jawab untuk menghubungkan node secara fisik ke media transmisi diimplementasikan dalam kartu/pengontrol antarmuka jaringan (NIC). Sebagian besar adaptor Ethernet yang dirancang untuk digunakan dengan kabel tembaga mampu beroperasi 10/100/1000, artinya adaptor tersebut mendukung Gigabit Ethernet, Fast Ethernet, dan 10BASE-T. Jenis adaptor yang berbeda harus disediakan untuk tautan serat. Adaptor yang mendukung 10 GbE atau 40 GbE memiliki harga premium yang cukup besar dibandingkan model Gigabit dasar. NIC juga dapat menyediakan beberapa port pada kartu yang sama. Ini memungkinkan koneksi ke jaringan yang berbeda atau menggabungkan tautan terpisah ke saluran bandwidth yang lebih tinggi.



Network Interface Card (NIC) with two RJ-45 ports. (Image © 123RF.com.)

- **Format Bingkai Ethernet**

Ethernet merangkum muatan dari protokol lapisan yang lebih tinggi dalam unit data protokol (PDU) yang disebut bingkai. Format dasar frame Ethernet dan header Ethernet ditunjukkan pada gambar berikut.



Header fields in an Ethernet frame.

- Preamble

  Pembukaan dan Start Frame Delimiter (SFD) digunakan untuk sinkronisasi jam dan sebagai bagian dari protokol CSMA/CD untuk mengidentifikasi tabrakan lebih awal. Pembukaan terdiri dari 8byte bergantian 1s dan 0s dengan SFD menjadi dua 1s berturut-turut di akhir. Ini secara teknis tidak dianggap sebagai bagian dari bingkai

- Pemeriksaan Kesalahan (Error Chechking)

  Bidang pengecekan kesalahan berisi checksum 32-bit (4-byte) yang disebut Cyclic Redundancy Check (CRC) atau Frame Check Sequence (FCS). CRC dihitung berdasarkan isi frame; node penerima melakukan perhitungan yang sama dan, jika cocok, menerima frame. Tidak ada mekanisme transmisi ulang jika kerusakan terdeteksi dan CRC juga tidak sepenuhnya akurat dalam mendeteksi kerusakan; ini adalah fungsi pemeriksaan kesalahan dalam protokol yang beroperasi pada lapisan yang lebih tinggi.

- **Format Alamat Kontrol Akses Media**

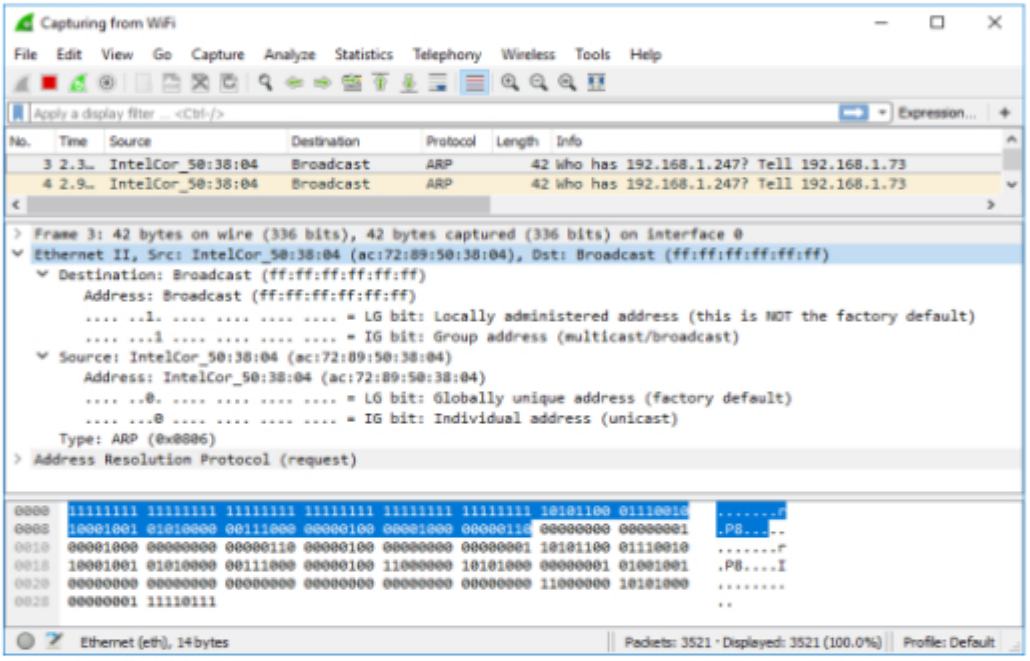
Alamat MAC/EUI adalah pengidentifikasi 48 bit (6 byte). Format nomor berbeda tergantung pada arsitektur sistem. Ini sering ditampilkan sebagai 6 grup dari 2 digit heksadesimal dengan pemisah titik dua atau tanda hubung atau tanpa pemisah sama sekali (misalnya, 00:60:8c:12:3a:bc atau 00608c123abc) atau sebagai 3 grup dari 4 digit heksadesimal dengan pemisah periode (0060.8c12.3abc, misalnya).

Tips: EUI-64 adalah alamat perangkat keras 64-bit. Mekanisme terjemahan memungkinkan alamat MAC 48-bit dikonversi ke EUI-64. Alamat EUI-64 dapat digunakan dengan IPv6.

- Burned-in Addresses

  EEE memberikan masing-masing produsen kartu kisaran angka, dan produsen membuat kode keras setiap antarmuka yang diproduksi dengan nomor unik dari jangkauan mereka. Ini disebut alamat yang dibakar atau alamat universal. Enam digit hex pertama (3 byte atau oktet), juga dikenal sebagai Organizationally Unique Identifier (OUI), mengidentifikasi produsen adaptor. Enam digit terakhir adalah nomor seri.

Sebuah organisasi dapat memutuskan untuk menggunakan alamat yang dikelola secara lokal sebagai pengganti sistem pengkodean universal pabrikan. Ini dapat digunakan untuk membuat MAC bermakna dalam hal lokasi di jaringan, tetapi menambahkan sejumlah besar biaya administrasi. Alamat yang dikelola secara lokal ditentukan dengan mengubah bit U/L dari 0 menjadi 1. Alamat lainnya dikonfigurasi menggunakan driver kartu atau perangkat lunak manajemen jaringan. Menjadi tanggung jawab administrator jaringan untuk memastikan bahwa semua antarmuka dikonfigurasi dengan MAC yang unik.



Captured Ethernet frame showing the resolved OUI and I/G and U/L bits in the destination (broadcast) and source addresses. (Screenshot courtesy of Wireshark.)

- Broadcast Address

  Bit I/G dari alamat MAC menentukan apakah frame dialamatkan ke node individu (0) atau grup (1). Yang terakhir ini digunakan untuk transmisi siaran dan multicast. Alamat MAC yang seluruhnya terdiri dari 1 adalah alamat broadcast (ff:ff:ff:ff:ff:ff) dan harus diproses oleh semua node dalam domain broadcast yang sama.

- **Panjang Bingkai dan Unit Transmisi Maksimum**

  Standar resmi IEEE 802.3 mendefinisikan bidang 2-byte untuk menentukan ukuran bidang data atau muatan. Payload biasanya antara 46 dan 1500 byte. Batas atas muatan juga disebut sebagai unit transmisi maksimum (MTU). Namun, sebagian besar produk Ethernet mengikuti spesifikasi DIX asli, yang disebut sebagai bingkai Tipe II, dan menggunakan bidang tersebut untuk menunjukkan jenis protokol lapisan jaringan yang terdapat dalam bingkai-IPv4 atau IPv6, misalnya. EtherType ini memiliki nilai 1536 atau lebih besar; sesuatu yang kurang dari itu ditafsirkan sebagai panjang data. Misalnya, IPv4 dikodekan sebagai nilai hex 0x0800, atau 2048 dalam desimal, sedangkan IPv6 adalah 0x86DD.

  Untuk mematuhi CSMA/CD, panjang minimum frame Ethernet adalah 64 byte, jadi payload harus minimal 46 byte. Jika hal ini tidak terjadi, secara otomatis diisi dengan data yang berlebihan. Ukuran maksimum frame Ethernet biasanya 1518 byte, tidak termasuk pembukaan. Beberapa produk Gigabit dan 10 GbE Ethernet mendukung bingkai jumbo dengan MTU yang jauh lebih besar. Produk tersebut tidak standar, bagaimanapun, membuat interoperabilitas antara vendor yang berbeda bermasalah.

- **Packet Sniffer dan Taps**

  Salah satu alat terpenting yang digunakan untuk dukungan jaringan adalah penganalisis protokol. Ini adalah alat yang memungkinkan pemeriksaan lalu lintas yang diterima oleh host atau melewati tautan jaringan. Sebuah penganalisa protokol tergantung pada sniffer paket. Sniffer menangkap frame yang bergerak melalui media jaringan.

  Tips: Seringkali istilah sniffer dan penganalisa protokol digunakan secara bergantian tetapi perlu diketahui bahwa mereka mungkin diimplementasikan secara terpisah.

  Sniffer berbasis perangkat lunak dasar yang diinstal ke host hanya akan menginterogasi frame yang diterima oleh adaptor jaringan dengan menginstal driver khusus. Ini memungkinkan frame untuk dibaca dari tumpukan jaringan dan disimpan ke file di disk. Mereka juga mendukung filter untuk mengurangi jumlah data yang diambil.

  Ada tiga opsi utama untuk menghubungkan sniffer ke titik yang sesuai di jaringan:

  - SPAN (switched port analyzer)/mirror port : bahwa sensor terpasang ke port yang dikonfigurasi secara khusus pada sakelar yang menerima salinan bingkai yang ditujukan ke port akses yang dinominasikan (atau semua port lainnya). Metode ini tidak sepenuhnya dapat diandalkan. Bingkai dengan kesalahan tidak akan dicerminkan dan bingkai dapat dijatuhkan di bawah beban berat.

- Passive test access point (TAP): adalah kotak dengan port untuk pemasangan kabel jaringan masuk dan keluar dan induktor atau pembagi optik yang secara fisik menyalin sinyal dari kabel ke port monitor. Ada jenis untuk kabel tembaga dan serat optik. Tidak seperti SPAN, tidak ada keputusan logika yang dibuat sehingga port monitor menerima setiap frame yang rusak atau salah bentuk atau tidak-dan penyalinan tidak terpengaruh oleh beban.
- Active TAP : perangkat bertenaga yang melakukan regenerasi sinyal (sekali lagi, ada varian tembaga dan serat), yang mungkin diperlukan dalam beberapa keadaan. Pensinyalan gigabit melalui kawat tembaga terlalu rumit untuk dipantau oleh TAP pasif dan beberapa jenis tautan serat mungkin terpengaruh secara negatif oleh pemisahan optik. Karena menjalankan fungsi aktif, TAP menjadi titik kegagalan link jika terjadi kehilangan daya.

TAP biasanya akan mengeluarkan dua aliran untuk memantau tautan dupleks penuh (satu saluran untuk hulu dan satu untuk hilir). Atau, ada TAP agregasi, yang membangun kembali aliran menjadi satu saluran, tetapi ini dapat menjatuhkan bingkai di bawah beban yang sangat berat.

- **tcpdump**

  tcpdump adalah utilitas penangkapan paket baris perintah untuk Linux, menyediakan antarmuka pengguna ke perpustakaan libpcap. Sintaks dasar dari perintah tersebut adalah:

  tcpdump -i eth0

  Di mana eth0 adalah antarmuka untuk mendengarkan (Anda dapat mengganti dengan kata kunci any untuk mendengarkan di semua antarmuka dari host multi-home). Utilitas kemudian akan menampilkan paket yang diambil hingga dihentikan secara manual (dengan menekan Ctrl+ C). Pengoperasian perintah dasar dapat dimodifikasi dengan sakelar. Misalnya, -w dan -r masing-masing mengalihkan output tulis ke file dan membaca konten file tangkap. The -v , -vv , dan -vvv dapat digunakan untuk meningkatkan jumlah detail yang ditampilkan tentang setiap frame sementara -e switch menunjukkan header Ethernet.

  tcpdump sering digunakan dengan semacam ekspresi filter:

  - Type : filter berdasarkan host , net , port , atau portrange .
  - Direction : filter menurut parameter sumber (src) atau tujuan (dst) (host, jaringan, atau port).
  - Protocol : filter dengan protokol bernama daripada nomor port (misalnya, arp , icmp , ip , ip6 , tcp , udp , dan sebagainya).

Filter expressions can be combined by using Boolean operators:

- and (-and-and-)
- or (||)
- not (!)

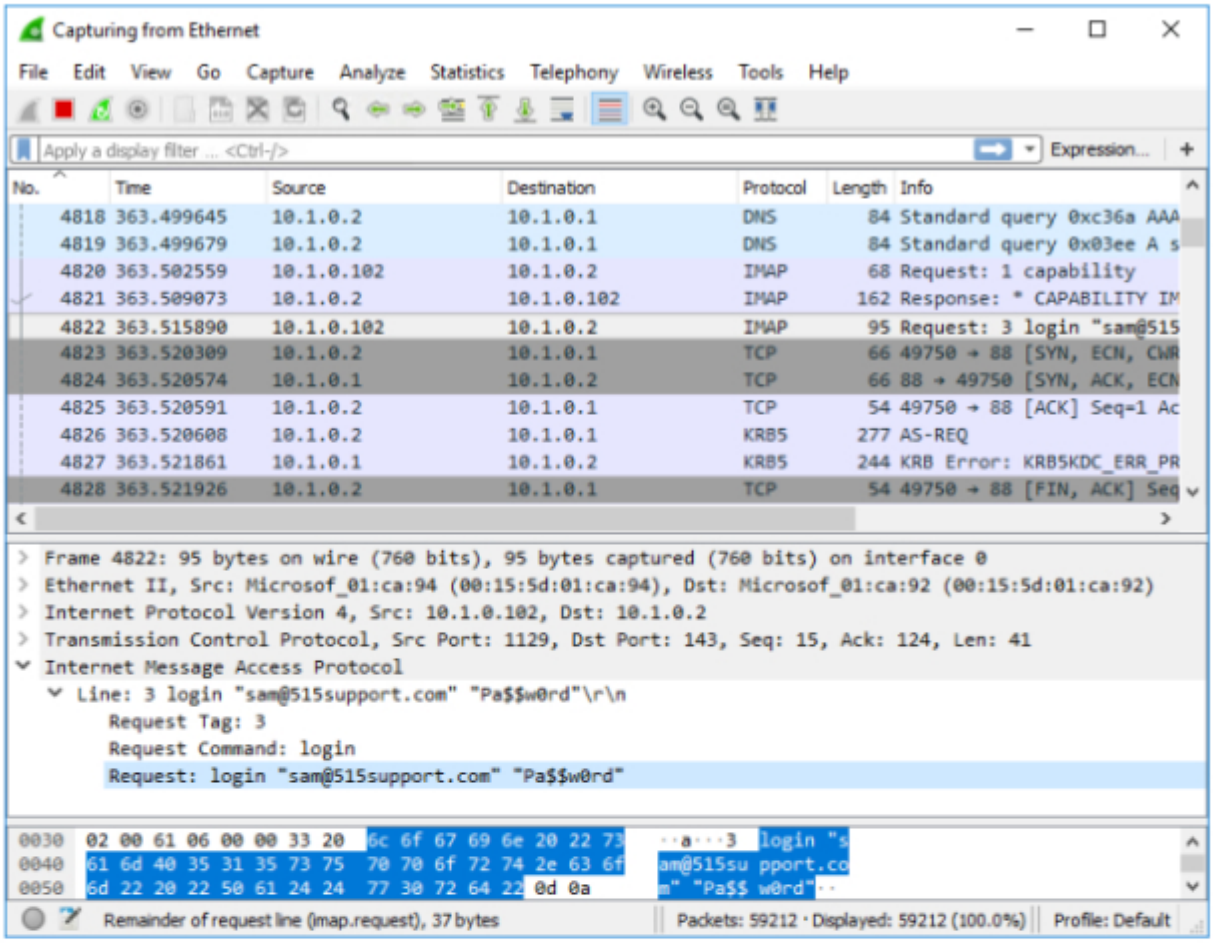
Sintaks filter dapat dibuat lebih detail dengan menggunakan tanda kurung untuk mengelompokkan ekspresi. Ekspresi filter yang kompleks harus diapit oleh tanda kutip. Misalnya, perintah berikut memfilter membingkai dengan IP sumber 10.1.0.100 dan port tujuan 53 atau 80:

tcpdump -i eth0 "src host 10.1.0.100 dan (port dst 53 atau port dst 80)"

Tips: Lihat tcpdump.org untuk bantuan lengkap dan contoh penggunaan. ngrep (github.com/jpr5/ngrep) adalah alat pengambilan dan analisis paket lain yang berguna. Selain sintaks filter standar, ini mendukung penggunaan ekspresi reguler (regexr.com) untuk mencari dan menyaring keluaran tangkapan. Anda juga dapat menggunakan alat netcat (nmap.org/ncat) untuk menyalin lalu lintas jaringan dari satu host ke host lain untuk analisis.

- **Wireshark**

  Wireshark (wireshark.org) adalah utilitas analisis dan penangkapan paket grafis open source, dengan paket penginstal untuk sebagian besar sistem operasi. Setelah memilih antarmuka untuk mendengarkan, output ditampilkan dalam tampilan tiga panel, dengan panel atas menampilkan setiap frame, panel tengah menampilkan bidang dari frame yang dipilih saat ini, dan panel bawah menampilkan data mentah dari frame. dalam hex dan ASCII.



Wireshark protocol analyzer. (Screenshot courtesy of Wireshark.)

Tips: There is also a command-line version of Wireshark called Tshark wireshark.org/docs/wsug_html_chunked/AppToolstshark.html.

- **Terapkan Fitur Pengalihan Ethernet Umum**

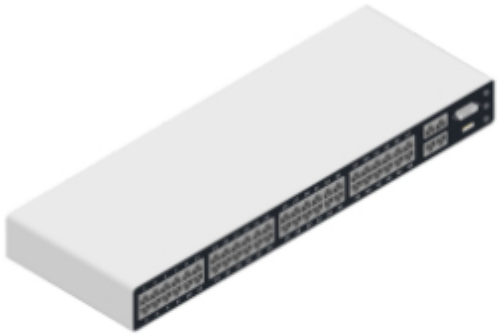
Pendahuluan: Menerapkan Fitur Pengalihan Ethernet Umum

Sakelar sekarang digunakan di hampir semua jaringan Ethernet, jadi Anda pasti akan menemukannya di lingkungan yang Anda dukung. Namun, ada banyak model sakelar Ethernet. Memahami berbagai kemampuan perangkat ini akan mempersiapkan Anda untuk mendukung berbagai lingkungan jaringan.

Mesin Linux mengirim ping berkelanjutan secara default, jadi dalam kasus ini Anda membatasi pesan ping menjadi 5. Namun, mesin Windows hanya mengirim empat permintaan ping secara default. Anda dapat menggunakan ping -t DST pada mesin Windows untuk membuat ping berkelanjutan.

- **Jenis Sakelar Ethernet (Ethernet Switch Types)**

  Switch Ethernet dari vendor yang berbeda datang dalam berbagai rentang untuk mendukung berbagai ukuran jaringan. Sementara model dasar mungkin menampilkan sedikitnya 5 hingga 48 port dan sedikit ruang untuk ekspansi, sakelar lanjutan mendukung interkoneksi melalui backplane berkecepatan tinggi dan kapasitas yang dapat diperluas melalui modul plug-in ditambah redundansi catu daya, konsol manajemen, dan transceiver untuk konektivitas serat optik.



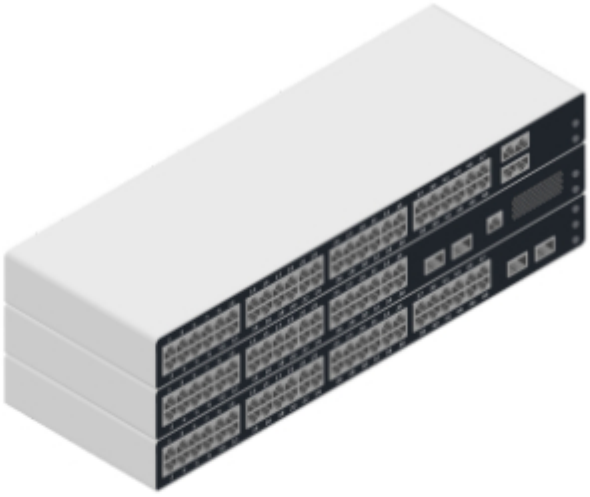
An example of a workgroup switch. (Image © 123RF.com.)

Pasar didominasi oleh platform Cisco Catalyst dan Nexus (lebih dari 55% penjualan), tetapi vendor terkenal lainnya termasuk HP® Enterprise, Huawei, Juniper®, Arista, Linksys®, D-Link, NETGEAR®, dan NEC.

Sakelar Ethernet dapat dibedakan menggunakan kategori umum berikut:

- Tidak terkelola versus terkelola : Pada jaringan SOHO, sakelar lebih cenderung tidak terkelola, unit mandiri yang dapat ditambahkan ke jaringan dan dijalankan tanpa konfigurasi apa pun. Fungsionalitas sakelar mungkin juga dibangun ke dalam router/modem Internet. Pada jaringan perusahaan, sakelar kemungkinan besar akan dikelola. Ini berarti pengaturan sakelar dapat dikonfigurasi. Jika sakelar yang dikelola dibiarkan tidak dikonfigurasi, fungsinya sama seperti sakelar yang tidak dikelola.
- Stackable : Sakelar yang dapat dihubungkan bersama dan beroperasi sebagai satu kelompok. Tumpukan sakelar dapat dikelola sebagai satu unit.
- Modular versus fixed-Switch tetap hadir dengan sejumlah port yang tidak dapat diubah atau ditingkatkan. Sakelar modular memiliki slot untuk kartu plug-in, artinya dapat dikonfigurasi dengan nomor dan jenis port yang berbeda.
- Desktop versus rak-mount-Switch unmanaged : sederhana dengan lima atau delapan port mungkin disediakan sebagai unit berdiri bebas kecil yang dapat ditempatkan pada desktop. Sebagian besar sakelar yang lebih besar dirancang

untuk dipasang ke rak ukuran standar yang digunakan untuk menampung peralatan jaringan.



An example of a modular chassis that allows provisioning multiple access switches. (Image © 123RF.com.)

- **Switch Interface Configuration**

Konfigurasi sakelar terkelola dapat dilakukan pada antarmuka baris perintah (CLI). Setelah Anda membuat koneksi ke antarmuka manajemen sakelar, Anda dapat mengonfigurasi pengaturan untuk setiap antarmuka port sakelar. Pengaturan ini mengontrol tautan jaringan yang dikonfigurasi untuk setiap perangkat klien yang terpasang ke sakelar. Sebagian besar sistem operasi sakelar bekerja dalam beberapa mode perintah atau hierarki. Misalnya, Cisco IOS memiliki tiga mode utama:

- Mode EXEC Pengguna : adalah mode hanya baca di mana perintah dapat digunakan untuk melaporkan konfigurasi, menunjukkan status sistem, atau menjalankan alat pemecahan masalah dasar.
- Mode EXEC yang diistimewakan/mode pengaktifan : memungkinkan pengguna untuk mem-boot ulang atau mematikan alat dan untuk mencadangkan dan memulihkan konfigurasi sistem.
- Mode konfigurasi global : memungkinkan pengguna untuk menulis pembaruan konfigurasi.

Kebanyakan switch CLI juga mendukung TAB dan/atau penggunaan ? untuk membuat daftar cara yang berbeda untuk menyelesaikan instruksi parsial.

Dalam mode pengguna, berbagai perintah acara dapat digunakan untuk menampilkan konfigurasi saat ini. Biasanya ada banyak perintah pertunjukan, tetapi dua yang paling penting adalah sebagai berikut:

- show config menampilkan konfigurasi switch. Konfigurasi startup (show startup-config) bisa berbeda dari konfigurasi yang sedang berjalan (show running-config). Jika ada beberapa perubahan yang tidak terdokumentasi pada sakelar, menggunakan perintah ini dan membandingkan output dapat mengungkapkan sumber masalah.
- show interface mencantumkan status semua antarmuka atau antarmuka yang ditentukan. Antarmuka diidentifikasi berdasarkan jenis, slot, dan nomor port. Misalnya, GigabitEthernet 0/2 (atau G0/2) adalah port #2 pada slot 10/100/1000 pertama (atau hanya slot). Antarmuka memiliki status saluran (naik jika host terhubung melalui kabel yang baik) dan status protokol (naik jika tautan Ethernet dibuat). Turun menunjukkan kesalahan sementara secara administratif turun menunjukkan bahwa port sengaja dinonaktifkan. show interface juga akan melaporkan detail konfigurasi dan statistik lalu lintas jika tautannya naik/naik.

Tips: Sakelar yang dapat ditumpuk mendahului pengidentifikasi antarmuka dengan ID modul. Misalnya, GigabitEthernet 3/0/2 adalah port kedua pada slot pertama di modul ketiga dalam tumpukan. Perhatikan bahwa penomoran ini bervariasi antar produsen. Juga, beberapa mulai dari nol dan beberapa dari satu.

```
FastEthernet1/0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is f41f.c253.7103 (bia f41f.c253.7103)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:51, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     18 packets input, 1758 bytes, 0 no buffer
     Received 4 broadcasts (2 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 2 multicast, 0 pause input
     0 input packets with dribble condition detected
     111 packets output, 13828 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
```

Viewing interface configuration on a Cisco switch. (Image © and Courtesy of Cisco Systems, Inc. Unauthorized use not permitted.)

Switch biasanya mendukung berbagai standar Ethernet sehingga adapter jaringan yang lebih lama dan yang lebih baru semuanya dapat dihubungkan ke jaringan yang sama. Dalam kebanyakan kasus, port pada sakelar diatur ke kecepatan negosiasi otomatis (10/100/1000) dan operasi dupleks penuh atau setengah. Konfigurasi statis dapat diterapkan secara manual jika perlu.

- **Auto MDI/MDI-X**

  Di bawah 100BASE-T, sistem akhir menggunakan media dependent interface (MDI) untuk mengirim pada pin 1 dan 2 dan menerima pada pin 3 dan 6. Ini juga disebut sebagai port uplink. Sebagai sistem perantara, port switch menggunakan MDI-X dan menerima pada pin 1 dan 2 dan mentransmisikan pada pin 3 dan 6. Kabel antara port antarmuka host dan port antarmuka switch harus lurus (baik T568A pada kedua ujungnya atau T568B pada kedua ujungnya).

  Ketika sebuah sakelar perlu dihubungkan ke sakelar lain, komunikasi akan gagal jika kedua antarmuka menggunakan MDI-X. Secara historis (pada hari-hari hub dan sakelar 10/100 awal), port uplink khusus dan/atau kabel crossover digunakan untuk membuat koneksi ini. Kabel crossover memiliki pemutusan T568A di satu ujung dan pemutusan T568B di ujung lainnya. Saat ini, sebagian besar antarmuka sakelar dikonfigurasikan untuk menggunakan auto-MDI/MDIX secara default. Ini berarti bahwa sakelar mendeteksi konfigurasi perangkat dan kabel kabel yang terhubung dan memastikan bahwa uplink MDI ke port MDIX telah dikonfigurasi. Ini juga akan memastikan tautan jika kabel crossover digunakan untuk menghubungkan sistem akhir secara tidak sengaja.

  Tips: Prinsip yang sama berlaku untuk Gigabit Ethernet dan lebih cepat. Sementara keempat pasangan membawa sinyal dua arah, antarmuka masih menggunakan tautan MDI ke MDI-X. Secara praktis, semua antarmuka Gigabit Ethernet harus mendukung MDI/MDI-X otomatis.

- **MAC Address Table and Port Security**

  Sebuah switch mempelajari alamat MAC dengan membaca alamat sumber ketika sebuah frame diterima pada sebuah port. Pemetaan alamat untuk port tersebut biasanya di-cache dalam tabel alamat MAC. Tabel alamat diimplementasikan sebagai memori yang dapat dialamatkan konten (CAM), jenis memori khusus yang dioptimalkan untuk pencarian, bukan akses acak. Akibatnya, tabel alamat MAC sering juga disebut sebagai tabel CAM. Entri tetap berada di tabel alamat MAC selama beberapa waktu sebelum dihapus. Ini memastikan masalah tidak ditemui saat kartu jaringan (alamat MAC) diubah.

Jika alamat MAC tidak dapat ditemukan di tabel alamat MAC, maka sakelar bertindak seperti hub dan mentransmisikan bingkai keluar dari semua port, kecuali port sumber. Inilah yang disebut dengan banjir.

Anda dapat menanyakan tabel alamat MAC dari sakelar untuk menemukan alamat MAC atau alamat yang terkait dengan port tertentu menggunakan perintah seperti:

tampilkan tabel alamat mac

```
NYACCESS1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000a.8aa2.135e    DYNAMIC     Fa0/23
   1    08cc.683e.fd18    DYNAMIC     Fa0/23
   1    08cc.683e.fd40    DYNAMIC     Fa0/23
   1    18e7.285f.0c28    DYNAMIC     Fa0/24
   1    44ad.d916.2598    DYNAMIC     Fa0/24
   1    5006.04be.159d    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 6
```

Displaying dynamic entries in the MAC address table of a Cisco switch. (Image © and Courtesy of Cisco Systems, Inc. Unauthorized use not permitted.)

Konfigurasi keamanan port memvalidasi alamat MAC sistem akhir yang terhubung ke port switch. Dalam kebanyakan skenario, Anda tidak akan mengharapkan alamat MAC server dan workstation sering berubah, kecuali untuk siklus peningkatan yang dapat diprediksi. Alamat MAC host yang tidak diketahui atau sering berubah mungkin mengindikasikan upaya penyusupan. Konfigurasi keamanan port memiliki dua elemen:

- Tentukan alamat MAC statis atau izinkan port mempelajari dan menerima sejumlah alamat tetap.
- Tentukan tindakan penegakan saat pelanggaran kebijakan terdeteksi (hanya peringatan atau matikan port, misalnya).

- **Port Aggregation**

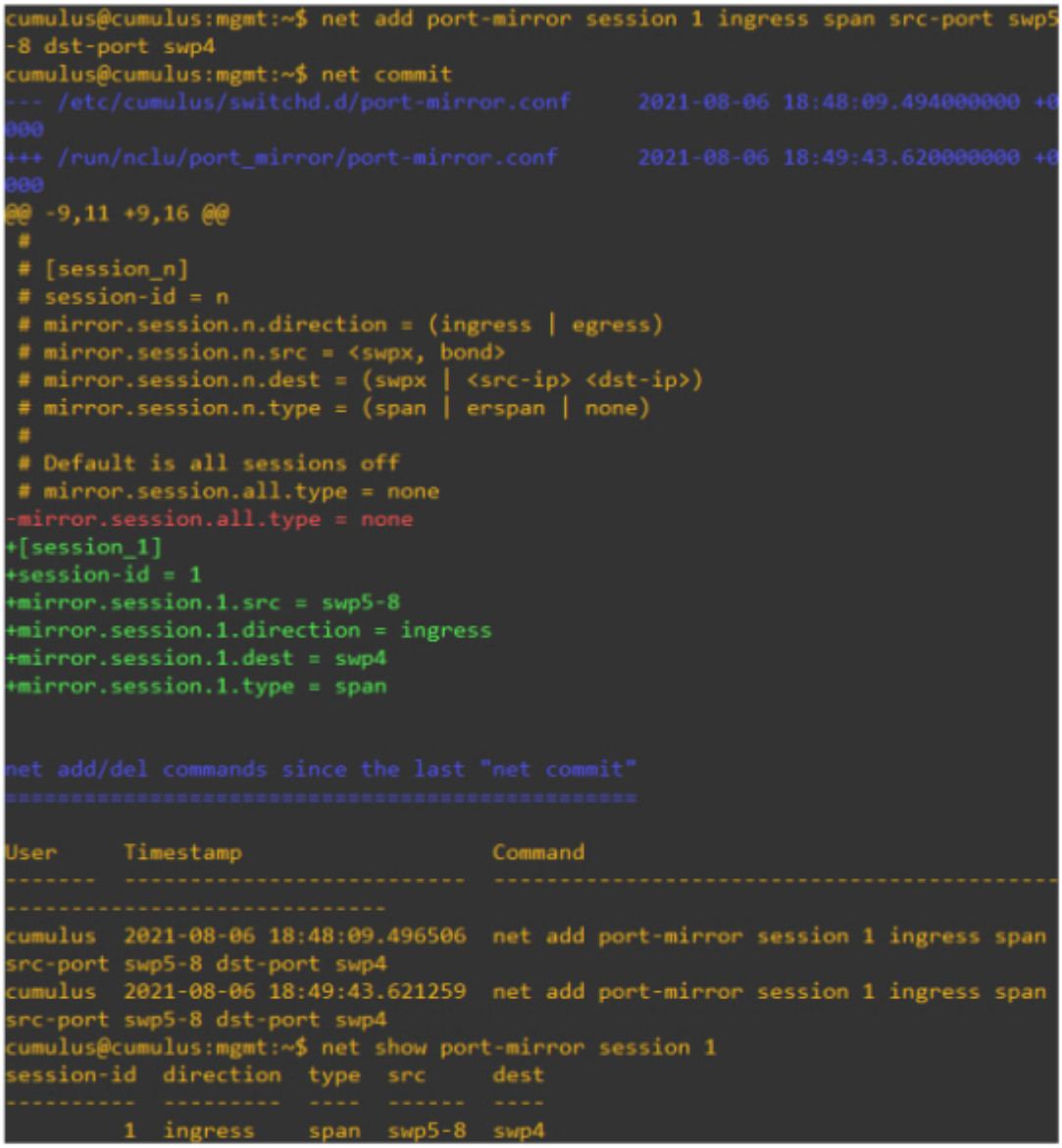
Agregasi port berarti menggabungkan dua atau lebih tautan kabel yang terpisah ke dalam satu saluran logis. Dari ujung host, ini juga bisa disebut kerja sama NIC. Istilah ikatan

juga secara luas menggantikan agregasi. Misalnya, adaptor jaringan tunggal dan segmen kabel mungkin mendukung 1 Gbps; ikatan ini dengan adaptor lain dan segmen kabel memberikan link 2 Gbps.

Agregasi port sering diimplementasikan oleh Link Aggregation Control Protocol (LACP). LACP dapat digunakan untuk melakukan negosiasi otomatis tautan terikat antara port sakelar dan sistem akhir, mendeteksi kesalahan konfigurasi, dan memulihkan dari kegagalan salah satu tautan fisik.

- **Port Mirroring**

Tidak seperti hub, switch meneruskan lalu lintas unicast hanya ke port tertentu yang terhubung ke antarmuka tujuan yang dimaksud. Ini mencegah sniffing lalu lintas unicast oleh host yang terhubung ke switch yang sama. Akan tetapi, ada keadaan di mana menangkap dan menganalisis lalu lintas jaringan adalah aktivitas yang sah, dan pencerminan port menyediakan fasilitas untuk melakukan ini. Pencerminan port menyalin semua paket yang dikirim ke satu atau lebih port sumber ke port mirror (atau tujuan). Pada sakelar Cisco, ini disebut sebagai penganalisis port yang diaktifkan (SPAN).



Configuring port mirroring on a Cumulus VX switch. (Screenshot courtesy of Nvidia.)

Port cermin akan digunakan oleh perangkat lunak manajemen atau pemantauan, seperti sniffer paket, penganalisis jaringan, atau sensor sistem deteksi intrusi (IDS). Baik lalu lintas masuk atau keluar, atau keduanya, dapat ditangkap. Opsional, untuk menghindari overloading sistem pemantauan, paket dapat disaring berdasarkan kriteria seperti ID protokol atau nomor port TCP/UDP.

Tips: Pencerminan port menuntut banyak pemrosesan dan dapat menyebabkan perangkat keras sakelar menjadi kelebihan beban dan akibatnya mogok. Jika memungkinkan, uji solusi keamanan apa pun yang memerlukan pencerminan port di bawah beban biasa sebelum menerapkannya di jaringan produksi.

- **Jumbo Frames and Flow Control**

  Beberapa jenis host, seperti yang mengimplementasikan jaringan area penyimpanan (SAN) memiliki persyaratan khusus. Lalu lintas yang diproses oleh host ini dapat dioptimalkan dengan mengonfigurasi pengaturan port untuk bingkai jumbo dan kontrol aliran.

  - Jumbo Frames

    Biasanya, bingkai Ethernet dapat membawa muatan data atau unit transmisi maksimum (MTU) hingga 1.500 byte. Saat Anda mentransfer data di sekitar jaringan penyimpanan dengan fabric switching 10 Gbps, batas 1500 byte berarti menggunakan banyak frame. Bingkai jumbo adalah bingkai yang mendukung muatan data hingga sekitar 9.000 byte. Ini mengurangi jumlah frame yang perlu ditransmisikan, yang dapat mengurangi jumlah pemrosesan yang perlu dilakukan oleh switch dan router. Ini juga mengurangi kebutuhan bandwidth, karena lebih sedikit header frame yang ditransmisikan. Namun, manfaat bingkai jumbo agak diperdebatkan.

    Saat menerapkan bingkai jumbo, sangat penting bahwa semua host dan peralatan (switch dan router) di sepanjang jalur komunikasi dapat dan dikonfigurasi untuk mendukungnya. Penting juga untuk memastikan bahwa setiap perangkat mendukung MTU yang sama. Selain itu, menghitung MTU dapat menjadi rumit jika ada header tambahan yang digunakan (untuk IPSec, misalnya).

    Nilai MTU pada output show interface akan menunjukkan apakah frame jumbo diterima pada port tertentu.

  - Flow Control

    Kontrol aliran IEEE 802.3x memungkinkan server untuk menginstruksikan sakelar untuk menjeda lalu lintas sementara untuk menghindari buffer yang berlebihan dan menyebabkannya menjatuhkan bingkai. Port switch dapat dikonfigurasi untuk mengaktifkan atau menonaktifkan (mengabaikan) penggunaan frame PAUSE. Mekanisme PAUSE global 802.3x tidak membedakan antara jenis lalu lintas, namun, yang dapat menimbulkan masalah dengan lalu lintas suara/video dan lalu lintas kritis infrastruktur, seperti pembaruan protokol perutean. Mekanisme class of service (CoS) dan quality of service (QoS) memastikan kinerja yang andal untuk aplikasi yang sensitif terhadap waktu ini dengan menandai dan mengatur lalu lintas. Mekanisme kontrol aliran prioritas (PFC) yang diperbarui (IEEE802.1Qbb) memungkinkan frame PAUSE untuk diterapkan ke kelas lalu lintas tertentu saja.

- **Power Over Ethernet**

  Power over Ethernet (PoE) adalah sarana untuk memasok daya listrik dari port switch melalui kabel data biasa ke perangkat bertenaga yang terhubung (PD), seperti handset VoIP, kamera IP, atau titik akses nirkabel. PoE didefinisikan dalam dua standar IEEE (sekarang keduanya digulirkan menjadi 802,3-2018):

  Perangkat yang diberdayakan 802.3af dapat menarik hingga sekitar 13 W melalui tautan. Daya disuplai sebagai 350mA@48V dan dibatasi hingga 15,4 W, tetapi penurunan tegangan pada kabel maksimum 100 kaki menghasilkan daya yang dapat digunakan sekitar 13 W.

  - 802.3at (PoE+)-Perangkat bertenaga dapat menarik hingga sekitar 25 W, dengan arus maksimum 600 mA.
  - 802.3bt (Ultra PoE)-Memasok hingga sekitar 51 W (Tipe 3) atau 73 W (Tipe 4) daya yang dapat digunakan. Sakelar PoE disebut sebagai peralatan sumber daya (PSE) rentang ujung (atau titik akhir). Jika sakelar yang ada tidak mendukung PoE, perangkat yang disebut injektor daya (atau midspan) dapat digunakan.

Saat perangkat terhubung ke port pada sakelar PoE, sakelar melewati fase deteksi untuk menentukan apakah perangkat tersebut mendukung PoE. Jika tidak, itu tidak memasok daya melalui port dan, oleh karena itu, tidak merusak perangkat non-PoE. Jika demikian, ini menentukan konsumsi daya perangkat dan mengatur level tegangan suplai dengan tepat.

Memberi daya perangkat ini melalui sakelar lebih efisien daripada menggunakan adaptor AC soket dinding untuk setiap alat. Ini juga memungkinkan perangkat lunak manajemen jaringan untuk mengontrol perangkat dan menerapkan skema, seperti membuat perangkat yang tidak digunakan masuk ke status tidur dan pembatasan daya.

Modul 4

Memecahkan Masalah Jaringan Ethernet

JELASKAN METODOLOGI PEMECAHAN MASALAH JARINGAN

Pendahuluan: Menjelaskan Metodologi Pemecahan Masalah Jaringan

Masalah jaringan dapat muncul dari berbagai sumber di luar kendali Anda. Sebagai profesional jaringan, pengguna Anda, manajer Anda, dan kolega Anda semua akan meminta Anda untuk mengidentifikasi dan menyelesaikan masalah tersebut secara efisien. Untuk melakukan itu, Anda memerlukan pemahaman mendasar yang kuat tentang alat dan proses yang terlibat dalam pemecahan masalah jaringan. Mampu menyelesaikan masalah di area ini adalah keterampilan penting untuk menjaga jaringan Anda berjalan dengan lancar.

Pemecahan masalah membutuhkan pendekatan praktik terbaik untuk pemecahan masalah dan komunikasi pelanggan/klien. Model pemecahan masalah memberi Anda proses yang telah terbukti yang menjadi dasar teknik dan pendekatan Anda.

Metodologi Pemecahan Masalah Jaringan

Saat anda mengalami masalah jaringan, Anda harus mencoba menyelesaikannya secepat mungkin. Namun, Anda juga harus meluangkan waktu yang cukup untuk menentukan apa yang menyebabkan masalah tersebut sehingga Anda dapat menghindari terulangnya masalah tersebut.

Anda harus memastikan bahwa Anda memahami urutan langkah-langkah dalam metodologi pemecahan masalah CompTIA® Network+®. Langkah-langkah ini dijelaskan secara lebih rinci dalam topik berikut.

1. Identifikasi masalahnya:

- Mengumpulkan informasi.
- Gandakan masalah, jika memungkinkan.
- Pertanyaan pengguna.
- Identifikasi gejala.
- Tentukan apakah ada yang berubah.
- Dekati beberapa masalah secara individual.

2. Menetapkan teori kemungkinan penyebab:

- Pertanyaan yang jelas.
- Pertimbangkan beberapa pendekatan.
- Model OSI top-to-bottom/bottom-to-top.
- Memecah dan menaklukkan.

3. Uji teori untuk menentukan penyebabnya:
- Setelah teori dikonfirmasi, tentukan langkah selanjutnya untuk menyelesaikan masalah.
- Jika teori tidak dikonfirmasi, buat kembali teori baru atau tingkatkan.

4. Menetapkan rencana tindakan untuk menyelesaikan masalah dan mengidentifikasi efek potensial.
5. Terapkan solusi atau tingkatkan seperlunya.
6. Verifikasi fungsionalitas sistem penuh, dan jika berlaku, terapkan tindakan pencegahan.
7. Dokumentasikan temuan, tindakan, dan hasil.

Identifikasi Masalah (Kumpulkan Informasi)

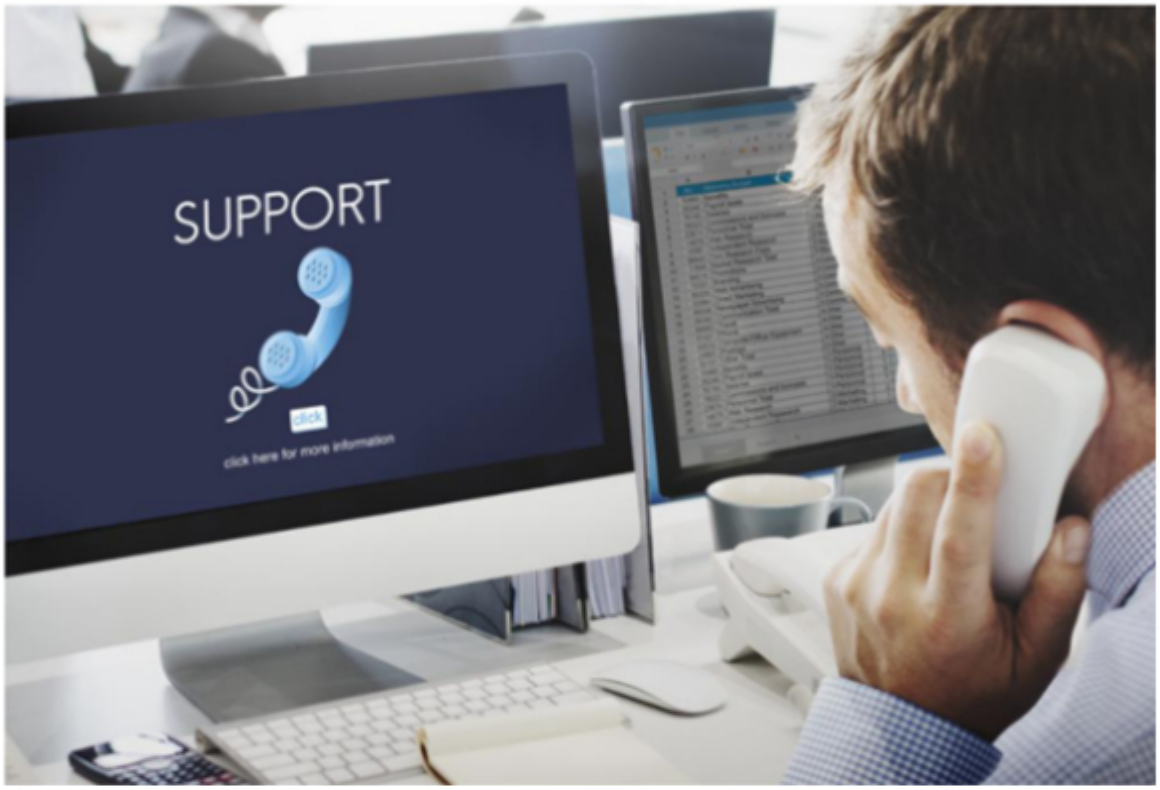
Langkah pertama dalam proses pemecahan masalah adalah mengidentifikasi masalah. Ada beberapa teknik dan pendekatan yang dapat membantu langkah ini.

Kumpulkan Informasi

Di awal, tentukan ruang lingkup masalah (yaitu, area yang terpengaruh). Ini membantu dalam dua cara. Pertama, jika itu adalah satu pengguna, maka itu tidak mendesak seperti panggilan luar biasa lainnya yang Anda miliki. Tetapi jika itu seluruh lantai tiga, maka itu lebih mendesak. Selain itu, fakta bahwa masalah mempengaruhi area yang lebih luas berarti tidak mungkin menjadi masalah dengan workstation satu pengguna. Mengetahui ruang lingkup masalah dapat membantu mengidentifikasi sumbernya dan memprioritaskan masalah dalam kaitannya dengan insiden lain.

Selain teknik pengumpulan informasi yang dibahas di sini, pertimbangkan sumber informasi tidak langsung yang mungkin ada:

- Periksa dokumentasi sistem, seperti log instalasi atau pemeliharaan, untuk informasi yang berguna.
- Periksa log pekerjaan terbaru atau konsultasikan dengan teknisi lain yang mungkin telah mengerjakan sistem baru-baru ini atau mungkin sedang mengerjakan beberapa masalah terkait.
- Gunakan situs dukungan vendor (basis pengetahuan) dan forum.



Pengumpulan informasi adalah langkah pertama dalam pemecahan masalah. (Gambar oleh rawpixel © 123RF.com.)

Identifikasi Gejala dan Duplikat Masalah

Gejala adalah fakta dan petunjuk dalam sistem yang terpengaruh yang dapat dikorelasikan dengan penyebab dan masalah yang diketahui. Untuk mengidentifikasi gejala, selesaikan tes berikut:

-Melakukan pemeriksaan fisik; mencari sesuatu yang tidak biasa.

- Periksa log sistem atau perangkat lunak diagnostik untuk informasi.
- Gandakan masalah pada sistem pengguna atau sistem pengujian. Anda harus mencoba mengikuti langkah yang sama seperti pengguna. Masalah yang bersifat sementara atau sulit untuk direproduksi seringkali merupakan masalah yang paling sulit untuk dipecahkan.

Identifikasi Masalah (Pertanyaan Pengguna)

Jika Anda tidak dapat mengidentifikasi gejala atau menduplikasi masalah, ada teknik tambahan yang dapat Anda gunakan untuk mendiagnosis masalah.

Pertanyaan Pengguna

Laporan pertama masalah biasanya akan datang dari pengguna atau teknisi lain, dan mereka akan menjadi salah satu sumber informasi terbaik, jika Anda dapat mengajukan pertanyaan yang tepat. Dasar untuk mendapatkan informasi pemecahan masalah dari pengguna adalah mengajukan pertanyaan yang bagus. Pertanyaan biasanya dibagi menjadi dua jenis:

- Pertanyaan terbuka mengundang seseorang untuk menjelaskan dengan kata-kata mereka sendiri. Contohnya adalah: "Apa masalahnya?" atau "Apa yang terjadi ketika Anda mencoba menyalakan komputer?" Pertanyaan terbuka baik untuk memulai, karena membantu menghindari asumsi Anda sendiri tentang apa yang salah, dan mendorong pengguna untuk memberi Anda semua informasi yang mereka bisa.
- Pertanyaan tertutup mengundang jawaban Ya/Tidak atau tanggapan tetap. Contohnya meliputi: "Dapatkah Anda melihat teks di layar?" atau "Apa yang dikatakan pesan kesalahan?" Pertanyaan tertutup dapat digunakan untuk menelusuri sifat masalah dan memandu pengguna untuk memberi Anda informasi yang berguna.

Tentukan Jika Ada yang Berubah

Ada dua pertanyaan kunci untuk ditanyakan saat mencoba mengidentifikasi penyebab masalah:

- Apakah itu pernah berhasil? Mudah-mudahan, pengguna Anda akan menjawab pertanyaan dengan jujur, karena jawaban yang benar itu penting-diperlukan dua pendekatan yang berbeda. Jika sistem bekerja sebelum 9:00, Anda harus bertanya apa yang terjadi pada pukul 9:00 Jika sistem tidak pernah bekerja, maka Anda tidak mencari sesuatu yang berhenti bekerja, tetapi untuk sesuatu yang tidak pernah bekerja di tempat pertama.
- Apa yang berubah sejak terakhir kali bekerja? Perubahan yang menyebabkan masalah mungkin tidak jelas. Mungkin pembersih jendela ada di dalam gedung, dan salah satunya tersandung kabel dan sekarang pengguna tidak dapat masuk. Mungkin seseorang telah memindahkan workstation pengguna dari satu ujung meja ke ujung lainnya dan menyambungkan kabel ke port lain . Periksa perubahan yang terdokumentasi menggunakan inventaris sistem, tetapi jika ini tidak mengungkapkan apa pun, cari perubahan yang tidak terdokumentasi di area lokal insiden tersebut.

Dekati Beberapa Masalah Secara Individual

Ketika Anda mulai menyelidiki gejala, Anda mungkin menemukan gejala lebih dari satu masalah. Mungkin pengguna telah melaporkan bahwa mesin kehilangan konektivitas Internet,

dan Anda menemukan bahwa mesin itu juga tidak menerima pembaruan pemeliharaan. Isu-isu itu bisa terkait, atau satu mungkin insidental dengan yang lain.

Jika masalah tampaknya tidak terkait, perlakukan setiap masalah sebagai kasus terpisah. Jika mereka tampaknya terkait, periksa dukungan luar biasa atau tiket pemeliharaan yang mungkin menunjukkan masalah yang ada.

Mungkin juga kasus bahwa pengguna melaporkan dua masalah yang berbeda pada saat yang sama, sering didahului oleh semacam pernyataan "Sementara Anda berada di jalur...". Perlakukan setiap masalah sebagai kasus terpisah. Dalam kebanyakan kasus, Anda harus menyarankan pengguna untuk memulai tiket dukungan terpisah.

Menetapkan Teori Kemungkinan Penyebab

Jika Anda mendapatkan jawaban yang akurat untuk pertanyaan awal Anda, Anda akan menentukan tingkat keparahan masalah (berapa banyak pengguna atau sistem yang terpengaruh), gambaran kasar tentang ke mana harus mencari (workstation atau server end), dan apakah akan mencari yang terbaru perubahan atau kelalaian dalam konfigurasi.

Anda mendiagnosis masalah dengan mengidentifikasi gejalanya. Dari mengetahui apa yang menyebabkan gejala tersebut, Anda dapat menguji setiap kemungkinan penyebab hingga Anda menemukan yang tepat. Terkadang gejala berasal dari lebih dari satu penyebab; sementara jenis masalah ini lebih jarang, jauh lebih sulit untuk memecahkan masalah.

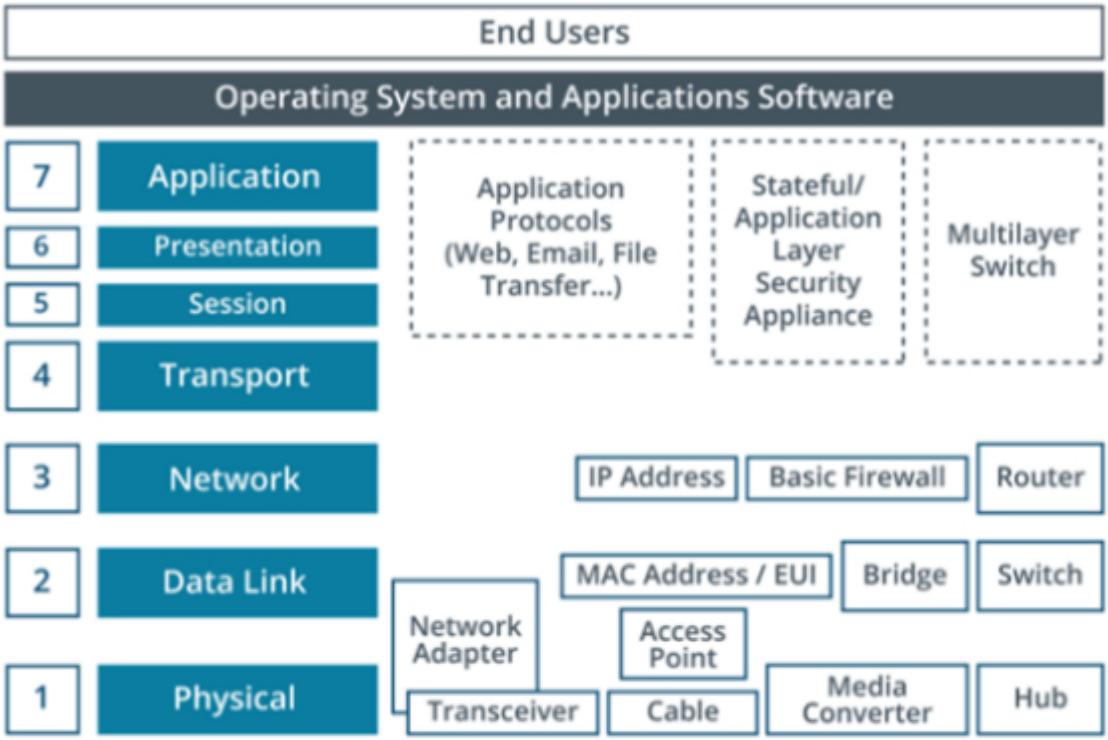
Sebuah sistem jaringan terdiri dari banyak komponen. Pencarian kesalahan perlu mengidentifikasi komponen mana yang menyebabkan masalah. Untuk masalah yang sulit, bersiaplah untuk mempertimbangkan beberapa pendekatan. Jika satu pendekatan tidak mengidentifikasi masalah, gunakan yang lain. Misalnya, Anda dapat mempertimbangkan dua gaya pendekatan pemecahan masalah yang berbeda:

- Pertanyaan yang jelas. Langkah melalui apa yang harus terjadi dan mengidentifikasi titik di mana ada kegagalan atau kesalahan. Pendekatan ini dapat dengan cepat mengidentifikasi kelalaian yang jelas, seperti kabel jaringan tidak dicolokkan.

-Metodis membuktikan fungsionalitas setiap komponen secara berurutan. Pendekatan ini lebih memakan waktu tetapi mungkin diperlukan untuk masalah yang sulit.

Pendekatan Model OSI Top-to-Bottom/Bottom-to-Top

Validasi metodis komponen jaringan dapat didekati dengan pengujian pada setiap lapisan model OSI secara berurutan. Ada banyak komponen yang membentuk sebuah jaringan.



Pemecahan masalah top-to-bottom atau bottom-to-top menggunakan model OSI.

Beberapa, atau beberapa, komponen ini mungkin salah ketika masalah dilaporkan kepada Anda. Adalah penting bahwa Anda mengatasi masalah secara logis dan metodis. Kecuali masalah sepele, pecahkan proses pemecahan masalah ke dalam kompartemen atau kategori, menggunakan model OSI sebagai panduan. Mulai dari atas atau bawah dan hanya bergerak ke atas atau ke bawah ketika Anda telah mengabaikan lapisan sebagai sumber masalahnya. Misalnya, saat memecahkan masalah workstation klien, Anda mungkin bekerja sebagai berikut:

1. Putuskan apakah masalahnya terkait dengan perangkat keras atau perangkat lunak (Hardware).
2. Putuskan subsistem perangkat keras mana yang terpengaruh (NIC atau kabel).
3. Putuskan apakah masalahnya ada di adaptor NIC atau konektor dan pengkabelan (cabling).
4. Uji teori Anda (ganti kabel dengan yang bagus).

Ketika Anda telah menelusuri seperti ini, masalahnya akan menjadi jelas. Tentu saja, Anda bisa membuat pilihan yang salah kapan saja, jadi Anda harus bersiap untuk kembali dan mengikuti jalan yang berbeda.

Tips: Jika Anda benar-benar kurang beruntung, dua (atau lebih) komponen mungkin rusak. Kesulitan lain terletak dalam menilai apakah komponen itu sendiri rusak atau tidak berfungsi karena komponen terkait rusak.

Pendekatan Divide and Conquer

Dalam pendekatan Divide and Conquer, daripada memulai dari atas atau bawah, Anda mulai dengan lapisan yang paling mungkin menyebabkan masalah dan kemudian bekerja ke bawah atau ke atas tergantung pada apa yang diungkapkan oleh pengujian Anda. Misalnya, jika Anda memulai diagnosis pada lapisan 3 dan tidak dapat mengidentifikasi masalah, Anda kemudian akan menguji pada lapisan 4. Sebaliknya, jika Anda menemukan masalah pada lapisan 3, pertama-tama Anda akan menguji lapisan 2. Jika tidak ada masalah pada lapisan 2 , Anda dapat kembali ke lapisan 3 dan bekerja dari sana.

Uji Teori untuk Menentukan Penyebabnya

Dengan mempertanyakan yang jelas atau dengan menggunakan satu atau lebih pendekatan diagnostik metodis, semoga Anda telah mengumpulkan cukup data untuk sampai pada teori awal tentang kemungkinan penyebabnya. Ingatlah bahwa Anda mungkin salah! Tanpa melompat ke kesimpulan, berangkat untuk membuktikan atau menyangkal kecurigaan Anda dengan menggunakan keterampilan pemecahan masalah dan toolkit Anda.

Jika Anda tidak dapat membuktikan penyebab masalahnya, Anda perlu mengembangkan dan menguji teori baru atau memutuskan untuk meningkatkan masalahnya. Eskalasi berarti merujuk masalah ke teknisi senior, manajer, atau pihak ketiga. Anda mungkin perlu mengeskalasi masalah karena salah satu alasan berikut:

- Masalahnya berada di luar pengetahuan atau kemampuan Anda untuk memecahkan masalah.
- Masalahnya termasuk dalam garansi sistem dan akan lebih baik ditangani oleh pemasok.
- Cakupan masalahnya sangat besar dan/atau solusinya memerlukan beberapa konfigurasi ulang besar jaringan.
- Pelanggan menjadi sulit atau kasar atau meminta bantuan pada item yang tidak didukung.

Beberapa alternatif eskalasi antara lain:

- Staf senior, pakar pengetahuan, pakar materi pelajaran, staf teknis, pengembang, pemrogram, dan administrator di perusahaan Anda.
- Pemasok dan produsen.

-Kontraktor/konsultan pendukung lainnya.

Saat Anda mengeskalasi masalah, Anda harus menetapkan fakta-fakta dasar, seperti ruang lingkup masalah dan kemungkinan penyebabnya dan dapat mengomunikasikannya dengan jelas kepada orang yang Anda maksudkan insiden tersebut.

Jika Anda dapat membuktikan penyebab masalah, Anda dapat mulai menentukan langkah selanjutnya untuk menyelesaikan masalah.

Tetapkan Rencana Aksi

Dengan asumsi Anda memilih untuk tidak mengeskalasi masalah, langkah selanjutnya dalam proses pemecahan masalah adalah membuat rencana tindakan. Rencana tindakan menetapkan langkah-langkah yang akan Anda ambil untuk memecahkan masalah. Biasanya ada tiga solusi untuk masalah apa pun:

- **Perbaikan** -Anda perlu menentukan apakah biaya perbaikan/waktu yang diperlukan untuk mengkonfigurasi ulang sesuatu menjadikan ini pilihan terbaik.
- **Ganti** -Seringkali, ini lebih mahal dan mungkin memakan waktu jika suku cadang tidak tersedia. Mungkin juga ada peluang untuk meningkatkan perangkat atau perangkat lunak.

Tips: Teknik dasar saat Anda memecahkan masalah kabel, konektor, atau perangkat adalah memiliki duplikat yang diketahui baik di tangan (yaitu, salinan lain dari kabel atau perangkat yang sama yang Anda tahu berfungsi) dan menguji dengan substitusi.

- **Abaikan** -Tidak semua masalah kritis. Jika tidak ada perbaikan atau penggantian yang hemat biaya, mungkin yang terbaik adalah mencari solusi atau hanya mendokumentasikan masalah dan melanjutkan.

Ketika Anda mempertimbangkan solusi, Anda harus menilai biaya dan waktu yang dibutuhkan. Pertimbangan lain adalah efek potensial pada sisa sistem. Contoh tipikal adalah menerapkan tambalan perangkat lunak, yang mungkin memperbaiki masalah tertentu tetapi menyebabkan program lain tidak berfungsi. Di sinilah sistem manajemen konfigurasi yang efektif berperan, karena ini akan membantu Anda memahami bagaimana sistem yang berbeda saling berhubungan dan menyebabkan Anda mencari otorisasi yang tepat untuk rencana Anda.

Terapkan Solusinya

Solusi untuk suatu masalah mungkin hanya melibatkan pengaturan ulang sistem ke konfigurasi dasarnya. Mungkin pengguna menginstal beberapa perangkat lunak yang tidak sah, menonaktifkan layanan yang diperlukan, atau mencabut kabel. Jika Anda kembali ke konfigurasi yang diketahui baik, Anda mungkin dapat menerapkan solusi secara langsung. Jika solusi memerlukan perubahan pada sistem atau lingkungan jaringan, Anda mungkin harus mengikuti rencana manajemen perubahan.

Jika Anda tidak memiliki otorisasi untuk menerapkan solusi, Anda perlu mengeskalasi masalah ke personel yang lebih senior. Jika penerapan solusi mengganggu jaringan yang lebih luas, Anda juga perlu mempertimbangkan waktu yang paling tepat untuk menjadwalkan pekerjaan konfigurasi ulang dan merencanakan cara memberi tahu pengguna jaringan lain. Saat Anda mengubah sistem sebagai bagian dari penerapan solusi, uji setelah setiap perubahan. Jika perubahan tidak menyelesaikan masalah, balikkan dan coba yang lain. Jika Anda membuat serangkaian perubahan tanpa mencatat apa yang telah Anda lakukan, Anda bisa menemukan diri Anda dalam posisi yang sulit.

Verifikasi Fungsi Sistem Penuh dan Terapkan Tindakan Pencegahan

Saat Anda menerapkan solusi, validasi bahwa itu memperbaiki masalah yang dilaporkan, dan sistem secara keseluruhan terus berfungsi secara normal. Dengan kata lain, mengidentifikasi hasil dan efek dari solusi. Pastikan Anda benar dan masalahnya teratasi. Bisakah pengguna sekarang masuk dengan benar? Apakah ada cara Anda dapat menyebabkan masalah lagi?

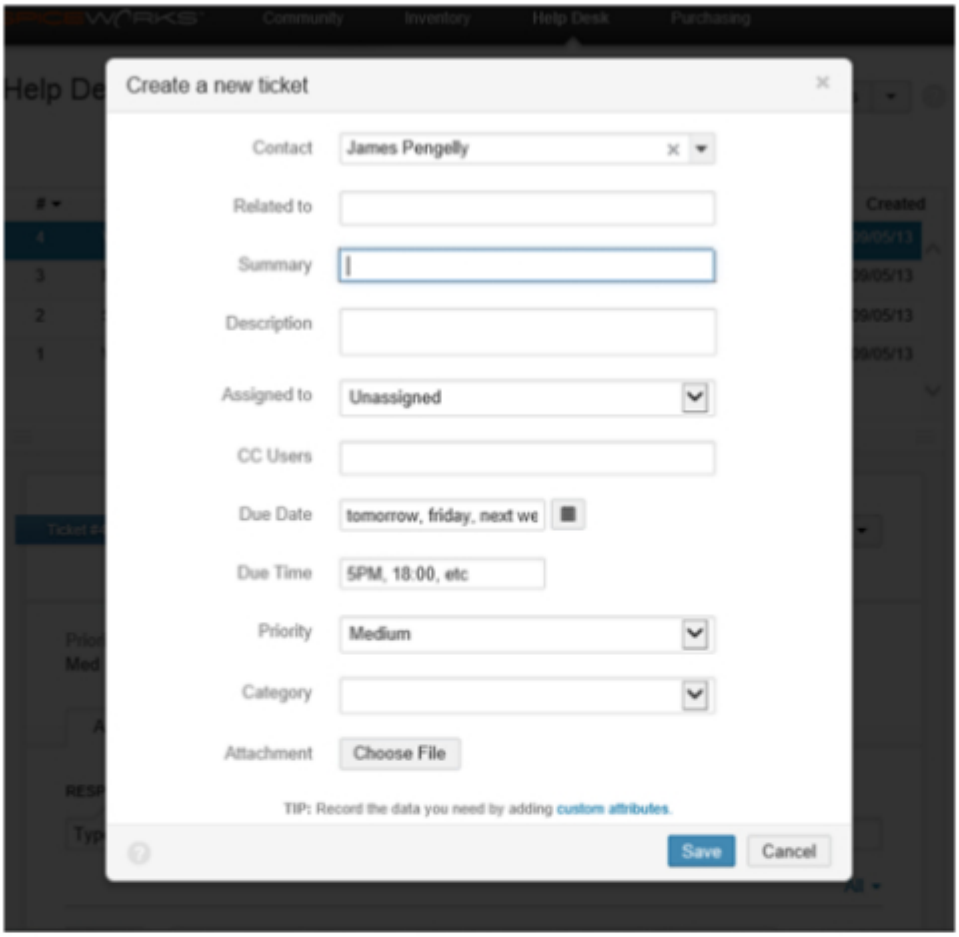
Sebelum Anda dapat menganggap suatu masalah telah selesai, Anda harus puas dengan pikiran Anda sendiri bahwa Anda telah menyelesaikannya dan Anda harus mendapatkan persetujuan dari pelanggan bahwa masalah tersebut telah diperbaiki. Nyatakan kembali apa masalahnya dan bagaimana cara mengatasinya, lalu konfirmasikan dengan pelanggan bahwa log insiden dapat ditutup.

Untuk menyelesaikan masalah sepenuhnya, Anda harus mencoba menghilangkan faktor apa pun yang dapat menyebabkan masalah berulang. Misalnya, jika pengguna mencolokkan laptopnya ke soket jaringan yang salah, pastikan soket tersebut diberi label yang jelas untuk membantu pengguna di masa mendatang. Jika server yang rusak menyebabkan waktu henti jaringan selama berjam-jam, pertimbangkan untuk menerapkan layanan failover untuk meminimalkan dampak insiden berikutnya.

Temuan Dokumen, Tindakan, dan Hasil

Sebagian besar pemecahan masalah terjadi dalam konteks sistem tiket. Ini menunjukkan siapa yang bertanggung jawab atas masalah yang diberikan dan apa statusnya. Ini memberi Anda kesempatan untuk menambahkan deskripsi lengkap tentang masalah dan solusinya, termasuk temuan, tindakan, dan hasil.

Ini sangat berguna untuk pemecahan masalah di masa mendatang, karena masalah yang sesuai dengan kategori yang sama dapat ditinjau untuk melihat apakah solusi yang sama berlaku. Ini juga membantu untuk menganalisis infrastruktur TI dengan mengumpulkan statistik tentang jenis masalah apa yang terjadi dan seberapa sering.



Membuat tiket di alat manajemen Dukungan TI Spiceworks. (Tangkapan layar milik Spiceworks.)

Saat Anda menyelesaikan log masalah, ingatlah bahwa orang lain selain Anda mungkin akan mengandalkannya. Juga, log dapat disajikan kepada pelanggan sebagai bukti aktivitas pemecahan masalah. Tulis dengan jelas dan ringkas, periksa kesalahan ejaan dan tata bahasa.

MEMECAHKAN MASALAH UMUM KONEKTIFITAS KABEL

Pendahuluan: Memecahkan Masalah Konektivitas Kabel Umum

Menerapkan pendekatan lapis demi lapis untuk pemecahan masalah jaringan dapat sangat membantu dengan mengisolasi gejala dan penyebab. Dalam topik ini, Anda akan menyelidiki beberapa masalah umum yang dapat memengaruhi jaringan kabel dan mengidentifikasi alat dan teknik yang dapat digunakan untuk memecahkan masalah pada lapisan fisik dan tautan data.

Spesifikasi dan Batasan

Saat memecahkan masalah tautan, Anda perlu membandingkan kinerja yang diharapkan dengan kinerja aktual saat ini. Untuk melakukan ini, Anda harus memahami bagaimana menilai dan membedakan spesifikasi dan batasan kecepatan, throughput, dan jarak.

Kecepatan versus Throughput

Pada lapisan fisik, sinyal yang ditransmisikan melalui saluran komunikasi terdiri dari serangkaian peristiwa yang disebut sebagai simbol. Sebuah simbol bisa menjadi sesuatu seperti pulsa tegangan tinggi dalam arus listrik atau transisi antara puncak dan palung dalam gelombang elektromagnetik. Jumlah simbol yang dapat ditransmisikan per detik disebut baud rate. Kecepatan baud diukur dalam hertz (atau MHz atau GHz).

Pada lapisan data link, laju bit nominal atau bandwidth dari tautan adalah jumlah informasi yang dapat ditransmisikan, diukur dalam bit per detik (bps), atau beberapa kelipatannya. Untuk mengirimkan informasi lebih efisien, metode pensinyalan mungkin mampu mewakili lebih dari satu bit per simbol. Ini juga membantu mengatasi kebisingan dan mendeteksi kesalahan. Penggunaan metode pengkodean ini berarti bahwa bit rate akan lebih tinggi dari baud rate. Dalam istilah Ethernet, kecepatan adalah kinerja yang diharapkan dari tautan yang telah dipasang dengan benar untuk beroperasi pada 10 Mbps, 100 Mbps, 1 Gbps, atau lebih baik.

Laju bit nominal tidak akan sering dicapai dalam praktik. Throughput adalah kecepatan transfer data rata-rata yang dicapai selama periode waktu tidak termasuk skema pengkodean, kesalahan, dan kerugian lain yang terjadi pada lapisan fisik dan tautan data. Throughput dapat dipengaruhi secara negatif oleh jarak tautan dan oleh gangguan (noise).

Tips: Throughput biasanya diukur pada jaringan atau lapisan transport. Seringkali istilah goodput digunakan untuk mengukur kecepatan transfer data rata-rata pada lapisan aplikasi. Ini memperhitungkan efek packet loss. Throughput juga terkadang diukur sebagai paket per detik.

Selain bandwidth atau throughput dan packet loss, kecepatan pengiriman paket juga merupakan karakteristik kinerja jaringan yang penting. Kecepatan diukur sebagai satuan waktu-biasanya milidetik (ms)-dan juga disebut sebagai latensi, atau penundaan. Latensi dapat terjadi di banyak lapisan model OSI. Namun, ini biasanya bukan faktor penting pada Ethernet lokal.

Tips: Istilah kecepatan juga digunakan untuk menggambarkan seberapa baik atau buruk kinerja tautan dalam hal throughput, tetapi perhatikan perbedaan antara bandwidth dan latensi.

Batasan Jarak, Atenuasi, dan Kebisingan

Setiap jenis media dapat secara konsisten mendukung laju bit tertentu hanya pada jarak yang ditentukan. Beberapa jenis media mendukung kecepatan bit yang lebih tinggi pada jarak yang lebih jauh daripada yang lain. Atenuasi dan kebisingan memberlakukan batasan jarak pada jenis media yang berbeda.

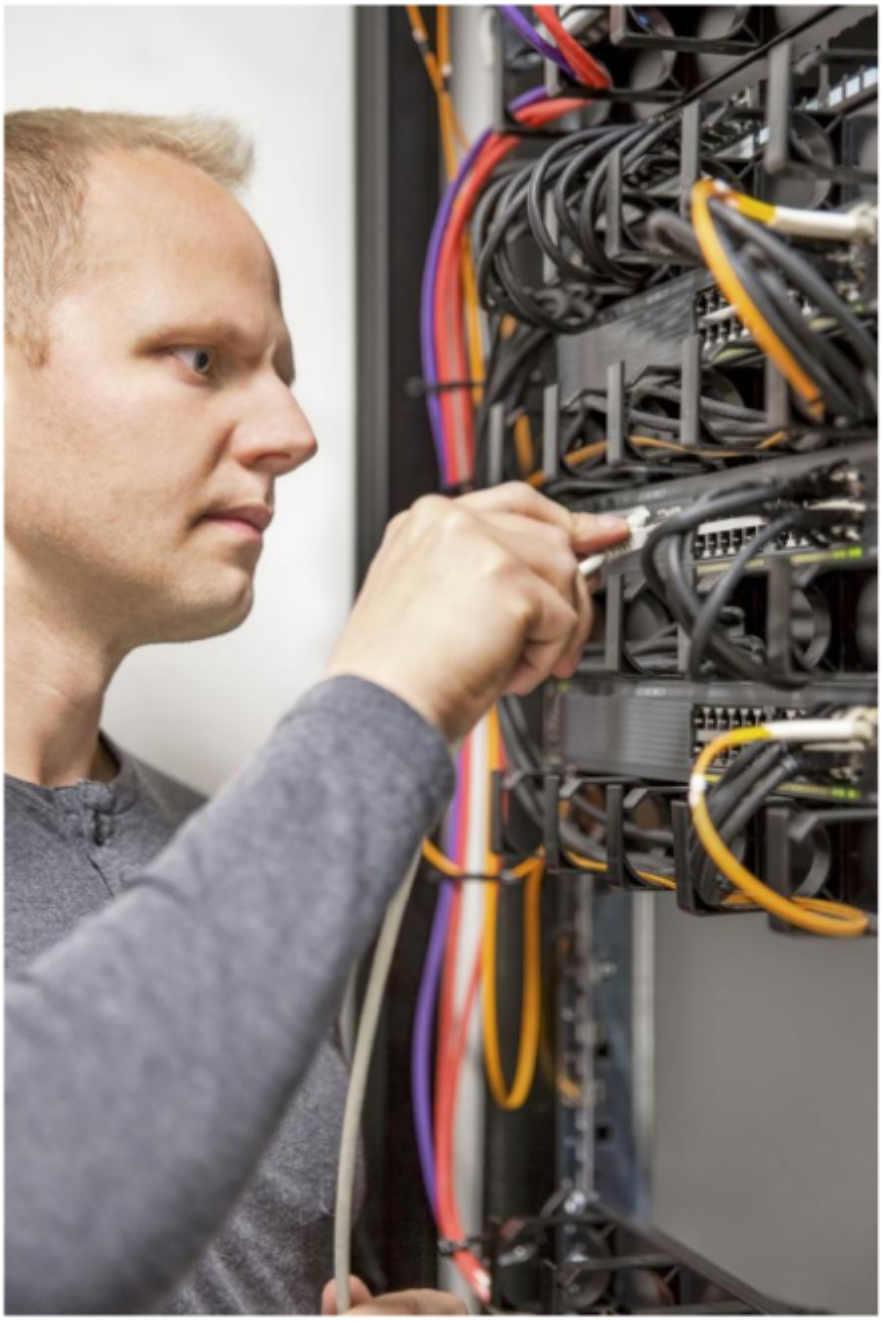
- Atenuasi adalah hilangnya kekuatan sinyal, dinyatakan dalam desibel (dB). dB menyatakan rasio antara dua pengukuran; dalam hal ini, kekuatan sinyal di tempat asal dan kekuatan sinyal di tempat tujuan.
- Kebisingan adalah segala sesuatu yang ditransmisikan di dalam atau di dekat saluran yang bukan merupakan sinyal yang dimaksudkan. Ini berfungsi untuk membuat sinyal itu sendiri sulit dibedakan, menyebabkan kesalahan dalam data dan memaksa pengiriman ulang. Ini dinyatakan sebagai rasio sinyal terhadap noise (SNR).

Masalah Kabel

Saat memecahkan masalah konektivitas kabel, Anda berfokus pada masalah di lapisan fisik. Pada lapisan satu, tautan Ethernet tipikal untuk stasiun kerja kantor mencakup komponen berikut:

- Transceiver jaringan di host (sistem akhir).
- Kabel patch antara host dan port dinding.
- Kabel terstruktur antara port dinding dan panel tambalan (tautan permanen).
- Kabel patch antara port panel patch dan port switch.
- Transceiver jaringan di port sakelar (sistem perantara).

Seluruh jalur kabel (kabel patch plus tautan permanen) disebut sebagai tautan saluran.



Memverifikasi koneksi kabel patch. (Gambar oleh Kjetil Kolbjornsrud © 123RF.com.)

Dengan asumsi Anda sedang menyelidiki kegagalan tautan (kehilangan total konektivitas), langkah pertama adalah memeriksa apakah kabel patch telah dihentikan dengan benar dan terhubung ke port jaringan. Jika Anda mencurigai adanya kesalahan, ganti kabel patch dengan kabel yang dikenal baik.

Jika Anda tidak dapat mengisolasi masalah ke kabel patch, uji transceiver. Anda dapat menggunakan alat loopback untuk menguji port yang buruk.

Tips: Jika Anda tidak memiliki alat loopback yang tersedia, pendekatan lain adalah dengan mengganti host yang berfungsi yang dikenal (hubungkan komputer lain ke tautan atau tukar port di sakelar). Namun, pendekatan ini mungkin berdampak buruk pada jaringan lainnya, dan masalah seperti keamanan port mungkin menjadikannya metode yang tidak dapat diandalkan.

Jika Anda dapat mengabaikan kabel patch yang rusak dan port/NIC jaringan yang buruk, Anda perlu menggunakan alat untuk menguji pemasangan kabel terstruktur. Solusinya mungkin melibatkan pemasangan tautan permanen baru, tetapi mungkin juga ada masalah penghentian atau gangguan eksternal.

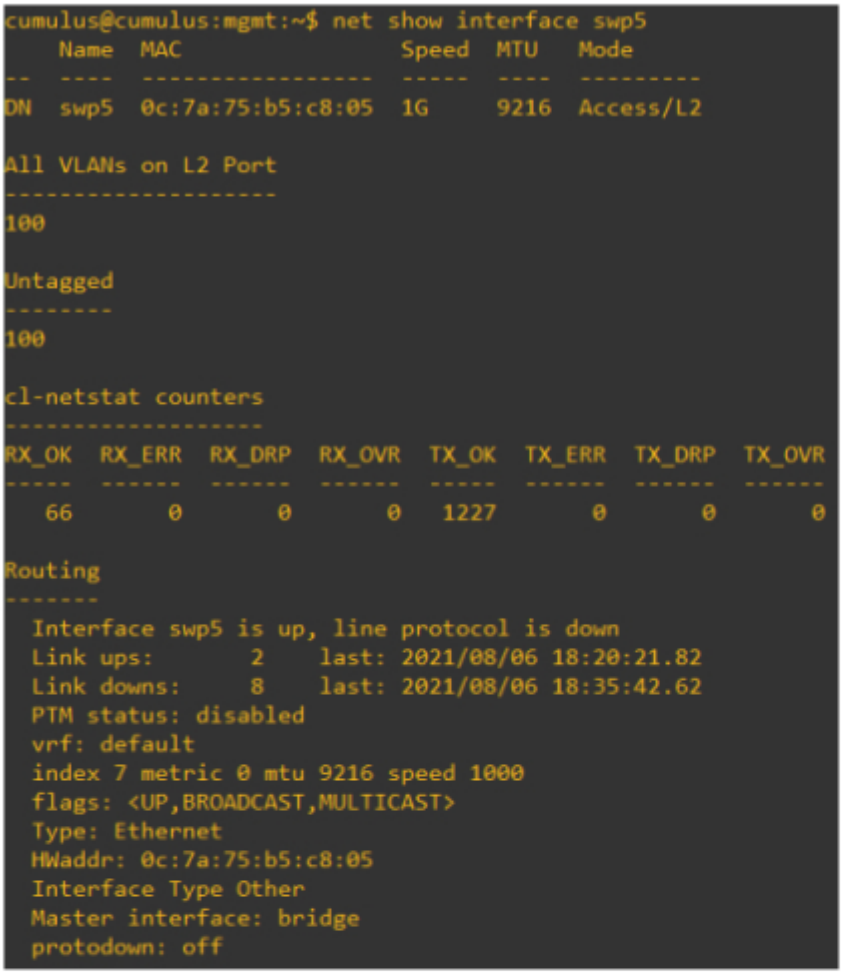
Loopback Plugs, Indikator Status, dan Konfigurasi Antarmuka

Adaptor loopback jaringan (atau colokan loopback) adalah steker RJ-45 berkabel khusus dengan rintisan kabel 6". Pinout pengkabelan adalah pin 1 (Tx) ke pin 3 (Rx) dan pin 2 (Tx) ke pin 6 (Rx). Artinya paket yang dikirim oleh NIC diterima dengan sendirinya. Ini digunakan untuk menguji port dan kartu jaringan yang buruk.

Pendekatan lain ketika Anda memecahkan masalah kabel yang dicurigai adalah dengan memeriksa lampu tautan atau indikator status LED koneksi jaringan pada NIC di satu ujung dan port sakelar/router di ujung lainnya. Anda akan memerlukan dokumentasi vendor untuk menafsirkan LED. Mungkin ada dua LED untuk status dan untuk tautan. Pada port sakelar, status tautan LED berikut adalah tipikal:

- **Hijau solid** -Tautan terhubung tetapi tidak ada lalu lintas.
- **Berkedip hijau** -Tautan beroperasi secara normal (dengan lalu lintas).
- **Tidak ada cahaya** - Tautan tidak berfungsi atau terputus di ujung yang lain.
- **Berkedip kuning** -Sebuah kesalahan telah terdeteksi (misalnya, ketidakcocokan dupleks atau pemblokiran pohon rentang).
- **Kuning solid** -Port dinonaktifkan.

Jika tidak ada masalah kegagalan perangkat keras yang jelas, Anda harus memverifikasi pengaturan pada port switch dan NIC. Sebagian besar adaptor dan sakelar berhasil menegosiasikan pengaturan port secara otomatis. Jika proses ini gagal, adaptor dan port dapat berakhir dengan kecepatan atau pengaturan dupleks yang tidak cocok. Dalam kebanyakan kasus, ini karena adaptor atau port switch telah dikonfigurasi secara manual. Jika host diatur ke konfigurasi tetap dan switch diatur ke autonegosiasi, switch akan default ke 10 Mbps/half-duplex karena host tidak akan bernegosiasi dengannya! Jadi, jika host dikonfigurasi secara manual ke 100 Mbps/full duplex, link akan gagal. Menyetel keduanya ke negosiasi otomatis biasanya akan menyelesaikan masalah. Ketidakcocokan kecepatan akan menyebabkan tautan gagal, sementara ketidakcocokan dupleks akan memperlambat tautan (ini akan menyebabkan kehilangan paket yang tinggi dan tabrakan yang terlambat).



Melihat konfigurasi antarmuka pada sakelar Cumulus VX. (Tangkapan layar milik Nvidia.)

Penguji Kabel

Saat memecahkan masalah tautan permanen, Anda harus memverifikasi bahwa jenis kabel sesuai dengan aplikasi. Misalnya, Anda tidak dapat mengharapkan Ethernet 10 GbE untuk dijalankan pada tautan Cat 5e 80 m. Anda mungkin juga perlu memverifikasi bahwa kabel tanpa pelindung belum dipasang di tempat yang lebih cocok untuk kabel berpelindung atau berpelindung. Menggunakan jenis kabel yang salah dapat mengakibatkan kecepatan yang lebih rendah dari yang diharapkan dan/atau banyak kesalahan checksum dan pengaturan ulang tautan. Periksa pengenal yang tercetak pada jaket kabel untuk memverifikasi jenis yang telah digunakan.

Dari sudut pandang keamanan, Anda juga harus memastikan bahwa tipe jaket kabel cocok untuk lokasi pemasangan, seperti menggunakan kabel dengan peringkat pleno di ruang pleno dan kabel dengan peringkat naik di ruang naik.

Jika kabel tidak dapat diakses, alat pengujian kabel juga dapat digunakan untuk mendiagnosis konektivitas yang terputus-putus atau masalah kinerja yang buruk. Waktu terbaik untuk memverifikasi pemasangan dan pemutusan kabel adalah setelah Anda membuat semua sambungan. Ini berarti Anda masih harus memiliki akses ke kabel berjalan. Mengidentifikasi dan memperbaiki kesalahan pada titik ini akan jauh lebih sederhana daripada saat Anda mencoba menyiapkan perangkat pengguna akhir.

Penguji kabel melaporkan informasi terperinci tentang sifat fisik dan listrik kabel. Misalnya, ia dapat menguji dan melaporkan kondisi kabel, crosstalk, redaman, kebisingan, hambatan, dan karakteristik lain dari kabel. Perangkat yang diklasifikasikan sebagai pengesah dapat digunakan untuk menguji dan mengesahkan pemasangan kabel ke kategori kinerja-misalnya, bahwa jaringan memenuhi TIA/EIA 568 Kategori 6A. Mereka menggunakan spesifikasi kinerja transportasi yang ditentukan untuk memastikan instalasi melebihi karakteristik kinerja yang diperlukan untuk parameter seperti redaman dan crosstalk.



Teknisi menggunakan sertifikasi kabel. (Gambar oleh Wavebreak Media © 123RF.com.)

Penguji kabel mungkin menggabungkan fungsi reflektometer domain waktu (TDR). TDR digunakan untuk mengukur panjang kabel dan dapat menemukan sirkuit terbuka dan pendek, kekusutan/tekukan tajam, dan ketidaksempurnaan lain pada kabel yang dapat memengaruhi kinerja. TDR mentransmisikan pulsa sinyal pendek dengan amplitudo dan durasi yang diketahui melalui kabel dan mengukur amplitudo yang sesuai dan waktu tunda yang terkait dengan pantulan sinyal yang dihasilkan. TDR menganalisis refleksi ini dan dapat menampilkan masalah

yang ditemukan dan lokasinya. TDR mengukur jumlah waktu yang dibutuhkan sinyal untuk memantul kembali dan oleh karena itu dapat menghitung jarak ke gangguan kabel hingga dalam satu meter, yang membuat mengisolasi masalah menjadi lebih sederhana.

Wire Map Testers and Tone Generators

Jika penguji kabel atau perangkat sertifikasi khusus tidak tersedia, multimeter dapat digunakan untuk memeriksa konektivitas fisik. Tujuan utama multimeter adalah untuk menguji sirkuit listrik, tetapi dapat menguji kontinuitas segala jenis kabel tembaga, keberadaan korsleting, dan integritas terminator. Untuk melakukan tes yang berguna, Anda perlu mengetahui bacaan yang diharapkan dari tes tertentu. Misalnya, jika resistansi yang diukur di seluruh kabel Ethernet UTP ditemukan 100 ohm, maka kabelnya boleh saja, tetapi jika resistansi antara kedua ujung kabel tidak terhingga, kabel tersebut putus. Banyak multimeter yang dirancang untuk penggunaan TIK menggabungkan fungsi penguji peta kawat. Ini juga tersedia sebagai perangkat khusus. Penguji peta kawat dapat mengidentifikasi masalah berikut:

- **Kontinuitas (terbuka)** -Konduktor tidak membentuk rangkaian karena kerusakan kabel atau karena konektor tidak terpasang dengan benar.
- **Pendek** -Dua konduktor bergabung di beberapa titik, biasanya karena kabel isolasi rusak, atau konektor kabelnya buruk.
- **Pin-out yang salah/penghentian yang salah/standar yang tidak cocok** -Konduktor salah disambungkan ke terminal di salah satu atau kedua ujung kabel. Transposisi berikut adalah umum:
    - **Pasangan terbalik** -Konduktor dalam pasangan telah disambungkan ke terminal yang berbeda (misalnya, dari pin 3 ke pin 6 dan pin 6 ke pin 3 daripada pin 3 ke pin 3 dan pin 6 ke pin 6).
    - **Crossed pair (TX/RX reverse)** -Konduktor dari satu pasangan telah dihubungkan ke pin milik pasangan yang berbeda (misalnya, dari pin 3 dan 6 ke pin 1 dan 2). Ini mungkin dilakukan dengan sengaja untuk membuat kabel crossover, tetapi kabel seperti itu tidak akan digunakan untuk menghubungkan host ke switch.

Kesalahan kabel kabel potensial lainnya adalah pasangan split. Di sinilah kedua ujung kabel tunggal dalam satu pasang dihubungkan ke terminal milik pasangan yang berbeda. Jenis kesalahan ini hanya dapat dideteksi oleh penguji peta kawat yang juga menguji crosstalk yang berlebihan. Ini umumnya jenis fungsi yang terkait dengan penguji kabel atau pengesah.

Sebuah generator nada jaringan dan probe digunakan untuk melacak kabel dari satu ujung ke ujung lainnya. Ini mungkin diperlukan jika kabel dibundel dan belum diberi label dengan benar. Perangkat ini juga dikenal sebagai Fox and Hound atau probe nada. Generator nada digunakan untuk menerapkan sinyal pada kabel yang akan dilacak di mana digunakan untuk mengikuti kabel di atas langit-langit dan melalui saluran.

Masalah Atenuasi dan Interferensi

Jika tautan kabel terlalu panjang, kehilangan desibel (dB) (atau kehilangan penyisipan) dapat berarti bahwa tautan mengalami masalah dengan tingkat kesalahan yang tinggi dan transmisi ulang (kehilangan bingkai atau paket) yang mengakibatkan penurunan kecepatan dan kemungkinan hilangnya konektivitas. Kehilangan penyisipan diukur dalam desibel (dB) dan mewakili rasio tegangan yang diterima dengan tegangan asli.

A dB menyatakan rasio antara dua nilai menggunakan skala logaritmik. Logaritma adalah alat matematika untuk melakukan operasi perkalian dan pembagian yang kompleks sebagai penjumlahan dan pengurangan yang lebih sederhana. Poin penting adalah bahwa skala logaritmik adalah nonlinier, sehingga perubahan kecil dalam nilai mewakili perubahan besar dalam kinerja yang diukur. Poin referensi berikut berguna untuk diingat:

- +3 dB berarti menggandakan, sedangkan -3 dB berarti mengurangi separuh.
- +6 dB berarti empat kali lipat, sedangkan -6 dB berarti seperempat.
- +10 dB berarti sepuluh kali rasio, sedangkan -10 dB adalah sepersepuluh.

Tips: Untuk pelajaran matematika dB yang lebih lama, lihat presentasinya di internetsociety.org/wp-content/uploads/2017/10/dB-Math.pdf.

Nilai maksimum yang diperbolehkan untuk insertion loss tergantung pada kategori link. Misalnya, Cat 5e pada 100 MHz memungkinkan hingga 24 dB, sedangkan Cat 6 memungkinkan hingga 21,7 dB pada 250 MHz. Saat Anda mengukur insertion loss itu sendiri, nilai yang lebih kecil lebih baik (20 dB insertion loss lebih baik dari 22 dB, misalnya). Pengesah kabel kemungkinan akan melaporkan margin, yang merupakan perbedaan antara kerugian aktual dan nilai maksimum yang diizinkan untuk standar kabel. Akibatnya, nilai margin yang lebih tinggi lebih baik. Misalnya, jika insertion loss yang diukur melalui kabel Cat 5e adalah 22 dB, marginnya adalah 2 dB; jika kabel lain berukuran 23 dB, marginnya hanya 1 dB, dan Anda hampir tidak memenuhi standar tautan yang dapat diterima. Kabel kelas atau terlindung yang lebih tinggi dapat mengatasi masalah; jika tidak,

Penempatan kabel yang hati-hati diperlukan selama pemasangan untuk memastikan bahwa kabel tidak terkena gangguan dari sumber seperti kabel daya listrik, lampu neon, motor, kipas listrik, pemancar radio, dan sebagainya. Interferensi elektromagnetik (EMI) adalah sesuatu yang harus dideteksi ketika kabel dipasang, jadi Anda harus mencurigai beberapa sumber baru yang telah dipasang baru-baru ini atau beberapa sumber yang tidak diperhitungkan selama pengujian (mesin atau sirkuit daya yang tidak diaktifkan ketika pengujian instalasi berlangsung, misalnya). Interferensi dari kabel data terdekat juga disebut sebagai crosstalk alien.

Tips: Interferensi frekuensi radio (RFI) adalah EMI yang terjadi pada frekuensi yang digunakan untuk transmisi radio.

Masalah Crosstalk

Crosstalk biasanya menunjukkan masalah dengan kabel yang buruk (kualitas buruk atau rusak atau jenis aplikasi yang tidak tepat), konektor yang buruk, atau penghentian yang tidak tepat. Periksa kabel apakah ada lilitan yang berlebihan di ujungnya dan untuk kekusutan atau titik hancur di sepanjang jalurnya. Crosstalk juga diukur dalam dB, tetapi tidak seperti insertion loss, nilai yang lebih tinggi menunjukkan lebih sedikit noise. Sekali lagi, pengukuran yang diharapkan bervariasi sesuai dengan kategori dan aplikasi kabel. Ada berbagai jenis crosstalk yang dapat diukur:

- **Near End (NEXT)** -Ini mengukur crosstalk pada pasangan penerima di ujung pemancar dan biasanya disebabkan oleh pelepasan pasangan yang berlebihan atau ikatan yang salah dari elemen terlindung.
- **Attenuation to Crosstalk Ratio, Near End (ACRN)** -Ini adalah perbedaan antara insertion loss dan NEXT. ACR setara dengan rasio signal-to-noise (SNR). Nilai tinggi berarti bahwa sinyal lebih kuat daripada noise yang ada; hasil yang mendekati 0 berarti tautan tersebut kemungkinan akan mengalami tingkat kesalahan yang tinggi.
- **Attenuation-to-Crosstalk Ratio, Far End (ACRF)** -Far End Crosstalk (FEXT) diukur pada pasangan penerima di ujung penerima. Perbedaan antara insertion loss dan FEXT memberikan ACRF, yang mengukur kinerja kabel terlepas dari panjang tautan sebenarnya.
- **Jumlah daya** -Gigabit dan Ethernet 10 GbE menggunakan keempat pasangan. Perhitungan crosstalk jumlah daya (PSNEXT, PSACRN, dan PSACRF) memastikan bahwa kabel cocok untuk jenis aplikasi ini. Mereka diukur dengan memberi energi pada tiga dari empat pasangan secara bergantian.

Tips: Konektivitas yang hilang sepenuhnya menunjukkan kabel putus (atau instalasi yang sepenuhnya salah), sementara kehilangan konektivitas yang terputus-putus lebih mungkin disebabkan oleh redaman, crosstalk, atau kebisingan.

Masalah Aplikasi Kabel

Saat berurusan dengan kabel patch dan peralatan jaringan lama, Anda perlu memperhitungkan aplikasi kabel yang tepat.

Kabel Straight Through dan Crossover

Ada dua format utama untuk kabel patch:

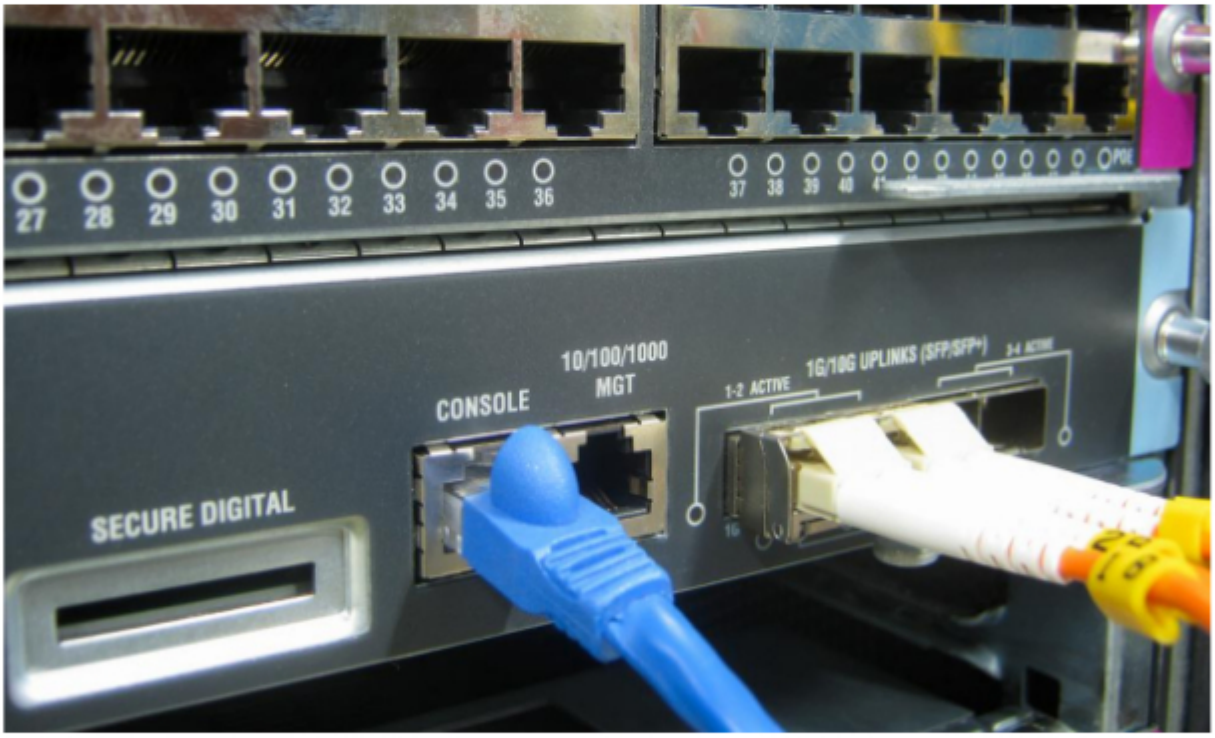
- **Straight through** -kabel diakhiri dengan T568A di kedua ujungnya atau T568B di kedua ujungnya. Jenis kabel ini digunakan untuk uplink (port MDI ke port MDIX).
- **Crossover** -kabel diakhiri dengan T568A di satu ujung dan T568B di ujung lainnya. Jenis kabel ini digunakan untuk menghubungkan sistem akhir (host) ke host lain atau hub ke hub.

Faktanya, kabel crossover tidak lagi diperlukan untuk jenis aplikasi ini, karena sakelar memiliki port uplink untuk tujuan ini atau dapat mendeteksi secara otomatis dan memilih antara koneksi crossover dan koneksi langsung. Ini disebut sebagai auto-MDI/MDI-X. Semua port Gigabit Ethernet mendukung auto-MDI/MDI-X.

Kabel Rollover/Kabel Konsol Kabel

konsol digunakan untuk menghubungkan PC atau laptop ke terminal baris perintah dari sakelar atau router. Sambungan port konsol pada alat adalah jack RJ-45 standar (tetapi disambungkan dengan cara yang berbeda ke Ethernet). Kabel konsol lama memiliki konektor serial DB-9 untuk ujung PC. Karena hampir tidak ada lagi komputer yang dilengkapi dengan port DB-9, kabel modern menggunakan konektor dan port USB. Kabel konsol biasanya berwarna biru pucat.

Program seperti Putty pada PC digunakan untuk membuat koneksi menggunakan pengaturan yang sesuai untuk link serial. Biasanya ini adalah 9.600 bps (baud), 8 bit data/1 stop bit, dan tidak ada paritas atau kontrol aliran. Pada beberapa peralatan yang lebih baru, kabel USB dapat digunakan.



Port konsol RJ-45 dengan kabel terhubung. Slot Secure Digital untuk pembaruan firmware dan port MGT di sebelah port konsol. (Gambar oleh Sorapop Udomsri © 123RF.com.)

Tips: Router biasanya memiliki port konsol dan AUX. Port AUX digunakan untuk menghubungkan ke router melalui modem dial-up. Port konsol hanya menggunakan tautan serial (atau modem nol).

Power over Ethernet Cat 3 atau lebih baik diperlukan untuk mendukung PoE, sedangkan PoE+ harus Cat 5e atau lebih baik. Menarik daya ke kabel menghasilkan lebih banyak panas. Jika panas ini tidak hilang, dapat mempengaruhi kecepatan data. Kinerja termal ditingkatkan dengan menggunakan kabel tembaga murni dengan konduktor yang lebih besar. Sebuah konduktor tipis akan menghasilkan lebih banyak panas melalui perlawanan. Kabel berpelindung juga mampu menyebarkan panas dengan lebih efisien.

Alat Pengujian Kabel Serat Optik

Meskipun kabel serat optik tidak mengalami redaman dengan cara yang sama seperti kabel tembaga atau pada tingkat yang sama, masih akan ada kehilangan kekuatan sinyal dari satu ujung sambungan ke ujung lainnya. Hal ini disebabkan ketidaksempurnaan mikroskopis dalam struktur serat kaca dan kehalusan tepi inti, yang menyebabkan sebagian kecil cahaya di dalam inti tersebar atau diserap. Seperti redaman pada kabel tembaga, kehilangan sinyal meningkat dengan bertambahnya panjang kabel. Spesifikasi EIA/TIA 568 untuk serat memungkinkan hilangnya sinyal antara 0,5 dB/km dan 3,5 dB/km, tergantung pada jenis serat yang digunakan dan panjang gelombang cahaya.

Atenuasi dapat diuji menggunakan sumber optik dan pengukur daya optik (atau pengukur cahaya serat), yang dapat dibeli bersama sebagai kit pengujian serat. Jika kerusakan diidentifikasi pada kabel yang terpasang, lokasi kerusakan dapat ditemukan dengan menggunakan **optical time domain reflectometer (OTDR)**. Ini mengirimkan pulsa cahaya ke kabel dan menghitung berapa lama waktu yang diperlukan untuk pantulan apa pun untuk memantul kembali dari jeda. Kabel yang rusak perlu diperbaiki (disambung) atau diganti. OTDR juga dapat digunakan untuk memverifikasi bahwa sambungan baru baik-baik saja.

Sebuah **penganalisis spektrum optik (OSA)** biasanya digunakan dengan multiplexing divisi panjang gelombang (WDM) untuk memastikan bahwa setiap saluran memiliki daya yang cukup. Pada jarak yang sangat jauh, redaman panjang gelombang yang berbeda dapat bervariasi. Ini disebut sebagai redaman spektral. OSA dapat menentukan apakah kabel yang ada cocok untuk digunakan kembali dengan WDM dan panjang gelombang mana yang akan mendukung jarak tautan yang diperlukan.

Saat Anda bekerja dengan kabel serat optik, penting untuk dipahami bahwa ketidakcocokan antara kabel yang digabungkan bersama akan mengakibatkan hilangnya data. Hal ini dapat terjadi jika kabel serat tidak disejajarkan dengan benar, ukurannya berbeda, atau mungkin mengalami kerusakan (untaian serat rusak/tidak berbentuk) selama pengangkutan.

Kabel Optik Kotor

Kotoran, debu, atau gemuk di jalur transmisi akan sangat mengurangi kekuatan sinyal atau memblokir transmisi sepenuhnya. Paling umum, ini terjadi pada konektor. Konektor harus ditutup dengan penutup debu saat dilepas dan area sekitarnya harus bebas debu sebelum melakukan pemutusan. Konektor harus dibersihkan menggunakan pelarut yang dirancang untuk serat optik, berhati-hatilah agar tidak menggunakan pelarut yang berlebihan. Metode

basah ke kering menerapkan setetes pelarut ke kain bebas serat dan memindahkan konektor dari tetesan basah melintasi bagian yang kering. Kontaminasi juga dapat terjadi ketika kabel disambung. Pastikan peralatan penyambungan dibersihkan sesuai dengan instruksi pabrik sebelum setiap operasi penyambungan.

Transceiver yang Salah Transceiver

yang digunakan di setiap antarmuka optik (apakah SFP, GBIC, atau konverter media lainnya) dirancang untuk digunakan dengan jenis serat optik tertentu. Misalnya, transceiver yang dirancang untuk serat mode tunggal menggunakan laser sedangkan transceiver serat multimode biasanya menggunakan LED. Transceiver yang berbeda dirancang untuk bekerja pada panjang gelombang optik yang berbeda (biasanya 850 nm, 1300 nm, atau 1550 nm). Ini berarti penting untuk memeriksa dokumentasi pabrikan untuk antarmuka guna memastikan jenis serat yang benar digunakan, tidak hanya untuk kabel serat optik, tetapi juga untuk kabel patch serat yang digunakan untuk menyambungkannya di setiap ujungnya. Ketidakcocokan antara kabel, kabel patch, dan antarmuka dapat menyebabkan hilangnya sinyal yang signifikan.

Modul 5
SKEMA PENGALAMATAN IPv4

Pendahuluan: Menjelaskan Skema Pengalamatan IPv4

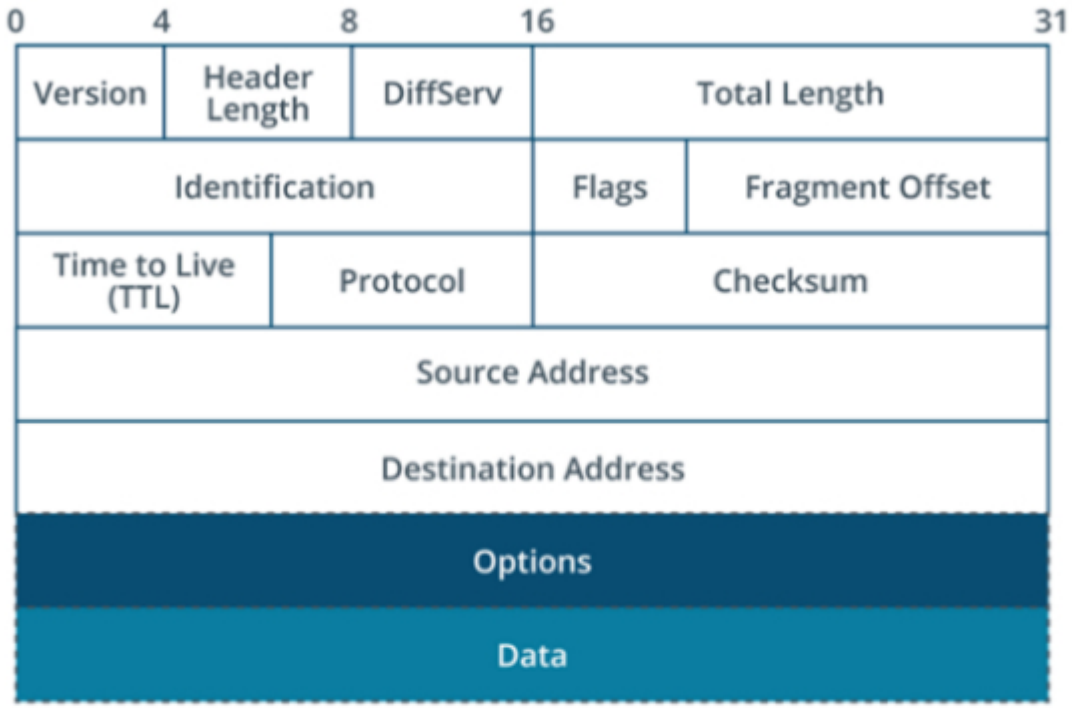
Transmission Control Protocol/Internet Protocol (TCP/IP) terdiri dari protokol dan standar pelengkap yang bekerja sama untuk menyediakan fungsionalitas sebagian besar jaringan modern. Internet Protocol (IP) berdiri di jantung suite protokol ini, menyediakan pengalamatan logis dan penerusan paket antara jaringan yang berbeda. Dalam topik ini, Anda akan mulai menyelidiki karakteristik IP dengan memeriksa struktur paket IPv4 dan format alamat IPv4.

Tips: Ada dua versi IP; versi 4 lebih banyak diadopsi dan merupakan versi yang dibahas dalam beberapa topik berikut. IPv6 memperkenalkan ruang alamat yang jauh lebih besar dan cara yang berbeda untuk mengonfigurasi klien dan akan dibahas nanti dalam pelajaran berikutnya.

IPv4 Datagram Header

Ethernet bekerja pada layer Physical dan Data Link dari model OSI (layer 1 dan 2). Ethernet adalah segmen jaringan tunggal, atau domain broadcast layer 2. Ethernet, dan produk lapisan 1/2 lainnya, tidak memiliki konsep beberapa jaringan atau subdivisi logis dalam jaringan. Fungsi ini diimplementasikan pada lapisan Network (lapisan 3). Sebagai protokol layer 3, Internet Protocol (IP) menyediakan pengalamatan dan penerusan jaringan yang logis.

Header Internet Protocol (IP) berisi bidang untuk mengelola fungsi pengalamatan dan penerusan logis.



IPv4 header.

Bidang Versi menunjukkan versi Protokol Internet yang digunakan (4), sedangkan bidang Panjang menunjukkan ukuran header dan ukuran paket total (termasuk muatan). Ukuran teoritis maksimum adalah 65.535 byte, tetapi paket sebenarnya biasanya akan jauh lebih kecil untuk menghindari fragmentasi ketika diangkut sebagai muatan frame Ethernet.

Bidang Protokol menjelaskan apa yang terkandung (dienkapsulasi) dalam muatan sehingga host penerima tahu bagaimana memprosesnya. Untuk sebagian besar paket, nilai tipe protokol IP di bidang Protokol akan menunjukkan segmen *Transmission Control Protocol* (TCP/6) atau *User Datagram Protocol* (UDP/17), yang bekerja pada lapisan Transport. Nilai yang ditetapkan ke protokol (seperti 6 untuk TCP dan 17 untuk UDP) dikelola oleh IANA.

Tips: Itu adalah nilai dalam desimal. Anda juga cenderung melihatnya dalam bentuk heksa (0x06 dan 0x11). Kedua format pada akhirnya mewakili nilai biner 8-bit (00000110 dan 00010001).

Beberapa protokol berjalan langsung di IP (bukan di lapisan Transport). Jenis protokol IP ini meliputi:

- *Internet Control Message Protocol* (ICMP/1) digunakan untuk pesan status dan pengujian konektivitas.
- *Internet Group Messaging Protocol* (IGMP/2) digunakan dengan multicasting.

- *Generic Routing Encapsulation* (GRE/47) digunakan untuk melakukan tunnel paket melalui jaringan perantara. Ini digunakan (misalnya) dalam beberapa implementasi *Virtual Private Network* (VPN).
- *Encapsulating Security Payload* (ESP/50) dan *Authentication Header* (AH/51) digunakan dengan bentuk IP terenkripsi (IPSec).
- *Enhanced Interior Gateway Routing Protocol* (EIGRP/88) dan *Open Shortest Path First* (OSPF/89) adalah protokol yang digunakan oleh router untuk bertukar informasi tentang jalur ke jaringan jarak jauh.

Format Alamat IPv4

Jaringan dalam sebuah internetwork harus memiliki cara unik untuk mengidentifikasi setiap jaringan logis dan setiap host individu dalam jaringan tersebut. Pada lapisan Data Link, sebuah antarmuka diidentifikasi dengan menggunakan MAC atau alamat perangkat keras. Jenis alamat ini hanya dapat digunakan untuk pengiriman frame secara lokal. Pada lapisan Jaringan, sumber IP dan alamat tujuan digunakan untuk meneruskan paket ke tujuan yang tepat. Alamat IP menyediakan dua informasi:

- Nomor jaringan (ID jaringan)-Nomor ini umum untuk semua host di jaringan IP yang sama.
- Nomor host (host ID)-Nomor ini mengidentifikasi host dalam jaringan IP.

Pengalamatan IPv4 32-bit

Alamat IPv4 panjangnya 32 bit. Dalam bentuk mentahnya, muncul sebagai berikut:
11000110011001101100100000000001

32 bit dibagi menjadi empat kelompok 8 bit (1 byte) yang dikenal sebagai oktet. Oleh karena itu, alamat IP sebelumnya dapat ditulis sebagai:
11000110 00110011 01100100 00000001

Hampir tidak mungkin bagi orang untuk menggunakan format biner sebagai nilai konfigurasi. Untuk membuat alamat IP lebih mudah digunakan, itu diformat menggunakan notasi desimal bertitik. Notasi ini mengharuskan setiap oktet dikonversi ke nilai desimal. Bilangan desimal dipisahkan menggunakan titik. Mengubah nomor sebelumnya ke notasi ini memberikan:
198.51.100.1



Dotted decimal notation.

Konversi Biner/Desimal

Contoh berikut menunjukkan proses konversi antara notasi biner dan desimal:

Dalam basis 2 (binary), digit dapat mengambil salah satu dari dua nilai yang berbeda (0 dan 1). Nilai tempat adalah pangkat dari 2 (21=2, 22=4, 23=8, 24=16, dan seterusnya). Anda harus mengingat nilai-nilai ini untuk dapat melakukan konversi biner/desimal menggunakan metode kolom. Pertimbangkan oktet 11101101 yang diwakili dalam basis 2. Gambar ini menunjukkan nilai tempat setiap digit dalam oktet di dua baris pertama, dengan oktet biner di baris ketiga. Baris empat dan lima menunjukkan bahwa di mana ada 1 dalam oktet, nilai tempat desimal ditambahkan ke jumlah:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128	64	32	16	8	4	2	1	
1	1	0	0	0	1	1	0	
128*1	64*1	32*0	16*0	8*0	4*1	2*1	1*0	
128	+64	+0	+0	+0	+4	+2	+0	= 198

Binary to decimal conversion.

Anda dapat menggunakan metode kolom yang sama untuk mengkonversi dari desimal ke biner. Misalnya, angka 51 dapat dikonversi sebagai berikut:

	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
	128	64	32	16	8	4	2	1
51 =	0	+0	+32	+16	+0	+0	+2	+1
	0	0	1	1	0	0	1	1

Decimal to binary conversion.

Jika semua bit dalam oktet diset ke 1, angka yang diperoleh adalah 255 (nilai maksimum yang mungkin). Demikian pula, jika semua bit diatur ke 0, angka yang diperoleh adalah 0 (nilai minimum yang mungkin). Oleh karena itu, secara teoritis alamat IPv4 dapat berupa nilai antara 0.0.0.0 dan 255.255.255.255. Namun, beberapa alamat tidak diizinkan atau dicadangkan untuk penggunaan khusus.

Network Mask

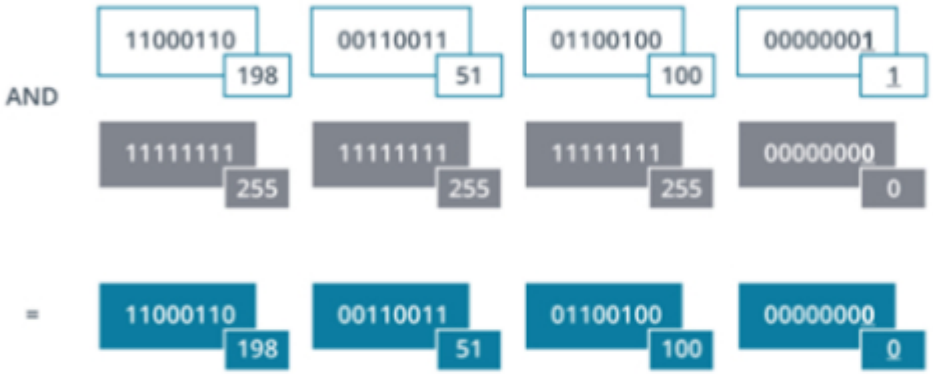
Alamat IP mewakili ID jaringan dan ID host. Network mask 32-bit (atau netmask) digunakan untuk membedakan kedua komponen ini dalam satu alamat IP. Mask menyembunyikan bagian ID host dari alamat IP dan dengan demikian mengungkapkan bagian ID jaringan.

Mask dan alamat IP adalah jumlah bit yang sama. Di mana pun ada biner 1 di mask, digit biner yang sesuai di alamat IP adalah bagian dari ID jaringan. Angka 1 dalam mask selalu bersebelahan. Misalnya, mask ini valid:
11111111 11111111 11111111 00000000

Tetapi string berikut ini bukan mask yang valid:

11111111 00000000 11111111 00000000

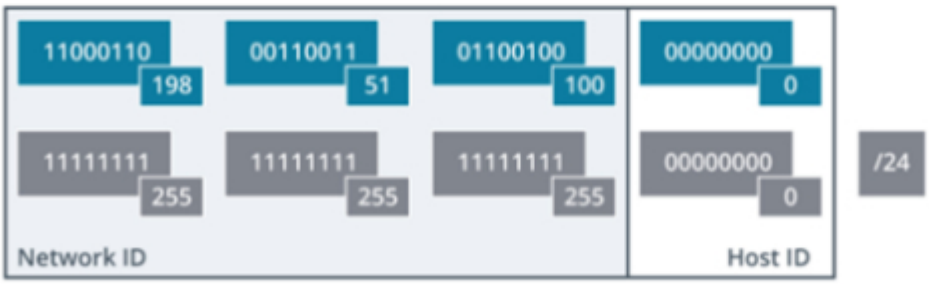
Bagian ID jaringan dari alamat IP diungkapkan dengan ANDing mask ke alamat IP. Ketika dua 1 di-AND bersama-sama, hasilnya adalah 1. Kombinasi lainnya menghasilkan 0. Misalnya, untuk menentukan ID jaringan dari alamat IP host 198.51.100.1 dengan mask 255.255.255.0 , notasi desimal bertitik dari alamat IP dan mask harus terlebih dahulu dikonversi ke notasi biner. Langkah selanjutnya adalah AND dua bilangan biner. Hasilnya dapat dikonversi kembali ke notasi desimal bertitik untuk menunjukkan ID jaringan (198.51.100.0). Satu-satunya perbedaan antara alamat IP host dan ID jaringan terletak pada oktet terakhir, yang tidak ditutupi.



ANDing alamat IP dan subnet mask untuk mendapatkan ID jaringan.

Alih-alih topeng desimal bertitik, jaringan ini dapat diidentifikasi menggunakan awalan atau notasi garis miring. Awalan hanyalah jumlah bit yang disetel ke 1 di topeng. Oleh karena itu, jaringan dapat disebut sebagai 198.51.100.0/24.

Masker default sejajar dengan batas oktet. Ini berarti bahwa nilai dalam topeng akan menjadi 255 atau nol. Misalnya, topeng 24-bit default adalah sebagai berikut:



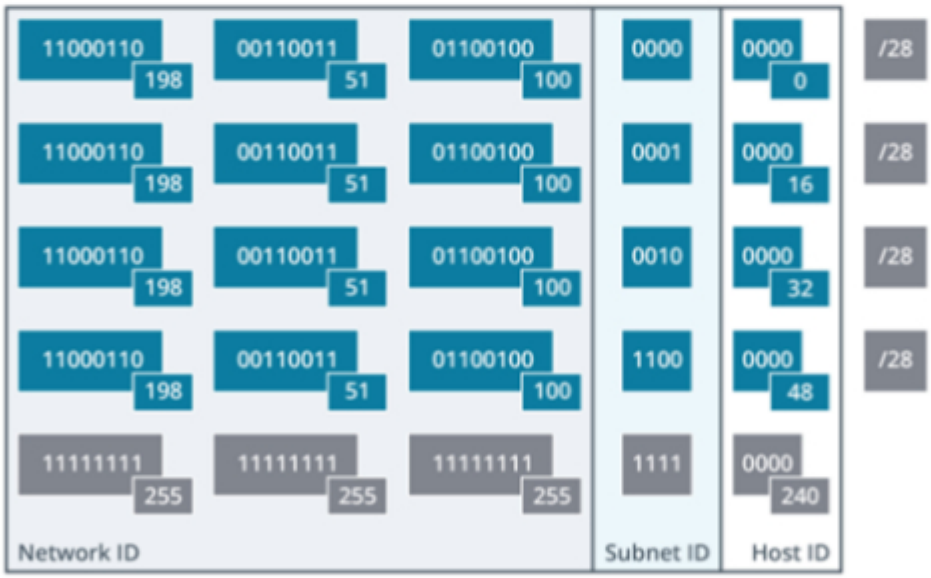
Bagian Network ID and host ID ketika menggunakan 24-bit mask.

Mask 8-bit adalah 255.0.0.0 dan mask 16-bit adalah 255.255.0.0.
Porsi jaringan yang lebih panjang, seperti 255.255.255.0, memungkinkan lebih banyak ID jaringan dalam keseluruhan internetwork, tetapi dengan lebih sedikit alamat host yang tersedia per jaringan. Netmask pendek (255.0.0.0) memungkinkan jutaan host per jaringan, tetapi hanya 126 alamat jaringan yang memungkinkan.

Subnet Mask
Ukuran relatif dari jaringan dan bagian host menentukan berapa banyak jaringan dan host per jaringan yang dapat didukung oleh skema pengalamatan. Teknik pengalamatan konvensional memiliki alamat IP dengan dua tingkatan hierarki, yaitu network ID dan host ID. Skema penggunaan seluruh batas oktet ini tidak fleksibel, sehingga sistem membagi jaringan menjadi subnetwork atau subnet dirancang.

Pengalamatan subnet memiliki tiga tingkat hierarki: ID jaringan, ID subnet, dan ID host. Untuk membuat subnet logis, bit dari bagian host dari alamat IP harus dialokasikan sebagai alamat subnetwork, bukan bagian dari ID host.

Ini berarti ID subnet terletak di dalam batas oktet. Misalnya, binary mask dengan 28 bit dapat menggunakan semua oktet, dengan batas awalan jaringan terletak di dalam oktet keempat:



Subnet adressing.
Ini menyisakan hanya 4 bit untuk rentang ID host.ID jaringan dan ID subnet menggunakan mask yang berbeda. Mask untuk seluruh jaringan masih 255.255.255.0. Host dalam jaringan menggunakan subnet mask 255.255.255.240.

Penting untuk dipahami bahwa hanya satu mask yang pernah diterapkan ke alamat IP pada setiap antarmuka. Mask yang berisi informasi subnet hanya digunakan dalam jaringan IP. Jaringan IP eksternal terus mengalamatkan seluruh jaringan dengan ID jaringannya (198.51.100.0/255.255.255.0). Host dalam jaringan menggunakan subnet mask yang lebih panjang untuk membedakan subnet. Ini adalah 198.51.100.0/255.255.255.240,198.51.100.16/255.255.255.240,198.51.100.32/255.255.255.240,198.51.100.48/255.255.255.240, dan seterusnya).

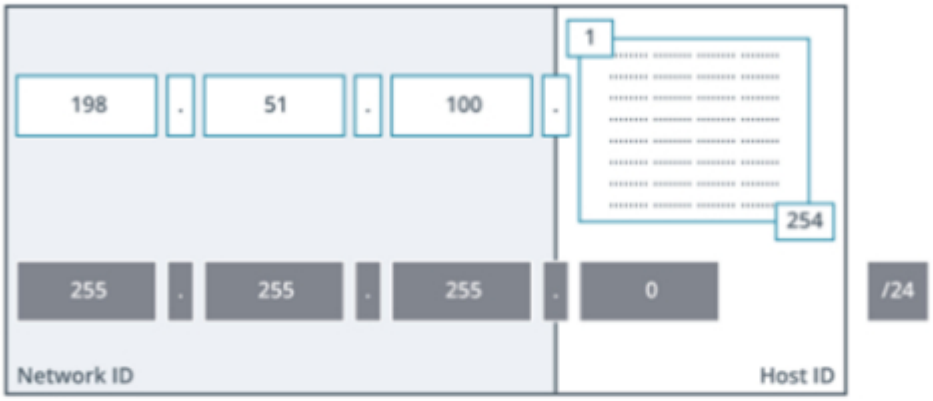
Karena angka 1 dalam mask selalu bersebelahan, setiap oktet dalam desimal dalam mask IPv4 akan selalu menjadi salah satu dari berikut ini.

Octet Mask Bits	Binary Octet	Decimal Equivalent
1	10000000	128
2	11000000	192
3	11100000	224
4	11110000	240
5	11111000	248
6	11111100	252
7	11111110	254
8	11111111	255

Cobalah untuk mengingat nilai-nilai ini untuk membuat konversi topeng antara format biner dan desimal lebih mudah. Misalnya, topeng yang lebih pendek dengan 14 bit memiliki mask berikut:
11111111 11111100 00000000 00000000 255 252 0 0

Host Address Ranges

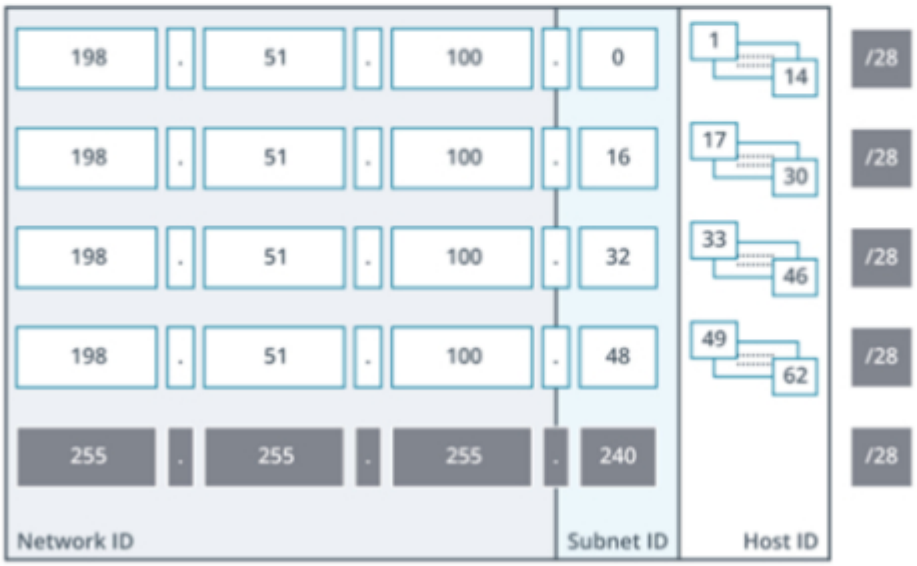
Jaringan IP 198.51.100.0/24 memungkinkan 254 kemungkinan ID host. Bagian ID host panjangnya 8 bit:



Host address range for a /24 network

8 bit dapat mengekspresikan 256 kemungkinan nilai (28). Namun, alamat pertama (198.51.100.0) tidak dapat ditetapkan ke host karena merupakan alamat jaringan. Demikian pula, alamat terakhir (198.51.100.255) dicadangkan (untuk digunakan sebagai alamat siaran).

Menggunakan beberapa dari 8 bit host ini sebagai ID subnet menciptakan jaringan ekstra, tetapi masing-masing subnet tersebut memiliki lebih sedikit alamat host (14 dalam contoh ini):



Host address range for a /28 network.

Tujuan dari subnetting adalah untuk membuat segmen domain broadcast layer 3 dengan host yang lebih sedikit. Trik dengan desain subnet adalah menyesuaikan skema dengan persyaratan jumlah subnetwork dan jumlah host per subnet. Setiap bit yang ditambahkan ke mask kira-kira membagi dua jumlah alamat host yang tersedia.

IPv4 FORWADING

Pendahuluan: IPv4 Forwarding

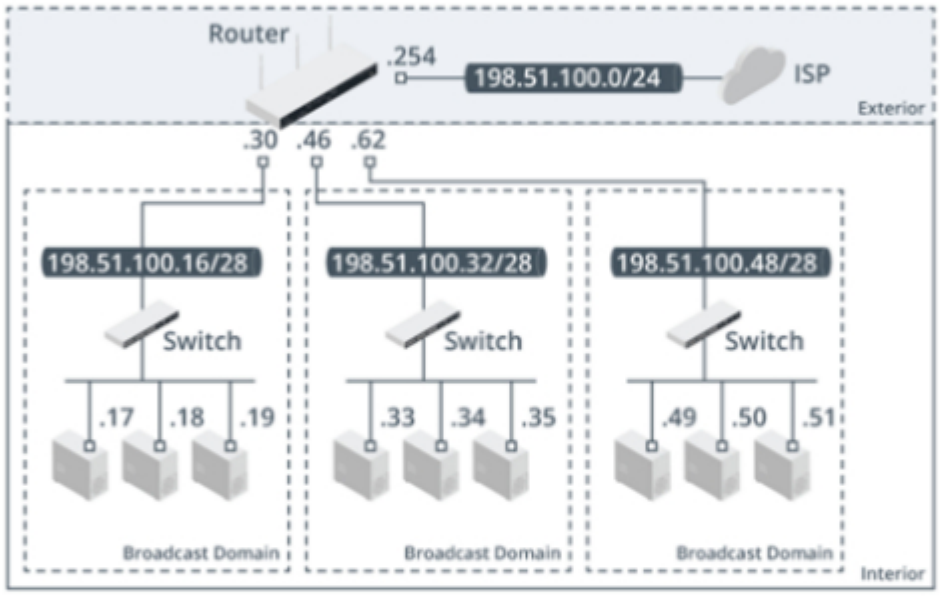
Fungsi inti dari IP adalah untuk memfasilitasi pembuatan sekelompok jaringan yang berbeda secara logis tetapi saling berhubungan, yang disebut sebagai internetwork. Ini berarti bahwa beberapa paket yang dialamatkan ke host di jaringan jarak jauh harus diteruskan melalui satu atau lebih sistem perantara yang membangun jalur antar jaringan.

Dalam topik ini, Anda akan mengidentifikasi prinsip-prinsip dasar yang digunakan IP untuk membedakan host dan jaringan lokal dan jarak jauh, ditambah metode di mana sebuah paket dapat dialamatkan ke lebih dari satu host.

Layer 2 versus Layer 3 Addressing and Forwarding

Saat merancang atau mendukung jaringan IP, penting untuk memahami bagaimana skema pengalamatan logis dari network, subnet, dan host ID pada layer network memetakan ke forwarding pada layer data link. Penerusan pada layer 3 disebut sebagai routing, sedangkan penerusan pada layer 2 disebut sebagai switching.

Gambar berikut mengilustrasikan bagaimana komponen switching dan routing dapat digunakan dalam jaringan tipikal. Seluruh jaringan terhubung ke Internet yang lebih luas melalui antarmuka WAN di router. Antarmuka router lainnya digunakan untuk membagi jaringan menjadi tiga subjaringan logis. Subnet ini dipetakan ke segmen layer 2, masing-masing diimplementasikan menggunakan switch.



Penempatan jaringan router dan switch. (Gambar © 123RF.com.)

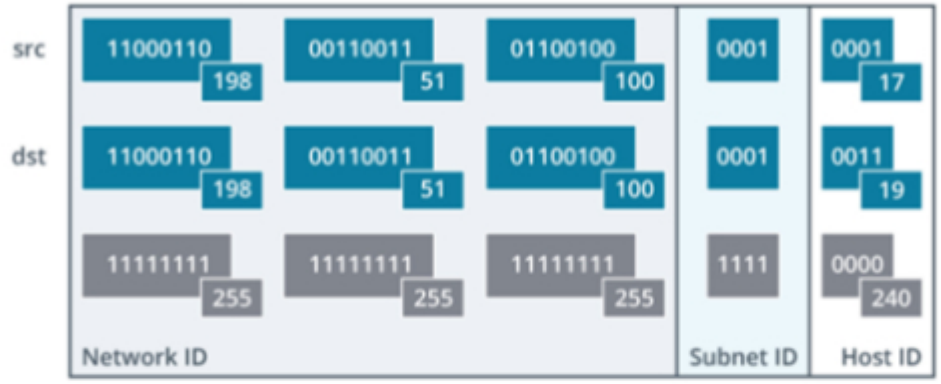
Node dalam setiap subnet dapat saling mengalamatkan secara langsung (mereka berada dalam domain broadcast yang sama), tetapi mereka hanya dapat berkomunikasi dengan node di subnet lain melalui router.

Dalam setiap subnet atau domain broadcast, node menggunakan alamat MAC untuk meneruskan frame satu sama lain, menggunakan mekanisme untuk menerjemahkan antara alamat IP layer 3 dan alamat MAC layer 2.

Lapisan Jaringan juga dapat mengakomodasi penerusan antara berbagai jenis jaringan lapisan 1/2. Zona pribadi diimplementasikan menggunakan Ethernet, tetapi hubungan antara antarmuka publik router dan ISP mungkin menggunakan teknologi yang berbeda, seperti *Digital Subscriber Line* (DSL)

Gateway Default IPv4

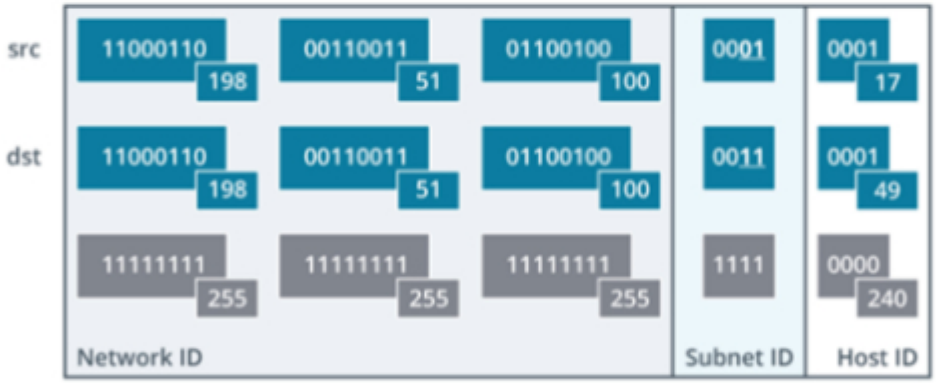
Ketika dua host sistem akhir mencoba untuk berkomunikasi melalui IPv4, protokol membandingkan sumber dan alamat tujuan di setiap paket dengan netmask. Jika bagian yang disamarkan dari alamat IP sumber dan tujuan cocok, maka antarmuka tujuan diasumsikan berada pada jaringan atau subnet IP yang sama.



Pencocokan ID jaringan sumber dan tujuan.

Pada gambar, 28 bit pertama dari alamat sumber dan tujuan adalah sama. Oleh karena itu, IP menyimpulkan alamat IPv4 tujuan berada di jaringan IP yang sama dan mencoba mengirimkan paket secara lokal.

Jika bagian yang di-mask tidak cocok, seperti pada gambar berikut, IP mengasumsikan paket harus dirutekan ke jaringan IP lain:



ID jaringan sumber dan tujuan yang berbeda.

Ketika alamat IPv4 tujuan berada di jaringan IP atau subnet yang berbeda, host meneruskan paket ke gateway default-nya, daripada mencoba mengirimkannya secara lokal. Gateway default adalah router yang dikonfigurasi dengan jalur ke jaringan jarak jauh.

Router menentukan apa yang harus dilakukan dengan paket dengan melakukan perbandingan yang sama antara alamat sumber dan tujuan dan netmask. Router kemudian menggunakan tabel peruteannya untuk menentukan antarmuka mana yang harus digunakan untuk

meneruskan paket. Jika tidak ada jalur yang cocok, router menjatuhkan paket dan menginformasikan host bahwa paket tersebut tidak dapat dikirimkan.

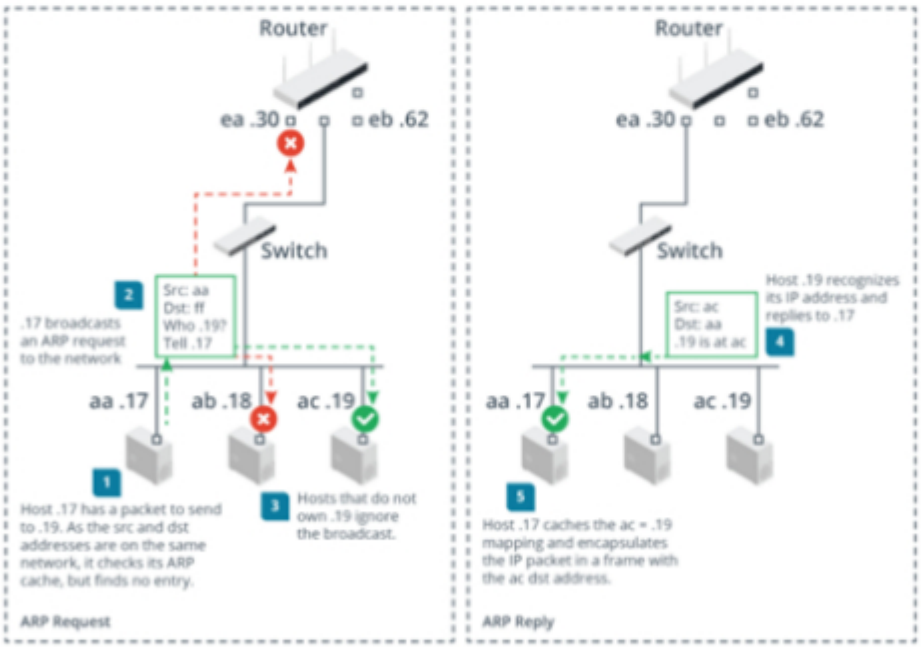
Jika pesan ditujukan untuk jaringan lain, proses diulang untuk membawanya ke tahap berikutnya, dan seterusnya.

Jalur ke jaringan IP lain dapat dikonfigurasi secara manual di tabel perutean atau dipelajari oleh protokol perutean dinamis. Protokol perutean dinamis memungkinkan router untuk berbagi informasi tentang jaringan yang dikenal dan kemungkinan jalur ke sana. Informasi ini memungkinkan mereka untuk memilih rute terbaik ke tujuan tertentu dan memilih rute alternatif jika salah satunya tidak tersedia.

Protokol Resolusi Alamat

Ketika dua host berkomunikasi melalui jaringan Ethernet menggunakan TCP/IP, alamat IP digunakan pada lapisan Jaringan untuk mengidentifikasi setiap antarmuka host. Namun, transmisi data harus dilakukan di tingkat Fisik dan Data Link menggunakan alamat lokal atau perangkat keras/MAC dari antarmuka. Paket TCP/IP mencakup Address Resolution Protocol (ARP) untuk melakukan tugas menyelesaikan alamat IP ke alamat perangkat keras.

Ketika host pengirim dan penerima berada dalam domain broadcast atau subnet yang sama, resolusi alamat lokal terjadi menggunakan permintaan ARP dan balasan ARP, seperti yang ditunjukkan pada gambar:



Permintaan dan balasan ARP. (Gambar © 123RF.com.)

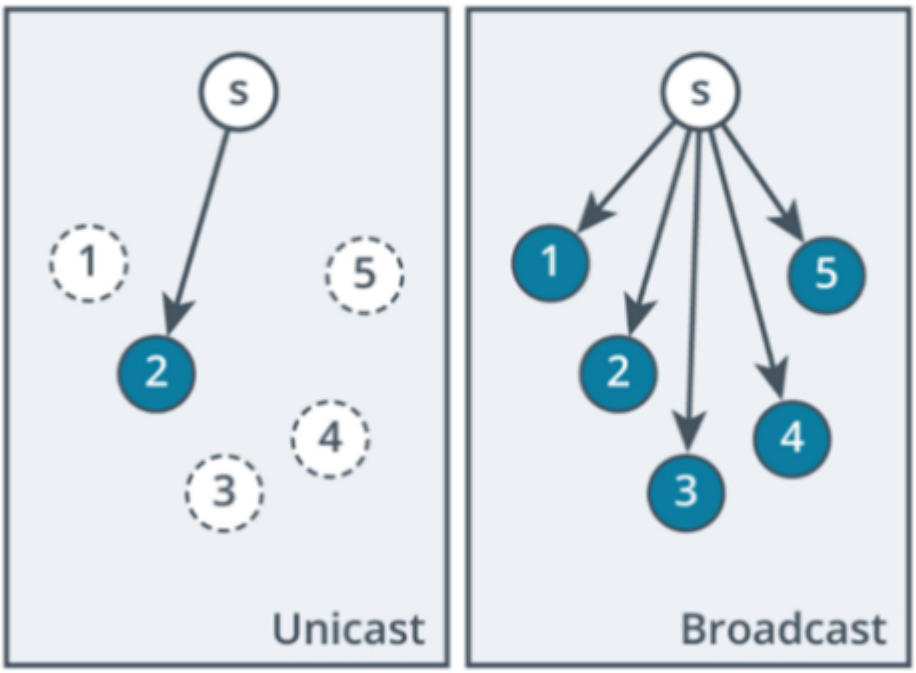
Jika alamat tujuan berada di jaringan jarak jauh, maka host lokal harus menggunakan gateway defaultnya untuk meneruskan paket. Oleh karena itu, harus menentukan alamat MAC dari default gateway menggunakan ARP.

Router juga menggunakan pesan ARP untuk antarmuka Ethernet-nya. Namun, pesan ARP hanya digunakan dengan Ethernet. Antarmuka publik router mungkin menggunakan jenis pembingkaian dan pengalamatan lokal yang berbeda.

Pengalamatan Unicast dan Broadcast

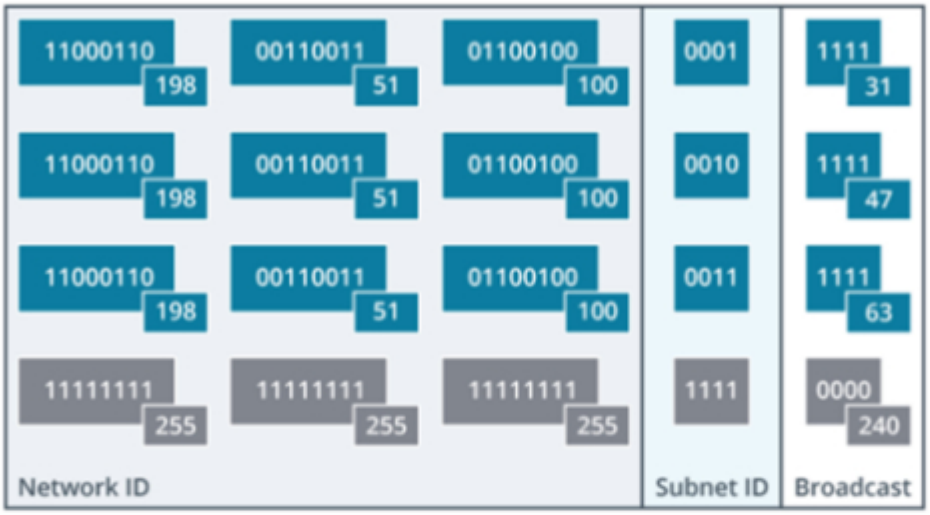
IPv4 menggunakan beberapa mekanisme untuk berkomunikasi dengan host lain. Ketika host IPv4 ingin mengirim paket ke satu penerima, ia menggunakan paket unicast, yang ditujukan ke alamat IP dari host tujuan. Namun, jika host lokal perlu berkomunikasi dengan banyak host, ia dapat menggunakan skema yang berbeda.

Salah satu cara menangani banyak host adalah dengan melakukan siaran. Broadcast dapat dilakukan dengan mengirimkan paket ke jaringan atau alamat broadcast subnet. Alamat broadcast adalah alamat terakhir di jaringan IP mana pun, atau dengan kata lain, alamat di jaringan IP mana pun di mana semua bit host disetel ke 1.



Unicast and broadcast addressing.

Misalnya, jika subnet mask adalah 255.255.255.240, empat digit terakhir dari oktet terakhir di alamat IP adalah bagian ID host. Jika digit ini disetel ke semua 1, itu adalah kemungkinan alamat terakhir sebelum ID subnet berikutnya, dan oleh karena itu alamat siaran jaringan:

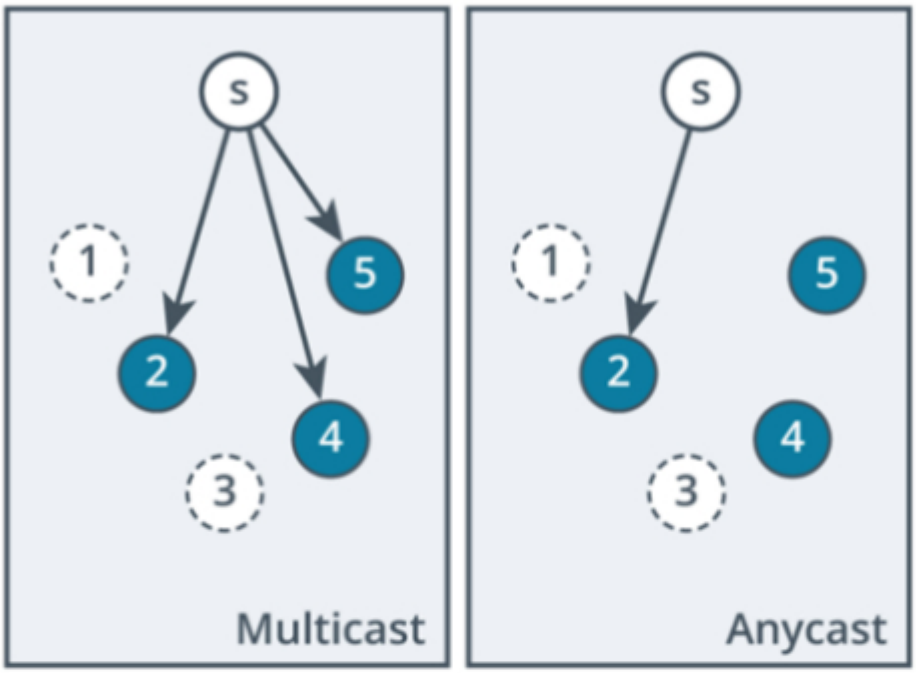


Broadcast addresses for four subnets.

Semua host yang berbagi alamat broadcast yang sama menerima paket. Mereka dikatakan berada dalam domain broadcast layer 3 yang sama. Batas domain broadcast ditetapkan pada lapisan Jaringan oleh router. Router tidak meneruskan siaran, kecuali dalam beberapa keadaan yang dikonfigurasi secara khusus.

Seperti lalu lintas unicast, paket IP harus dikirimkan ke host menggunakan alamat MAC lapisan 2. Pada lapisan 2, siaran dikirimkan menggunakan alamat MAC grup (ff:ff:ff:ff:ff:ff). Ini berarti bahwa ada juga cakupan domain broadcast pada layer 2. Dengan perangkat lama seperti hub dan bridge, setiap port pada semua node yang terhubung secara fisik adalah bagian dari domain broadcast layer 2 yang sama. Ini juga terjadi dengan sakelar dasar atau tidak terkelola. Secara default, switch membanjiri siaran keluar dari setiap port kecuali port sumber.

Pengalamatan Multicast dan Anycast
Sementara sebagian besar lalu lintas IPv4 adalah unicast atau siaran, skema pengalamatan lain digunakan dalam keadaan khusus.



Multicast and anycast addressing.

Pengalamatan Multicast
Multicasting IPv4 memungkinkan satu host di Internet (atau jaringan IP pribadi) untuk mengirim konten ke host lain yang telah mengidentifikasi diri mereka tertarik untuk menerima konten host asal. Paket multicast dikirim ke alamat IP tujuan dari rentang khusus yang dikonfigurasi untuk digunakan dengan grup multicast tersebut.

Pada lapisan 2, multicast dikirimkan menggunakan rentang alamat MAC khusus. Sakelar harus mampu multicast. Jika sakelar tidak berkemampuan multicast, ia akan memperlakukan multicast seperti siaran dan membanjiri transmisi multicast dari semua port.

Maksud untuk menerima multicast dari host tertentu ditandai dengan bergabung dengan grup multicast. Internet Group Management Protocol (IGMP) biasanya digunakan untuk mengkonfigurasi keanggotaan grup dan alamat IP.

Pengalamatan Anycast
Anycast berarti sekelompok host dikonfigurasi dengan alamat IP yang sama. Saat router meneruskan paket ke grup anycast, router menggunakan algoritme dan metrik prioritas untuk memilih host yang "paling dekat" (yang akan menerima paket dan dapat memprosesnya paling cepat). Ini memungkinkan layanan di belakang alamat IP disediakan dengan lebih andal. Ini memungkinkan penyeimbangan beban dan failover antara host server yang berbagi alamat IP.

KONFIGURASI JARINGAN DAN SUBNET IP

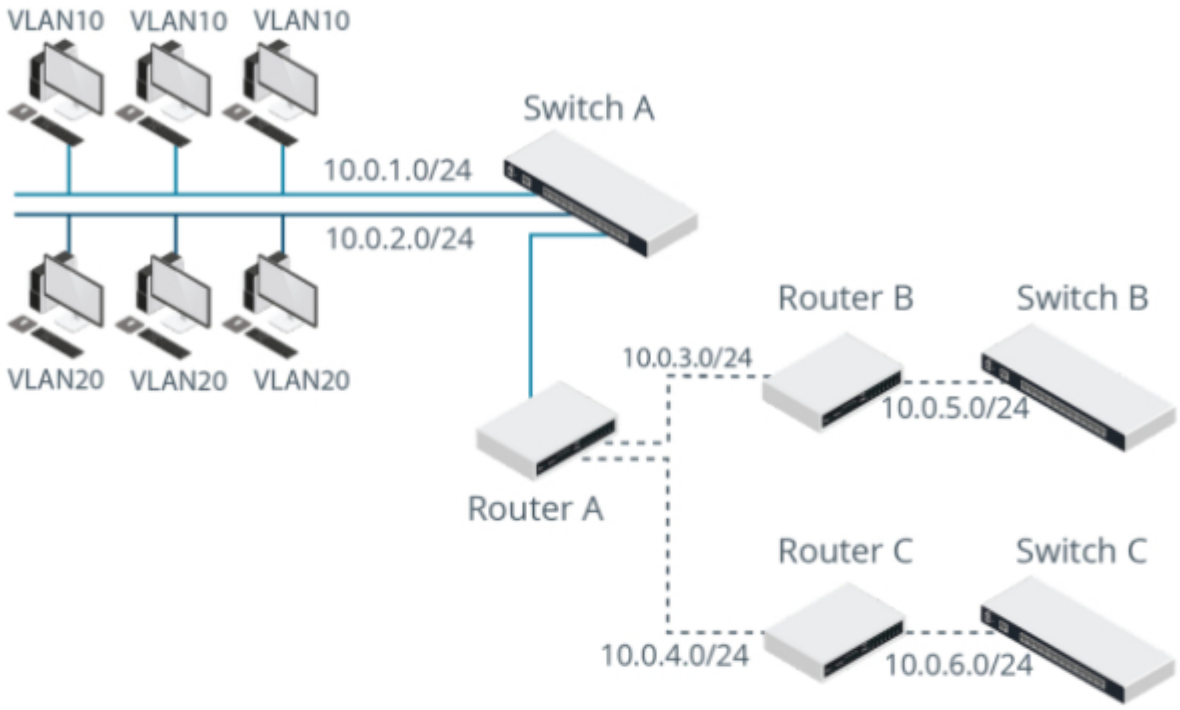
Pendahuluan: Konfigurasi Jaringan dan Subnet IP
Organisasi dengan jaringan besar perlu membagi jaringan tersebut menjadi segmen yang lebih kecil untuk meningkatkan kinerja dan keamanan. Segmen jaringan diwakili pada lapisan Jaringan oleh subnet. Memahami prinsip-prinsip dasar segmentasi dan subnetting akan sangat penting untuk kemajuan karir di jaringan.

Virtual LANs and Subnets
Jaringan Ethernet modern dibangun menggunakan sakelar. Dalam konfigurasi defaultnya, setiap port pada switch akan berada di segmen lokal yang sama atau, dengan kata lain, dalam domain broadcast yang sama. Setiap host dalam domain siaran dapat menghubungi host lain menggunakan skema pengalamatan logis yang sama (subnet IP) dan dengan pengalamatan perangkat keras/MAC.

Jika terlalu banyak host yang terhubung ke sakelar yang sama, lalu lintas siaran dapat menjadi berlebihan dan mengurangi kinerja. Pada lapisan 2, LAN virtual (VLAN) adalah sarana untuk mengatasi masalah ini. Setiap antarmuka pada sakelar yang dikelola dapat diberi ID VLAN. Menggunakan VLAN berarti bahwa kelompok komputer yang berbeda pada kabel yang sama dan terhubung ke sakelar yang sama dapat terlihat berada di segmen LAN yang terpisah. Setiap VLAN adalah domain siaran terpisah.

Pada lapisan 3, subnetting adalah proses membagi secara logis jaringan IP menjadi subnetwork yang lebih kecil (subnet), dengan setiap subnet memiliki alamat yang unik. Skema subnetting dapat diterapkan untuk mewakili desain VLAN di topologi layer 3.

Misalnya, desain subnet berikut mengalokasikan subnet terpisah (10.0.1.0 dan 10.0.2.0) untuk dua VLAN yang dikonfigurasi pada Switch A dan untuk tautan WAN serial yang dikonfigurasi antara Router A dan Router B dan C (10.0.3.0 dan 10.0.4.0). Router B dan C juga memiliki subnet masing-masing untuk jaringan lokal mereka (10.0.5.0 dan 10.0.6.0).



Subnet design. (Images © 123RF.com.)

Selain memecah domain siaran, subnet dapat digunakan untuk mencapai tujuan desain jaringan lainnya:

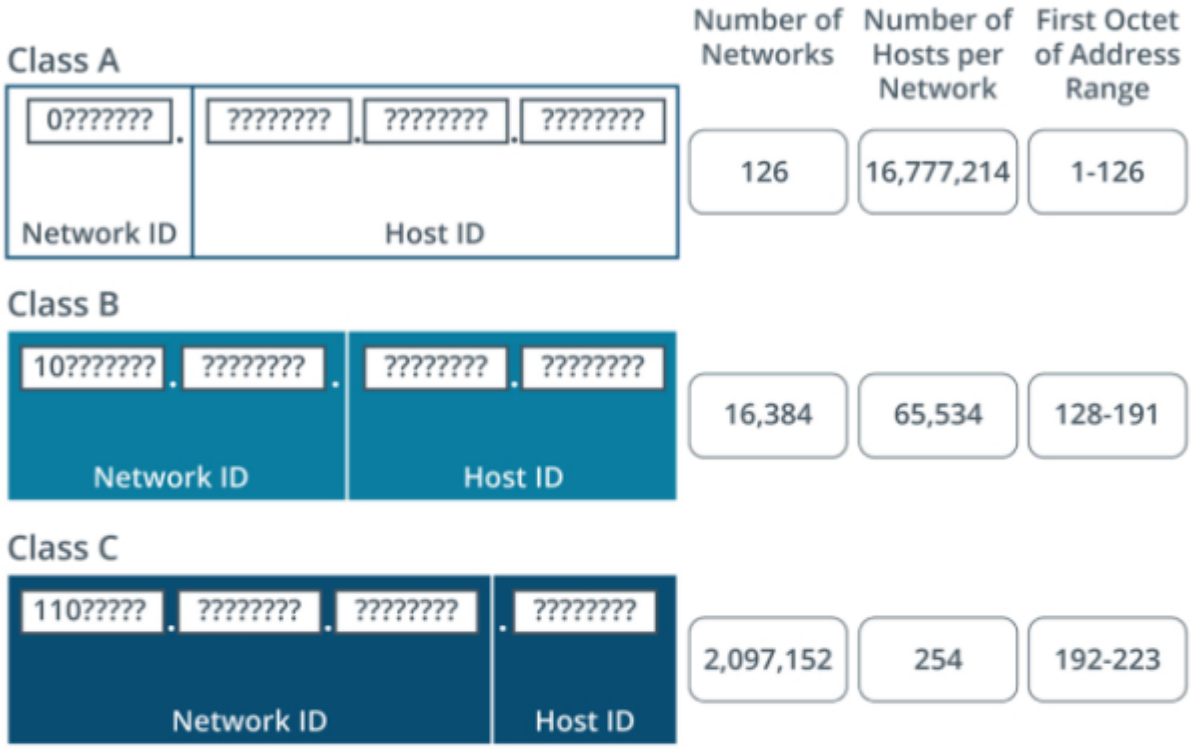
Banyak organisasi memiliki lebih dari satu situs dengan tautan WAN di antara mereka. Tautan WAN biasanya membentuk subnet terpisah.

Sangat berguna untuk membagi jaringan menjadi zona yang berbeda secara logis untuk keamanan dan kontrol administratif.

Jaringan yang menggunakan teknologi fisik dan tautan data yang berbeda, seperti Token Ring dan Ethernet, harus dipisahkan secara logis sebagai subnet yang berbeda.

Classful Addressing

Sejauh ini, kami telah mempertimbangkan jaringan IP dan ID subnet menggunakan topeng atau awalan jaringan. Ini disebut sebagai pengalamatan tanpa kelas. Skema pengalamatan classful digunakan pada 1980-an, sebelum penggunaan netmask untuk mengidentifikasi bagian ID jaringan dari sebuah alamat dikembangkan. Pengalamatan classful mengalokasikan ID jaringan berdasarkan oktet pertama dari alamat IP.



Class A, Class B, and Class C networks.

Alamat jaringan Kelas A mendukung sejumlah besar host-lebih dari 16 juta. Namun, hanya ada 126 alamat jaringan Kelas A. Ada 16.000 jaringan Kelas B, masing-masing berisi hingga sekitar 65.000 host. Akhirnya, jaringan Kelas C hanya mendukung masing-masing 254 host, tetapi ada lebih dari 2 juta host.

Saat mempertimbangkan pengalamatan classful, Anda harus dapat mengidentifikasi kelas alamat dari oktet pertama alamat IP. Tabel ini menunjukkan cara mengidentifikasi kelas alamat dari oktet pertama alamat IP dalam desimal.

First Octet	Class
1 to 126	Class A
128 to 191	Class B
192 to 223	Class C

Sementara router telah melakukan perutean tanpa kelas selama bertahun-tahun, terminologi kelas masih sangat banyak digunakan. Bahkan di bawah pengalamatan tanpa kelas, kelas lama sering digunakan sebagai nama untuk netmask yang sejajar dengan batas oktet keseluruhan:

- Kelas A: 255.0.0.0 (/8)
- Kelas B: 255.255.0.0 (/16)
- Kelas C: 255.255.255.0 (/24)

Pengalamatan berkelas juga penting karena menetapkan beberapa rentang alamat IP yang tidak dapat digunakan untuk pengalamatan host biasa atau untuk pengalamatan melalui Internet.

Public versus Private Addressing

Alamat IP publik adalah alamat yang dapat membuat koneksi dengan jaringan dan host IP publik lainnya melalui Internet. Alokasi alamat IP publik diatur oleh IANA dan dikelola oleh pendaftar regional dan ISP. Host yang berkomunikasi satu sama lain melalui LAN dapat menggunakan skema pengalamatan publik tetapi biasanya akan menggunakan pengalamatan pribadi.

Private IP Address Ranges

Alamat IP pribadi dapat diambil dari salah satu kumpulan alamat yang didefinisikan dalam RFC 1918 sebagai tidak dapat dirutekan melalui Internet:

- 10.0.0.0 to 10.255.255.255 (Class A private address range).
- 172.16.0.0 to 172.31.255.255 (Class B private address range).
- 192.168.0.0 to 192.168.255.255 (Class C private address range).

Setiap organisasi dapat menggunakan alamat pribadi di jaringannya tanpa mendaftar ke registri atau ISP, dan beberapa organisasi dapat menggunakan rentang ini secara bersamaan. Akses internet dapat difasilitasi untuk host yang menggunakan skema pengalamatan pribadi dalam dua cara:

- Melalui router yang dikonfigurasi dengan satu atau blok alamat IP publik yang valid; router menerjemahkan antara alamat pribadi dan publik menggunakan proses yang disebut Network Address Translation (NAT).

- Melalui server proxy yang memenuhi permintaan sumber daya Internet atas nama klien. Server proxy itu sendiri harus dikonfigurasi dengan alamat IP publik pada antarmuka eksternal.

Automatic Private IP Addressing (APIPA)
Konfigurasi IP host dapat diterapkan secara statis atau dapat menggunakan metode konfigurasi otomatis. Konfigurasi otomatis pada jaringan IPv4 biasanya berarti menggunakan server Dynamic Host Configuration Protocol (DHCP).

Automatic Private IP Addressing (APIPA) dikembangkan oleh Microsoft sebagai sarana untuk klien yang tidak dapat menghubungi server DHCP untuk berkomunikasi di jaringan lokal. Jika host Windows tidak menerima respons dari server DHCP dalam jangka waktu tertentu, ia akan memilih alamat secara acak dari kisaran 169.254.1.1 hingga 169.254.254.254.

Tips: Alamat ini berasal dari salah satu rentang alamat yang disediakan untuk pengalamatan pribadi (169.254.0.0/16). Subnet pertama dan terakhir seharusnya tidak digunakan.

Jenis pengalamatan ini disebut sebagai tautan lokal dalam dokumentasi standar (RFC 3927). Mekanisme pengalamatan lokal tautan juga dapat diimplementasikan pada sistem operasi lain, seperti Bonjour® untuk platform macOS® atau Avahi untuk Linux®.

Other Reserved Address Ranges
Ada dua kelas tambahan alamat IP (D dan E) yang menggunakan nilai di atas 223.255.255.255:

- Alamat Kelas D (224.0.0.0 hingga 239.255.255.255) digunakan untuk multicasting.
- Alamat Kelas E (240.0.0.0 hingga 255.255.255.255) dicadangkan untuk penggunaan dan pengujian eksperimental.

Alamat Loopback
Sementara secara nominal bagian dari Kelas A, kisaran 127.0.0.0 hingga 127.255.255.255 (atau 127.0.0.0/8) dicadangkan. Rentang ini digunakan untuk mengkonfigurasi alamat loopback, yang merupakan alamat khusus yang biasanya digunakan untuk memeriksa apakah TCP/IP diinstal dengan benar pada host lokal. Antarmuka loopback tidak memerlukan antarmuka fisik untuk berfungsi. Paket yang dikirim ke antarmuka loopback tidak diproses oleh adaptor jaringan tetapi diproses seperti biasa oleh tumpukan TCP/IP host. Setiap host IP secara otomatis dikonfigurasi dengan alamat loopback default, biasanya 127.0.0.1. Pada beberapa host, seperti router, lebih dari satu alamat loopback mungkin dikonfigurasi. Antarmuka loopback juga dapat dikonfigurasi dengan alamat dari rentang IP apa pun yang sesuai, selama alamat tersebut unik di jaringan. Sebuah host akan memproses paket yang dialamatkan ke alamat loopback terlepas dari antarmuka yang diterimanya.

Lainnya
Beberapa rentang alamat IPv4 lainnya dicadangkan untuk penggunaan khusus dan tidak dapat dirutekan secara publik:

- 0.0.0.0/8-Digunakan saat alamat tertentu tidak diketahui. Ini biasanya digunakan sebagai alamat sumber oleh klien yang mencari sewa DHCP.
- 255.255.255.255-Digunakan untuk menyiarkan ke jaringan lokal ketika alamat jaringan lokal tidak diketahui.
- 100.64.0.0/10, 192.0.0.0/24, 192.88.99.0/24, 198.18.0.0/15-Disisihkan untuk berbagai keperluan khusus.
- 192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24-Disisihkan untuk digunakan dalam dokumentasi dan contoh.

Desain Skema Alamat IPv4

Faktor-faktor berikut harus dipertimbangkan ketika merencanakan skema pengalamatan jaringan IPv4:

- Jumlah jaringan IP dan subjaringan yang diperlukan.
- Jumlah host per subnet yang harus didukung.
- ID jaringan harus berasal dari rentang publik atau privat yang valid (bukan dari loopback, rentang cadangan lokal tautan, rentang multicast, atau rentang cadangan/eksperimen, misalnya).

- Jaringan dan/atau ID host tidak boleh semuanya 1 dalam biner-ini dicadangkan untuk siaran.
- Jaringan dan/atau ID host tidak boleh semuanya 0 dalam biner; 0 berarti "jaringan ini." Setiap host ID harus unik pada jaringan IP atau subnet.
- ID jaringan harus unik di Internet (jika Anda menggunakan skema pengalamatan publik) atau di sistem internal internetwork Anda (jika Anda menggunakan skema pengalamatan pribadi).

Saat Anda melakukan kalkulasi subnet, coba pikirkan jumlah bit mask. Ini membantu untuk mengingat bahwa setiap kekuatan 2 adalah dua kali lipat dari yang sebelumnya:

2^2	2^3	2^4	2^5	2^6	2^7	2^8
4	8	16	32	64	128	256

Ingat juga nilai desimal untuk jumlah bit yang disetel ke 1 dalam oktet di dalam topeng:

1	2	3	4	5	6	7	8
128	192	224	240	248	252	254	255

Dalam contoh berikut, jaringan yang dirancang adalah subnetting alamat jaringan 172.30.0.0/16. Proses merancang skema adalah sebagai berikut:

1. Cari tahu berapa banyak subnet yang diperlukan (ingat untuk memungkinkan pertumbuhan di masa mendatang), lalu bulatkan angka ini ke pangkat 2.
   Misalnya, jika Anda membutuhkan 12 subnet, pangkat 2 terdekat berikutnya adalah 16. Eksponen adalah jumlah bit yang perlu Anda tambahkan ke mask default Anda. Misalnya, 16 adalah 24 (2 pangkat 4), jadi Anda perlu menambahkan 4 bit ke awalan jaringan. Dalam format desimal bertitik, subnet mask menjadi 255.255.240.0 .

2. Cari tahu berapa banyak host yang harus didukung oleh setiap subnet dan apakah ada cukup ruang tersisa dalam skema untuk mengakomodasi mereka.
   Misalnya, alamat jaringan berada dalam rentang /16, dan Anda menggunakan 4 bit untuk subnetting, jadi Anda memiliki 32-20 = 12 bit untuk host di setiap subnet. Jumlah host per subnet dapat dinyatakan dengan menggunakan rumus 2 n -2, di mana n adalah jumlah bit yang telah Anda alokasikan untuk ID host. 12 bit cukup untuk 4094 host di setiap subnet.
   Tips: Anda kurangi 2 karena setiap alamat jaringan dan alamat broadcast subnet tidak dapat ditetapkan ke host.

Tips: Di mana pun 1 muncul di topeng biner, digit yang sesuai di alamat IP adalah bagian dari jaringan atau alamat subnet. Saat Anda merencanakan apa topeng Anda, ingat aturan ini. Alokasikan lebih banyak bit di topeng jika Anda membutuhkan lebih banyak subnet. Alokasikan lebih sedikit bit di mask jika Anda membutuhkan lebih banyak host per subnet.
Sebagai perbandingan, jika Anda memiliki alamat jaringan /24 (atau Kelas C) dan mencoba mengalokasikan 16 subnet, akan ada cukup ruang yang tersisa untuk hanya 14 host per subnet (24-2).

3. Kerjakan subnetnya. Cara termudah untuk menemukan ID subnet pertama adalah dengan mengurangi oktet paling tidak signifikan dalam topeng (240 dalam contoh ini) dari 256. Ini memberikan ID subnet pertama, yang, secara penuh, adalah 172.30.16.0/20.
   ID subnet berikutnya adalah semua ID subnet terendah lebih tinggi dari yang sebelumnya-32, 48, 64, dan seterusnya.

4. Tentukan rentang host untuk setiap subnet. Ambil alamat subnet dan tambahkan biner 1 untuk host pertama. Untuk host terakhir, ambil ID subnet berikutnya dan kurangi dua digit biner darinya. Dalam hal ini, masing-masing adalah 172.30.16.1 dan 172.30.31.254 . Ulangi untuk semua subnet.

MODUL 6

Mendukung Jaringan IPv4 dan IPv6

PENGANTAR PELAJARAN
IP diimplementasikan pada host jaringan menggunakan berbagai macam antarmuka konfigurasi dan alat. Anda harus yakin tentang memilih alat yang sesuai untuk digunakan untuk menyelesaikan tugas dukungan atau pemecahan masalah tertentu.

Pelajaran ini juga memperkenalkan konsep pengalamatan IPv6 dan menyoroti beberapa perbedaan utama antara IPv6 dan IPv4.

TUJUAN PELAJARAN
Dalam pelajaran ini, Anda akan:

- Gunakan alat yang sesuai untuk menguji konfigurasi IP.
- Memecahkan masalah jaringan IP.
- Jelaskan skema pengalamatan IPv6.

A. Gunakan Alat yang Tepat untuk Menguji Konfigurasi IP

Pendahuluan: Gunakan Alat yang Tepat untuk Menguji Konfigurasi IP
Utilitas baris perintah TCP/IP memungkinkan Anda untuk mengumpulkan informasi tentang bagaimana sistem Anda dikonfigurasi dan bagaimana mereka berkomunikasi melalui jaringan IP. Ketika digunakan untuk pemecahan masalah, utilitas ini dapat memberikan informasi tentang masalah komunikasi dan penyebabnya.

- **IP Interface Configuration in Windows**

  Setiap adaptor host harus dialokasikan alamat IP dan subnet mask yang sesuai, ditambah alamat IP dari gateway default (router) untuk jaringannya. Biasanya, sebuah host juga dikonfigurasi dengan alamat server domain name system (DNS) yang dapat menyelesaikan alamat IP ke label nama, membuat identifikasi host dan layanan menjadi lebih sederhana.
  Nilai konfigurasi IP ini dapat ditetapkan secara statis atau dinamis. Mengkonfigurasi sejumlah besar host dengan parameter pengalamatan statis yang valid adalah tugas manajemen yang kompleks. Kebanyakan host dikonfigurasi untuk mendapatkan alamat secara otomatis, menggunakan layanan yang disebut Dynamic Host Configuration Protocol (DHCP).
  Di bawah Windows, setiap adaptor Ethernet diberi nama. Pada versi Windows awal, adaptor pertama diberi nama "Local Area Connection", tetapi versi terbaru hanya menggunakan label "Ethernet." Adaptor tambahan diidentifikasi sebagai "Ethernet2," "Ethernet3," dan seterusnya. Nama baru dapat diterapkan jika perlu. Konfigurasi IP

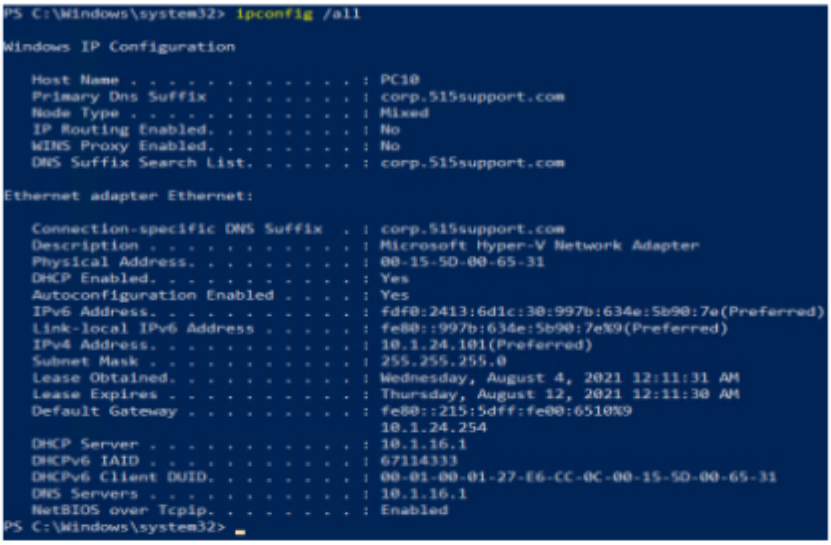
untuk setiap antarmuka adaptor sering diatur menggunakan dialog Properti GUI yang diakses melalui applet Koneksi Jaringan. Namun, Anda juga dapat mengonfigurasi antarmuka menggunakan perintah netsh.
antarmuka netsh ip set alamat "Ethernet" dhcp
antarmuka netsh ip set alamat "Ethernet" statis 10.1.0.1 255.255.255.0 10.1.0.254

Di Windows, semua perubahan pada konfigurasi antarmuka jaringan bersifat persisten, artinya perubahan tersebut terus berlaku saat sistem di-boot ulang.
Anda juga dapat menggunakan netsh untuk melaporkan konfigurasi IP (netsh interface ip show config , misalnya).

netsh diimplementasikan dalam antarmuka prompt perintah lama. Konfigurasi berbasis skrip sekarang lebih cenderung menggunakan cmdlet PowerShell. Cmdlet Get-NetAdapter dan Get-NetIPAddress dapat digunakan untuk menanyakan konfigurasi yang ada. Konfigurasi baru dapat diterapkan menggunakan New-NetIPAddress atau yang sudah ada dapat dimodifikasi menggunakan Set-NetIPAddress.

- **IP CONFIG**
  Sementara netsh dan PowerShell menawarkan banyak fungsionalitas granular, perintah ipconfig masih banyak digunakan untuk pelaporan konfigurasi dasar dan tugas-tugas dukungan. ipconfig dapat digunakan sebagai berikut:

  - ipconfig tanpa sakelar apa pun akan menampilkan alamat IP, subnet mask, dan gateway default (router) untuk semua antarmuka jaringan yang terikat TCP/IP.
  - ipconfig /all menampilkan parameter konfigurasi TCP/IP lengkap untuk setiap antarmuka, termasuk apakah Dynamic Host Configuration Protocol (DHCP) diaktifkan untuk antarmuka dan alamat perangkat keras antarmuka (MAC).
  - ipconfig /renew interface memaksa klien DHCP untuk memperbarui sewa yang dimilikinya untuk alamat IP.
  - ipconfig /release interface melepaskan alamat IP yang diperoleh dari Server DHCP sehingga antarmuka tidak lagi memiliki alamat IP.
  - ipconfig /displaydns menampilkan cache penyelesai Domain Name System (DNS).
  - ipconfig /flushdns membersihkan cache resolver DNS.
  - ipconfig /registerdns mendaftarkan host dengan server DNS (jika mendukung pembaruan dinamis).



Identifying the current IP configuration with ipconfig. (Screenshot used with permission from Microsoft.)

Tips: Ada juga /release6 dan /renew6 switch untuk digunakan dengan DHCPv6 (server DHCP yang mendukung IPv6).

- **ifconfig and ip**

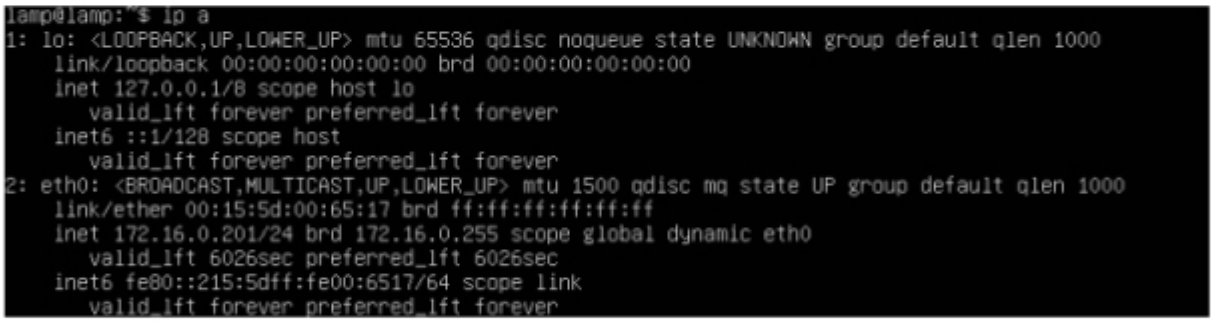
  Di Linux, antarmuka Ethernet secara klasik diidentifikasi sebagai eth0, eth1 , eth2 , dan seterusnya, meskipun beberapa paket jaringan sekarang menggunakan skema yang berbeda, seperti awalan en. Di Linux, Anda perlu membedakan antara konfigurasi yang berjalan dan konfigurasi persisten. Konfigurasi persisten adalah yang diterapkan setelah reboot atau setelah adaptor jaringan diinisialisasi ulang. Metode penerapan konfigurasi IP ke antarmuka adaptor khusus untuk setiap distribusi. Secara historis, konfigurasi persisten diterapkan dengan mengedit file /etc/network/interfaces dan membawa antarmuka naik atau turun dengan skrip ifup dan ifdown. Banyak distribusi sekarang menggunakan paket NetworkManager, yang dapat dioperasikan menggunakan GUI atau alat nmcli. Atau, konfigurasi jaringan mungkin dikelola menggunakan manajer konfigurasi systemd-networkd. Selain itu, distribusi Ubuntu terbaru menggunakan netplan untuk mengabstraksi beberapa kompleksitas mendasar ini ke file konfigurasi yang ditulis dalam YAML bukan bahasa markup (YAML). File konfigurasi YAML dirender oleh systemd-networkd atau NetworkManager.

  Dalam hal mengelola konfigurasi yang sedang berjalan, Anda juga perlu membedakan antara paket perintah lama dan saat ini. ifconfig adalah bagian dari paket net-tools lawas. Penggunaan perintah ini tidak digunakan lagi di sebagian besar distribusi Linux modern. ifconfig masih dapat digunakan dengan aman untuk melaporkan konfigurasi antarmuka jaringan.



ifconfig output.

net-tools telah digantikan oleh paket iproute2. Alat-alat ini dapat berinteraksi dengan baik dengan paket manajer konfigurasi jaringan modern. Sebagai bagian dari paket iproute2, perintah ip memiliki opsi untuk mengelola rute serta konfigurasi antarmuka lokal. Fungsi pelaporan dasar ifconfig (tampilkan konfigurasi alamat saat ini) dilakukan dengan menjalankan ip addr ; untuk melaporkan satu antarmuka saja, gunakan ip addr show dev eth0 . Perintah ip link menunjukkan status antarmuka, sementara tautan ip -s melaporkan statistik antarmuka.



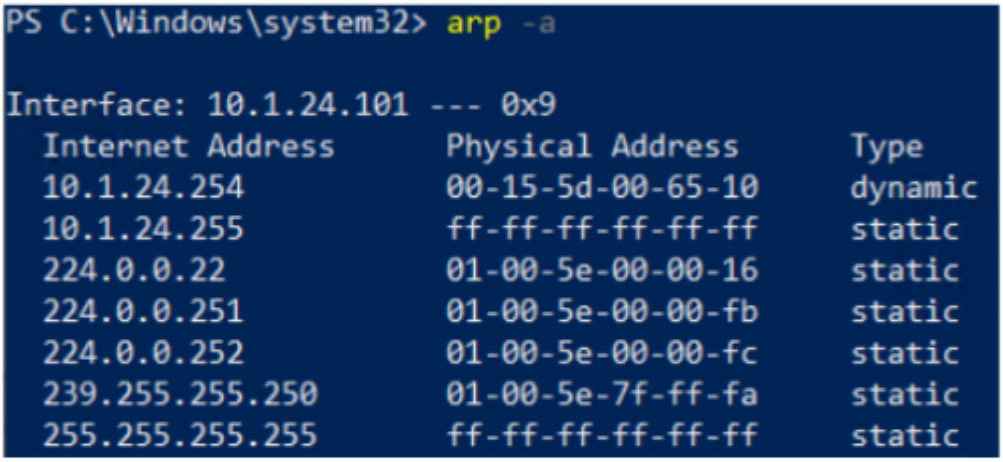
ip a command output.

Perintah ip link set eth0 up|down digunakan untuk mengaktifkan atau menonaktifkan antarmuka, sedangkan ip addr add|delete dapat digunakan untuk mengubah konfigurasi alamat IP. Perubahan ini tidak persisten dan hanya berlaku untuk konfigurasi yang sedang berjalan, kecuali dijalankan sebagai bagian dari skrip startup.

- **ARP Cache Utility**
  Address Resolution Protocol (ARP) digunakan oleh host untuk menentukan alamat MAC mana yang terkait dengan alamat IP di jaringan lokal. Kueri ARP dikirim sebagai siaran. Siaran ARP dapat menghasilkan lalu lintas yang cukup besar di jaringan, yang dapat mengurangi kinerja. Untuk mengoptimalkan proses ini, hasil siaran ARP di-cache dalam tabel ARP. Jika entri digunakan dalam periode waktu habis, entri disimpan dalam cache selama beberapa menit sebelum dihapus.

Utilitas arp dapat digunakan untuk melakukan fungsi yang terkait dengan cache tabel ARP. Anda akan menggunakan ini untuk mendiagnosis masalah yang dicurigai dengan pengalamatan lokal dan pengiriman paket.

- arp -a (atau arp -g) menunjukkan konten cache ARP. Anda dapat menggunakan ini dengan IPAddress untuk melihat cache ARP hanya untuk antarmuka yang ditentukan. Cache ARP tidak harus berisi alamat MAC dari setiap host di segmen lokal. Tidak akan ada entri cache jika belum ada pertukaran frame baru-baru ini.
- arp -s IPAddress MACAddress menambahkan entri ke cache ARP. Di bawah Windows, MACAddress perlu dimasukkan dengan tanda hubung di antara setiap byte hex.
- arp -d * menghapus semua entri dalam cache ARP; itu juga dapat digunakan dengan IPAddress untuk menghapus satu entri.



Output from the arp command showing network (IP) addresses mapped to physical (MAC) addresses. Host interfaces are learned (dynamic), while broadcast and multicast interfaces are configured statically. (Screenshot used with permission from Microsoft.)

Di Linux, perintah ip neigh menunjukkan entri di cache ARP lokal (menggantikan perintah arp lama).

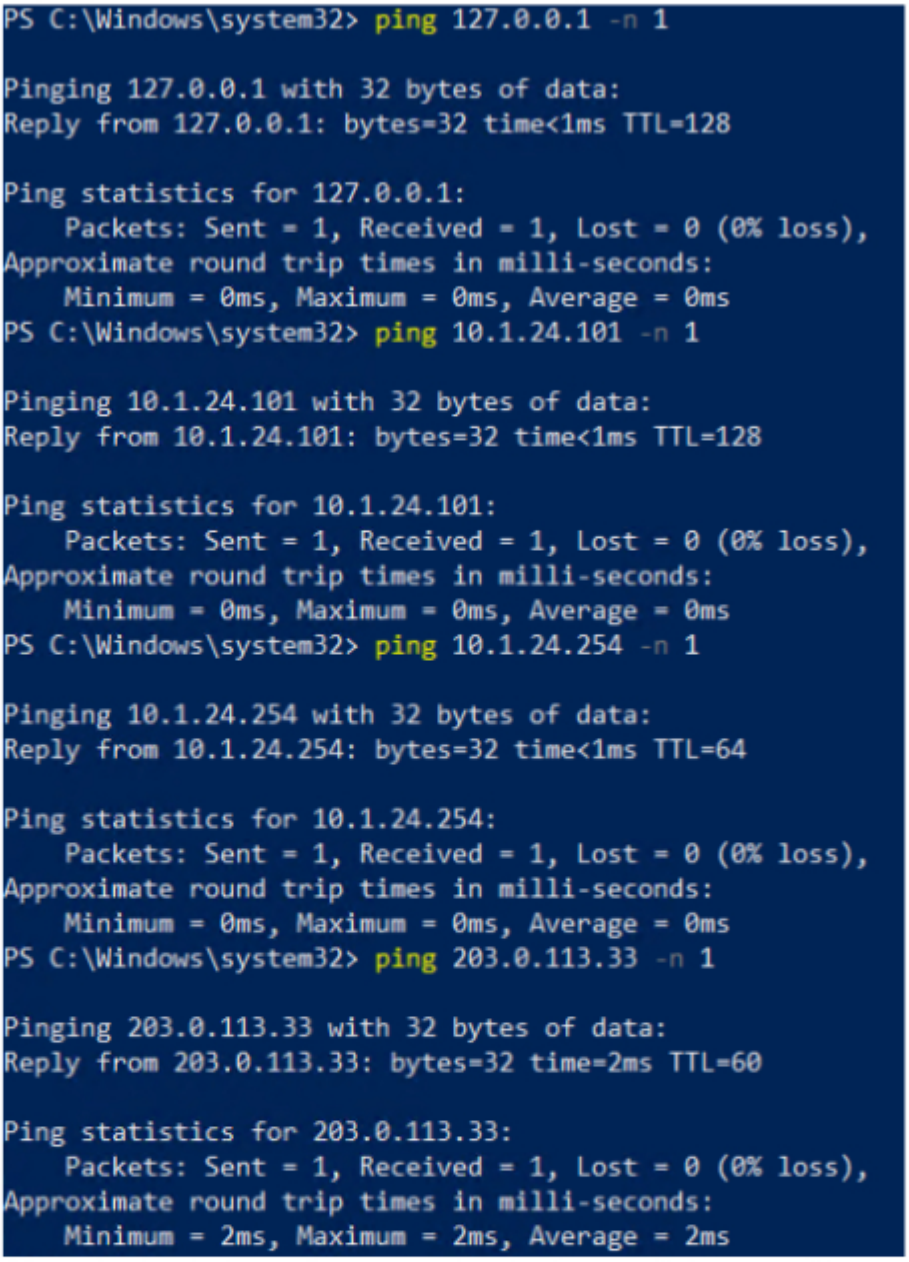
- **Protokol Pesan Kontrol Internet dan ping**

Internet Control Message Protocol (ICMP) digunakan untuk melaporkan kesalahan dan mengirim pesan tentang pengiriman paket. Pesan ICMP dihasilkan dalam kondisi kesalahan di sebagian besar jenis lalu lintas unicast, tetapi tidak untuk paket siaran atau multicast.

ICMP juga dapat digunakan untuk menguji dan memecahkan masalah konektivitas pada jaringan IP. Utilitas ping mengirimkan nomor dan ukuran paket permintaan ICMP yang dapat dikonfigurasi ke host tujuan. ping diimplementasikan pada host Windows dan

Linux. ping dapat digunakan untuk melakukan tes konektivitas dasar yang tidak bergantung pada host target yang menjalankan aplikasi atau layanan tingkat yang lebih tinggi.

- Penggunaan ping dasar
  Tes konektivitas dasar dilakukan dengan menjalankan ping IPAddress, di mana IPAddress adalah alamat IPv4 atau IPv6.
  Jika penyelidikan berhasil (seperti pada upaya pertama yang ditunjukkan pada tangkapan layar), output akan menampilkan pesan "Balas dari IPAddress" dan waktu yang diperlukan untuk respons server tiba. Ukuran milidetik Waktu Perjalanan Pulang Pergi (RTT) dapat digunakan untuk mendiagnosis masalah latensi pada tautan.



Using ping in Windows. (Screenshot used with permission from Microsoft.)

Bidang header IP Time to Live (TTL) dikurangi satu setiap kali sebuah paket diteruskan oleh router (disebut sebagai hop). Kolom keluaran TTL pada perintah ping menunjukkan nilai penghitung saat paket tiba di tujuannya.

Tips: Untuk mengetahui jumlah hop yang dibutuhkan, Anda perlu mengetahui nilai awalnya. Sistem operasi dan versi OS yang berbeda menggunakan nilai default yang berbeda. Misalnya, jika Anda melakukan ping ke host jarak jauh dari host Windows 10 dan nilai TTL dalam

outputnya adalah 52, maka Anda tahu bahwa paket tersebut membutuhkan 12 hop (64-52) untuk mencapai tujuannya.

- Pesan Kesalahan ping
  Jika probe ping tidak berhasil, salah satu dari dua pesan biasanya diterima:
  - ☐ Host tujuan tidak dapat dijangkau-Tidak ada informasi perutean (yaitu, komputer lokal tidak tahu cara mencapai alamat IP tersebut). Ini mungkin disebabkan oleh semacam kesalahan konfigurasi pada host lokal, seperti gateway default yang salah, oleh hilangnya konektivitas dengan router, atau oleh kesalahan konfigurasi perutean.
  - ☐ Tidak ada balasan (Waktu permintaan habis.) - Tuan rumah tidak tersedia atau tidak dapat merutekan balasan ke komputer Anda. Meminta time out saat TTL dikurangi menjadi 0 karena paket sedang berulang (karena tabel perutean yang rusak), saat kemacetan menyebabkan penundaan, atau saat host tidak merespons.
- ping Switches
  ping dapat digunakan dengan beberapa sakelar. Anda dapat menggunakan nama host atau nama domain yang sepenuhnya memenuhi syarat daripada alamat IP untuk menguji resolusi nama. Saat melakukan ping berdasarkan nama, -4 atau -6 memaksa alat untuk masing-masing menanyakan catatan host IPv4 atau catatan host IPv6. Juga, -t terus melakukan ping ke host hingga terputus (dengan menekan Ctrl+C).
  ping memiliki sintaks yang berbeda ketika digunakan di Linux. Secara default, perintah dijalankan hingga dihentikan secara manual, kecuali dijalankan dengan jumlah paket yang ditetapkan oleh -c switch.

B. Memecahkan masalah Jaringan IP

Pendahuluan: Jelaskan Skema Pengalamatan IPv4
Sementara beberapa skenario dukungan memerlukan pendekatan top-to-bottom atau bottom-to-top, secara praktis banyak aktivitas pemecahan masalah dimulai dengan lapisan jaringan. Tes konektivitas dan informasi konfigurasi dapat mengidentifikasi masalah dalam lapisan ini atau menginformasikan keputusan Anda apakah akan naik atau turun lapisan untuk menentukan penyebab masalah.

Kegagalan Perangkat Keras dan Masalah Antarmuka Jaringan
Saat Anda menggunakan model pemecahan masalah Jaringan CompTIA+, adalah bijaksana untuk mengesampingkan kegagalan perangkat keras fisik dan masalah lapisan Data Link sebelum mendiagnosis masalah lapisan Jaringan atau layanan. Kegagalan pada lapisan Jaringan lebih umum, tetapi jika Anda dapat mengisolasi masalah konektivitas ke segmen jaringan tertentu, penyebabnya mungkin terletak pada kegagalan perangkat keras daripada masalah konfigurasi.

- Masalah Daya

Seperti sistem komputer lainnya, jaringan membutuhkan daya yang stabil untuk beroperasi dengan baik. Anomali daya, seperti lonjakan dan lonjakan, dapat merusak perangkat, pemadaman listrik (kehilangan daya yang sangat singkat) dapat menyebabkan sistem terkunci atau reboot, sementara kegagalan daya (pemadaman) akan mematikan semuanya, termasuk lampu. Situs perusahaan memiliki sistem untuk melindungi dari masalah ini. Catu daya tidak terputus (UPS) dapat membuat server, sakelar, dan router tetap berjalan selama beberapa menit. Ini memberikan waktu untuk beralih di sumber daya sekunder (generator) atau mematikan sistem dengan anggun, semoga menghindari kehilangan data. Sebagian besar masalah daya harus diteruskan ke tukang listrik atau ke perusahaan listrik, tergantung di mana letak kesalahannya.

- Masalah Kegagalan Perangkat Keras
  Jika daya tidak menjadi masalah, pertimbangkan komponen lain yang mungkin mengalami kegagalan perangkat keras, termasuk adaptor jaringan host, peralatan sakelar/router/modem, dan kabel di antara keduanya. Anda dapat menguji kesalahan pemasangan kabel tertentu dan port yang buruk menggunakan penguji dan sertifikasi kabel dan loopback. Kegagalan perangkat keras yang lengkap relatif jarang terjadi, jadi jika Anda dapat mengesampingkan masalah daya dan kabel, maka untuk adaptor jaringan, pastikan driver berfungsi dengan benar. Hal termudah untuk dilakukan adalah mengganti driver (di Windows®, gunakan Device Manager untuk melakukan ini). Untuk peralatan jaringan, gunakan LED status untuk mengonfirmasi pengoperasian dan memeriksa apakah hal-hal seperti kartu plug-in dan modul terpasang dengan benar. Anda juga harus mempertimbangkan panas berlebih sebagai penyebab potensial masalah perangkat keras. Pastikan ada aliran udara yang baik di sekitar ventilasi masuk dan keluar. Pastikan kipas dan komponen internal tidak tersumbat oleh debu dan sistem tidak terkena sinar matahari langsung.

  Pada lapisan data link, sebagian besar host berkabel terhubung ke jaringan melalui switch. Jika Anda mencurigai perangkat seperti sakelar, analisis topologi jaringan Anda. Anda harus dapat melihat pengguna yang mengalami masalah, mengidentifikasi bagian mana dari jaringan yang terpengaruh, dan mengidentifikasi masalah yang menjembatani atau berpindah perangkat.

  Ketika Anda telah mempersempit masalah ke perangkat, Anda harus menentukan apa sifat masalahnya. Itu selalu layak mengatur ulang sakelar untuk melihat apakah itu menyelesaikan masalah. Seringkali, memulai ulang perangkat jaringan dapat menghapus kesalahan apa pun.

- Masalah Status Interface
  Jika Anda dapat mengisolasi masalah ke satu host dan kemudian mengesampingkan masalah kabel dan transceiver di lapisan fisik, ingatlah bahwa konfigurasi tautan data mungkin tidak berfungsi. Gunakan indikator status LED dan utilitas baris perintah

sakelar untuk memeriksa status antarmuka. Jika status jalur dan protokol tidak naik/naik, periksa apakah negosiasi otomatis pengaturan kecepatan dan dupleks telah dikonfigurasi dan apakah gagal. Jika pengaturan kecepatan (10, 100, atau 1000 Mbps) tidak cocok antara host dan port switch, link akan gagal.

Perintah status antarmuka juga akan melaporkan apakah ada tabrakan yang dihasilkan. Tabrakan mungkin terjadi jika pengaturan dupleks pada port sakelar dan host tidak cocok atau jika perangkat hub lama atau NIC host terhubung ke sakelar. Jika tidak satu pun dari kondisi ini berlaku, periksa NIC atau driver host yang salah.

Masalah Konfigurasi IP

Jika Anda dapat mengesampingkan masalah pada lapisan Physical dan Data Link, hal berikutnya yang perlu diperiksa adalah pengalamatan dasar dan konfigurasi protokol. Jika sebuah host tidak dapat melakukan pencarian tetangga untuk menghubungi node lain di jaringan lokal, pertama-tama gunakan ipconfig (Windows) atau ip atau ifconfig (Linux) untuk memverifikasi konfigurasi host.

- Alamat IP salah

  Setiap host sistem akhir harus memiliki subnet mask yang sama dengan tetangganya dan alamat IP yang menghasilkan alamat host unik yang valid di dalam subnet tersebut. Tetangga dalam pengertian ini adalah host lain dalam domain broadcast layer 2 yang sama. Misalnya, jika subnetnya adalah 192.168.1.0/24, pertimbangkan konfigurasi alamat host berikut:

  - ☐ Host A: IP: 192.168.1.10, Mask: 255.255.255.0
  - ☐ Host B: IP: 192.168.1.11, Mask: 255.255.255.0
  - ☐ Host C: IP: 192.168.0.21, Mask: 255.255.255.0

  Host A dan Host B memiliki konfigurasi yang valid, tetapi Host C memiliki alamat di subnet yang berbeda (192.168.0.0 dibandingkan dengan 192.168.1.0). Host A dan B akan mencoba menggunakan gateway default untuk meneruskan paket ke Host C. Host C tidak mungkin dapat berkomunikasi di jaringan sama sekali.

  Saat Anda menemukan topeng nondefault, akan sedikit lebih sulit untuk mengidentifikasi rentang host yang valid. Misalnya, jika alamat subnet adalah 198.51.100.16/28, pertimbangkan konfigurasi alamat host berikut:

  - ☐ Host A: IP: 198.51.100.10, Mask: 255.255.255.240
  - ☐ Host B: IP: 198.51.100.11, Mask: 255.255.255.240
  - ☐ Host C: IP: 198.51.100.21, Mask: 255.255.255.240

Batas awalan jaringan terletak di dalam oktet terakhir, jadi Anda tidak dapat mengandalkan tiga oktet pertama saja. Sekali lagi, host C berada di subnet yang berbeda.

Juga, ingat bahwa alamat jaringan dan alamat broadcast tidak dapat digunakan sebagai alamat host.

- Subnet Mask salah

Masalah lain yang mungkin muncul jika netmask salah, adalah bahwa tuan rumah dapat menerima komunikasi, tetapi salah merutekan balasannya, berpikir bahwa tuan rumah yang berkomunikasi dengannya berada di subnet yang berbeda. Balasan mungkin masih dapat diterima, meskipun mungkin melalui gateway default (router), bukan secara langsung.

- ☐ Host A: IP: 192.168.1.10, Mask: 255.255.255.0
- ☐ Host B: IP: 192.168.1.11, Mask: 255.255.255.0
- ☐ Host C: IP: 192.168.1.21, Mask: 255.255.255.240

Karena menggunakan awalan yang lebih panjang dari yang seharusnya, Host C akan berpikir perlu merutekan ke subnet yang berbeda untuk berkomunikasi dengan host A dan B. Ini akan menyebabkan paket-paket masuk melalui router, menempatkan beban yang tidak perlu di atasnya.

Skenario lain untuk topeng yang salah adalah topeng lebih pendek dari yang seharusnya:

- ☐ Host A: IP: 192.168.1.10, Mask: 255.255.255.0
- ☐ Host B: IP: 192.168.1.11, Mask: 255.255.255.0
- ☐ Host C: IP: 192.168.1.21, Mask: 255.255.0.0
- ☐ Host D: IP: 192.168.0.10, Mask: 255.255.255.0

Dalam hal ini, masalahnya tidak akan jelas jika host A, B, dan C semuanya berada di jaringan lokal yang sama, karena mereka akan dapat menggunakan pesan ARP dan menerima balasan. Namun, host C tidak akan dapat menghubungi host D, karena menganggap bahwa host D berada di jaringan lokal yang sama, padahal sebenarnya ia perlu merutekan pesan untuk 192.168.0.0/24 melalui gateway default.

Tips: Dalam skenario ini, router mungkin mengirim pesan status pengalihan ICMP ke host C.

Masalah Duplikat IP dan Alamat MAC

Dua sistem dapat berakhir dengan alamat IP yang sama karena kesalahan konfigurasi; mungkin kedua alamat ditetapkan secara statis, atau satu diberi alamat yang merupakan bagian dari lingkup DHCP. Jika Windows mendeteksi alamat IP duplikat, itu akan menampilkan peringatan dan menonaktifkan IP. Linux® biasanya tidak memeriksa alamat IP duplikat. Jika ada dua sistem dengan IP duplikat, semacam kondisi balapan akan menentukan mana yang menerima lalu lintas. Jelas, ini bukan cara yang baik untuk mengkonfigurasi jaringan, dan Anda harus mengidentifikasi dan memperbaiki mesin. Untuk melakukan ini, dapatkan alamat MAC dari kedua antarmuka menggunakan ping dan kemudian arp -a untuk memeriksa tabel cache ARP. Di Linux, Anda dapat menggunakan alat arping (arping -D) untuk melaporkan balasan duplikat. Setelah diidentifikasi, konfigurasikan setiap host untuk menggunakan alamat unik.

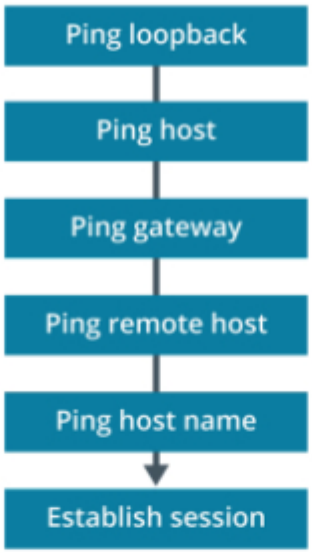
Alamat MAC duplikat akan menyebabkan masalah yang mirip dengan alamat IP duplikat. Kedua host akan bersaing untuk menanggapi permintaan ARP, dan komunikasi dapat dibagi di antara mereka atau hanya menjangkau salah satu host. Duplikat alamat MAC tidak mungkin muncul kecuali jaringan menggunakan pengalamatan yang dikelola secara lokal.

Tips: Masalah dengan pengalamatan MAC dapat menjadi tanda bahwa seseorang mencoba melakukan serangan spoofing. Serangan spoofing dibahas nanti dalam kursus.

Untuk mendiagnosis masalah alamat MAC, gunakan utilitas arp untuk memverifikasi alamat MAC yang direkam untuk setiap host dan ipconfig atau ip neigh untuk memeriksa alamat MAC yang ditetapkan ke antarmuka. Periksa juga alamat MAC dan tabel ARP pada setiap sakelar dan router yang terlibat dalam jalur komunikasi. Anda dapat menggunakan penganalisis protokol untuk memeriksa lalu lintas ARP dan mengidentifikasi host IP mana yang mencoba mengklaim alamat MAC yang sama.

- **Problem Isolation**

  Jika konfigurasi alamat pada host lokal tampaknya benar, Anda dapat menyelesaikan serangkaian tes konektivitas menggunakan ping untuk menentukan kemungkinan lokasi dan cakupan kesalahan.



A general ping sequence for identifying connectivity issues.

1. Ping alamat loopback (ping 127.0.0.1) untuk memverifikasi TCP/IP diinstal dan dimuat dengan benar. Jika gagal, instal ulang tumpukan protokol jaringan.
2. Ping alamat IP host lokal untuk memverifikasi bahwa itu ditambahkan dengan benar dan untuk memverifikasi bahwa adaptor jaringan berfungsi dengan benar. Jika Anda tidak dapat melakukan ping ke alamat Anda sendiri, mungkin ada kesalahan konfigurasi, atau adaptor jaringan atau driver adaptor mungkin rusak.
3. Ping alamat IP gateway default untuk memverifikasi bahwa itu aktif dan berjalan dan Anda dapat berkomunikasi dengan host lain di jaringan lokal.
4. Ping alamat IP host lain pada subnet yang sama untuk menguji konfigurasi lokal atau masalah tautan.
5. Jika host lokal tidak dapat di-ping dan kesalahannya adalah tujuan tidak dapat dijangkau, maka pastikan konfigurasi IP tidak mengandung alamat IP atau netmask yang salah. Jika ini benar tetapi waktu ping masih habis, curigai masalah keamanan (seperti masalah keamanan port sakelar) atau masalah pada tautan data atau lapisan fisik.
6. Ping alamat IP dari host jarak jauh untuk memverifikasi bahwa Anda dapat berkomunikasi melalui router. Jika alamat IP jarak jauh tidak dapat dihubungi, periksa parameter gateway default pada host lokal untuk mengesampingkan masalah gateway yang salah. Jika gateway dikonfigurasi dengan benar dan Anda dapat melakukan ping ke router, Anda harus mulai menyelidiki infrastruktur perutean.

Tips: Saat melakukan pengujian menggunakan ping, selalu perhatikan bahwa ICMP dapat diblokir oleh firewall atau perangkat lunak keamanan lainnya, terutama saat melakukan ping ke host jarak jauh.

- Masalah DNS Salah

Jika Anda berhasil melakukan semua tes konektivitas dengan alamat IP tetapi tidak dapat melakukan ping dengan nama host, maka ini menunjukkan masalah resolusi nama. Banyak layanan menggunakan nama host dan nama domain untuk membuatnya lebih mudah dikonfigurasi ulang dan lebih mudah diakses orang. Domain Name System (DNS) digunakan untuk memetakan nama-nama ini ke alamat IP. Ketika sebuah host menerima permintaan klien untuk mengakses nama dan tidak memiliki pemetaan IP yang di-cache, ia meminta server DNS yang dikonfigurasi sebagai resolver untuk melakukan pencarian dan mengembalikan alamat IP. Karena resolusi nama adalah layanan penting, sebagian besar host dikonfigurasi dengan server DNS primer dan sekunder untuk redundansi. Alamat server dimasukkan sebagai alamat IP. Pada sebagian besar host workstation, alamat ini kemungkinan akan dikonfigurasi secara otomatis melalui DHCP.

Di Windows, Anda dapat melihat server DNS menggunakan ipconfig /all. Di Linux, alamat server DNS dicatat di /etc/resolv.conf . Biasanya, paket seperti NetworkManager atau systemd-networkd akan menambahkan entri. Entri yang ditambahkan secara langsung akan ditimpa saat reboot.

Jika host tidak dapat menyelesaikan nama, periksa apakah alamat server DNS yang benar telah dikonfigurasi dan Anda dapat melakukan ping ke alamat tersebut. Jika ada kesalahan konfigurasi, perbaiki (jika antarmuka dikonfigurasi secara statis) atau selidiki server pengalamatan otomatis. Jika ada kesalahan konektivitas, periksa jalur jaringan antara host dan server DNS-nya.

- Multicast Flooding Issues

  Multicast adalah jenis transmisi satu-ke-banyak yang dirancang untuk pengiriman paket yang lebih efisien. Daripada pemancar mengirimkan paket unicast terpisah ke setiap penerima, salinan paket yang sama dikirimkan ke setiap penerima yang telah bergabung dengan grup multicast yang relevan. Grup multicast dibuat pada lapisan 3 oleh protokol seperti Internet Group Management Protocol (IGMP).

  Pada layer 2, jika sebuah switch tidak multicast-aware, ia akan memperlakukan transmisi multicast sebagai broadcast dan membanjirinya di semua port dalam broadcast domain. Ini dapat menghabiskan banyak bandwidth dan memperlambat jaringan. Masalah ini menjadi sangat akut jika sakelar membanjiri lalu lintas multicast ke LAN virtual (VLAN) yang tidak perlu menerimanya. Untuk mengatasi hal ini, pengintaian IGMP dapat diaktifkan sebagai opsi global pada sakelar dan sebagai opsi per-VLAN. Pengintaian IGMP berarti sakelar membaca pesan IGMP dan dapat menentukan apakah host pada port akses atau satu atau lebih host dalam VLAN telah bergabung dengan grup multicast. Lalu lintas multicast disaring dari port dan VLAN yang tidak memiliki host yang berpartisipasi dalam grup multicast.

C. Jelaskan Skema Pengalamatan IPv6

Pendahuluan: Jelaskan Skema Pengalamatan IPv6

Topik sebelumnya berfokus pada IP versi 4 (IPv4), yang masih merupakan versi mainstream dari protokol. Dalam topik ini, Anda akan belajar menjelaskan pengalamatan IP versi 6 (IPv6). Sebagai profesional jaringan, Anda harus menyadari keterbatasan IPv4 dan peningkatan adopsi IPv6. Anda perlu memahami karakteristik IPv6, serta bagaimana ia dapat beroperasi dengan implementasi IPv4 yang ada.

IPv4 versus IPv6

Dalam IPv4, skema pengalamatan didasarkan pada bilangan biner 32-bit. 32 bit dapat mengekspresikan 232 alamat unik (lebih dari empat miliar). Namun, cara pengalokasian alamat tidak efisien, yang menyebabkan pemborosan alamat yang tersedia. Inefisiensi dalam skema pengalamatan dan permintaan yang tak henti-hentinya untuk lebih banyak alamat berarti bahwa pasokan alamat IPv4 yang tersedia telah habis.

IP versi 6 (IPv6) memberikan solusi jangka panjang untuk masalah kehabisan ruang alamat ini. Skema pengalamatan 128-bitnya memiliki ruang untuk 340 undecillion alamat unik. Meskipun hanya sebagian kecil dari skema yang saat ini dapat dialokasikan ke host, masih ada ruang alamat yang cukup dalam alokasi itu untuk setiap orang di planet ini untuk memiliki sekitar 4.000 alamat. Selain mengatasi pertumbuhan jaringan perusahaan biasa dan pelanggan akses Internet, IPv6 dirancang untuk memenuhi permintaan miliaran perangkat pribadi dan perangkat tertanam dengan konektivitas Internet.

Tips: Blog ini menjelaskan mengapa kami melompat dari IPv4 ke IPv6: colocationamerica.com/blog/ipv4-ipv6-what-happened-to-ipv5.htm.

Paket IPv6 terdiri dari dua atau tiga elemen: header utama, yang panjangnya tetap (tidak seperti IPv4), satu atau lebih header ekstensi opsional, dan payload. Seperti header IPv4, ada bidang untuk alamat sumber dan tujuan serta versi (0110 atau 0x06 untuk IPv6). Beberapa bidang header lainnya adalah sebagai berikut:

Field	Explanation
Traffic Class	Describes the packet's priority.
Flow Label	Used for quality of service (QoS) management, such as for real-time streams. This is set to 0 for packets not part of any delivery sequence or structure.
Payload Length	Indicates the length of the packet payload, up to a maximum of 64 KB; if the payload is bigger than that, this field is 0 and a special Jumbo Payload (4 GB) option is established.
Next Header	Used to describe what the next extension header (if any) is, or where the actual payload begins.
Hop Limit	Replaces the TTL field in IPv4 but performs the same function.

Header ekstensi menggantikan bidang Opsi di IPv4. Ada beberapa header ekstensi yang telah ditentukan sebelumnya untuk mencakup fungsi seperti fragmentasi dan reassembly, keamanan (IPSec), perutean sumber, dan sebagainya.

Format Alamat IPv6

Alamat IPv6 berisi delapan nomor 16-bit (byte ganda atau oktet ganda), dengan setiap nomor byte ganda dinyatakan sebagai 4 digit hex. Misalnya, pertimbangkan alamat biner berikut:

0010 0000 0000 0001 : 0000 1101 1011 1000 : 0000 0000 0000 0000 : 0000 0000 0000 0000 : 0000 1010 1011 1100 : 0000 0000 0000 0000 : 1101 1110 1111 0000 : 0001 0010 0011 0100

Nilai biner ini dapat direpresentasikan dalam notasi hex sebagai:

2001:0db8:0000:0000:0abc:0000:def0:1234

Menggunakan notasi kanonik, notasi hex dapat dikompresi lebih lanjut. Di mana byte ganda berisi 0 di depan, mereka dapat diabaikan. Selain itu, satu rangkaian 0 yang berdekatan dapat diganti dengan penanda tempat titik dua ganda. Dengan demikian, alamat sebelumnya akan menjadi:

2001:db8::abc:0:def0:1234

Anda hanya dapat menggunakan kompresi titik dua ganda sekali di alamat yang diberikan. Misalnya, 2001:db8::abc::def0:1234 tidak valid karena tidak jelas mana dari dua alamat berikut yang diwakili:

2001:db8:0000:0abc:0000:0000:def0:1234

2001:db8:0000:0000:0abc:0000:def0:1234

Di mana alamat IPv6 digunakan sebagai bagian dari URL (alamat web), karena kedua format menggunakan pembatas titik dua untuk mengartikan hal yang berbeda, alamat IPv6 harus dimasukkan dalam tanda kurung. Misalnya: https://[2001:db8::abc:0:def0:1234]/index.htm.

IPv6 Network Prefixes

Alamat IPv6 dibagi menjadi dua bagian: 64 bit pertama digunakan sebagai ID jaringan, sedangkan 64 bit kedua menunjukkan antarmuka tertentu. Tidak seperti di IPv4, alamat antarmuka (atau bagian ID host) selalu memiliki panjang 64-bit yang sama.



In IPv6, the interface identifier is always the last 64 bits. The first 64 bits are used for network addressing.

Alamat jaringan ditulis menggunakan notasi tanpa kelas, di mana /nn adalah panjang awalan jaringan dalam bit. Dalam ID jaringan 64-bit, seperti halnya netmask IPv4, panjang awalan jaringan yang diberikan digunakan untuk menentukan apakah dua alamat termasuk dalam jaringan IP yang sama. Misalnya, jika awalannya adalah /48, maka jika 48 bit pertama dari alamat IPv6 sama dengan alamat lain, keduanya akan menjadi milik jaringan IP yang sama. Ini berarti bahwa jaringan organisasi tertentu dapat diwakili oleh awalan perutean global sepanjang 48 bit, dan mereka kemudian memiliki 16 bit tersisa di ID jaringan untuk mensubnet jaringan mereka. Sebagai contoh,

2001:db8:3c4d::/48

akan mewakili alamat jaringan, sedangkan:

2001:db8:3c4d:0001::/64

akan mewakili subnet dalam alamat jaringan itu.

Seperti IPv4, IPv6 dapat menggunakan pengalamatan unicast, multicast, dan anycast. Tidak seperti IPv4, tidak ada pengalamatan siaran.

IPv6 Unicast Addressing

Seperti IPv4, alamat unicast IPv6 mengidentifikasi antarmuka jaringan tunggal. Pengalamatan unicast IPv6 tercakup; lingkup adalah wilayah jaringan. Cakupan global menyediakan skema pengalamatan publik yang setara di IPv4, sementara skema tautan lokal menyediakan pengalamatan pribadi.

- IPv6 Global Addressing

  Alamat unicast dengan cakupan global dapat dirutekan melalui Internet dan setara dengan alamat IPv4 publik. Bagian dari alamat global adalah:

  - ☐ 3 bit pertama (001) menunjukkan bahwa alamat berada dalam lingkup global. Sebagian besar ruang alamat IPv6 tidak digunakan. Cakupan untuk pengalamatan unicast unik global hanya menempati 1/8 dari total ruang alamat. Dalam hex, alamat unicast cakupan global akan dimulai dengan 2 (0010) atau 3 (0011).
  - ☐ 45 bit berikutnya dialokasikan secara hierarkis ke registry regional dan dari mereka ke ISP dan pengguna akhir.
  - ☐ 16 bit berikutnya mengidentifikasi alamat subnet khusus situs.
  - ☐ 64 bit terakhir adalah ID antarmuka.



IPv6 global unicast address format.

- Interface ID/EUI-64

  ID antarmuka 64-bit dapat ditentukan dengan menggunakan dua teknik.

  Salah satunya adalah dengan menggunakan alamat MAC antarmuka. Ini dikenal sebagai alamat yang diturunkan dari MAC atau pengidentifikasi antarmuka. Karena alamat MAC saat ini 48 bit (6 byte), mekanisme terjemahan (relatif) sederhana

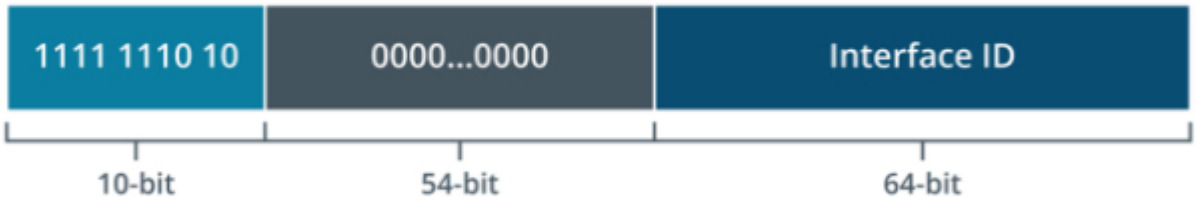
memungkinkan perangkat lunak driver untuk membuat ID antarmuka 64-bit (UEI-64) dari 48 bit ini.

Dua perubahan terjadi untuk mendapatkan ID antarmuka EUI-64 dari alamat MAC antarmuka. Pertama, digit fffe ditambahkan di tengah alamat MAC. Kedua, 8 bit pertama, atau 2 digit hex, dikonversi ke biner, dan bit ke-7 (atau bit U/L) dibalik (dari 0 ke 1 atau 1 ke 0). Misalnya, alamat MAC 00608c123abc akan menjadi alamat EUI-64 02608cfffe123abc, yang (bila dinyatakan dalam byte ganda) menjadi 0260:8cff:fe12:3abc, atau (tanpa awalan 0) 260:8cff:fe12:3abc.

Dalam teknik kedua, yang disebut sebagai ekstensi privasi, perangkat klien menggunakan nomor pseudorandom untuk ID antarmuka. Ini dikenal sebagai ID atau token antarmuka sementara. Ada beberapa kekhawatiran bahwa menggunakan pengidentifikasi antarmuka akan memungkinkan host untuk diidentifikasi dan dipantau secara ketat saat menghubungkan ke Internet, dan menggunakan token mengurangi ini sampai tingkat tertentu.

IPv6 Link Local Addressing

Tautan alamat lokal menjangkau satu subnet (tidak diteruskan oleh router). Node pada link yang sama disebut sebagai tetangga. Rentang lokal tautan adalah fe80::/10. Tautan alamat lokal dimulai dengan fe80 terdepan, dengan 54 bit berikutnya diatur ke 0, dan 64 bit terakhir adalah ID antarmuka.



IPv6 link local unicast address format.

Setara dalam IPv4 adalah Automatic Private IP Addressing (APIPA) dan 169.254.0.0 alamatnya. Namun, tidak seperti IPv4, sebuah host IPv6 selalu dikonfigurasi dengan alamat link lokal (satu untuk setiap link), meskipun juga memiliki alamat unik global.

Alamat lokal tautan juga ditambahkan dengan indeks zona (atau id lingkup) dalam bentuk %1 (Windows) atau %eth0 (Linux). Ini digunakan untuk menentukan sumber alamat dan membuatnya unik untuk tautan tertentu. Misalnya, host tertentu mungkin memiliki tautan ke alamat loopback, Ethernet, dan VPN. Masing-masing tautan ini dapat menggunakan alamat lokal tautan yang sama, sehingga masing-masing diberi ID zona untuk membuatnya unik.

Indeks zona dihasilkan oleh sistem host, jadi saat dua host berkomunikasi, mereka mungkin merujuk ke tautan menggunakan ID zona yang berbeda.

Tips: Meskipun relatif jarang bagi sebuah antarmuka untuk memiliki lebih dari satu alamat IPv4, di IPv6 biasanya sebuah antarmuka memiliki beberapa alamat.

IPv6 Interface Autoconfiguration and Testing

Di IPv6, interface harus selalu dikonfigurasi dengan *link local address*. Satu atau lebih alamat yang dapat dirutekan dapat ditetapkan ke interface selain alamat lokal tautan. Seperti IPv4, Anda dapat menetapkan alamat IPv6 yang dapat dirutekan secara statis atau menggunakan skema pengalamatan otomatis. Konfigurasi alamat statis umumnya akan disediakan untuk router dan mungkin beberapa jenis server.

- Neighbor Discovery Protocol and Router Advertisements

  Protokol Neighbor Discovery (ND) melakukan beberapa fungsi pada jaringan IPv6 yang dilakukan ARP dan ICMP di bawah IPv4. Fungsi utama ND adalah:

  - ☐ Address autoconfiguration-Memungkinkan host untuk mengonfigurasi alamat IPv6 untuk antarmukanya secara otomatis dan mendeteksi apakah alamat sudah digunakan di jaringan lokal, dengan menggunakan pesan neighbor solicitation (NS) dan neighbor advertising (NA).
  - ☐ Prefix discovery Memungkinkan host untuk menemukan awalan jaringan yang diketahui yang telah dialokasikan ke segmen lokal. Ini memfasilitasi penentuan next-hop (apakah sebuah paket harus dialamatkan ke host lokal atau router). Penemuan awalan menggunakan pesan router solicitation (RS) dan router advertising (RA). RA berisi informasi tentang awalan jaringan yang dilayani oleh router, informasi tentang opsi konfigurasi otomatis, ditambah informasi tentang parameter tautan, seperti MTU dan batas hop. Router mengirim RA secara berkala dan sebagai tanggapan atas permintaan router yang diprakarsai oleh host.
  - ☐ Local address resolution-Memungkinkan host untuk menemukan node dan router lain di jaringan lokal (tetangga). Proses ini juga menggunakan pesan Neighbor Solicitation (NS) dan Neighbor Advertisement (NA).
  - ☐ Redirection-Mengaktifkan router untuk menginformasikan host rute yang lebih baik ke tujuan tertentu.

- Stateless Address Autoconfiguration

  IPv4 memiliki sistem untuk menghasilkan *link local addresses*, tetapi ini tidak dapat dirutekan di luar jaringan lokal. Akibatnya, IPv4 sangat bergantung pada Dynamic Host Configuration Protocol (DHCP) untuk konfigurasi otomatis alamat. IPv6 menggunakan sistem autoconfiguration alamat yang lebih fleksibel yang disebut stateless address autoconfiguration (SLAAC):

  - ☐ Tuan rumah membuat *link local addresses* dan menguji keunikannya dengan menggunakan protokol Neighbor Discovery (ND).
  - ☐ Tuan rumah mendengarkan *router advertisement* (RA) atau mengirimkan permintaan router (RS) menggunakan pesan protokol ND. Router dapat menyediakan awalan jaringan, mengarahkan host ke server DHCPv6 untuk melakukan konfigurasi otomatis stateful, atau melakukan beberapa kombinasi konfigurasi stateless dan stateful.

- ICMPv6

  IPv6 menggunakan versi terbaru dari ICMP. Fitur-fitur baru utama adalah:

  - ☐ Pesan kesalahan-ICMPv6 mendukung jenis tujuan yang tidak dapat dijangkau dan waktu yang melebihi pengiriman pesan seperti ICMPv4. Salah satu perubahannya adalah pengenalan kelas kesalahan Paket Terlalu Besar. Di bawah IPv6, router tidak lagi bertanggung jawab atas fragmentasi dan reassembly paket, sehingga host harus memastikan bahwa mereka cocok dengan MTU dari berbagai link yang digunakan.
  - ☐ Pesan informasi-ICMPv6 mendukung fungsi ICMPv4, seperti gema dan pengalihan, ditambah kelas pesan baru yang dirancang untuk mendukung Neighbor Discovery (ND) dan Multicast Listener Discovery (MLD), seperti iklan dan permintaan router dan tetangga.

IPv6 Multicast Addressing

Alamat multicast digunakan untuk mengirim paket dari satu sumber ke beberapa antarmuka jaringan. Tidak seperti IPv4, router IPv6 harus mendukung multicast. Bagian-bagian dari alamat multicast dibagi sebagai berikut:

- ☐ 8 bit pertama menunjukkan bahwa alamat berada dalam lingkup multicast (1111 1111 atau dst).
- ☐ 4 bit berikutnya digunakan untuk menandai jenis multicast jika perlu; jika tidak, mereka disetel ke 0.

- ☐ 4 bit berikutnya menentukan ruang lingkup; misalnya, 1 adalah simpul-lokal (untuk semua antarmuka pada simpul yang sama) dan 2 adalah tautan lokal.
- ☐ 112 bit terakhir mendefinisikan grup multicast dalam lingkup itu.

Protokol Multicast Listener Discovery (MLD) memungkinkan node untuk bergabung dengan grup multicast dan menemukan apakah anggota grup ada di subnet lokal.

Alamat siaran tidak diimplementasikan di IPv6. Sebaliknya, host menggunakan alamat multicast yang sesuai untuk situasi tertentu. Alamat multicast yang terkenal adalah yang dicadangkan untuk jenis fungsi siaran ini. Mereka memungkinkan antarmuka untuk mengirimkan ke semua antarmuka atau router pada node yang sama atau link lokal.

Dalam IPv4, resolusi alamat IP ke antarmuka perangkat keras tertentu dilakukan menggunakan ARP. ARP cerewet dan mengharuskan setiap node untuk memproses pesannya, apakah itu relevan dengan node atau tidak. IPv6 menggantikan ARP dengan protokol Neighbor Discovery (ND).

Setiap alamat unicast untuk sebuah antarmuka dikonfigurasi dengan alamat multicast node yang diminta yang sesuai. Ini memiliki awalan ff02::1:ff ditambah 24 bit terakhir dari alamat unicast. Alamat node yang diminta digunakan oleh ND untuk melakukan resolusi alamat. Ini sangat mengurangi jumlah host yang mungkin menerima pesan ND (turun menjadi satu dalam banyak kasus) dan karena itu jauh lebih efisien daripada mekanisme siaran ARP yang lama.

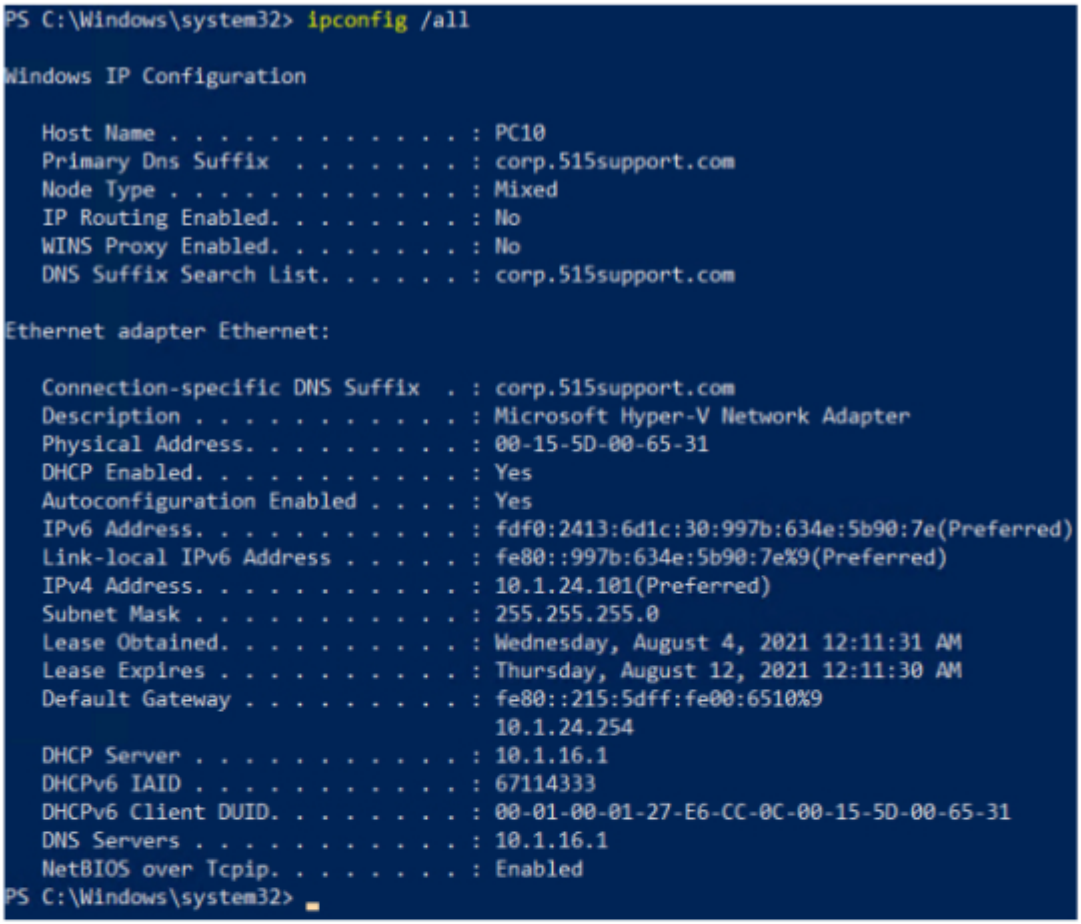
Mekanisme Transisi IPv4 dan IPv6

Sebuah jaringan kemungkinan harus menjalankan IPv4 dan IPv6 di beberapa atau semua segmen dan untuk konektivitas dengan internetwork. Interoperabilitas ini dapat diimplementasikan menggunakan host tumpukan ganda atau dengan mekanisme tunneling.

- Dual Stack

  Dual stack hosts dan router dapat menjalankan IPv4 dan IPv6 secara bersamaan dan berkomunikasi dengan perangkat yang dikonfigurasi dengan salah satu jenis alamat. Sebagian besar sistem operasi desktop dan server modern menerapkan IP tumpukan ganda. Sebagian besar sistem tumpukan ganda modern akan mencoba memulai komunikasi menggunakan IPv6 secara default.

  Tips: Sebagian besar layanan ditangani menggunakan nama daripada alamat IP. Ini berarti bahwa preferensi untuk IPv6 daripada IPv4 atau ketersediaan salah satu metode pengalamatan bergantung pada catatan Domain Name Server (DNS) untuk jaringan.



Dual stack IP in Windows. (Screenshot used with permission from Microsoft.)

- Tunneling

  Sebagai alternatif dari dual stack, tunneling dapat digunakan untuk mengirimkan paket IPv6 melalui jaringan IPv4. Tunneling berarti bahwa paket IPv6 dimasukkan ke dalam paket IPv4 dan diarahkan melalui jaringan IPv4 ke tujuannya. Keputusan perutean didasarkan pada alamat IPv4 sampai paket mendekati tujuannya, di mana paket IPv6 dikeluarkan dari paket pembawa IPv4 dan diteruskan sesuai dengan aturan perutean IPv6. Ini membawa overhead protokol yang tinggi dan hampir tidak seefisien mengoperasikan host tumpukan ganda.

  Dalam tunneling otomatis 6to4, tidak diperlukan konfigurasi host untuk mengaktifkan tunnel. Alamat 6to4 menggunakan awalan 2002::/16. 6to4 telah banyak digantikan oleh protokol yang disempurnakan yang disebut IPv6 Rapid Deployment (6RD). Dengan 6RD, awalan 2002::/16 digantikan oleh awalan yang dikelola ISP dan ada berbagai peningkatan kinerja lainnya.

Microsoft menyediakan dukungan untuk tunneling oleh host Windows menggunakan protokol Teredo-nya. Teredo terowongan paket IPv6 sebagai pesan UDP berbasis IPv4 melalui port 3544. Teredo memerlukan klien dan server yang kompatibel. Paket Miredo open-source mengimplementasikan Teredo untuk sistem operasi UNIX/Linux.

Pilihan lain untuk tunneling adalah Generic Routing Encapsulation (GRE). GRE memungkinkan berbagai macam protokol lapisan Jaringan untuk dienkapsulasi di dalam tautan titik-ke-titik virtual. Protokol ini memiliki keuntungan karena awalnya dirancang untuk IPv4, protokol ini dianggap sebagai mekanisme yang matang dan dapat membawa paket v4 dan v6 melalui jaringan IPv4.

Common IPv6 Address Prefixes

Gunakan tabel berikut untuk membantu Anda mengenali beberapa kelas alamat IPv6 yang umum digunakan dengan notasi awalan atau digit heksadesimal.

Type	Prefix	Leading Hex Characters
Global unicast	2000::/3	2 3
Link local unicast	fe80::/10	fe80
Multicast	ff00::/8	ff
Multicast (link local)	ff02::/16	ff02::1 (all nodes) ff02::2 (all routers) ff02::1:2 (DHCP)
Solicited-node	ff02::1:ff00:0/104	ff02::1:ff
Unspecified	::/128	0::0
Loopback	::1/128	::1
Documentation/Examples	2001:db8::/32	2001:db8

Alamat unicast unik secara global juga secara luas disebut sebagai /48s.

Blok 0000::/8 (yaitu, alamat IPv6 di mana bit pertama adalah 0000 0000) dicadangkan untuk fungsi khusus. Di dalam blok ini, ada dua alamat khusus yang ditentukan:

- Alamat tidak ditentukan (0:0:0:0:0:0:0:0)-Sebuah host yang belum mendapatkan alamat yang valid. Hal ini sering dinyatakan sebagai ::.
- Alamat loopback (0:0:0:0:0:0:0:1)-Digunakan untuk pengujian (untuk host mengirim paket ke dirinya sendiri). Hal ini sering dinyatakan sebagai ::1.

Modul 7

Mengkonfigurasi dan Mengatasi Masalah Router

BANDINGKAN DAN KONTRASKAN KONSEP PERUTERAN

Pendahuluan: Bandingkan dan Kontraskan Konsep Perutean

Sebagai profesional jaringan, Anda harus memahami cara router membuat keputusan penerusan dan bagaimana Anda dapat menerapkannya sehingga Anda dapat mendukung internetwork dari semua ukuran dan jenis. Dalam topik ini, Anda akan memeriksa tabel perutean dan bagaimana tabel tersebut digunakan untuk memilih jalur penerusan.

Routing Tables and Path Selection

Sebagian besar komputer server dan workstation sistem akhir dikonfigurasikan dengan adaptor jaringan tunggal yang terhubung hanya ke satu jaringan. Meskipun berpotensi mampu merutekan, mereka tidak dilengkapi dengan antarmuka yang diperlukan dan pengetahuan tentang lokasi jaringan lain. Router adalah sistem perantara multihomed dengan tautan dan informasi topologi jaringan untuk memfasilitasi penerusan paket antar subnet atau di sekitar internetwork.

Informasi tentang lokasi jaringan IP lain dan host disimpan dalam tabel routing. Setiap entri dalam tabel perutean mewakili rute yang tersedia ke jaringan atau host tujuan. Parameter utama berikut menentukan entri perutean:

- **Protokol** -Sumber rute.
- **Tujuan** -Rute dapat didefinisikan ke host tertentu tetapi lebih umum diarahkan ke ID jaringan. Awalan tujuan paling spesifik (masker terpanjang) akan dipilih sebagai jalur penerusan jika ada lebih dari satu kecocokan.
- **Interface** -Antarmuka lokal yang digunakan untuk meneruskan paket di sepanjang rute yang dipilih. Ini mungkin direpresentasikan sebagai alamat IP antarmuka atau sebagai ID antarmuka lapisan 2.
- **Gateway/next hop** -Alamat IP dari router berikutnya di sepanjang jalur ke tujuan.

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

C>* 10.0.0.2/32 is directly connected, lo, 00:06:52
S>* 10.0.1.0/24 [1/0] via 10.0.2.254, eth0, 00:02:26
C>* 10.0.2.0/24 is directly connected, eth0, 00:02:26
C>* 10.0.3.0/24 is directly connected, eth1, 00:06:51
S>* 10.0.4.0/24 [1/0] via 10.0.3.254, eth1, 00:06:49
```

Tabel perutean pada router VyOS menunjukkan entri rute yang terhubung dan statis.

Static and Default Routes

Entri tabel perutean jatuh ke dalam empat kategori umum:

- Rute jaringan langsung, untuk subnet yang terhubung langsung dengan router.
- Rute jaringan jarak jauh, untuk subnet dan jaringan IP yang tidak terhubung langsung.
- Rute host, untuk rute ke alamat IP tertentu. Rute host memiliki awalan jaringan /32.
- Rute default, yang digunakan saat kecocokan yang tepat untuk jaringan atau rute host tidak ditemukan.

Directly Connected Routes

Jaringan IP atau subnet untuk setiap antarmuka router yang aktif secara otomatis ditambahkan ke tabel perutean. Ini dikenal sebagai rute yang terhubung langsung.

Static Routes

statis ditambahkan secara manual ke tabel perutean dan hanya berubah jika diedit oleh administrator. Mengkonfigurasi entri perutean statis dapat berguna dalam beberapa keadaan, tetapi dapat menjadi masalah jika topologi perutean sering berubah, karena setiap rute pada setiap perute yang terpengaruh perlu diperbarui secara manual.

Tips: Rute statis dapat dikonfigurasi baik sebagai non-persistent atau persisten/permanen. Rute non-persisten dihapus dari tabel perutean jika router di-boot ulang. Rute non-persisten mungkin ditambahkan sebagai tindakan pemecahan masalah, misalnya. Jika rute statis tidak dapat dijangkau, itu akan dinonaktifkan.

Default Route

default adalah tipe khusus dari rute statis yang mengidentifikasi router hop berikutnya untuk tujuan yang tidak dapat ditandingi oleh entri tabel perutean lain. Alamat tujuan 0.0.0.0/0 (IPv4) atau ::/0 (IPv6) digunakan untuk mewakili rute default. Rute default juga digambarkan sebagai pintu gerbang pilihan terakhir. Sebagian besar sistem akhir dikonfigurasi dengan rute default (menunjuk ke gateway default). Ini mungkin juga cara paling sederhana bagi router tepi untuk meneruskan lalu lintas ke router ISP.

Contoh Tabel Perutean

Sebagai contoh entri rute yang terhubung langsung, statis, dan default yang mungkin muncul di tabel perutean, pertimbangkan contoh berikut dari tiga router yang terhubung secara seri:

Router B Routing Table		
Network	Interface	Source
10.0.1.0/24	G0	Static
10.0.2.0/24	G0	Connected
10.0.3.0/24	G1	Connected
10.0.4.0/24	G1	Static



Router A Routing Table		
Network	Interface	Source
10.0.1.0/24	G0	Connected
10.0.2.0/24	G1	Connected
10.0.3.0/24	G1	Static
10.0.4.0/24	G1	Static

Router C Routing Table		
Network	Interface	Source
0.0.0.0/0	G0	Static
10.0.3.0/24	G0	Connected
10.0.4.0/24	G1	Connected

Tabel perutean untuk tiga router yang terhubung secara seri. (Gambar © 123RF.com.)

Pertama, perhatikan tabel routing dari router A:

- Router terhubung langsung ke jaringan 10.0.1.0/24 (melalui antarmuka G0) dan 10.0.2.0/24 (melalui antarmuka G1).
- Router telah dikonfigurasi dengan rute statis ke 10.0.3.0/24 dan 10.0.4.0/24, keduanya dapat dijangkau melalui antarmuka G1.

Router B telah dikonfigurasi dengan cara yang sama, tetapi di sini jaringan 10.0.2.0/24 dan 10.0.3.0/24 terhubung langsung dan jalur ke 10.0.1.0/24 dan 10.0.4.0/24 dikonfigurasi sebagai entri statis.

Router C telah dikonfigurasi secara berbeda. Ini terhubung langsung ke 10.0.3.0/24 dan 10.0.4.0/24, tetapi satu-satunya rute statis yang dikonfigurasi adalah untuk 0.0.0.0/0. Ini adalah rute default. Meskipun router tidak memiliki pengetahuan khusus tentang jaringan 10.0.1.0/24 dan 10.0.2.0/24, router akan meneruskan paket untuk tujuan ini melalui antarmuka G0-nya.

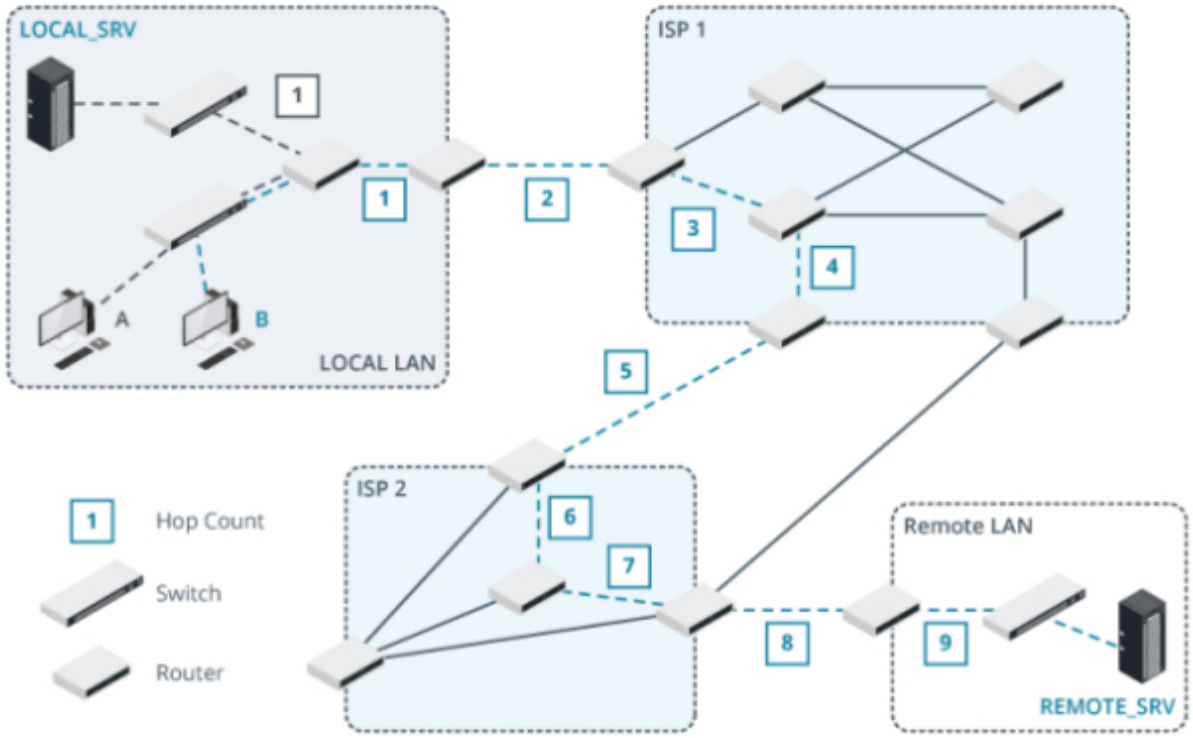
Packet Forwarding

Ketika sebuah router menerima sebuah paket, ia membaca alamat tujuan dalam paket dan mencari alamat IP jaringan tujuan yang cocok dan awalan di tabel peruteannya. Jika ada kecocokan, router akan meneruskan paket dari salah satu antarmukanya dengan mengenkapsulasi paket dalam bingkai baru:

- Jika paket dapat dikirimkan ke jaringan yang terhubung langsung melalui antarmuka Ethernet, router menggunakan ARP (IPv4) atau Neighbor Discovery (ND dalam IPv6) untuk menentukan alamat antarmuka dari host tujuan.
- Jika paket dapat diteruskan melalui gateway melalui antarmuka Ethernet, itu memasukkan alamat MAC router hop berikutnya ke dalam bingkai baru.
- Jika paket dapat diteruskan melalui gateway melalui jenis antarmuka lain (misalnya, leased line atau DSL), router mengenkapsulasi paket dalam tipe bingkai yang sesuai.
- Jika alamat tujuan tidak dapat dicocokkan dengan entri rute, paket akan diteruskan melalui rute default atau dijatuhkan (dan host sumber diberitahu bahwa itu tidak terkirim).

Hop Count

Jika paket diteruskan melalui gateway, proses ini diulang pada setiap router untuk mengirimkan paket melalui internetwork. Setiap router di sepanjang jalur dihitung sebagai satu hop. Misalnya, dalam jaringan yang ditunjukkan pada gambar, host A membutuhkan 1 hop untuk berkomunikasi dengan LOCAL_SRV melalui antarmuka yang terhubung langsung pada router LAN. Perhatikan bahwa sakelar tidak dihitung sebagai hop. Host B mengambil beberapa hop (9) untuk berkomunikasi dengan REMOTE_SRV, dengan lalu lintas diarahkan melalui dua jaringan ISP. Perhatikan juga jalur alternatif yang bisa ditempuh. Apakah ada yang memiliki jumlah hop yang lebih rendah?



Mengukur jumlah hop melalui internetwork. (Gambar © 123RF.com.)

Time To Live

Di setiap router, field header IP Time to Live (TTL) berkurang setidaknya 1. Ini bisa lebih besar jika router macet. TTL secara nominal adalah jumlah detik sebuah paket dapat tetap berada di jaringan sebelum dibuang. Sementara TTL didefinisikan sebagai satuan waktu (detik), dalam prakteknya diartikan sebagai hitungan hop maksimum. Ketika TTL adalah 0, paket tersebut dibuang. Ini mencegah paket yang dialamatkan dengan buruk dari sirkulasi jaringan secara permanen.

Fragmentation

IP menyediakan pengiriman upaya terbaik yang tidak dapat diandalkan dan tanpa koneksi. Pengiriman tidak dijamin, dan paket mungkin hilang, dikirim tidak berurutan, digandakan, atau tertunda. Ada kemungkinan bahwa karena keterbatasan dalam jaringan yang mendasarinya, IP dapat memecah paket menjadi potongan-potongan yang lebih mudah diatur agar sesuai dengan Unit Transmisi Maksimum (MTU) dari bingkai protokol Data Link.

Di IPv4, bidang header IP ID, Flags, dan Fragment Offset digunakan untuk merekam urutan paket yang dikirim dan untuk menunjukkan apakah datagram IP telah dibagi antara beberapa frame untuk transportasi melalui protokol Data Link yang mendasarinya. Misalnya, MTU frame Ethernet biasanya 1500 byte. Datagram IP yang lebih besar dari 1500 byte harus terfragmentasi di lebih dari satu bingkai Ethernet. Datagram yang melewati internetwork mungkin harus dienkapsulasi dalam tipe bingkai Data Link yang berbeda, masing-masing dengan MTU yang berbeda.

Sebagian besar sistem mencoba menghindari fragmentasi IP. IPv6 tidak mengizinkan router untuk melakukan fragmentasi. Sebagai gantinya, tuan rumah melakukan penemuan jalur MTU untuk mengerjakan MTU yang didukung oleh setiap hop dan membuat datagram IP yang sesuai dengan MTU terkecil.

BANDINGKAN DAN KONTRASKAN KONSEP PERUTEAN DINAMIS

Pendahuluan: Bandingkan dan Kontraskan Konsep Perutean Dinamis

Jaringan yang kompleks perlu bertukar informasi perutean dengan cepat untuk mencegah pemadaman, membuat pembaruan perutean statis tidak praktis dalam banyak kasus. Masalah ini diselesaikan dengan menerapkan protokol perutean dinamis. Dalam topik ini, Anda akan membandingkan protokol ini untuk memahami fitur yang membuatnya kurang lebih sesuai untuk jaringan yang berbeda. Anda juga akan mengidentifikasi skema pengalamatan lanjutan yang memaksimalkan pemanfaatan ruang alamat IPv4 yang langka.

Dynamic Routing Protocols

Dynamic Routing Protocols menggunakan algoritma dan metrik untuk membangun dan memelihara basis informasi perutean. Basis data ini menyimpan informasi tentang jaringan tempat router terhubung dan di mana ada banyak jalur, memprioritaskan satu dari yang lain. Informasi ini dapat dibagikan dengan tetangga router. Rute yang dipelajari adalah rute yang dikomunikasikan ke router oleh router lain. Router dapat menambahkan rute yang dipelajari dari satu atau lebih protokol perutean ke tabel perutean IP-nya.

Topology and Metrics

Algoritma yang digunakan untuk pemilihan jalur dapat dikategorikan menurut topologi dan metrik yang mereka gunakan untuk membangun dan memperbarui basis informasi perutean dan memprioritaskan jalur yang optimal (atau paling murah). Sebagian besar algoritma diklasifikasikan sebagai vektor jarak atau sebagai status tautan. Beberapa protokol menggunakan metode hibrida yang berbeda untuk melakukan pemilihan jalur secara lebih efisien.

Untuk setiap protokol yang dijalankan, router memelihara basis informasi perutean dari rute yang ditemukan oleh protokol tersebut. Basis data ini terpisah dari tabel perutean IP yang digunakan untuk menentukan jalur penerusan. Basis data protokol perutean mungkin berisi lebih dari satu rute ke awalan tujuan yang sama. Dalam hal ini, metrik dihitung untuk menentukan jalur mana yang akan dipilih untuk digunakan dalam tabel perutean IP. Jalur dengan metrik biaya terendah lebih disukai.

Jenis algoritma menentukan faktor mana yang digunakan untuk menghitung metrik. Misalnya, protokol vektor jarak menggunakan jumlah hop ke tujuan sebagai metrik. Rute dengan hop paling sedikit adalah jalur dengan biaya paling rendah dan akan dipilih untuk digunakan.

Convergence

Convergence adalah proses di mana router yang menjalankan algoritma perutean dinamis menyetujui topologi jaringan. Router harus mampu beradaptasi dengan perubahan seperti jaringan yang baru ditambahkan, kegagalan antarmuka router atau router, kegagalan tautan, dan sebagainya. Router harus dapat mengkomunikasikan perubahan ke router lain dengan cepat untuk menghindari lubang hitam dan loop. Lubang hitam berarti bahwa sebuah paket dibuang tanpa pemberitahuan kembali ke sumbernya; loop menyebabkan paket diteruskan ke seluruh jaringan sampai TTL-nya habis masa berlakunya.

Sebuah jaringan di mana semua router berbagi topologi yang sama digambarkan sebagai kondisi mapan. Waktu yang dibutuhkan untuk mencapai kondisi mapan adalah ukuran kinerja konvergensi protokol perutean.

Tips: Antarmuka mengepak adalah salah satu yang sering berubah dari online ke offline dan offline ke online. Demikian pula, route flapping mengacu pada router yang mengubah properti

dari rute yang diiklankan dengan cepat dan sering. Mengepakkan dapat menyebabkan masalah konvergensi yang serius.

Interior versus Exterior Gateway Protocols

Selain algoritma yang digunakan untuk menentukan topologi jaringan, *routing protocols* dapat diklasifikasikan menurut cara mereka menangani batasan administratif. Sebuah jaringan di bawah kendali administratif pemilik tunggal disebut sebagai **autonomous system (AS)** . **Interior Gateway Protocol (IGP)** adalah salah satu yang mengidentifikasi rute dalam AS.

Exterior Gateway Protocol (EGP) adalah salah satu yang dapat mengiklankan rute antara sistem otonom. EGP mencakup bidang untuk mengomunikasikan ID sistem otonom jaringan dan memungkinkan pemilik jaringan untuk menentukan apakah mereka dapat menggunakan jalur melalui jaringan organisasi lain.

Beberapa protokol yang paling populer tercantum dalam tabel berikut.

Protocol	Type	Class	Transport
Routing Information Protocol (RIP)	Distance Vector	IGP	UDP (port 520 or 521)
Enhanced Interior Gateway Routing Protocol (EIGRP)	Distance Vector/Hybrid	IGP	Native IP (88)
Open Shortest Path First (OSPF)	Link State	IGP	Native IP (89)
Border Gateway Protocol (BGP)	Path Vector	EGP	TCP (port 179)

Faktor lain yang digunakan untuk membandingkan protokol perutean atau versi protokol adalah apakah mereka mendukung pengalamatan tanpa kelas. Meskipun semua protokol modern menggunakan pengalamatan tanpa kelas, Anda harus memahami bahwa protokol kelas lama

tidak menggunakan subnet mask atau awalan jaringan. Mereka menentukan ID jaringan IPv4 berdasarkan nilai tiga bit pertama dari alamat tersebut.

Terakhir, beberapa versi protokol lama hanya mendukung IPv4. Jika perutean IPv6 diperlukan, Anda harus memilih versi protokol perutean dinamis yang mendukungnya. Sebagian besar router sekarang mengoperasikan perutean tumpukan ganda dari IPv4 dan IPv6. Setiap versi IP memiliki tabel perutean terpisah.

Routing Information Protocol

Routing Information Protocol (RIP) adalah protokol routing vektor jarak. RIP hanya mempertimbangkan satu bagian informasi tentang topologi jaringan - router hop berikutnya untuk mencapai jaringan atau subnet tertentu (vektor). Ini mempertimbangkan hanya satu metrik untuk memilih jalur optimal ke jaringan tujuan yang diberikan - yang memiliki jumlah hop (jarak) terendah.

RIP mengirimkan pembaruan rutin (biasanya setiap 30 detik) dari seluruh basis data peruteannya ke router tetangga. Itu juga dapat mengirim pembaruan yang dipicu setiap kali terjadi perubahan. Ketika sebuah router menerima pembaruan dari tetangga, ia menambahkan rute yang tidak diketahui ke tabel peruteannya sendiri, meningkatkan jumlah hop sebesar 1, dan mengidentifikasi pencetus pembaruan sebagai hop berikutnya ke jaringan yang ditentukan.

Pada gambar berikut, RIP telah digunakan untuk menyebarkan informasi rute antara tiga router yang terhubung dalam sebuah rantai. Router A mempelajari jaringan 10.0.3.0/24 dan 10.0.4.0/24 dari Router B. Router A menambahkan 1 ke metrik jumlah hop dari rute-rute ini. Router B belajar tentang 10.0.1.0/24 dari Router A dan tentang 10.0.4.0/24 dari Router C. Router A dan Router C tidak bertukar informasi apapun secara langsung. Proses distance vector dimana Router A mempelajari jaringan Router C sering disebut sebagai "routing by rumor."

Router B Routing Table			
Network	Interface	Metric	Source
10.0.1.0/24	G0	1	RIP
10.0.2.0/24	G0	0	Connected
10.0.3.0/24	G1	0	Connected
10.0.4.0/24	G1	1	RIP

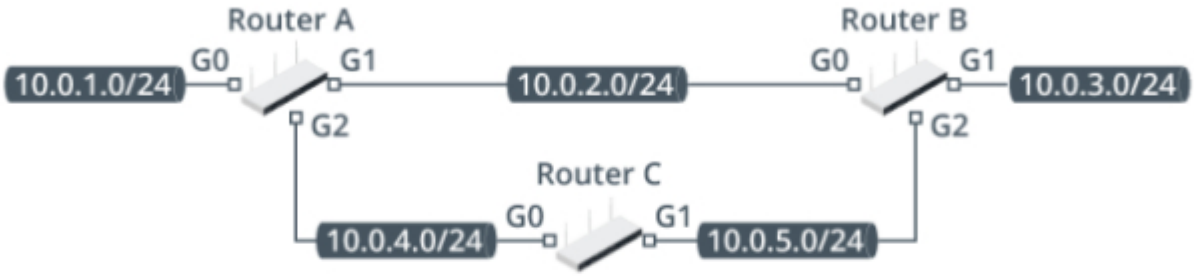


Router A Routing Table			
Network	Interface	Metric	Source
10.0.1.0/24	G0	0	Connected
10.0.2.0/24	G1	0	Connected
10.0.3.0/24	G1	1	RIP
10.0.4.0/24	G1	2	RIP

Router C Routing Table			
Network	Interface	Metric	Source
10.0.1.0/24	G0	2	RIP
10.0.2.0/24	G0	1	RIP
10.0.3.0/24	G0	0	Connected
10.0.4.0/24	G1	0	Connected

Router yang terhubung secara seri bertukar pembaruan jalur vektor jarak.

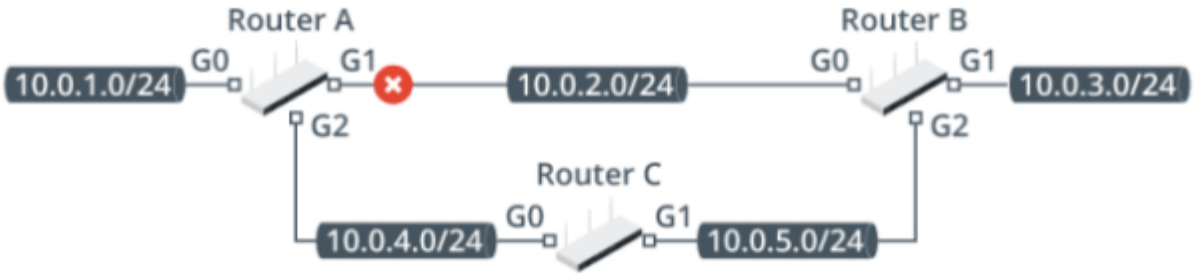
Contoh berikut mengilustrasikan topologi mesh di mana terdapat banyak jalur antar jaringan. Router A memiliki dua kemungkinan jalur ke jaringan 10.0.3.0/24, yang dipelajarinya dari Router B dan Router C. Router A dapat meneruskan paket dari antarmuka G1-nya melalui jaringan 10.0.2.0/24, yang akan membutuhkan satu hop untuk mencapai tujuan. Itu juga bisa meneruskan paket keluar dari G2 dan mencapai tujuan melalui Router C dan kemudian Router B. Ini membutuhkan dua hop dan karenanya tidak digunakan sebagai rute yang disukai.



Router A Routing Table				
Network	Interface	Metric	Via	Source
10.0.1.0/24	G0	0		Connected
10.0.2.0/24	G1	0		Connected
10.0.2.0/24	G2	2	10.0.4.0	RIP
10.0.3.0/24	G1	1	10.0.2.0	RIP
10.0.3.0/24	G2	2	10.0.4.0	RIP
10.0.4.0/24	G2	0		Connected
10.0.5.0/24	G1	2	10.0.2.0	RIP
10.0.5.0/24	G2	1	10.0.4.0	RIP

Router yang terhubung dalam topologi mesh bertukar pembaruan jalur vektor jarak.

Jika link G1 Router A down, entri tersebut akan dihapus dari tabel routing dan rute alternatif melalui 10.0.4.0/24 akan dipilih:



Router A Routing Table				
Network	Interface	Metric	Via	Source
10.0.1.0/24	G0	0		Connected
10.0.2.0/24	G1	0		Connected
10.0.2.0/24	G2	2	10.0.4.0	RIP
10.0.3.0/24	G1	1	10.0.2.0	RIP
10.0.3.0/24	G2	2	10.0.4.0	RIP
10.0.4.0/24	G2	0		Connected
10.0.5.0/24	G1	2	10.0.2.0	RIP
10.0.5.0/24	G2	1	10.0.4.0	RIP

Router yang terhubung dalam topologi mesh bertukar pembaruan jalur vektor jarak.

Untuk membantu mencegah pengulangan, jumlah hop maksimum yang diperbolehkan adalah 15. Akibatnya, ini membatasi ukuran maksimum jaringan RIP, karena jaringan yang memiliki jumlah hop 16 atau lebih tinggi tidak dapat dijangkau.

Versi RIP

Ada tiga versi RIP:

- RIPv1 adalah protokol berkelas dan menggunakan siaran yang tidak efisien untuk mengomunikasikan pembaruan melalui port UDP 520.
- RIPv2 mendukung pengalamatan tanpa kelas dan menggunakan transmisi multicast yang lebih efisien melalui port UDP 520. Ini juga mendukung otentikasi.
- RIPng (generasi berikutnya) adalah versi protokol yang dirancang untuk IPv6. RIPng menggunakan port UDP 521.

Kesederhanaan RIP membuatnya cocok untuk jaringan kecil dengan rute failover terbatas. Algoritma vektor jarak mengharuskan router secara berkala menyebarkan seluruh tabel perutean mereka ke tetangga terdekatnya. Ini tidak terukur untuk lingkungan dengan sejumlah besar jaringan. Algoritma vektor jarak menyediakan konvergensi yang lebih lambat daripada algoritma status tautan. Untuk jaringan yang lebih kompleks dengan jalur redundan, protokol perutean dinamis lainnya harus dipertimbangkan.

Enhanced Interior Gateway Routing Protocol

Interior Gateway Routing Protocol (IGRP) dikembangkan oleh Cisco untuk menyediakan protokol perutean untuk perutean dalam domain atau sistem otonom. Keterbatasan dalam IGRP, seperti kurangnya dukungan untuk pengalamatan tanpa kelas, menyebabkan pengembangan **Enhanced IGRP (EIGRP)** . Ada versi untuk IPv4 dan IPv6.

EIGRP biasanya digolongkan sebagai vektor jarak jauh atau protokol routing hybrid. Seperti RIP, EIGRP adalah protokol vektor jarak karena bergantung pada router tetangga untuk melaporkan jalur ke jaringan jarak jauh. Tidak seperti RIP, yang didasarkan pada matrik jumlah hop sederhana, EIGRP menggunakan metrik yang terdiri dari elemen pembobotan administrator. Dua elemen default adalah bandwidth dan delay:

- **Bandwidth** -Menerapkan biaya berdasarkan link bandwidth terendah di jalur.
- **Delay** -Menerapkan biaya berdasarkan waktu yang dibutuhkan paket untuk melintasi tautan. Metrik ini paling penting jika rute digunakan untuk membawa data sensitif waktu, seperti suara atau video. Penundaan dihitung sebagai nilai kumulatif untuk semua antarmuka keluar di jalur.

Di mana RIP mengirimkan pembaruan berkala dari seluruh basis informasi peruteannya, EIGRP mengirim pembaruan penuh ketika pertama kali menjalin kontak dengan tetangga dan setelah itu hanya mengirim pembaruan ketika ada perubahan topologi. Ini lebih efisien dan tidak terlalu mengganggu jaringan besar, memberikan kinerja konvergensi terbaik dalam banyak skenario. EIGRP memang menggunakan pesan halo biasa untuk mengonfirmasi konektivitas dengan tetangganya. Tidak seperti RIP, EIGRP memelihara tabel topologi di samping basis informasi peruteannya. Tabel topologi digunakan untuk mencegah loop sementara juga mendukung jumlah hop maksimum yang lebih besar daripada RIP (nominal hingga 255). Dalam hal ini, EIGRP memiliki beberapa kesamaan dengan protokol routing link state.

Tidak seperti RIP, EIGRP adalah protokol IP asli, yang berarti dienkapsulasi secara langsung dalam datagram IP, daripada menggunakan TCP atau UDP. Itu ditandai dengan nomor protokol 88 di bidang Protokol dari header IP. Pembaruan ditransmisikan menggunakan pengalamatan multicast.

Open Shortest Path First

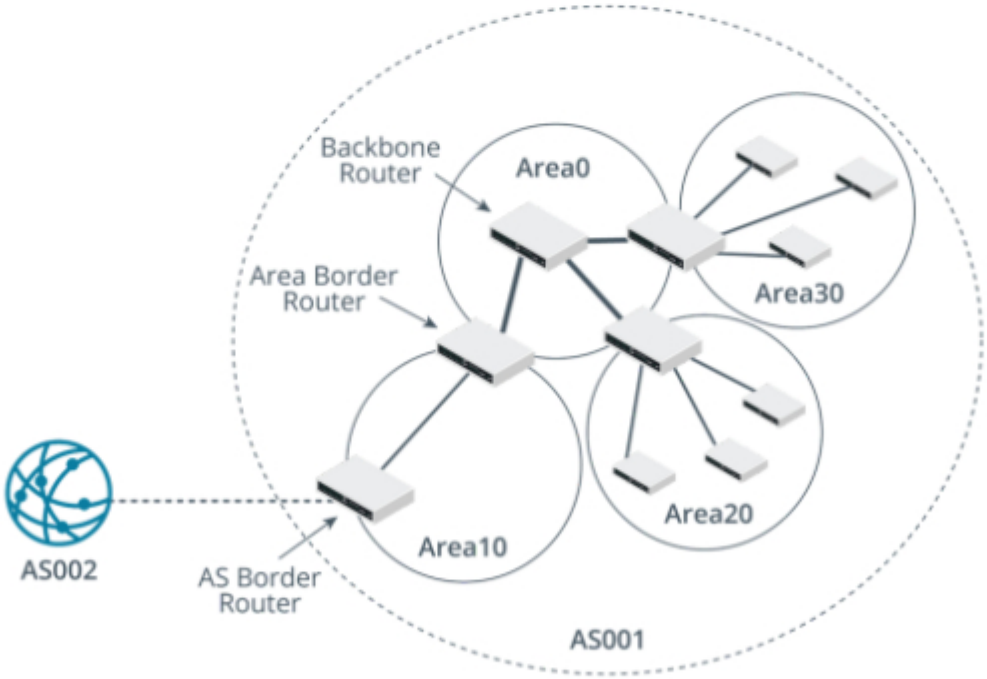
Algoritma vektor jarak bergantung pada tetangga yang terhubung langsung untuk informasi tentang jaringan jarak jauh. Sebaliknya, algoritma status tautan memungkinkan router untuk menyimpan topologi jaringan lengkap dan menilai jalur berbiaya paling rendah dari basis data topologi ini.

Open Shortest Path First (OSPF) adalah protokol link state yang paling banyak diadopsi. Ini cocok untuk organisasi besar dengan beberapa jalur redundan antar jaringan. Ini memiliki kinerja konvergensi yang lebih baik daripada RIP. Itu dirancang dari awal untuk mendukung pengalamatan tanpa kelas.

Di mana RIP dan EIGRP adalah sistem perutean datar, OSPF bersifat hierarkis. Jaringan dan host dan router yang terhubung dalam sistem otonom dikelompokkan ke dalam area OSPF. Router dalam area tertentu berbagi database topologi yang sama dari jaringan yang mereka layani. Router yang dapat terhubung ke beberapa area dikenal sebagai router perbatasan area. Tulang punggung (selalu disebut Area 0) dibuat oleh kumpulan router perbatasan. Tulang punggung ini hanya terlihat oleh router perbatasan dan tidak terlihat oleh router dalam area tertentu.

Di area tertentu, router bertukar pesan hello OSPF, baik sebagai bentuk paket keep-alive dan untuk memperoleh tetangga yang dapat digunakan untuk bertukar informasi routing. Tetangga berbagi pembaruan Link State Advertisement (LSA) untuk membangun database link state (LSDB) yang konsisten yang mewakili topologi jaringan area tersebut. Router menerapkan algoritme yang disebut shortest path first (SPF) untuk menganalisis LSDB dan menambahkan rute bebas loop yang paling murah ke tabel peruteannya. Penggunaan tabel topologi dari seluruh jaringan untuk memilih rute adalah perbedaan utama antara status tautan dan algoritma vektor jarak.

Pembaruan kecil dan sering digunakan oleh OSPF mengarah pada konvergensi yang lebih cepat dan lebih efisien mendukung jaringan yang lebih besar. Penggunaan area untuk membagi jaringan meminimalkan jumlah lalu lintas perutean yang harus dilalui di sekitar jaringan secara keseluruhan, yang selanjutnya meningkatkan kinerja konvergensi. Namun, algoritma status tautan bisa lebih mahal untuk diterapkan karena membutuhkan lebih banyak sumber daya CPU dan memori.



Topologi OSPF tipikal. (Gambar © 123RF.com.)

Pesan dikirim sebagai multicast menggunakan format datagram OSPF sendiri. Ini ditandai sebagai nomor protokol 89 di bidang Protokol datagram IP. Ada berbagai jenis dan mekanisme paket untuk memastikan pengurutan dan pengiriman yang andal dan untuk memeriksa kesalahan. OSPF juga mendukung otentikasi plaintext atau kriptografi.

Border Gateway Protocol

Border Gateway Protocol (BGP) dirancang untuk digunakan antara domain perutean dalam jaringan mesh dan dengan demikian digunakan sebagai protokol perutean di Internet, terutama antara ISP.

Semua protokol yang dibahas sejauh ini telah diklasifikasikan sebagai protokol gateway interior (IGP) yang digunakan untuk komunikasi antar router dalam satu domain perutean, yang disebut sistem otonom (AS). Nomor sistem otonom (ASN) dialokasikan ke ISP oleh IANA melalui berbagai pendaftar regional. BGP adalah jenis protokol gateway eksterior (sebenarnya, ini menggantikan protokol bernama EGP) untuk komunikasi antar router dalam sistem otonom yang terpisah. Ketika BGP digunakan dalam AS, itu disebut sebagai BGP Interior (IBGP), dan ketika diterapkan di antara sistem otonom, itu disebut sebagai BGP Eksterior (EBGP).

AS dirancang untuk menyembunyikan kompleksitas jaringan pribadi dari Internet publik. Jika semua lokasi Internet harus disebarkan ke semua router Internet, tabel perutean akan menjadi terlalu besar untuk diproses. Router tepi untuk setiap AS hanya bertukar informasi jangkauan jaringan sebanyak yang diperlukan untuk mengakses sistem otonom lainnya (jalur AS), daripada jaringan dan host dalam setiap AS. BGP mengutamakan stabilitas dan bisa lambat untuk konvergen.

BGP bekerja dengan prefiks jaringan tanpa kelas yang disebut Network Layer Reachability Information (NLRI). Pemilihan jalur didasarkan pada beberapa metrik, termasuk jumlah lompatan, bobot, preferensi lokal, asal, dan komunitas. BGP bukanlah algoritma vektor jarak murni. Bahkan, BGP lebih sering digolongkan sebagai protokol routing path vector.

BGP bekerja melalui TCP pada port 179.

Administrative Distance

Jika sebuah router memiliki banyak entri ke jaringan yang sama dalam tabel routingnya, router tersebut harus menentukan rute mana yang akan dipilih. Faktor penentu pertama adalah bahwa awalan yang lebih panjang lebih disukai daripada yang lebih pendek. Ini disebut sebagai pencocokan awalan terpanjang. Misalnya, tabel perutean berisi dua entri berikut:

198.51.100.0/24 g0

198.51.100.0/28 g1

Jika router menerima paket untuk 198.51.100.1, paket akan dirutekan melalui g1 , karena memiliki awalan yang lebih panjang dan lebih spesifik.

Setiap protokol perutean yang didukung oleh router dapat menambahkan satu rute untuk setiap awalan tujuan yang diberikan ke tabel perutean. Ini berarti bahwa mungkin ada lebih dari satu rute dengan awalan panjang yang identik di tabel perutean. Setiap protokol perutean menggunakan metriknya untuk menentukan jalur dengan biaya terendah. Namun, karena protokol perutean menggunakan metode yang berbeda untuk menghitung metrik, itu tidak dapat digunakan untuk membandingkan rute dari protokol yang berbeda dalam tabel perutean IP secara keseluruhan. Sebagai gantinya, nilai jarak administratif (AD) digunakan untuk menyatakan kepercayaan relatif dari protokol yang memasok rute. Nilai AD default dikodekan ke router tetapi dapat disesuaikan oleh administrator jika perlu.

Source	AD
Local interface/Directly connected	0
Static route	1
BGP	20
EIGRP	90
OSPF	110
RIP	120
Unknown	255

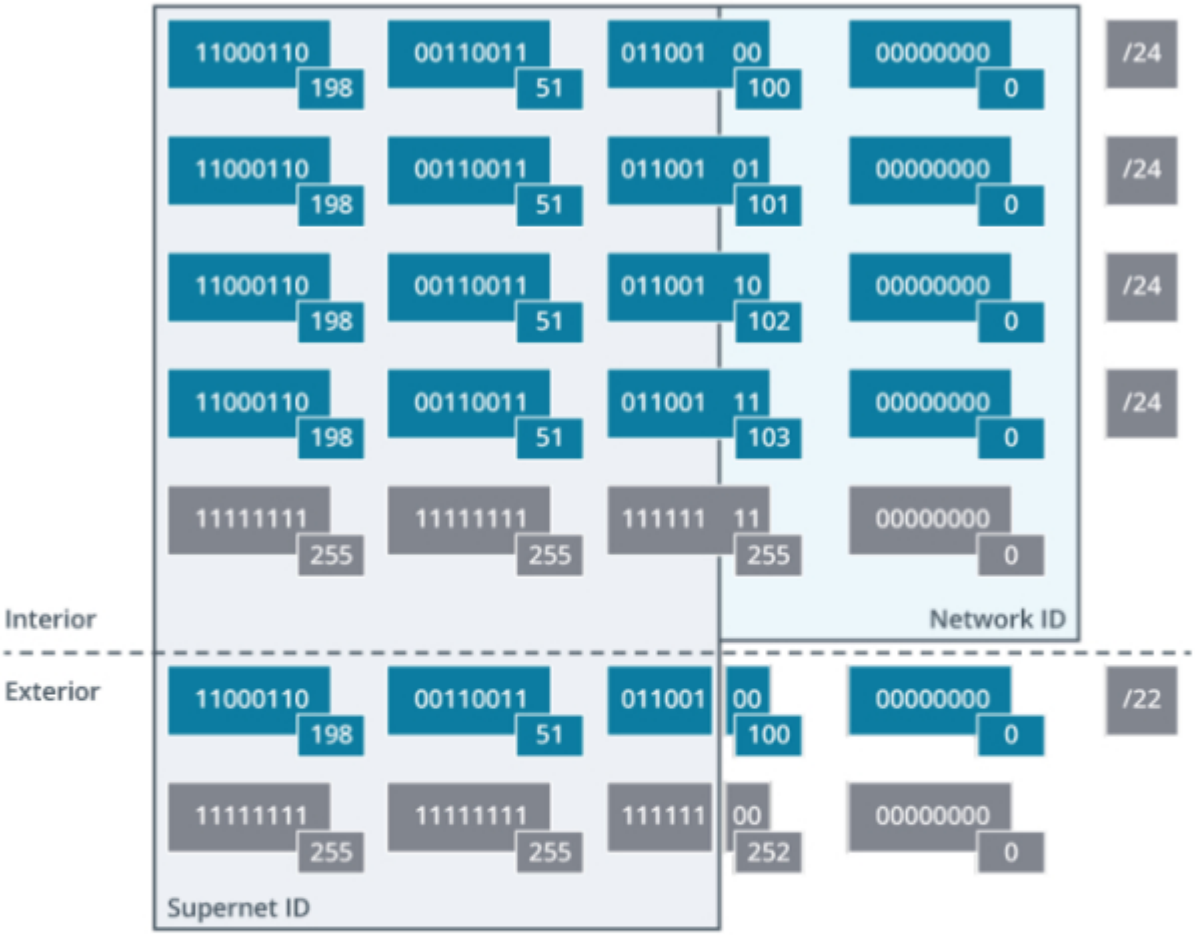
Ini berarti, misalnya, bahwa dengan panjang awalan yang identik, rute statis akan lebih disukai daripada apa pun selain jaringan yang terhubung langsung dan bahwa rute yang ditemukan oleh OSPF akan lebih disukai daripada yang dilaporkan oleh RIP. Nilai 255 untuk rute yang tidak diketahui berarti tidak akan digunakan.

Sebaliknya, rute statis dengan AD tinggi dapat didefinisikan berfungsi sebagai cadangan jika pembaruan rute yang dipelajari gagal. Dalam keadaan normal, router akan lebih memilih rute yang dipelajari karena memiliki AD yang lebih rendah.

Classless Inter-Domain Routing

Pengalamatan tanpa kelas dirancang untuk memecahkan dua masalah utama skema pengalamatan classful karena semakin banyak jaringan bergabung dengan internet hingga awal 1990-an. Yang pertama adalah bahwa alamat jaringan, khususnya, alamat Kelas B, menjadi

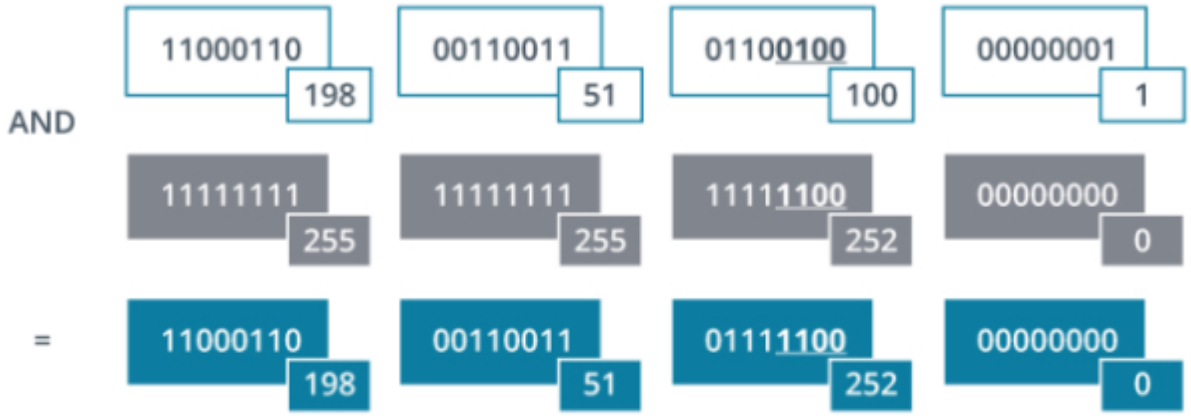
sangat langka dan yang kedua mendekati pertumbuhan eksponensial dalam tabel perutean Internet. Classless Inter-Domain Routing (CIDR) menggunakan bit yang biasanya ditetapkan ke ID jaringan untuk menutupi kompleksitas skema pengalamatan subnet dan host dalam jaringan itu. CIDR juga kadang-kadang digambarkan sebagai supernetting.



Menggunakan CIDR/supernetting untuk meringkas empat /24 jaringan sebagai satu /22 jaringan.

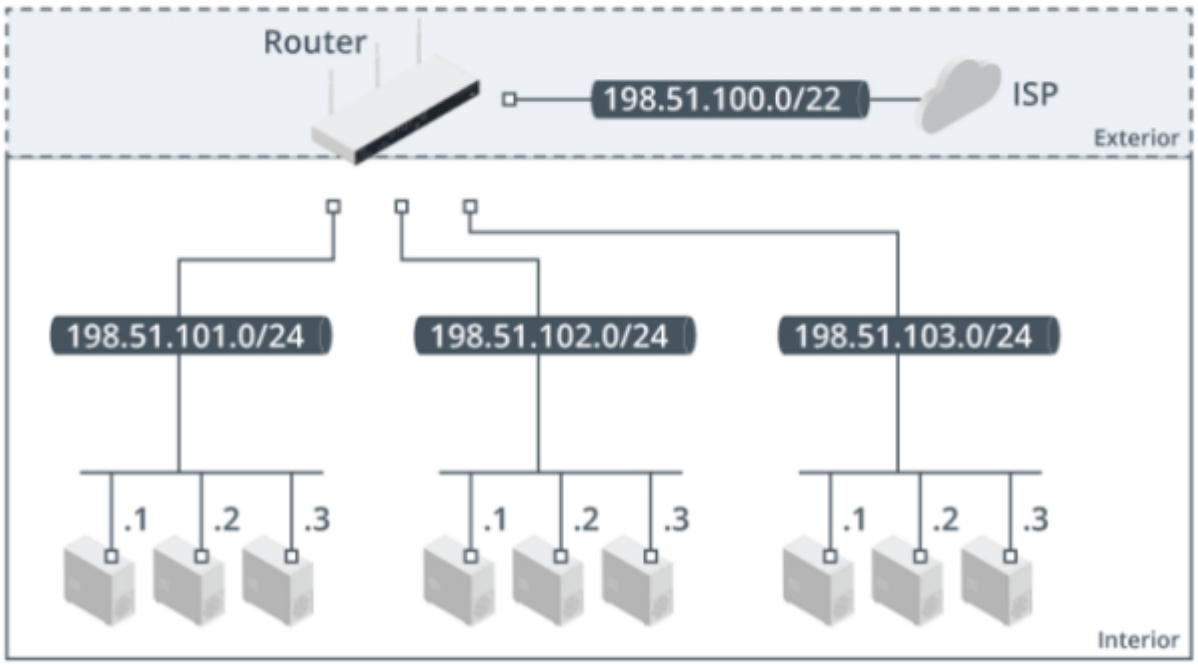
Misalnya, daripada mengalokasikan alamat jaringan Kelas B (atau /16) ke perusahaan, beberapa alamat Kelas C (atau /24) yang berdekatan dapat ditetapkan. Empat /24 alamat jaringan memberikan 1.016 host. Namun, ini berarti perutean yang rumit dengan banyak entri dalam tabel perutean untuk mewakili empat jaringan IP di lokasi yang sama. Menggunakan CIDR menciutkan entri perutean ini menjadi satu entri tunggal. Jika alamat jaringan yang ditetapkan ke perusahaan adalah 198.51.101.0 hingga 198.51.103.0 dan Anda ingin melihat ini sebagai satu jaringan, Anda perlu mengalokasikan dua bit dari alamat jaringan untuk merangkum empat jaringan. Ini membuat awalan supernet /22 atau subnet mask 255.255.252.0.

Proses ANDing masih digunakan untuk menentukan apakah akan merutekan. Jika hasil ANDed menunjukkan ID jaringan yang sama dengan alamat tujuan, maka itu adalah jaringan yang sama. Dalam contoh berikut ini, alamat IP pertama milik supernet, tetapi yang kedua ada di jaringan perusahaan yang berbeda:



Membandingkan awalan jaringan.

Router eksternal ke jaringan hanya menggunakan awalan /22 ini, sehingga kompleksitas subnet LAN disembunyikan dan tidak perlu menyumbat tabel peruteannya. Router internal LAN menggunakan awalan /24 atau bahkan beberapa awalan untuk membuat subnet dengan ukuran berbeda.



CIDR iklan rute publik dan pribadi. (Gambar © 123RF.com.)

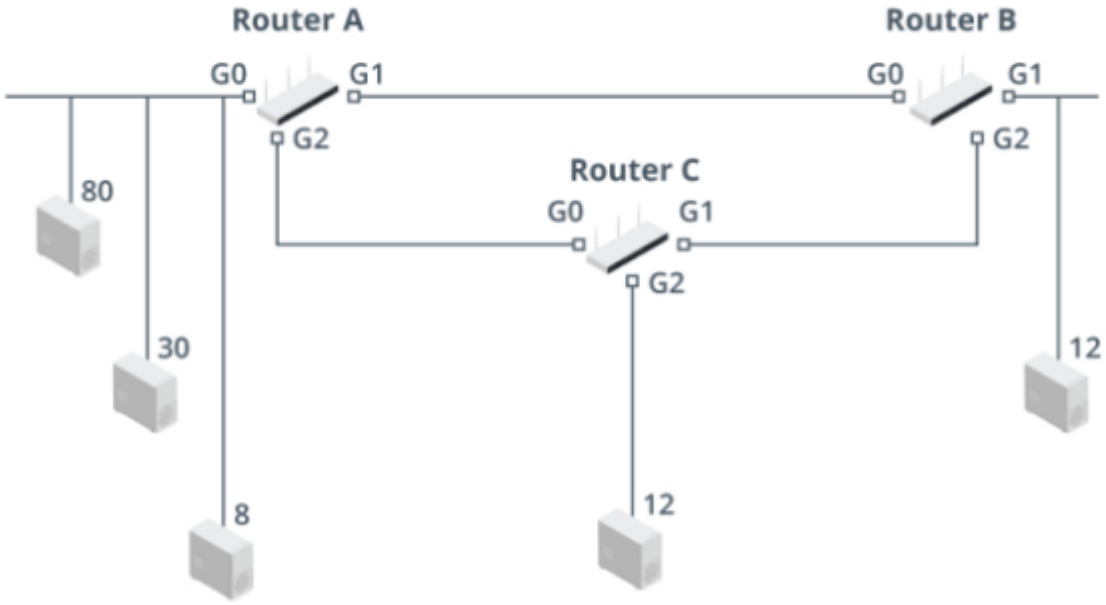
Tips: Ingatlah bahwa baik subnetting maupun supernetting memerlukan penggunaan protokol perutean tanpa kelas (yang tidak menentukan network mask berdasarkan oktet pertama dalam alamat IP). Protokol perutean dinamis yang mendukung pengalamatan tanpa kelas termasuk RIPv2, EIGRP, OSPF, dan BGPv4.

Variable Length Subnet Masks

Ruang alamat IPv4 hampir habis, sehingga menyulitkan ISP untuk mengalokasikan alamat publik ke perusahaan yang menginginkannya. Untuk mengurangi ini, metode alokasi alamat IP yang lebih efisien harus digunakan. Supernetting menyederhanakan informasi yang dibutuhkan router Internet untuk menemukan jaringan IP. Teknik pengalamatan tanpa kelas komplementer, yang disebut variable length subnet masking (VLSM), memungkinkan perancang jaringan untuk mengalokasikan rentang alamat IP ke subnet yang sesuai dengan prediksi kebutuhan jumlah subnet dan host per subnet secara lebih dekat. Tanpa VLSM, Anda harus mengalokasikan rentang alamat subnet yang berukuran sama dan menggunakan subnet mask yang sama di seluruh jaringan.

VLSM memungkinkan netmask panjang yang berbeda untuk digunakan dalam jaringan IP yang sama, memungkinkan lebih banyak fleksibilitas dalam proses desain.

Untuk contoh ini, pertimbangkan sebuah perusahaan dengan tiga situs, masing-masing dengan ukuran jaringan dan persyaratan alamat IP yang berbeda. Ada juga subnet yang mewakili tautan WAN point-to-point antara router.



Persyaratan VLSM untuk alamat host. (Gambar © 123RF.com.)

Desain VLSM biasanya dimulai dengan mengidentifikasi subnet dengan host terbanyak dan mengatur skema dalam urutan menurun. Seperti halnya perhitungan subnet lainnya, perlu diingat bahwa setiap pangkat 2 adalah dua kali lipat dari yang sebelumnya:

2^2	2^3	2^4	2^5	2^6	2^7	2^8
4	8	16	32	64	128	256

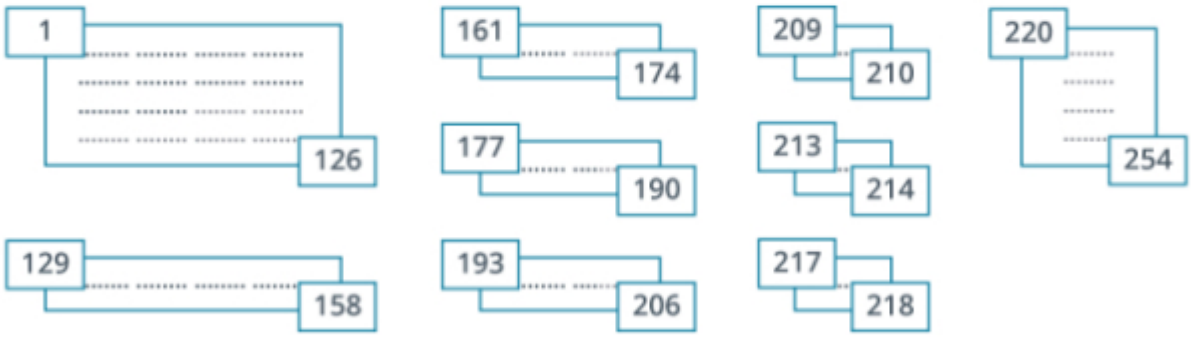
- Dalam contoh, persyaratan terbesar adalah untuk 80 host. 26 memiliki maksimum 64 nilai, yang tidak cukup, sehingga kecocokan terdekat dalam tabel adalah 2 7 . Ini memberitahu kita bahwa kita membutuhkan 7 bit untuk pengalamatan host. Ini sebenarnya memungkinkan untuk 126 alamat host setelah jaringan dan alamat broadcast telah diperhitungkan (2 7 -2). Menggunakan 7 bit membuat awalan /25 (32 dikurangi 7).
- Persyaratan berikutnya secara teknis dipenuhi oleh ruang alamat host 5 bit, tetapi karena hal ini memungkinkan tepat 30 alamat, tidak akan ada ruang untuk pertumbuhan. Menggunakan 6 bit mungkin lebih aman, tetapi untuk skenario ini, kami akan memilih kecocokan terdekat dan mengadopsi awalan /27.
- Tiga persyaratan berikutnya adalah untuk 8, 12, dan 12 host. Ini semua membutuhkan 4 bit, yang memberikan hingga 14 alamat yang dapat digunakan.
- Router menggunakan link point-to-point, jadi tidak lebih dari dua alamat yang diperlukan. Ini dapat dipenuhi dengan memilih awalan /30.

Desain VLSM

Desain VLSM akhir diringkas dalam tabel berikut:

Office/Subnet	Required Number of IP Addresses	Mask Bits	Actual Number of IP Addresses	Prefix
Main Office 1 (Router A)	80	7	126	/25
Main Office 2 (Router A)	30	5	30	/27
Main Office 3 (Router A)	8	4	14	/28
Branch Office (Router B)	12	4	14	/28
Branch Office (Router C)	12	4	14	/28
Router A - Router B	2	2	2	/30
Router A - Router C	2	2	2	/30
Router B - Router C	2	2	2	/30

Semua subnet kecuali untuk Kantor Utama 2 memiliki ruang untuk berkembang.



Desain VLSM mengatasi pemanfaatan ruang.

Faktanya, jika Anda menganalisis desain akhir, Anda akan menemukan bahwa ada 36 alamat yang tidak digunakan di akhir rentang. Akibatnya, akan ada ruang untuk menggunakan awalan /26 untuk grup yang terdiri dari 30 host.

Rentang alamat IP aktual yang dihasilkan oleh desain VLSM ditunjukkan dalam tabel ini.

Office	Subnet	Subnet Mask	Useable Host Address Range	Broadcast Address
Main Office 1 (Router A)	198.51.100.0/25	255.255.255.128	1-126	127
Main Office 2 (Router A)	198.51.100.128/27	255.255.255.224	129-158	159
Main Office 3 (Router A)	198.51.100.160/28	255.255.255.240	161-174	175
Branch Office (Router B)	198.51.100.176/28	255.255.255.240	177-190	191
Branch Office (Router C)	198.51.100.192/28	255.255.255.240	193-206	207
Router A - Router B	198.51.100.208/30	255.255.255.252	209-210	211
Router A - Router C	198.51.100.212/30	255.255.255.252	213-214	215
Router B - Router C	198.51.100.216/30	255.255.255.252	217-218	219

Topologi jaringan VLSM dapat diringkas dengan diagram ini:

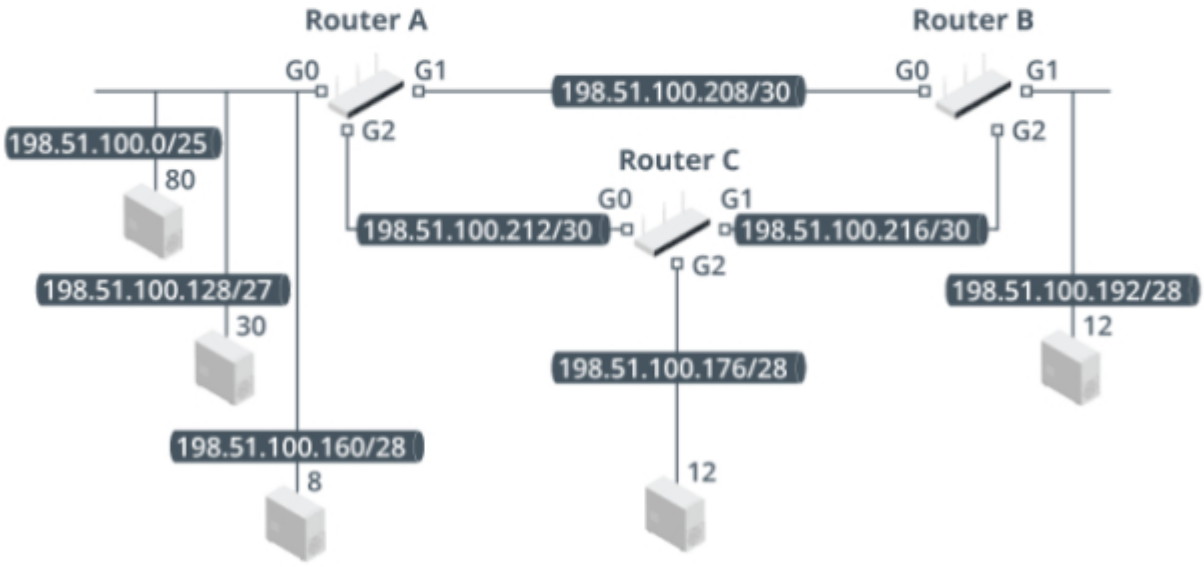


Diagram topologi desain VLSM. (Gambar © 123RF.com.)

INSTAL DAN PECAHKAN MASALAH ROUTER

Pendahuluan: Memasang dan Memecahkan Masalah Router

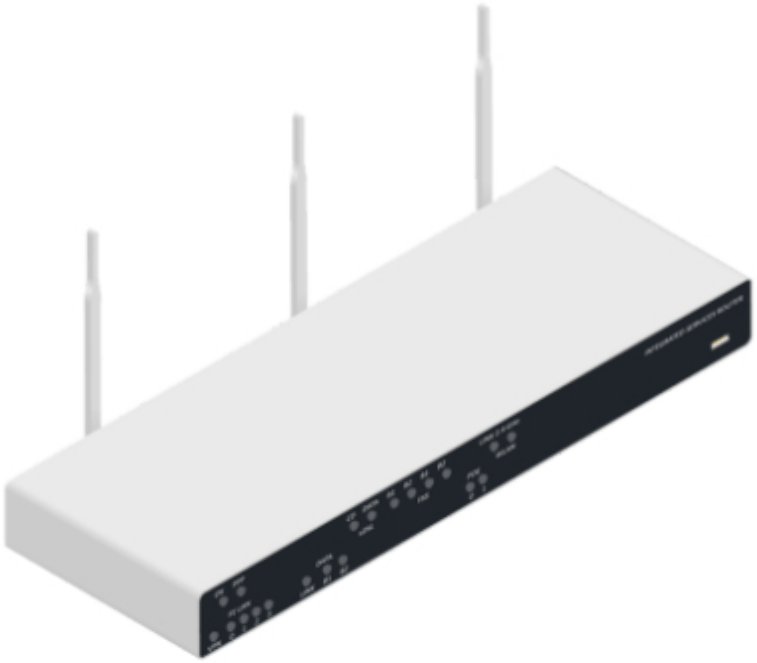
Selain memahami berbagai jenis algoritma perutean, Anda harus dapat memasang perangkat perutean ke tempat yang sesuai di jaringan. Topik ini akan membantu Anda menginstal dan mengkonfigurasi router, dan menggunakan alat baris perintah untuk menguji infrastruktur perutean.

Edge Router

Router berfungsi untuk menghubungkan jaringan jarak jauh secara fisik dan membagi jaringan IP otonom menjadi beberapa subnet. Penempatan router terutama didorong oleh jaringan IP dan subnet yang telah dibuat:

- Host dengan alamat di subnet atau jaringan IP yang sama tidak boleh dipisahkan oleh router. Sebaliknya, host dengan alamat di subnet atau jaringan IP yang berbeda harus dipisahkan oleh router.
- Router tepi, ditempatkan di perimeter jaringan, ditandai dengan membedakan antarmuka eksternal (menghadap ke Internet) dan internal. Router ini dapat melakukan pembingkaian untuk mengemas ulang data dari format bingkai LAN pribadi ke format bingkai akses Internet WAN. Router pelanggan disebut sebagai tepi pelanggan (CE), sedangkan router penyedia layanan disebut sebagai tepi penyedia (PE).

Router tepi yang dirancang untuk bekerja dengan DSL atau metode akses broadband kabel disebut router kantor kecil/kantor rumah (SOHO). Router dengan fungsionalitas terintegrasi serupa sering digunakan oleh perusahaan untuk konektivitas kantor cabang.



Sebuah router layanan terintegrasi. Jenis perangkat ini menggabungkan akses Internet DSL dengan sakelar Ethernet, Wi-Fi, dan VoIP untuk solusi "satu kotak" untuk situs jarak jauh dan kantor cabang. (Gambar © 123RF.com.)

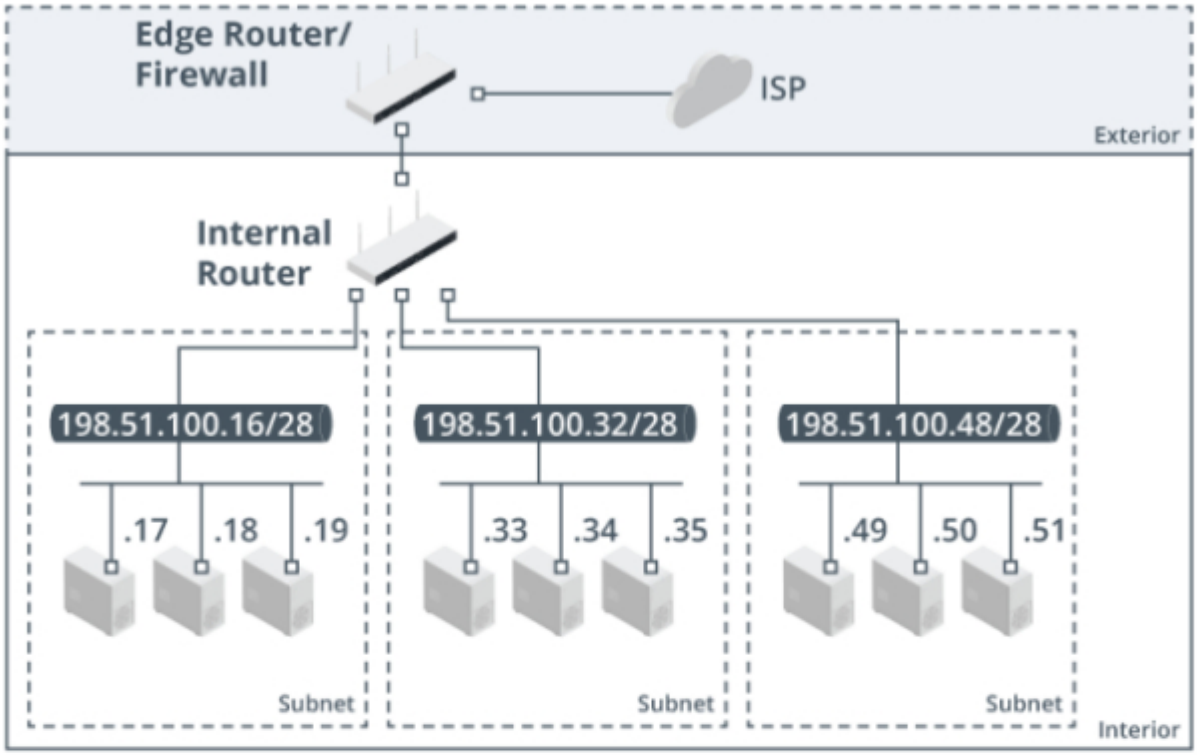
Router yang dirancang untuk melayani jaringan menengah hingga besar adalah peralatan yang kompleks dan mahal. Mereka menampilkan prosesor khusus untuk menangani proses perutean dan penerusan, dan memori untuk buffer data. Sebagian besar router kelas ini juga akan mendukung kartu plug-in untuk antarmuka WAN. Fitur penting lainnya adalah dukungan untuk berbagai metode dalam mengonfigurasi jaringan pribadi virtual (VPN) situs-ke-situs.



Sebuah router layanan canggih. Jenis perangkat ini menyediakan konektivitas tepi jaringan melalui jaringan Carrier Ethernet. (Gambar © 123RF.com.)

Router Internal

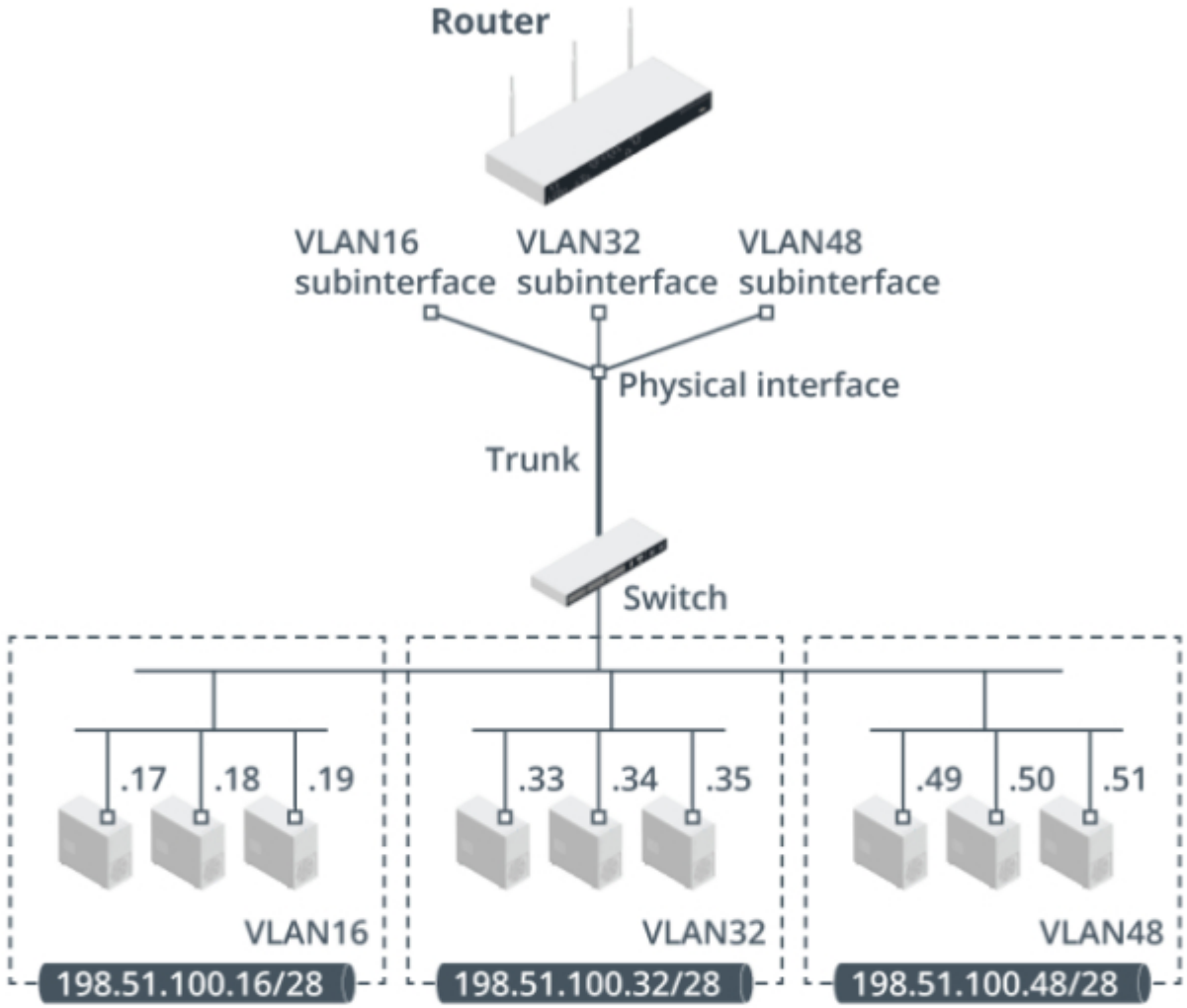
Router internal tidak memiliki interface publik. Router internal diposisikan untuk mengimplementasikan topologi jaringan apa pun yang diperlukan. Gambar tersebut menunjukkan contoh sederhana dari konfigurasi jaringan yang khas. Router/firewall edge menyediakan akses ke Internet. Lalu lintas antara subnet lokal dikendalikan oleh router internal yang terpisah.



Penempatan jaringan edge dan router internal. (Gambar © 123RF.com.)

Sebuah jaringan juga dapat menggunakan topologi yang lebih kompleks, seperti pembagian ke dalam area OSPF.

Subinterfaces Banyak jaringan tersegmentasi menggunakan fitur LAN virtual (VLAN) dari switch yang dikelola. Lalu lintas antar VLAN harus dirutekan. Dalam skenario ini, dimungkinkan untuk menggunakan router dengan satu antarmuka (router satu tangan atau router pada tongkat) yang terhubung ke port trunk pada sakelar. Port trunk membawa semua lalu lintas VLAN-ke-VLAN yang harus dirutekan. Antarmuka fisik router dikonfigurasi dengan beberapa subinterface atau antarmuka virtual. Setiap subinterface dikonfigurasi dengan ID VLAN tertentu. Subinterface menerima lalu lintas dari VLAN tertentu dan kemudian mengarahkannya ke subinterface yang melayani VLAN tujuan.



Router pada topologi Stick dengan subinterface yang melayani setiap VLAN/subnet. (Gambar © 123RF.com.)

Layer 3 Capable Switches

Melewati lalu lintas antara alat router dan switch melalui tautan trunk relatif tidak efisien dan tidak berskala dengan baik hingga puluhan VLAN. Akibatnya, jaringan perusahaan biasanya menggunakan sakelar lapisan 3 di inti jaringan mereka. switch berkemampuan lapisan 3 adalah sakelar yang dioptimalkan untuk perutean antar VLAN. Itu dapat menggunakan perutean statis dan dinamis untuk mengidentifikasi VLAN mana alamat IP yang harus diteruskan. switch lapisan 3 dapat mempertahankan tabel pemetaan alamat IP ke alamat MAC sehingga ketika jalur dibuat, ia dapat menggunakan penerusan berbasis perangkat keras latensi rendah. Namun, switch layer 3 biasanya tidak memiliki antarmuka WAN sehingga biasanya tidak digunakan untuk perutean di tepi jaringan.

Konfigurasi Router

Karena alat perute tidak memiliki layar atau keyboard, perangkat ini dikonfigurasikan secara lokal baik melalui koneksi serial yang dikenal sebagai port konsol atau (lebih biasanya) dari jarak jauh melalui jaringan dengan menggunakan protokol seperti Secure Shell (SSH). SSH dapat digunakan untuk berkomunikasi dengan router melalui alamat IP dari antarmuka yang dikonfigurasi. Namun, karena antarmuka fisik apa pun dapat mengalami kesalahan perangkat keras atau untuk sementara tidak tersedia karena berbagai alasan, itu dianggap praktik terbaik untuk membuat antarmuka virtual, yang dikenal sebagai antarmuka loopback, di sistem operasi router dan menetapkan alamat IP untuk digunakan. dalam mengelola router dari jarak jauh. Ini adalah cara memberi router alamat IP internal, tidak terhubung ke jaringan fisik apa pun, yang karenanya tidak bergantung pada tautan jaringan tertentu yang tersedia.

```
vyos@vyos:~$ conf
[edit]
vyos@vyos# set protocols rip interface eth0
[edit]
vyos@vyos# set protocols rip interface eth1
[edit]
vyos@vyos# set protocols rip redistribute connected
[edit]
vyos@vyos# commit && save && exit
Saving configuration to '/config/config.boot'...
Done
exit
vyos@vyos:~$ show ip rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface

     Network            Next Hop         Metric From            Tag Time
R(n) 10.0.0.1/32        10.0.2.254            2 10.0.2.254        0 02:57
C(r) 10.0.0.2/32        0.0.0.0               1 self              0
R(n) 10.0.1.0/24        10.0.2.254            2 10.0.2.254        0 02:57
C(i) 10.0.2.0/24        0.0.0.0               1 self              0
C(i) 10.0.3.0/24        0.0.0.0               1 self              0
```

Mengonfigurasi RIP pada router perangkat lunak berbasis VyOS. Host dapat dikonfigurasi di terminal lokal atau dari komputer jarak jauh melalui Secure Shell (SSH).

Setelah menempatkan router pada titik yang tepat dalam jaringan, menghubungkan kabelnya, dan membuat sesi manajemen, tugas konfigurasi utama adalah sebagai berikut:

- Terapkan konfigurasi IP ke setiap antarmuka.
- Konfigurasikan satu atau lebih protokol perutean dan/atau rute statis sehingga router dapat menjalankan fungsinya.

Show route, show ip route , show ipv6 route , atau perintah serupa akan menampilkan tabel routing yang aktif. Selain tujuan, gateway, AD/metrik, dan antarmuka, output akan menunjukkan sumber rute, diidentifikasi sebagai kode huruf (C = terhubung, S = statis, R = RIP, B = BGP, D = EIGRP, O = OSPF, dan seterusnya).

route

Perintah rute digunakan untuk melihat dan memodifikasi tabel perutean sistem akhir host Windows dan Linux.

Terlepas dari alamat loopback dan subnet lokal, tabel routing untuk sistem akhir umumnya berisi satu entri untuk rute default. Rute default direpresentasikan sebagai tujuan 0.0.0.0/0. Setiap lalu lintas yang tidak ditujukan ke subnet lokal dikirim melalui rute default ini.

Di Windows, untuk menampilkan tabel perutean, jalankan pencetakan rute.

```
PS C:\Windows\system32> route print
===========================================================================
Interface List
  9...00 15 5d 00 65 31 ......Microsoft Hyper-V Network Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.1.24.254      10.1.24.101     15
       10.1.24.0    255.255.255.0         On-link       10.1.24.101    271
     10.1.24.101  255.255.255.255         On-link       10.1.24.101    271
     10.1.24.255  255.255.255.255         On-link       10.1.24.101    271
       127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
       127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
       224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
       224.0.0.0        240.0.0.0         On-link       10.1.24.101    271
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link       10.1.24.101    271
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  9     31 ::/0                     fe80::215:5dff:fe00:6510
  1    331 ::1/128                  On-link
  9     31 fdf0:2413:6d1c:30::/64   On-link
  9    271 fdf0:2413:6d1c:30:997b:634e:5b90:7e/128
                                    On-link
```

Tabel perutean IPv4 dan IPv6 untuk host Windows. Untuk IPv4, host menggunakan 10.1.0.254 sebagai gateway default. Konfigurasi IPv6 tidak memiliki rute dari jaringan lokal. (Tangkapan layar digunakan dengan izin dari Microsoft.)

Untuk menambahkan rute, sintaks untuk alat versi Windows adalah:

route [-f -p] tambahkan DestinationIP mask Netmask GatewayIP metrik MetricValue jika Antarmuka

Variabel dalam sintaks didefinisikan sebagai:

- DestinationIP adalah jaringan atau alamat host.
- Netmask adalah subnet mask untuk DestinationIP.
- GatewayIP adalah router yang digunakan untuk menghubungi jaringan atau host.
- MetricValue adalah biaya rute.
- Antarmuka adalah adaptor yang harus digunakan host (digunakan jika host multihomed).

Sebagai contoh:

rute tambahkan 192.168.3.0 mask 255.255.255.0 192.168.5.1 metrik 2

Rute yang ditambahkan dengan cara ini tidak permanen secara default. Ini berarti bahwa mereka disimpan dalam memori dan akan dibuang jika mesin dihidupkan ulang. Rute dapat dikonfigurasi secara permanen (disimpan dalam registri) menggunakan sakelar -p. Alat ini juga memungkinkan untuk menghapus rute (route delete) dan dimodifikasi (route change).

Rute versi Linux melakukan fungsi yang sama, tetapi sintaksnya berbeda. Tabel routing ditunjukkan dengan memasukkan rute tanpa parameter. Parameter perubahan tidak didukung, dan perintah tidak dapat digunakan untuk menambahkan rute persisten. Rute nonpersistent dapat ditambahkan menggunakan sintaks umum berikut:

rute tambahkan -net 192.168.3.0 netmask 255.255.255.0 metrik 2 dev eth0

```
lamp@lamp:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         172.16.0.254    0.0.0.0         UG    100    0        0 eth0
172.16.0.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0
172.16.0.254    0.0.0.0         255.255.255.255 UH    100    0        0 eth0
```

Output dari perintah rute Linux.

Tips: Rangkaian alat iproute2 dirancang untuk menggantikan alat baris perintah lama yang tidak digunakan lagi di Linux. Anda dapat menggunakan ip route show dan ip route add untuk mencapai tujuan yang sama.

tracert dan traceroute

Alat traceroute memungkinkan Anda untuk menguji seluruh jalur antara dua node dengan maksud untuk mengisolasi node atau link yang menyebabkan masalah.

traceroute

traceroute didukung pada OS Linux dan router (seperti Cisco IOS). traceroute menggunakan pesan probe UDP secara default. Perintah mengeluarkan probe UDP untuk port 32767 dengan TTL 1. Hop pertama harus mengurangi ini menjadi nol dan merespons dengan pesan ICMP Time Exceeded. Perintah kemudian menambah TTL satu per satu dan mengirimkan probe kedua, yang seharusnya mencapai router hop kedua. Proses ini diulang sampai node akhir tercapai, yang seharusnya membalas dengan respon ICMP Port Unreachable.

Output menunjukkan jumlah hop, alamat IP dari antarmuka masuknya router atau host (yaitu, antarmuka dari mana router menerima probe), dan waktu yang dibutuhkan untuk menanggapi setiap probe dalam milidetik (ms). Jika tidak ada pengakuan yang diterima dalam periode waktu habis, tanda bintang akan ditampilkan pada probe. Perhatikan bahwa meskipun ini dapat menunjukkan bahwa antarmuka router tidak merespons, bisa juga router dikonfigurasikan untuk menjatuhkan paket dengan TTL kedaluwarsa secara diam-diam.

traceroute dapat dikonfigurasi untuk mengirim probe ICMP Echo Request daripada UDP dengan menggunakan traceroute -I . Perintah traceroute -6 atau traceroute6 digunakan untuk jaringan IPv6.

tracert

Pada sistem Windows, fungsi yang sama dilakukan dengan menggunakan perintah tracert. tracert menggunakan probe ICMP Echo Request secara default. Perintah mengeluarkan probe Permintaan Echo dengan TTL 1. Hop pertama harus mengurangi ini menjadi nol dan merespons dengan respons Time Exceeded. tracert kemudian menambah TTL satu per satu setiap kali untuk menemukan jalur lengkap.

```
PS C:\Windows\system32> tracert 203.0.113.33

Tracing route to 203.0.113.33 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  10.1.24.254
  2    <1 ms    <1 ms    <1 ms  10.1.128.253
  3     1 ms     *        1 ms  198.51.100.30
  4     1 ms     1 ms     1 ms  198.51.100.253
  5     2 ms     2 ms     1 ms  203.0.113.33

Trace complete.
```

Menggunakan tracert di Windows untuk memplot jalur dari host di Inggris ke server web CompTIA. (Tangkapan layar digunakan dengan izin dari Microsoft.)

tracert dapat digunakan dengan beberapa switch, yang harus mendahului alamat IP atau host target.

Anda dapat menggunakan sakelar -d untuk menekan resolusi nama, -h untuk menentukan jumlah maksimum hop (standarnya adalah 30), dan -w untuk menentukan batas waktu dalam ms (standarnya adalah 4000). Jika, setelah meningkatkan nilainya, tujuan kemudian dapat dijangkau, Anda mungkin memiliki masalah bandwidth yang harus diselesaikan. Saat digunakan dengan nama host (bukan alamat IP), tracert dapat dipaksa menggunakan IPv6 alih-alih IPv4 dengan menambahkan -6 switch.

tracert -6 www.microsoft.com

Missing Route Issues

Jika Anda dapat melakukan ping ke gateway default host, tetapi Anda tidak dapat melakukan ping ke beberapa atau semua host di jaringan jarak jauh, maka Anda harus mencurigai adanya masalah perutean. Dalam banyak kasus, ini karena router telah offline dan tidak ada jalur alternatif ke jaringan. Anda juga harus siap untuk mempertimbangkan masalah konfigurasi.

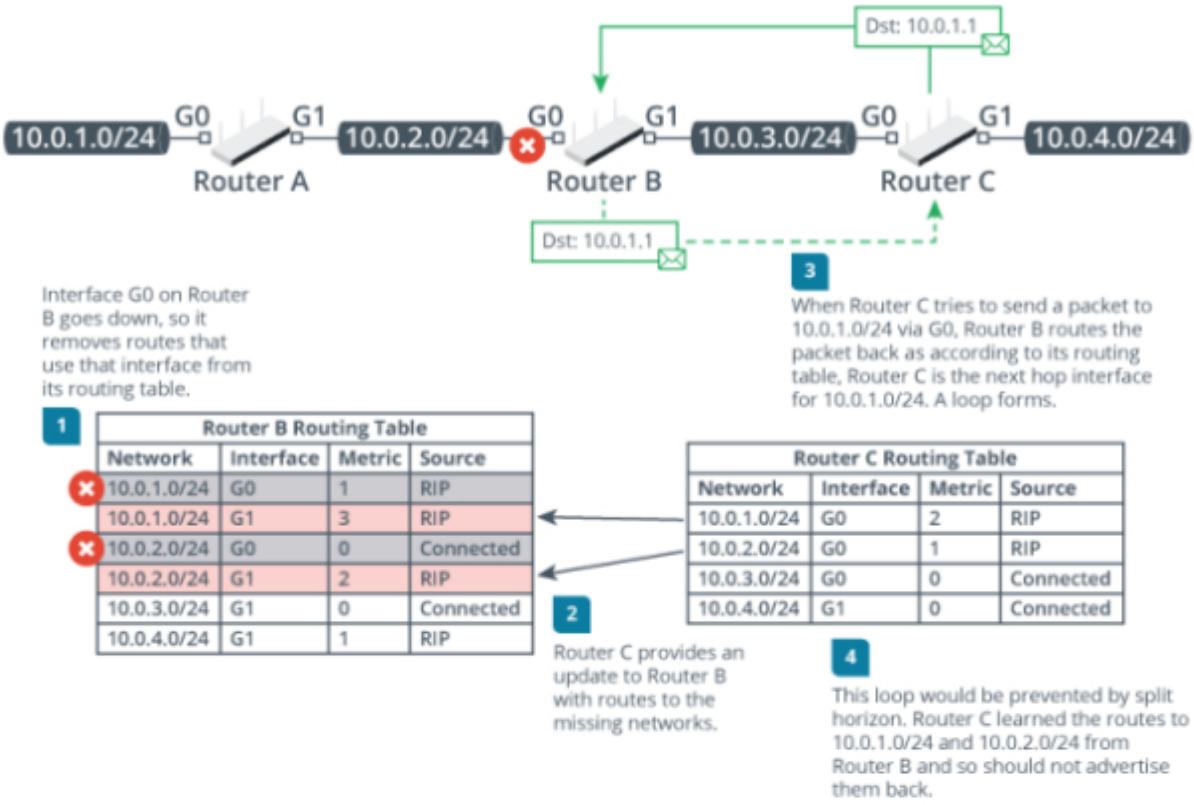
Jika Anda menduga ada masalah dengan konfigurasi router dan topologi jaringan, gunakan traceroute untuk mencoba mengidentifikasi di mana jalur jaringan gagal dan perintah rute atau tampilkan rute untuk menyelidiki tabel perutean sistem perantara pada titik di jalur tersebut.

Saat memeriksa tabel perutean, Anda dapat menggunakan show ip route wxyz untuk memeriksa keberadaan rute ke jaringan IP tertentu. Rute yang hilang mungkin muncul karena entri perutean statis yang diperlukan belum dimasukkan atau salah dimasukkan. Rute yang hilang juga dapat muncul karena router gagal berkomunikasi dengan tetangganya sehingga tidak menerima pembaruan protokol perutean. Melakukan tinjauan konfigurasi perangkat berarti memeriksa apakah konfigurasi yang berjalan sesuai dengan baseline yang didokumentasikan.

Anda mungkin mulai memecahkan masalah ini dengan melakukan ping ke node router yang bertetangga dengan sistem yang bermasalah untuk memeriksa konektivitas dasar. Jika ada jalur jaringan dan tetangga aktif, Anda akan menyelidiki konfigurasi protokol (mungkin ada masalah autentikasi atau parameter yang salah).

Routing Loop Issues

Routing loop terjadi ketika dua router menggunakan satu sama lain sebagai jalur ke jaringan. Paket-paket terjebak dalam lingkaran loop perutean sampai TTL berakhir. Salah satu gejala dari loop perutean potensial adalah bagi router untuk menghasilkan pesan kesalahan ICMP Time Exceeded.



routing loop dibuat antara router B dan C. (Gambar © 123RF.com.)

Protokol perutean menggunakan berbagai mekanisme untuk mencegah loop. Misalnya, protokol vektor jarak menggunakan mekanisme berikut:

- **Jumlah hop maksimum** -Jika biaya melebihi nilai tertentu (16 dalam RIP), jaringan dianggap tidak dapat dijangkau. Sebuah rute racun adalah salah satu yang diiklankan dengan jumlah hop 16. Ini dapat memberikan pemberitahuan kegagalan eksplisit ke router lain.
- **Holddown timer** -Jika sebuah node menyatakan jaringan tidak dapat dijangkau, tetangganya memulai holddown timer. Setiap pembaruan tentang rute yang diterima dari node lain akan dibuang selama durasi timer. Ini dirancang untuk memastikan bahwa semua node telah mengumpulkan informasi tentang jaringan yang tidak dapat dijangkau.
- **Split horizon** -Mencegah pembaruan perutean agar tidak disalin kembali ke sumbernya. Pada contoh di atas, ini akan mencegah router C mengirim pembaruan tentang rute ke router A melalui router B ke router B.

Protokol status tautan mencoba memastikan bahwa setiap node memiliki tampilan jaringan yang konsisten melalui pembaruan berkelanjutan dan tepat waktu yang membanjiri semua node dalam domain perutean. Loop dalam domain perutean status tautan biasanya menunjukkan bahwa pembaruan tidak disebarkan dengan benar.

Anda dapat menggunakan traceroute untuk mendiagnosis loop perutean dengan mencari alamat IP yang muncul beberapa kali di output.

Asymmetrical Routing Issues

Routing asimetris mengacu pada topologi di mana jalur kembali berbeda dengan jalur maju. Ini biasa terjadi di mana ada penyeimbang beban dan di mana perutean terjadi melalui beberapa jalur redundan di Internet atau internetwork kompleks lainnya. Perutean asimetris bermasalah di mana jalur kembali memiliki latensi yang jauh lebih tinggi daripada jalur maju atau di mana perbedaan antara jalur menyebabkan firewall stateful atau perangkat terjemahan alamat jaringan (NAT) menyaring atau menjatuhkan komunikasi. Jenis perangkat ini tidak boleh ditempatkan di tengah jaringan di mana jalur maju dan kembali bisa berbeda. Perutean asimetris yang bermasalah dapat disebabkan oleh rute statis atau dinamis yang tidak dikonfigurasi dengan benar.

Low Optical Link Budget Issues

Selain konfigurasi perutean, Anda juga harus mempertimbangkan masalah fisik dan tautan data saat memecahkan masalah perutean WAN dan pusat data. Salah satu masalah tersebut adalah konektivitas yang buruk di seluruh tautan serat optik.

Anggaran tautan optik , atau anggaran kerugian, adalah jumlah kerugian yang diderita oleh semua komponen di sepanjang jalur transmisi serat. Ini dihitung menggunakan parameter berikut:

- **Attenuation** -Ini adalah kerugian pada panjang kabel, berdasarkan jenis serat dan panjang gelombang yang digunakan. Mode tunggal memiliki kerugian hingga 0,4 dB/km, sedangkan multimode dapat dari 0,8 dB/km hingga 3 dB/km.
- **Connectors** -Setiap konektor di jalur mengalami kerugian, biasanya diasumsikan 0,75 dB.
- **Splices** - Sambungan tambahan dalam kabel dianggarkan sekitar 1 dB untuk mekanis dan 0,3 dB untuk fusi.

Biasanya, perkiraan anggaran kerugian dihitung saat merencanakan tautan. Tautan diuji saat penerapan menggunakan optical time domain reflectometer (OTDR) untuk mendapatkan nilai aktual. Perbedaan antara nilai-nilai ini dapat mengungkapkan kesalahan instalasi atau beberapa sumber kehilangan sinyal yang tidak terduga.

FOA memiliki kalkulator anggaran kerugian di thefoa.org/tech/ref/Loss_Budget/Loss_Budget.htm.

Anggaran kerugian harus lebih kecil dari anggaran daya. Anggaran daya dihitung dari daya pancar transceiver (Tx) dan sensitivitas penerima (Rx), yang keduanya biasanya diukur dalam

dB per miliwatt atau dBm. Misalnya, jika Tx adalah -8 dBm dan Rx adalah -15 dBm, maka anggaran dayanya adalah 7 dB.

dBm mengukur kekuatan sinyal terhadap nilai referensi, di mana 0 dBm adalah 1 miliwatt. Sebuah dBm negatif adalah tipikal dari transceiver Ethernet, yang menghasilkan kurang dari 1 mw.

Jika anggaran kerugian adalah 5 dB, margin antara anggaran daya dan anggaran kerugian akan menjadi 2 dB. Margin adalah faktor keamanan untuk memperhitungkan kondisi pemasangan yang kurang optimal (seperti tikungan atau tegangan), penuaan, perbaikan kerusakan yang tidak disengaja (sambungan tambahan), dan kinerja di bawah kondisi termal yang berbeda (suhu ekstrem dapat menyebabkan kerugian).

Jika margin antara daya pemancar dan anggaran tautan rendah, tautan cenderung tidak mencapai bandwidth yang diharapkan. Mungkin ada peluang untuk meningkatkan kinerja dengan sambungan yang lebih baik atau lebih sedikit, atau mungkin perlu menggunakan amplifier untuk meningkatkan sinyal. Kebanyakan tanaman outdoor akan dirancang dengan margin minimal 5 dB. Di pusat data di mana kondisinya kurang bervariasi, margin yang lebih rendah mungkin dapat diterima.

Modul 8

Menjelaskan Topologi dan Jenis Jaringan

Penjelasan Jenis dan Karakteristik Jaringan

- Pendahuluan: Menjelaskan Jenis dan Karakteristik Jaringan
  Jenis dan topologi jaringan menentukan skala dan aliran data melalui jaringan pada lapisan 1, 2, dan 3. Mengenal berbagai topologi sangat penting untuk merancang atau memecahkan masalah jaringan. Tidak peduli apa peran spesifik Anda dalam implementasi dan manajemen jaringan, Anda perlu memahami karakteristik topologi jaringan tempat Anda bekerja dan mengidentifikasi bagaimana topologi mempengaruhi kinerja jaringan dan pemecahan masalah.

- ***Client-Server versus Peer-to-Peer Networks***
  Sebuah jaringan terdiri dari node dan link. Node sistem perantara melakukan fungsi penerusan, sedangkan node sistem akhir adalah yang mengirim dan menerima lalu lintas data. Node sistem akhir dapat diklasifikasikan sebagai klien atau server:

- Server membuat aplikasi jaringan dan sumber daya tersedia untuk host lain.

- Seorang klien mengkonsumsi layanan yang disediakan oleh server.

  A ***client-server*** adalah jaringan di mana beberapa node, seperti PC, laptop, dan smartphone, sebagian besar bertindak sebagai klien. Server adalah komputer yang lebih kuat. Layanan dan sumber daya aplikasi disediakan, dikelola, dan diamankan secara terpusat.

  A ***peer-to-peer*** adalah jaringan di mana setiap sistem akhir bertindak sebagai klien dan server. Ini adalah model terdesentralisasi di mana penyediaan, manajemen, dan keamanan layanan dan data didistribusikan di sekitar jaringan.

  Jaringan bisnis dan perusahaan biasanya klien-server, sedangkan jaringan perumahan lebih sering peer-to-peer (atau workgroup). Namun, perhatikan bahwa dalam jaringan client-server, seringkali, node akan berfungsi sebagai klien dan server pada saat yang bersamaan. Misalnya, komputer yang menghosting aplikasi web bertindak sebagai server untuk klien browser tetapi itu sendiri adalah klien dari layanan database yang berjalan di komputer server lain. Ini adalah sifat jaringan yang dikelola secara terpusat yang benar-benar mendefinisikannya sebagai client-server.

- Jenis Jaringan
  Jenis jaringan terutama mengacu pada ukuran dan cakupannya. Ukuran jaringan dapat diukur sebagai jumlah node, sedangkan ruang lingkup mengacu pada area di mana node berbagi alamat jaringan yang sama didistribusikan.

- ***Local Area Networks***
  A local area network (LAN) menggambarkan jenis jaringan yang terbatas pada satu lokasi geografis. Dalam LAN, semua node dan segmen terhubung langsung dengan kabel atau teknologi nirkabel jarak pendek. Itu tidak memerlukan sistem telekomunikasi sewaan untuk berfungsi. Sebagian besar infrastruktur jaringan di LAN akan langsung dimiliki dan dikelola oleh satu organisasi. Beberapa contoh khas LAN meliputi:

  - Jaringan rumah/perumahan-dengan router Internet dan beberapa komputer, ditambah perangkat seluler, konsol game, dan printer.

  - Jaringan kantor kecil/kantor rumah (SOHO)-Jaringan berorientasi bisnis yang mungkin menggunakan server terpusat selain perangkat klien dan printer, tetapi sering kali masih menggunakan router/switch/titik akses Internet tunggal untuk menyediakan konektivitas.

  - Jaringan usaha kecil dan menengah (UKM)-Jaringan yang mendukung puluhan pengguna. Jaringan tersebut akan menggunakan kabel terstruktur dan beberapa switch dan router untuk menyediakan konektivitas.

  - Enterprise LANs-Jaringan yang lebih besar dengan ratusan atau ribuan server dan klien. Jaringan seperti itu akan membutuhkan beberapa peralatan switch dan router kelas perusahaan untuk mempertahankan tingkat kinerja. Istilah jaringan area kampus (CAN) kadang-kadang digunakan untuk LAN yang menjangkau beberapa gedung di dekatnya.

  - Pusat Data-Jaringan yang hanya menampung server dan penyimpanan, bukan perangkat klien pengguna akhir.

  Istilah jaringan area lokal nirkabel (WLAN) digunakan untuk LAN berbasis *Wi-Fi*. WLAN terbuka (publik) sering disebut sebagai hotspot.

- ***Wide Area Networks***
  A wide area network (WAN) adalah jaringan jaringan, dihubungkan oleh tautan jarak jauh. Sebuah WAN perusahaan yang khas akan menghubungkan situs kantor utama dengan beberapa situs kantor cabang, mungkin di negara yang berbeda. WAN dapat menghubungkan dua atau lebih LAN besar atau dapat digunakan untuk pekerja jarak jauh yang terhubung ke jaringan perusahaan melalui jaringan publik seperti Internet. WAN cenderung menggunakan perangkat dan tautan jaringan yang disewa, dioperasikan dan dikelola oleh penyedia layanan.

  Istilah *metropolitan area network* (MAN) kadang-kadang digunakan untuk sesuatu yang sedikit lebih kecil dari WAN: jaringan seluruh kota yang mencakup beberapa bangunan.

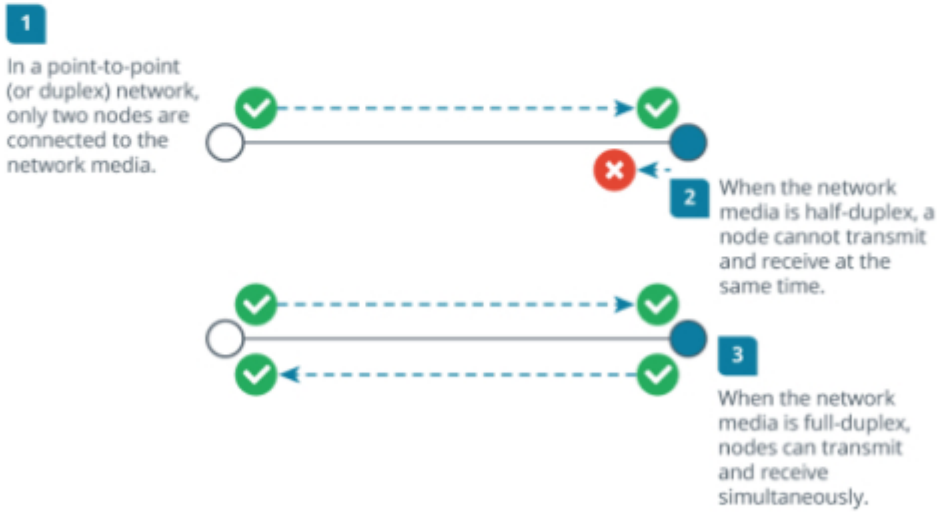
- ***Personal Area Networks***
  Istilah *personal area network* (PAN) dan *wireless PAN* (WPAN) telah mendapatkan beberapa mata uang selama beberapa tahun terakhir. Mereka merujuk pada fakta bahwa seseorang mungkin membuat hubungan jaringan jarak dekat antara berbagai perangkat, seperti smartphone, tablet, headset, dan printer. Karena fungsionalitas digital dan jaringan terus tertanam di semakin banyak objek sehari-hari, peralatan (*Internet of Things*), dan pakaian, penggunaan PAN hanya akan tumbuh.

- Topologi Jaringan
  Dimana jenis mendefinisikan ruang lingkup jaringan, topologi menggambarkan struktur fisik atau logis dari jaringan dalam hal node dan link.

  Topologi jaringan fisik menggambarkan penempatan node dan bagaimana mereka dihubungkan oleh media jaringan. Misalnya, dalam satu jaringan, node mungkin terhubung langsung melalui satu kabel; di jaringan lain, setiap node mungkin terhubung ke switch melalui kabel terpisah. Kedua jaringan ini memiliki topologi fisik yang berbeda.

  Topologi logis menggambarkan aliran data melalui jaringan. Misalnya, dengan topologi jaringan fisik yang berbeda yang dijelaskan sebelumnya, jika dalam setiap kasus node dapat mengirim pesan satu sama lain, topologi logisnya sama. Implementasi fisik yang berbeda (terhubung langsung melalui kabel versus terhubung ke sakelar yang sama) mencapai tata letak logis yang sama.

  Dalam jenis topologi yang paling sederhana, satu tautan dibuat antara dua node. Ini disebut tautan titik-ke-titik. Karena hanya dua perangkat yang berbagi koneksi, mereka dijamin memiliki tingkat bandwidth.

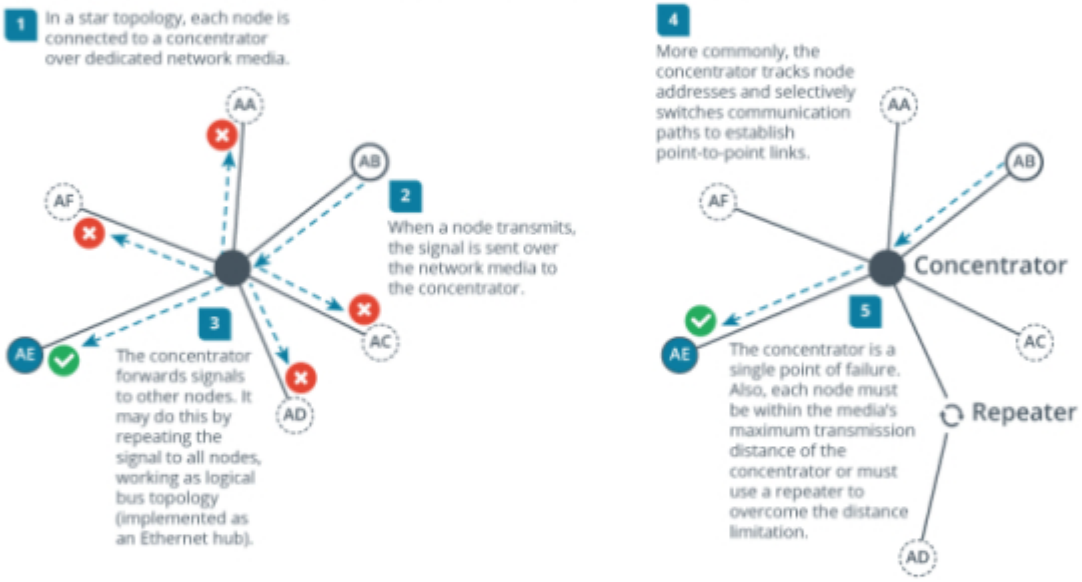


Topologi point-to-point fisik menggunakan jenis media yang berbeda untuk komunikasi half-duplex dan duplex.

Tautan point-to-point dapat berupa topologi fisik atau logis. Misalnya, pada WAN, dua router mungkin terhubung secara fisik melalui beberapa jaringan perantara dan perangkat fisik tetapi masih berbagi tautan point-to-point logis, di mana masing-masing hanya dapat menangani router lainnya. Dengan topologi fisik atau logika, hubungan 1:1 yang mendefinisikan link point-to-point.

- Topologi Bintang

  Dalam topologi star, setiap node titik akhir terhubung ke node penerusan pusat, seperti hub, switch, atau router. Node pusat menengahi komunikasi antara titik akhir. Topologi star merupakan topologi fisik yang paling banyak digunakan. Misalnya, jaringan SOHO tipikal didasarkan pada satu alat router Internet yang dapat dihubungkan oleh klien dengan kabel atau nirkabel. Topologi star mudah dikonfigurasi ulang dan mudah dipecahkan karena semua data melewati titik pusat, yang dapat digunakan untuk memantau dan mengelola jaringan. Kesalahan secara otomatis diisolasi ke media, node (kartu jaringan), atau hub, switch, atau router di pusat bintang.



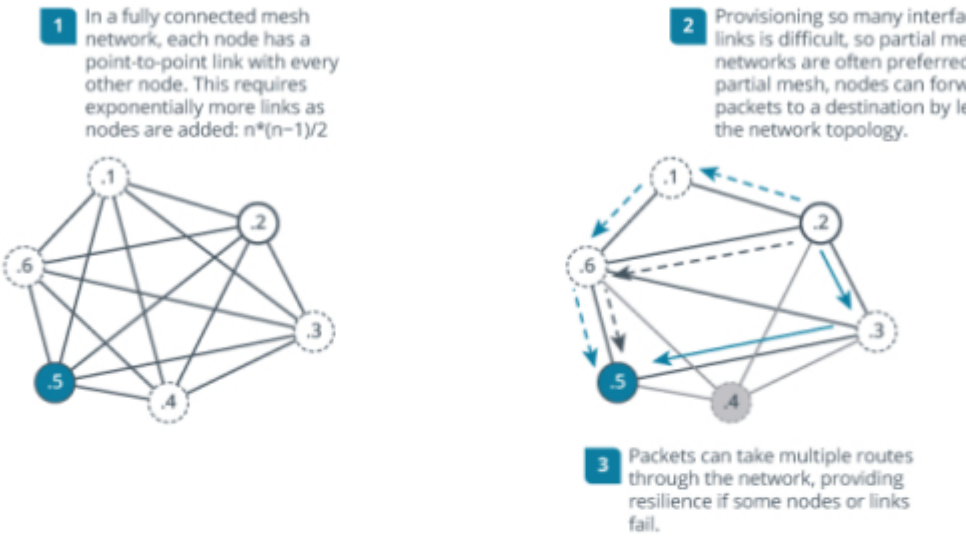
Topologi star menggunakan berbagai jenis konsentrator.

Anda mungkin juga menemukan topologi hub-and-spoke. Ini adalah tata letak yang sama dengan topologi bintang. Terminologi hub-and-spoke digunakan ketika berbicara tentang WAN dengan situs jarak jauh.

- Topologi Mesh

  Topologi mesh biasanya digunakan di WAN, terutama jaringan publik seperti Internet. Secara teori, jaringan mesh mensyaratkan bahwa setiap perangkat memiliki tautan point-to-point dengan setiap perangkat lain di jaringan (terhubung sepenuhnya). Namun, pendekatan ini biasanya tidak praktis. Jumlah link yang dibutuhkan oleh mesh penuh dinyatakan sebagai n (n -1)/2, di mana n adalah jumlah node. Misalnya, jaringan hanya empat node akan membutuhkan enam link, sedangkan jaringan 40 node akan

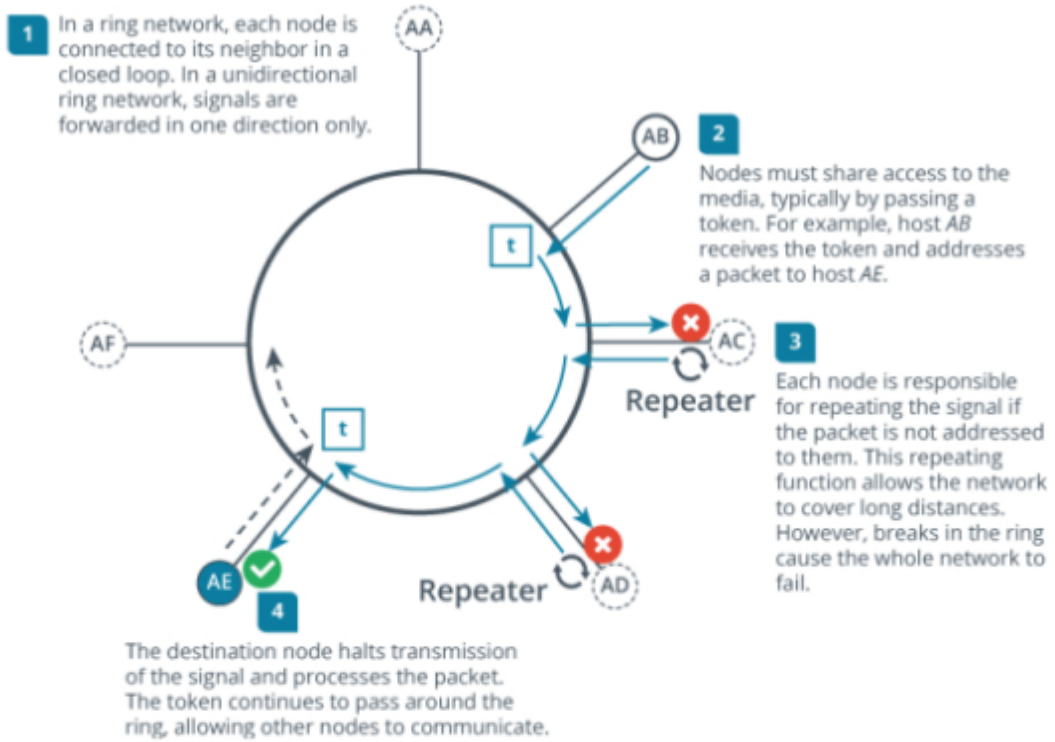
membutuhkan 780 link! Akibatnya, pendekatan hybrid sering digunakan, dengan hanya perangkat yang paling penting yang saling berhubungan dalam mesh, mungkin dengan link tambahan untuk toleransi kesalahan dan redundansi. Dalam hal ini, topologi disebut sebagai mesh parsial.



Contoh topologi mesh yang terhubung penuh dan parsial.

Jaringan mesh memberikan redundansi yang sangat baik, karena rute lain, melalui perangkat perantara, tersedia di antara lokasi jika terjadi kegagalan tautan.

- Topologi Cincin
  Dalam topologi ring fisik, setiap node dihubungkan ke tetangganya dalam loop tertutup. Sebuah node menerima transmisi dari tetangga hulunya dan meneruskannya ke tetangga hilirnya sampai transmisi mencapai tujuan yang diinginkan. Setiap node dapat meregenerasi transmisi, meningkatkan jangkauan potensial jaringan.

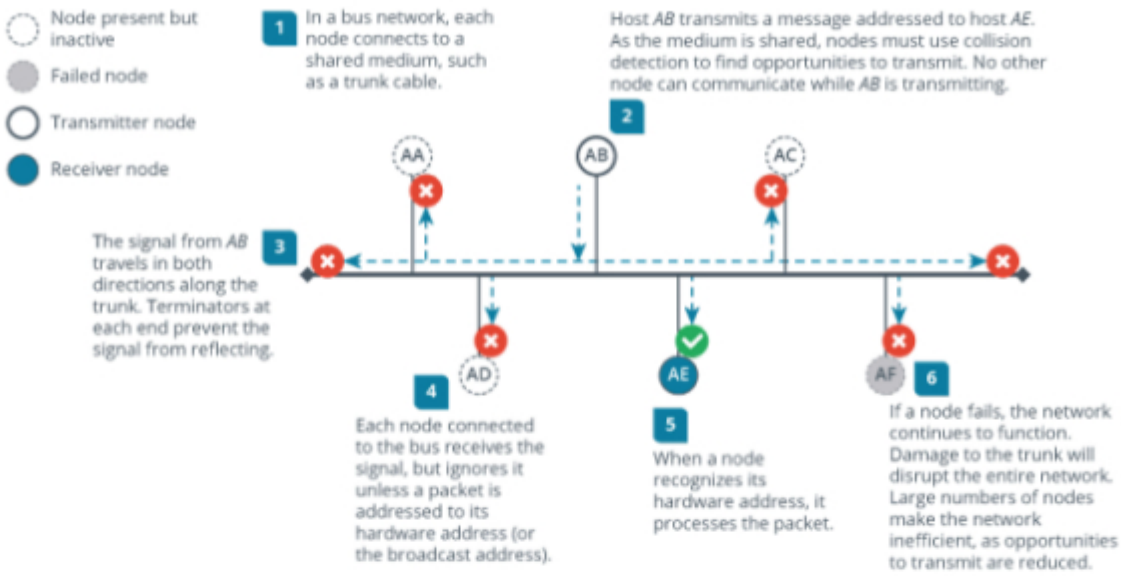


Topologi cincin.

Topologi ring fisik tidak lagi digunakan pada LAN, tetapi tetap menjadi fitur dari banyak WAN. Sistem dua cincin (cincin putar balik ganda) dapat digunakan untuk memberikan toleransi kesalahan. Dering ganda ini memungkinkan sistem untuk terus beroperasi jika terjadi pemutusan pada salah satu ring.

- Topologi Bus

  Topologi bus fisik dengan lebih dari dua node adalah topologi akses bersama, artinya semua node berbagi bandwidth media. Hanya satu node yang dapat aktif pada satu waktu, sehingga node harus bersaing untuk menempatkan sinyal pada media. Semua node terhubung langsung ke satu segmen kabel melalui kabel tap. Sebuah sinyal berjalan menuruni bus di kedua arah dari sumber dan diterima oleh semua node yang terhubung ke segmen tersebut. Bus diakhiri di kedua ujung kabel untuk menyerap sinyal ketika telah melewati semua perangkat yang terhubung.



Topologi bus fisik. (Images © 123RF.com.)

Jenis topologi bus fisik ini adalah dasar dari jaringan Ethernet paling awal tetapi tidak lagi digunakan secara luas. Jaringan bus relatif sulit untuk dikonfigurasi ulang (menambah atau menghapus node dapat mengganggu seluruh jaringan), memberlakukan batasan pada jumlah maksimum node pada segmen kabel, dan sulit untuk memecahkan masalah (kesalahan kabel dapat terjadi di mana saja pada segmen kabel). Mungkin yang paling penting, kesalahan di mana saja di kabel berarti semua node tidak dapat berkomunikasi.

Tips: Jaringan bus memang memungkinkan kabel untuk dihubungkan menggunakan perangkat yang disebut repeater. Dua panjang kabel yang dihubungkan oleh repeater dianggap sebagai satu panjang kabel untuk tujuan topologi bus. Repeater adalah perangkat pasif dan tidak dianggap sebagai node jaringan seperti halnya switch atau router.

Sebuah topologi bus logis adalah salah satu di mana node menerima data yang dikirimkan semua pada waktu yang sama, terlepas dari tata letak kabel fisik jaringan. Karena media transmisi digunakan bersama, hanya satu node yang dapat mengirimkan pada satu waktu. Node dalam segmen bus logis yang sama berada dalam domain tabrakan yang sama. Ketika Ethernet digunakan dengan perangkat hub warisan, ini dapat digambarkan sebagai topologi bus logika bintang fisik

- Topologi Hibrida
-
- Topologi hybrid adalah segala sesuatu yang menggunakan campuran point-to-point, star, mesh, ring, dan topologi fisik dan/atau logika bus. Sebagaimana dicatat, hub Ethernet menetapkan topologi bus logis, tetapi topologi fisik adalah bintang. Topologi

warisan umum lainnya adalah cincin berkabel bintang, di mana node dalam cincin dihubungkan ke unit akses multistasiun pusat (MAU) daripada ke tetangganya. MAU mengimplementasikan ring logis dan menangani token passing.

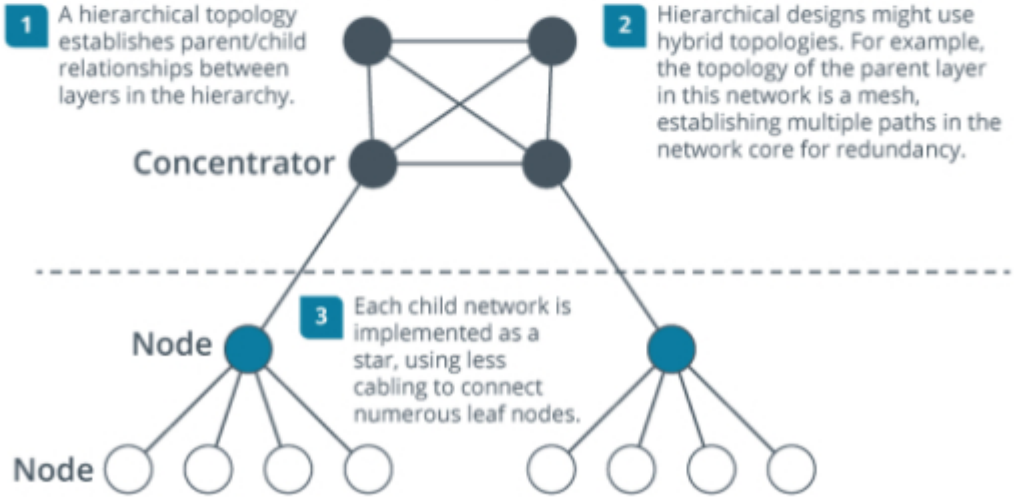
Pada jaringan modern, topologi hybrid sering digunakan untuk menerapkan redundansi dan toleransi kesalahan atau untuk menghubungkan situs di WAN:

- Jaringan star-corporate hierarki sering dirancang dalam hierarki, juga dikenal sebagai topologi pohon. Ini dapat dikombinasikan dengan topologi bintang untuk mengimplementasikan setiap node di pohon secara keseluruhan. Tautan antara node di pohon disebut sebagai tulang punggung atau batang karena mereka mengumpulkan dan mendistribusikan lalu lintas dari beberapa area jaringan yang berbeda.

- Hirarki star-mesh-Atau, node di bagian atas hierarki dapat dikonfigurasi dalam mesh parsial atau penuh untuk redundansi. Sakelar yang lebih rendah dalam hierarki membentuk topologi bintang yang menghubungkan sistem akhir ke jaringan.

- Star of stars-Sebuah WAN dapat dikonfigurasi sebagai hub-and-spoke antara kantor pusat dan kantor cabang, dengan setiap situs menerapkan topologi bintang untuk menghubungkan sistem akhir. Ini juga disebut sebagai topologi kepingan salju.

- Bintang dengan cincin Sebagai alternatif, topologi cincin dapat digunakan untuk menghubungkan situs yang terpisah secara geografis, dengan setiap situs menerapkan topologi bintang untuk menghubungkan sistem akhir.



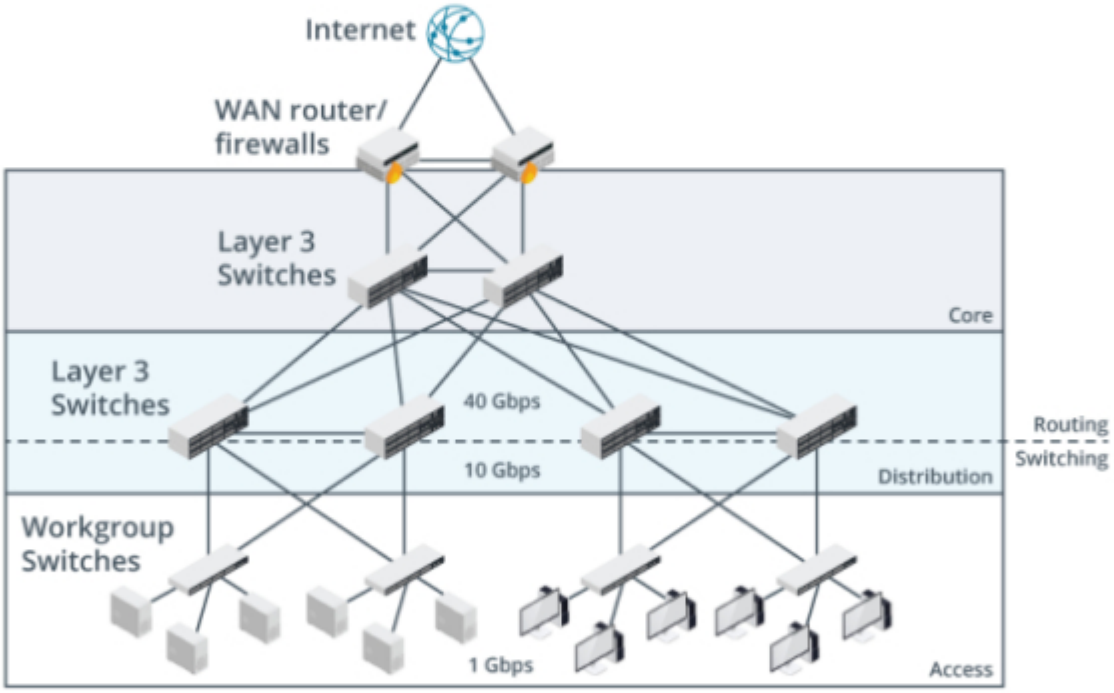
Contoh topologi hibrid hierarkis di mana jaringan mesh mendistribusikan lalu lintas antara beberapa jaringan bintang.

Explain Tiered Switching Architecture

- Pendahuluan: Jelaskan Arsitektur Switching Berjenjang
  Ethernet, switching, dan perutean IP adalah teknologi utama yang digunakan untuk mengimplementasikan jaringan kabel lokal. Namun, ada banyak jenis dan ukuran jaringan, dan berbagai cara merancang kabel dan penerusan agar sesuai dengan kebutuhan organisasi dan anggaran besar dan kecil. Meskipun Anda mungkin tidak bertanggung jawab atas desain jaringan pada tahap karir Anda ini, penting bagi Anda untuk dapat mengidentifikasi komponen dan keuntungan dari hierarki jaringan berjenjang.

- Hirarki Jaringan Tiga Tingkat
  Model hierarki memecah desain jaringan yang besar dan kompleks menjadi bagian-bagian yang lebih kecil berdasarkan fungsi yang dilakukan. Setiap fungsi dapat dinilai oleh perancang jaringan untuk mengidentifikasi perangkat keras dan perangkat lunak yang paling efisien yang digunakan untuk mengimplementasikannya.

  Sebagai contoh praktis dari model jenis ini, banyak jaringan kantor perusahaan mengikuti prinsip desain Cisco untuk hirarki tiga tingkat: akses, distribusi, dan inti.



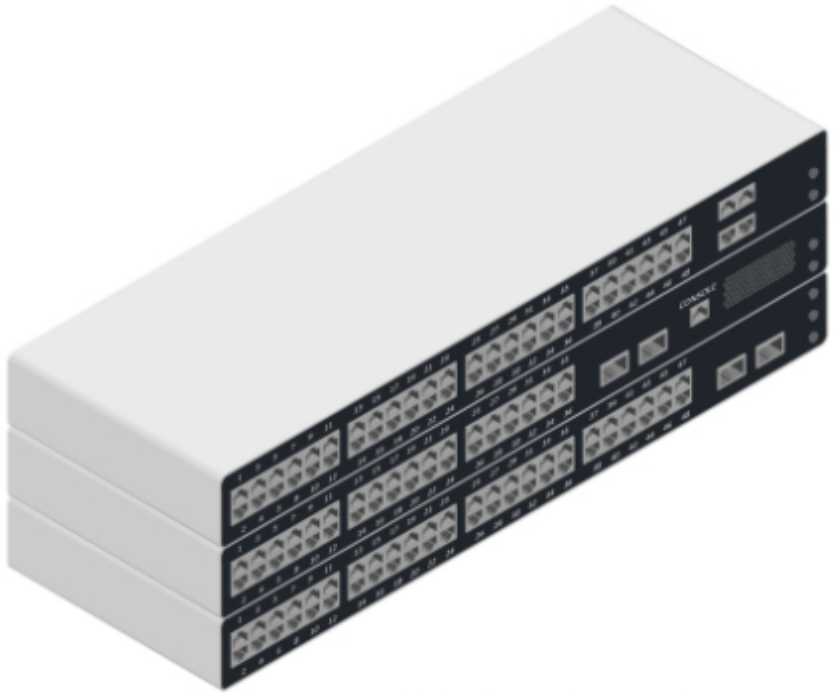
Lapisan inti, distribusi, dan akses dalam arsitektur jaringan tiga tingkat. (Images © 123RF.com.)

- Akses/Lapisan Tepi
  Lapisan akses atau tepi memungkinkan perangkat pengguna akhir, seperti komputer, printer, dan ponsel cerdas untuk terhubung ke jaringan. Lapisan akses diimplementasikan untuk setiap situs menggunakan kabel terstruktur dan port dinding

untuk akses kabel dan titik akses untuk akses nirkabel. Keduanya akhirnya terhubung ke switch workgroup. Switch yang digunakan untuk melayani lapisan akses mungkin juga disebut sebagai switch LAN atau sakelar data. Sistem akhir terhubung ke switch di lapisan akses/tepi dalam topologi bintang. Tidak ada hubungan langsung antara sakelar akses.

- Lapisan Distribusi/Agregasi
  Distribusi atau lapisan agregasi menyediakan interkoneksi toleransi kesalahan antara blok akses yang berbeda dan baik inti atau blok distribusi lainnya. Setiap switch akses memiliki tautan mesh penuh atau sebagian ke setiap router atau sakelar lapisan 3 di blok lapisan distribusinya. Lapisan distribusi sering digunakan untuk mengimplementasikan kebijakan lalu lintas, seperti batas perutean, penyaringan, atau *quality of service* (QoS).

- Switch berkemampuan lapisan 3 yang digunakan untuk mengimplementasikan lapisan distribusi/agregasi memiliki kemampuan yang berbeda dengan lapisan 2 hanya sakelar kelompok kerja yang digunakan di tingkat akses. Alih-alih port akses 1 Gbps dan port uplink 10 Gbps, seperti tipikal dari sakelar kelompok kerja, antarmuka dasar pada switch agregasi adalah 10 Gbps dan port uplink/backbone akan menjadi 40 Gbps (atau mungkin 40 Gbps/100 Gbps). Switch Layer 3 bekerja berdasarkan prinsip "rute sekali, alihkan banyak," yang berarti bahwa begitu sebuah rute ditemukan, rute tersebut di-cache dengan alamat MAC tujuan dan komunikasi selanjutnya dialihkan tanpa menjalankan pencarian perutean. Sementara router menggunakan prosesor generik dan firmware untuk memproses paket yang masuk, switch layer 3 menggunakan *application-specific integrated circuit* (ASIC). Ini dapat berdampak pada kinerja relatif kedua jenis perangkat. Switch Layer 3 bisa jauh lebih cepat, tetapi tidak selalu fleksibel. Switch Layer 3 biasanya tidak dapat melakukan perutean WAN dan hanya bekerja dengan protokol perutean interior. Seringkali switch layer 3 hanya mendukung Ethernet.



Contoh switch inti/distribusi. (Image © 123RF.com.)

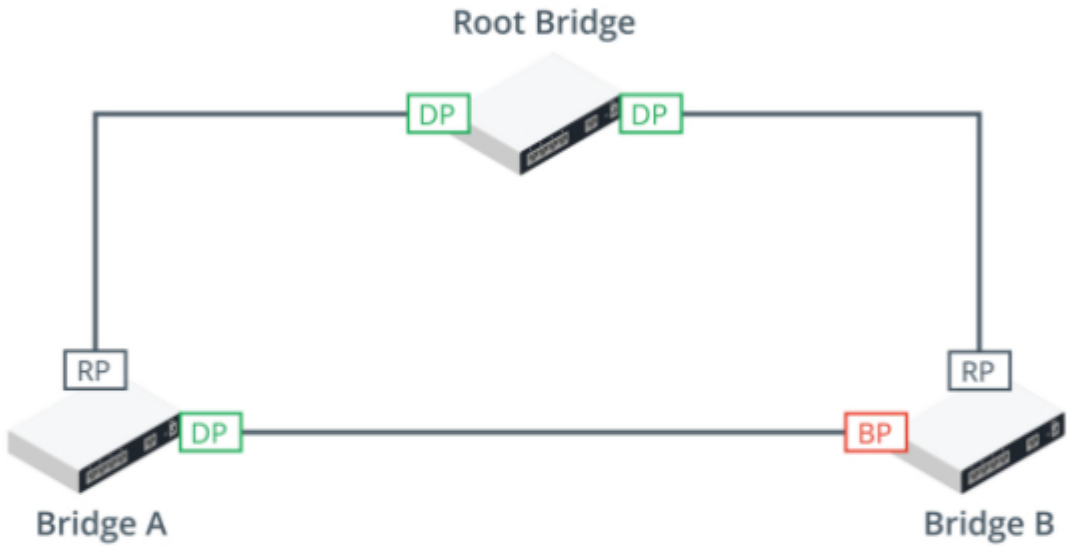
- Lapisan Inti
  Lapisan inti menyediakan tulang punggung jaringan yang sangat tersedia. Perangkat seperti komputer klien dan server tidak boleh dipasang langsung ke inti. Tujuannya harus tetap sederhana: menyediakan jalur lalu lintas yang berlebihan agar data terus mengalir di sekitar lapisan akses dan distribusi jaringan. Router atau sakelar lapisan 3 di lapisan inti membentuk topologi mesh penuh dengan sakelar di blok lapisan distribusi.

  Tips: Dalam model inti dua tingkat atau runtuh, inti harus diimplementasikan sebagai mesh penuh. Ini tidak praktis jika ada sejumlah besar sakelar inti.

- Spanning Tree Protocol
  Model jaringan tiga tingkat memanfaatkan topologi mesh atau mesh parsial untuk mengimplementasikan tautan redundan. Beberapa jalur adalah bagian dari desain jaringan yang baik karena meningkatkan ketahanan; jika satu link gagal, maka jaringan dapat tetap beroperasi dengan meneruskan frame melalui jalur yang berbeda. Namun, sebagai protokol lapisan 2, Ethernet tidak memiliki konsep waktu untuk hidup, sehingga lalu lintas siaran lapisan 2 dapat terus berulang melalui jaringan dengan banyak jalur tanpa batas.

  Spanning Tree Protocol (STP) adalah sarana untuk jembatan atau switch untuk mengatur diri mereka sendiri ke dalam hierarki. Sakelar di bagian atas hierarki adalah root. Switch dengan ID terendah, yang terdiri dari nilai prioritas dan alamat MAC, akan dipilih sebagai root.

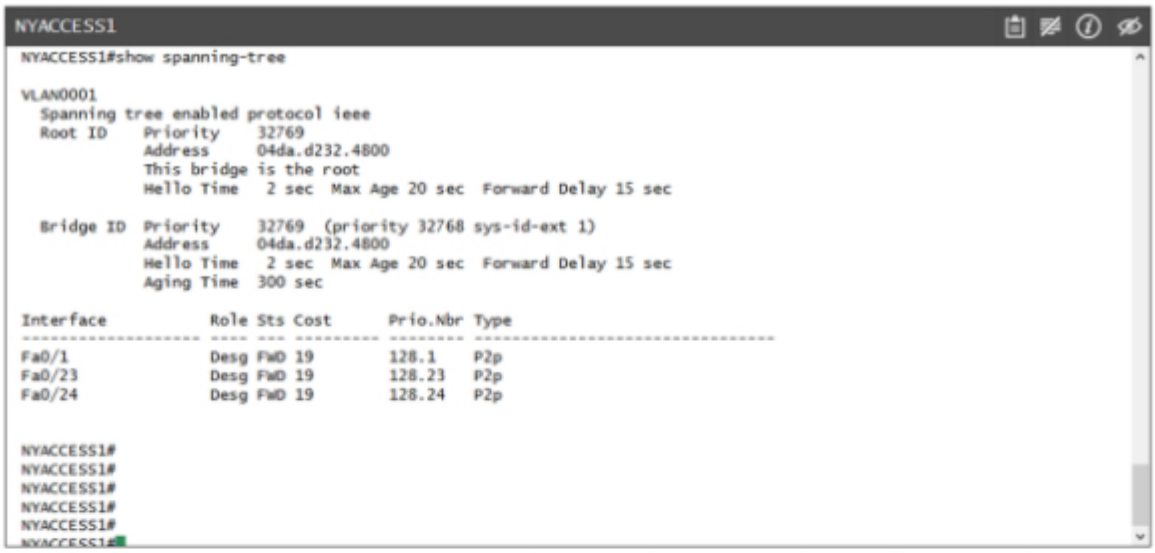
Setiap switch kemudian menentukan jalur terpendek ke jembatan akar dengan bertukar informasi dengan switch lain. Informasi STP ini dikemas sebagai bridge protocol data unit (BPDU). Port yang meneruskan "naik" ke root, mungkin melalui switch perantara, diidentifikasi sebagai port root. Port yang dapat meneruskan lalu lintas "turun" melalui jaringan dengan biaya paling rendah diidentifikasi sebagai port yang ditunjuk. Port yang akan membuat loop diidentifikasi sebagai port yang memblokir atau tidak ditunjuk. Selanjutnya, jembatan bertukar Pemberitahuan Perubahan Topologi jika perangkat ditambahkan atau dihapus, memungkinkan mereka untuk mengubah status port penerusan/pemblokiran dengan tepat.



Spanning tree configuration. (Images © 123RF.com.)

Gambar ini menunjukkan konfigurasi minimum yang diperlukan untuk mencegah loop dalam jaringan dengan tiga jembatan atau sakelar. Jembatan akar memiliki dua designated ports (DP) yang terhubung ke Jembatan A dan Jembatan B. Jembatan A dan B keduanya memiliki root ports (RP) yang terhubung kembali ke antarmuka di jembatan akar. Jembatan A dan B juga memiliki koneksi langsung satu sama lain. Di Jembatan A, antarmuka ini aktif dan lalu lintas untuk Jembatan B dapat diteruskan langsung di atasnya. Di Jembatan B, antarmuka diblokir (BP) untuk mencegah loop, dan lalu lintas untuk Jembatan A harus diteruskan melalui jembatan akar.

- Spanning Tree Protocol Configuration
  Jika switch mendukung STP (tidak semua mendukung), switch itu harus beroperasi secara default tanpa konfigurasi. Administrator dapat (dan harus) menentukan nilai prioritas untuk membuat pilihan satu switch sebagai root di atas yang lain lebih mungkin. Root biasanya akan menjadi bagian dari backbone bandwidth tinggi atau grup switch inti; kinerja akan menurun jika sakelar pada segmen bandwidth rendah menjadi root.



Viewing spanning tree configuration on a Cisco switch. (Image © and Courtesy of Cisco Systems, Inc. Unauthorized use not permitted.)

- Tabel berikut menunjukkan status berbeda yang dapat digunakan oleh port.

State	Forwards Frames?	Learns MACs?	Notes
Blocking	No	No	Drops all frames other than BPDUs.
Listening	No	No	Port is listening for BPDUs to detect loops.
Learning	No	Yes	The port discovers the topology of the network and builds the MAC address table.
Forwarding	Yes	Yes	The port works as normal.
Disabled	No	No	The port has been disabled by the administrator.

Ketika semua port pada semua switch berada dalam status penerusan atau pemblokiran, jaringan konvergensi. Ketika jaringan tidak konvergen, tidak ada komunikasi yang dapat terjadi. Di bawah standar 802.1D asli, ini membuat jaringan tidak tersedia untuk waktu yang lama-puluhan detik-selama perubahan konfigurasi. STP sekarang lebih mungkin diimplementasikan sebagai 802.1D-2004/802.1w atau Rapid STP (RSTP). Versi cepat membuat pemadaman beberapa detik atau kurang. Di RSTP, status pemblokiran, mendengarkan, dan dinonaktifkan digabungkan ke dalam status membuang.

- Switching Loop and Broadcast Storm Issues
  Loop switching adalah tempat frame yang dibanjiri mengedarkan jaringan secara terus-menerus. Karena switch membanjiri siaran, seperti permintaan ARP atau DHCP, keluar dari semua port, frame ini akan turun satu tautan ke switch berikutnya, yang akan mengirim siaran kembali ke tautan yang berlebihan, dan kembali ke switch asal. Saat ini berulang, switch mulai melihat alamat MAC sumber yang terkait dengan beberapa port

dan menghapus pemetaan tabel alamat MAC, yang menyebabkan mereka mulai membanjiri lalu lintas unicast juga.

-

Tanpa intervensi, loop ini akan berlanjut tanpa batas, menyebabkan badai siaran. Badai siaran akan menyebabkan pemanfaatan jaringan mendekati kapasitas maksimum, dan pemanfaatan CPU dari sakelar melonjak hingga 80 persen atau lebih. Ini membuat segmen yang diaktifkan secara efektif tidak dapat digunakan sampai badai siaran berhenti. Badai siaran dapat dengan cepat menghabiskan semua bandwidth tautan dan merusak peralatan jaringan.

Jika ada loop, spanning tree harus menutup port. Ini akan mengisolasi masalah ke segmen jaringan. Periksa port fisik yang sesuai dengan antarmuka yang dinonaktifkan untuk koneksi berulang. Pada panel patch, ini bisa berarti kabel patch yang menghubungkan dua port pada switch yang sama. Di lantai kantor, itu bisa berarti kabel tambalan di antara dua port dinding. Periksa switch untuk peristiwa log yang terkait dengan pengepakan alamat MAC.

Jika badai siaran terjadi di jaringan di mana STP sudah diaktifkan, Anda harus menyelidiki kemungkinan penyebab berikut:

- Pastikan versi STP yang kompatibel diaktifkan di semua switch..

- Verifikasi konfigurasi fisik segmen yang menggunakan peralatan lama, seperti hub Ethernet.

- Selidiki perangkat jaringan di lingkungan pengguna dan verifikasi bahwa mereka tidak terhubung sebagai bagian dari loop. Sumber masalah yang umum termasuk switch desktop yang tidak dikelola dan handset VoIP.

Explain Virtual LANs

- Pendahuluan: Jelaskan LAN Virtual
  Sebagian besar jaringan menggunakan LAN virtual (VLAN), baik untuk meningkatkan keamanan jaringan dan kinerja jaringan, sehingga konsep ini penting untuk Anda pahami. Dalam topik ini, Anda akan mengidentifikasi manfaat segmentasi jaringan dan karakteristik serta fungsi VLAN.

- ID dan Keanggotaan LAN Virtual
  Pada lapisan data link dan jaringan, segmen adalah sekelompok host dalam domain siaran yang sama. Pada lapisan jaringan, grup ini diidentifikasi sebagai jaringan IP atau sebagai subnet dalam jaringan IP. Pada lapisan tautan data, domain siaran dapat dibuat dengan menghubungkan host ke switch tidak terkelola yang sama. Namun, pendekatan berbasis perangkat keras ini tidak fleksibel, jadi sakelar yang dikelola memungkinkan konfigurasi LAN virtual (VLAN) untuk mengisolasi port ke domain siaran yang terpisah.

Tips: Jika VLAN berisi beberapa jaringan atau subnet IP, node akan menerima lalu lintas siaran untuk semua subnet. Namun, ini akan menjadi konfigurasi yang sangat kompleks. Biasanya, jaringan akan dirancang dengan pemetaan 1:1 antara VLAN dan subnet.

Menerapkan VLAN dapat mengurangi lalu lintas siaran ketika jaringan telah berkembang melampaui sejumlah host atau pengguna tertentu. Selain mengurangi dampak lalu lintas siaran, dari sudut pandang keamanan, setiap VLAN dapat mewakili zona terpisah. VLAN juga digunakan untuk memisahkan node berdasarkan jenis lalu lintas dan kebutuhan Kualitas Layanan. Misalnya, adalah hal yang biasa untuk menempatkan semua handset VoIP pada VLAN suara untuk meminimalkan gangguan yang datang dari node yang mengirim email atau mengunduh file besar di jaringan yang sama. Sakelar dan router kemudian dapat dikonfigurasi untuk memberikan prioritas VLAN VoIP di atas VLAN data biasa.

VLAN dengan ID 1 disebut sebagai VLAN default. Kecuali dikonfigurasi secara berbeda, semua port pada switch default berada di VLAN 1.

Cara paling sederhana untuk menetapkan node ke VLAN adalah dengan mengkonfigurasi antarmuka port pada switch dengan ID VLAN dalam kisaran 2 hingga 4.094. Misalnya, dari antarmuka manajemen switch , port 1 hingga 10 dapat dikonfigurasi sebagai VLAN dengan ID 10 dan port 11 hingga 20 dapat ditetapkan ke VLAN 20. Host A yang terhubung ke port 2 akan berada di VLAN 10, dan host B terhubung ke port 12 akan berada di VLAN 20. Host A dan Host B tidak akan dapat berkomunikasi secara langsung, meskipun mereka terhubung ke switch yang sama. Setiap VLAN biasanya dikonfigurasi dengan alamat subnet dan rentang alamat IP-nya sendiri. Komunikasi antara VLAN harus melalui router IP atau switch yang mampu layer 3.

```
interface swp5
  bridge-access 100

interface swp6
  bridge-access 100

interface swp7
  bridge-access 100

interface swp8
  bridge-access 100

interface swp9
  bridge-access 200

interface swp10
  bridge-access 200

interface swp11
  bridge-access 200

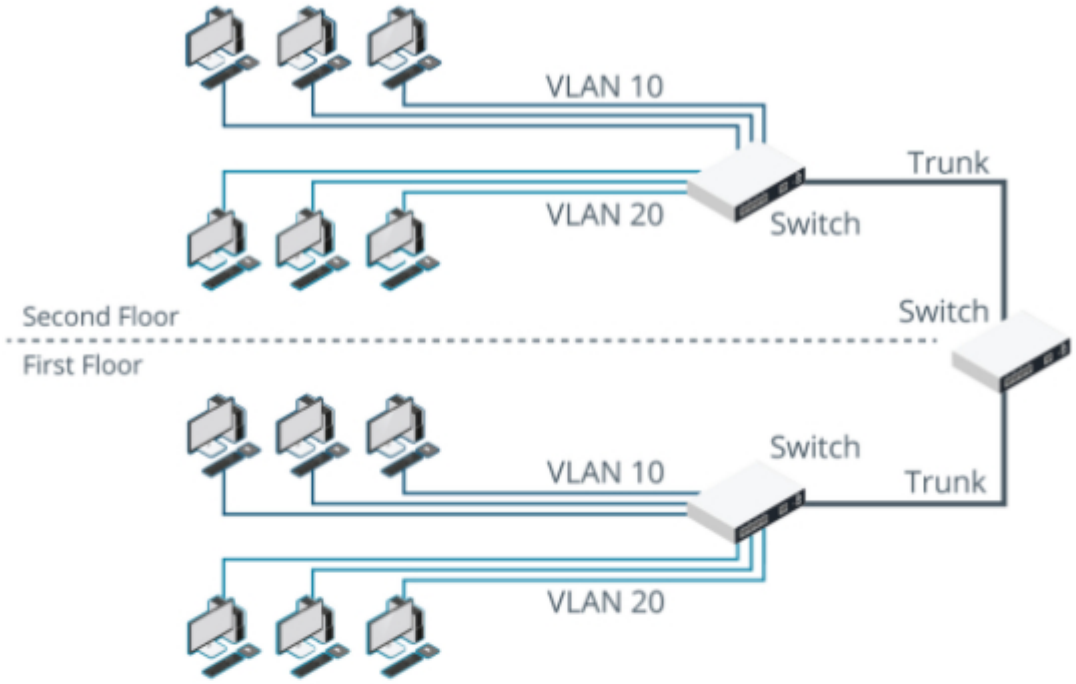
interface swp12
  bridge-access 200

interface bridge
  bridge-ports swp5 swp6 swp7 swp8 swp9 swp10 swp11 swp12
  bridge-vids 10 100 200
  bridge-vlan-aware yes
```

Output switch Cumulus VX menunjukkan port switch swp 5-8 yang dikonfigurasi dalam VLAN 100 dan port 9-12 di VLAN 200.

Jenis penugasan berbasis port ini digambarkan sebagai VLAN statis. Node atau host juga dapat ditetapkan ke VLAN dinamis menggunakan beberapa fitur host, seperti alamat MAC atau kredensial otentikasi yang diberikan oleh pengguna.

- Trunking dan IEEE 802.1Q
  Pada jaringan besar, satu switch tidak akan menyediakan port yang cukup untuk semua host yang perlu terhubung ke jaringan. Ini berarti bahwa beberapa switch harus saling berhubungan untuk membangun struktur jaringan. Beberapa switch juga dapat digunakan untuk menyediakan tautan yang berlebihan. Interkoneksi antara switch disebut sebagai trunks. Salah satu port pada setiap switch akan dikonfigurasi sebagai port trunk untuk tujuan ini.



VLAN trunk link. (Images © 123RF.com.)

Ketika frame yang ditujukan untuk VLAN yang berbeda diangkut melintasi trunk, VLAN ID (VID) dari setiap frame harus dipertahankan agar switch penerima dapat meneruskannya dengan benar. VID biasanya ditentukan oleh standar IEEE 802.1Q. Di bawah 802.1Q, lalu lintas per-VLAN diidentifikasi oleh tag yang dimasukkan dalam bingkai Ethernet antara bidang Alamat Sumber dan EtherType. Tag berisi informasi tentang VID (dari 1 hingga 4.094) dan prioritas (digunakan untuk fungsi QoS). Nilai EtherType diatur untuk mengidentifikasi frame sebagai 802.1Q.



Construction of an 802.1Q (VLAN tagged) Ethernet frame.

- Port yang Ditandai dan Tidak Ditandai
  Jika port switch hanya akan berpartisipasi dalam satu VLAN, port tersebut dapat dikonfigurasi sebagai tidak ditandai. Ini juga disebut sebagai port akses atau port host. Port yang tidak ditandai/akses menggunakan logika penandaan port berikut:

  - Jika sebuah frame dialamatkan ke port di VLAN yang sama pada switch yang sama, tidak ada tag yang perlu ditambahkan ke frame.

- Jika frame perlu diangkut melalui link trunk, switch menambahkan tag 802.1Q yang relevan untuk mengidentifikasi VLAN, dan kemudian meneruskan frame melalui port trunk.

- Jika switch menerima bingkai yang diberi tag 802.1Q pada port akses, ia akan menghapus tag sebelum meneruskannya.

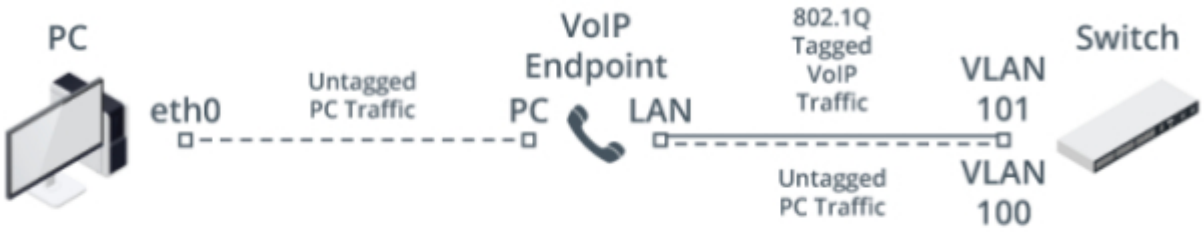
Sebaliknya, port yang diberi tag biasanya adalah port yang beroperasi sebagai trunk; yaitu, mampu mengangkut lalu lintas yang ditujukan ke beberapa VLAN menggunakan format bingkai 802.1Q. Sebuah trunk dapat digunakan untuk menghubungkan switch atau untuk menghubungkan switch ke router. Dalam beberapa keadaan, host yang terpasang ke port mungkin perlu dikonfigurasi untuk menggunakan beberapa VLAN dan perlu dilampirkan ke port trunk, bukan port akses. Pertimbangkan host virtualisasi dengan beberapa sistem operasi tamu. Server virtual mungkin perlu dikonfigurasi untuk menggunakan VLAN yang berbeda.

- VLAN suara
  Voice over IP (VoIP) mentransmisikan lalu lintas suara sebagai paket data, bukan melalui jalur transmisi berbasis sirkuit. Persyaratan bandwidth dan latensi dari lalu lintas suara berarti sering kali perlu memprioritaskannya di atas jenis paket data lainnya. Ini dapat dicapai dengan menggunakan VLAN khusus untuk lalu lintas suara. Namun, dalam banyak kasus, VoIP telah diimplementasikan ke dalam infrastruktur jaringan yang awalnya dirancang hanya untuk komputer desktop dan laptop, dengan jumlah port akses jaringan fisik yang terbatas.

  Untuk mengakomodasi kurangnya port dinding khusus untuk handset, sebagian besar titik akhir VoIP menghubungkan switch tertanam hanya dengan dua port eksternal. Handset terhubung melalui port uplink ke port dinding dan melalui kabel terstruktur ke switch akses. PC atau laptop terhubung ke handset melalui port lain. Handset meneruskan lalu lintas data dari PC ke switch akses sebagai bingkai yang tidak ditandai. Handset mengirimkan lalu lintas suara melalui tautan fisik yang sama tetapi menggunakan bingkai yang diberi tag 802.1Q.

  Biasanya, untuk antarmuka sakelar untuk memproses bingkai yang diberi tag, itu harus dikonfigurasi sebagai port trunk. Ini menambah banyak kerumitan konfigurasi, sehingga sebagian besar sakelar sekarang mendukung konsep suara atau VLAN tambahan untuk membedakan lalu lintas PC dan VoIP tanpa harus mengkonfigurasi trunk. Dalam contoh berikut, konfigurasi antarmuka menetapkan lalu lintas dari PC ke VLAN 100 dan lalu lintas suara ke VLAN 101:

```
interface GigabitEthernet0/0
switchport mode access
switchport access vlan 100
switchport voice vlan 101
```



Berbagi satu port dinding fisik antara PC dan handset VoIP. Konfigurasi antarmuka handset dan switch memungkinkan lalu lintas VoIP ditetapkan ke VLAN yang berbeda dari lalu lintas data PC. (Images © 123RF.com.)

Switch hanya akan menerima bingkai yang ditandai yang cocok dengan ID VLAN suara yang dikonfigurasi. Untuk menghindari keharusan mengkonfigurasi ini secara manual, ID VLAN suara dan parameter konfigurasi lainnya dapat dikomunikasikan ke handset menggunakan protokol seperti *Cisco Discovery Protocol* (CDP).

Modul 9
COMPARE AND CONTRAST TRANSPORT PROTOCOL

Pendahuluan: Bandingkan dan Kontraskan Protokol Transportasi
Anda telah melihat bagaimana IP menyediakan pengalamatan dan pengiriman pada lapisan 3 model OSI. Pada lapisan 4, paket protokol TCP/IP juga mendefinisikan bagaimana aplikasi yang berbeda pada host yang terpisah membangun koneksi dan melacak komunikasi. Memahami bagaimana protokol aplikasi menggunakan port untuk membuat koneksi sangat penting untuk dapat mengonfigurasi dan mendukung layanan jaringan.

Port dan Koneksi Lapisan Transportasi
Pada Layer 3, IP menyediakan fungsionalitas pengalamatan dan perutean untuk internetwork. Protokol pada lapisan Transport (Layer 4) berkaitan dengan pengiriman data aplikasi multipleks.

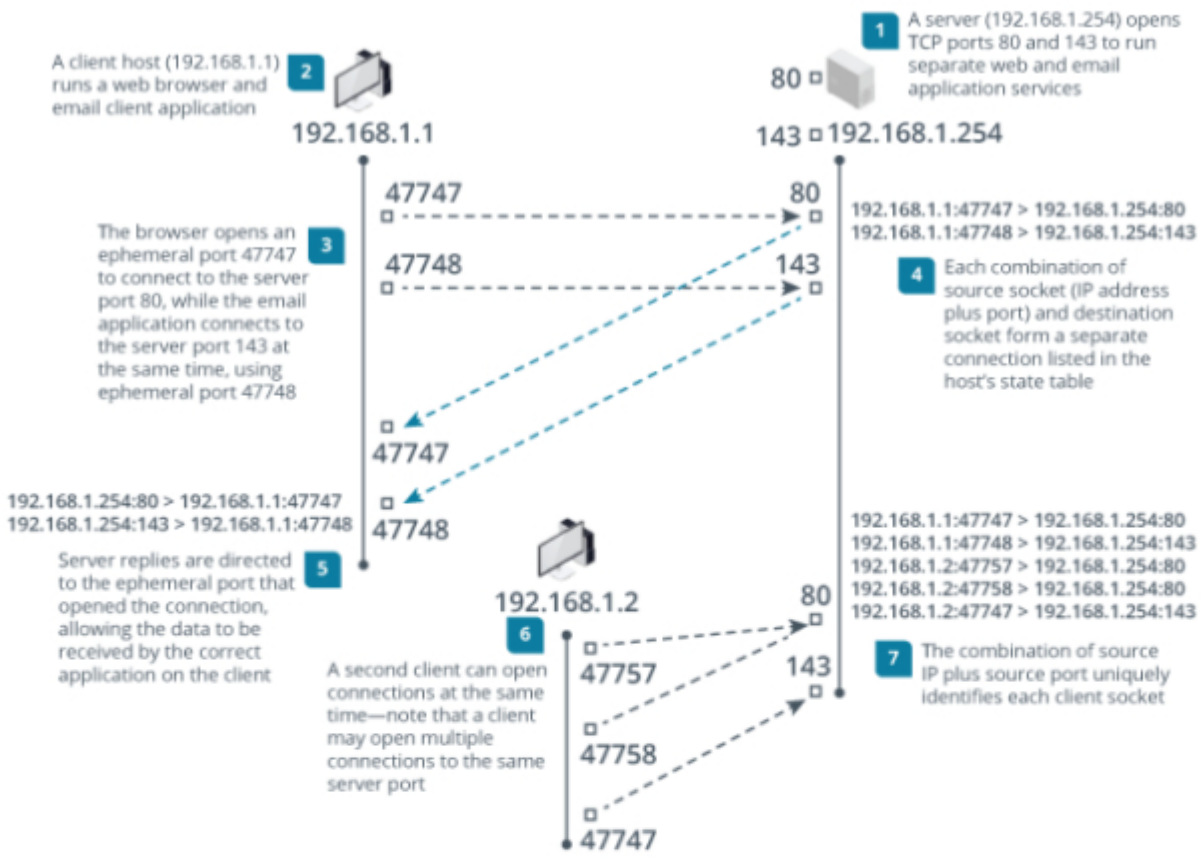
Sebuah host TCP/IP mungkin menjalankan beberapa layanan atau berkomunikasi dengan beberapa server, klien, atau rekan secara paralel. Ini berarti bahwa paket yang masuk harus diarahkan ke layanan atau aplikasi yang sesuai. Untuk memfasilitasi ini, setiap aplikasi diberi nomor identifikasi unik yang disebut port. Sebuah host dapat mengoperasikan beberapa port secara bersamaan.

Nomor port 0 hingga 1.023 ditetapkan sebelumnya oleh Internet Assigned Numbers Authority (IANA) ke aplikasi server "terkenal". Penetapan port ini didokumentasikan di iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml. Aplikasi server lain telah terdaftar di kisaran port 1.024 hingga 49.151.

Port yang tersisa (hingga 65.535) ditujukan untuk penggunaan pribadi atau dinamis. Selain aplikasi server yang membutuhkan port, setiap aplikasi klien harus menetapkan nomor portnya sendiri untuk melacak permintaannya. Port klien juga disebut sebagai port sementara atau port sumber.

Tips: Implementasi OS TCP/IP tidak selalu sesuai dengan rekomendasi ini. Misalnya, versi Windows dan UNIX/Linux yang lebih lama menggunakan 1.024-5.000 untuk port klien. Kernel Linux modern sering menggunakan 32.768–60.999.

Nomor port digunakan bersama dengan alamat IP sumber untuk membentuk soket. Setiap soket terikat pada proses perangkat lunak. Hanya satu proses yang dapat mengoperasikan soket pada satu waktu. Koneksi terbentuk ketika soket klien meminta layanan dari soket server. Sambungan diidentifikasi secara unik dengan kombinasi port server dan alamat IP dan port klien dan alamat IP. Oleh karena itu, soket server dapat mendukung banyak koneksi dari sejumlah soket klien.



Multiplexing application ports as sockets at the Transport layer. (Images © 123RF.com.)

Transmission Control Protocol

Transmission Control Protocol (TCP) bekerja pada lapisan Transport untuk menyediakan komunikasi yang berorientasi koneksi dan terjamin menggunakan pengakuan untuk memastikan bahwa pengiriman telah terjadi. Jika paket hilang, mereka dapat ditransmisikan ulang. TCP hanya dapat digunakan untuk transmisi unicast.

TCP mengambil data dari lapisan Aplikasi sebagai aliran byte dan membaginya menjadi segmen-segmen, yang masing-masing diberi header. Segmen TCP menjadi muatan datagram IP yang mendasarinya. Penggunaan sequencing, acknowledgment, dan retransmissions berarti bahwa TCP memerlukan banyak bidang header untuk memelihara informasi status. Bidang utama di header segmen TCP adalah:

Field	Explanation
Source port	TCP port of sending host.
Destination port	TCP port of destination host.
Sequence number	The ID number of the current segment (the sequence number of the last byte in the segment). This allows the receiver to rebuild the message correctly and deal with out-of-order packets.
Ack number	The sequence number of the next segment expected from the other host (that is, the sequence number of the last segment received +1). Packets might be out-of-order because they are delayed, but they could also be lost completely or arrive in a damaged state. In the first case, the lack of acknowledgement results in the retransmission of data and, in the second case, a Negative Acknowledgement (NAK or NACK) forces retransmission.
Data length	Length of the TCP segment.
Flags	Type of content in the segment (ACK, SYN, FIN, and so on).
Window	The amount of data the host is willing to receive before sending another acknowledgement. TCP's flow control mechanism means that if it is getting overwhelmed with traffic, one side can tell the other to slow the sending rate.
Checksum	Ensures validity of the segment. The checksum is calculated on the value of not only the TCP header and payload but also part of the IP header, notably the source and destination addresses. Consequently, the mechanism for calculating the checksum is different for IPv6 (128-bit addresses) than for IPv4 (32-bit addresses).
Urgent Pointer	If urgent data is being sent, this specifies the end of that data in the segment.
Options	Allows further connection parameters to be configured. The most important of these is the Maximum Segment Size. This allows the host to specify how large the segments it receives should be, minimizing fragmentation as they are transported over data link frames.

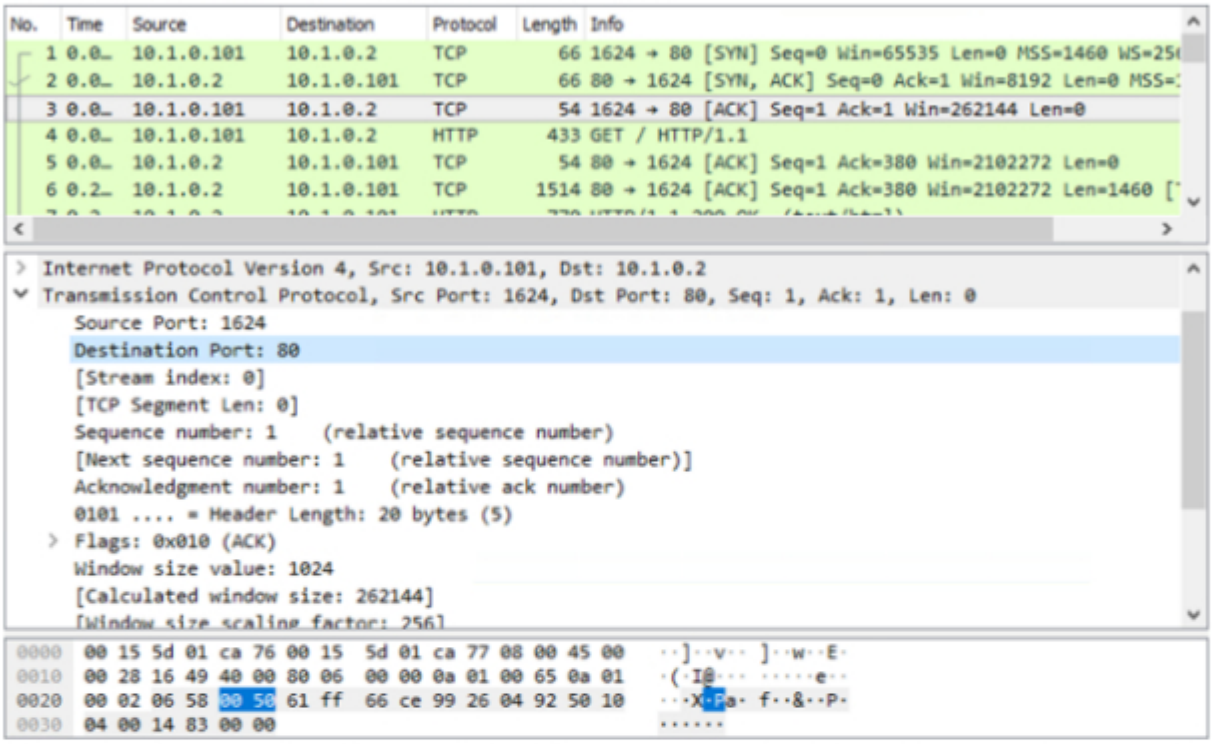
TCP Handshake and Teardown

Koneksi TCP biasanya dibuat untuk mentransfer satu file, jadi sesi klien untuk sesuatu seperti halaman web (HTTP) mungkin melibatkan beberapa koneksi TCP yang dibuka

dengan server. Koneksi ini dikelola menggunakan transaksi jabat tangan, yang menggunakan sejumlah flag TCP.

TCP Three-Way Handshake

Koneksi dibuat menggunakan jabat tangan tiga arah:



Observing the 3-way handshake with the Wireshark protocol analyzer. (Screenshot courtesy of Wireshark.)

1. Klien mengirimkan segmen dengan flag TCP SYN yang disetel ke server dengan nomor urut yang dibuat secara acak. Klien memasuki status SYN-SENT.
2. Server, saat ini dalam status LISTEN (dengan asumsi sedang online), merespons dengan segmen SYN/ACK, yang berisi nomor urut yang dibuat secara acak. Server memasuki status SYN-RECEIVED.
3. Klien merespons dengan segmen ACK. Klien menganggap koneksi ESTABLISHED.
4. Server membuka koneksi dengan klien dan memasuki status ESTABLISHED. Server dapat (biasanya) mendukung ribuan atau bahkan jutaan koneksi TCP secara bersamaan.

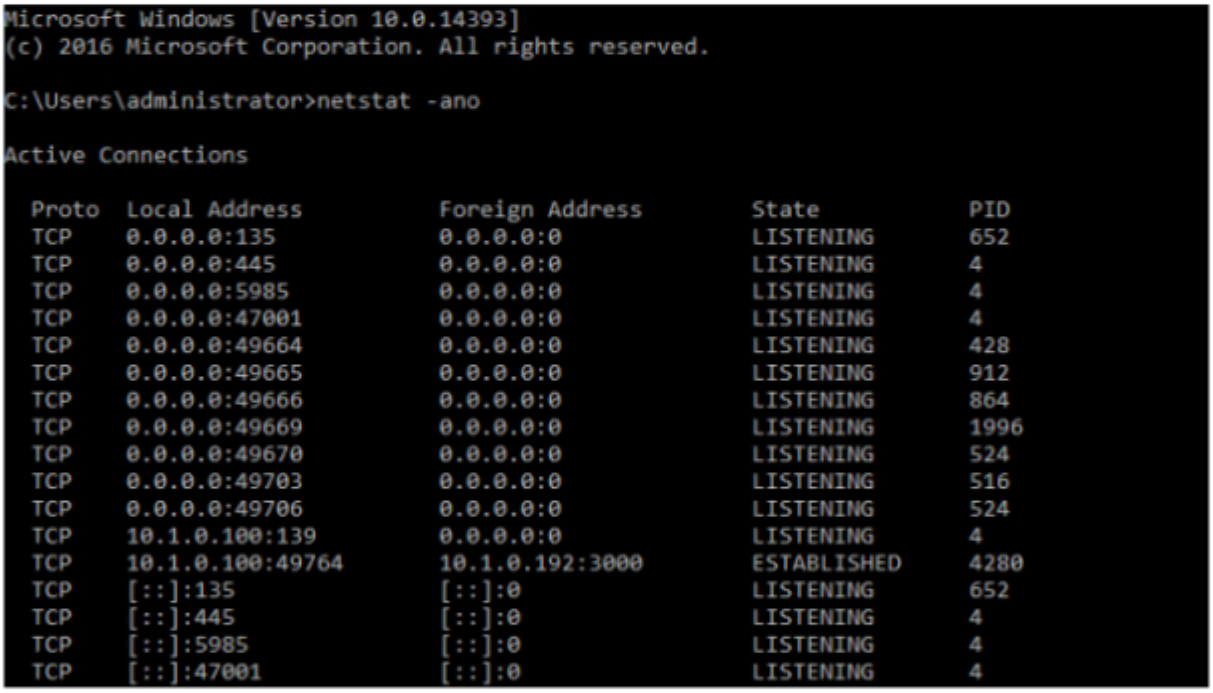
Tip: Mesin pengirim mengharapkan pengakuan reguler untuk segmen yang dikirimnya dan, jika suatu periode berlalu tanpa pengakuan, ia menganggap informasi tidak sampai dan secara otomatis mengirim ulang. Overhead ini membuat sistem relatif lambat. Transmisi berorientasi koneksi cocok ketika keandalan dan integritas data penting.

Penghancuran Koneksi TCP

Ada juga fungsi untuk mengatur ulang koneksi dan (dalam beberapa implementasi) menjaga koneksi tetap hidup jika tidak ada data aktual yang sedang dikirim (host dikonfigurasikan untuk membatasi koneksi yang tidak digunakan). Untuk menutup koneksi, juga disebut sebagai teardown, langkah-langkah dasar berikut dilakukan:

1. Klien mengirimkan segmen FIN ke server dan memasuki status FIN-WAIT1.
2. Server merespons dengan segmen ACK dan memasuki status TUTUP-TUNGGU.
3. Klien menerima segmen ACK dan memasuki status FIN-WAIT2. Server mengirimkan segmen FIN sendiri ke klien dan beralih ke status LAST-ACK.
4. Klien merespons dengan ACK dan memasuki status TIME-WAIT. Setelah periode yang ditentukan, klien menutup koneksinya.
5. Server menutup koneksi ketika menerima ACK dari klien.

Beberapa implementasi dapat menggunakan satu langkah lebih sedikit dengan menggabungkan respons FIN dan ACK ke dalam operasi segmen tunggal.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\administrator>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       652
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       428
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       912
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       864
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       1996
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       524
  TCP    0.0.0.0:49703          0.0.0.0:0              LISTENING       516
  TCP    0.0.0.0:49706          0.0.0.0:0              LISTENING       524
  TCP    10.1.0.100:139         0.0.0.0:0              LISTENING       4
  TCP    10.1.0.100:49764       10.1.0.192:3000        ESTABLISHED     4280
  TCP    [::]:135               [::]:0                 LISTENING       652
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:5985              [::]:0                 LISTENING       4
  TCP    [::]:47001             [::]:0                 LISTENING       4
```

Mengamati koneksi TCP dengan alat netstat. (Tangkapan layar digunakan dengan izin dari Microsoft.)

Host juga dapat mengakhiri sesi secara tiba-tiba menggunakan segmen reset (RST). Ini tidak akan menjadi perilaku khas dan mungkin perlu diselidiki. Server atau alat keamanan mungkin menolak koneksi menggunakan RST, aplikasi klien atau server mungkin salah, atau mungkin ada semacam aktivitas pemindaian mencurigakan yang sedang berlangsung.

User Datagram Protocol

User Datagram Protocol (UDP) juga bekerja pada lapisan Transport, tetapi tidak seperti TCP, ini adalah metode komunikasi tanpa koneksi dan tanpa jaminan tanpa pengakuan atau kontrol aliran. Tidak ada jaminan mengenai pengiriman pesan atau mekanisme pengiriman ulang paket yang hilang atau rusak. Ketika aplikasi menggunakan UDP, itu harus menentukan mekanisme keandalan di header lapisan aplikasi atau logika perangkat lunak, jika ini diperlukan.

UDP cocok untuk aplikasi yang mengirim sejumlah kecil data di setiap paket dan tidak memerlukan pengakuan tanda terima. Ini digunakan oleh protokol lapisan Aplikasi yang perlu mengirim lalu lintas multicast atau siaran. Ini juga dapat digunakan untuk aplikasi yang mentransfer data sensitif waktu tetapi tidak memerlukan keandalan yang lengkap, seperti suara atau video. Menggunakan paket kecil berarti bahwa jika beberapa paket hilang atau tiba dalam keadaan rusak, paket tersebut hanya bermanifestasi sebagai gangguan kecil dalam kualitas pemutaran. Pengurangan overhead berarti pengiriman secara keseluruhan lebih cepat.

Tabel ini menunjukkan struktur datagram UDP.

Field	Explanation
Source port	UDP port of sending host.
Destination port	UDP port of destination host.
Sequence number	The ID number of the current segment (the sequence number of the last byte in the segment). This allows the receiver to rebuild the message correctly and deal with out-of-order packets.
Message length	Size of the UDP packet.
Flags	Type of content in the segment (ACK, SYN, FIN, and so on).
Checksum	Ensures validity of the packet

Ukuran header adalah 8 byte, dibandingkan dengan 20 byte (atau lebih) untuk TCP.

Common TCP and UDP Ports

Tabel berikut mencantumkan beberapa nomor port yang terkenal dan terdaftar.

Port Number	Transport Protocol	Service or Application	Description
20	TCP	ftp-data	File Transfer Protocol-Data
21	TCP	ftp	File Transfer Protocol-Control
22	TCP	ssh/sftp	Secure Shell/FTP over SSH
23	TCP	telnet	Telnet
25	TCP	smtp	Simple Mail Transfer Protocol
53	TCP/UDP	domain	Domain Name System
67	UDP	bootps	BOOTP/DHCP Server
68	UDP	bootpc	BOOTP/DHCP Client
69	UDP	tftp	Trivial File Transfer Protocol
80	TCP	http	HTTP

110	TCP	pop	Post Office Protocol
123	UDP	ntp/sntp	Network Time Protocol/Simple NTP
143	TCP	imap	Internet Message Access Protocol
161	UDP	snmp	Simple Network Management Protocol
162	UDP	snmp-trap	Simple Network Management Protocol Trap
389	TCP/UDP	ldap	Lightweight Directory Access Protocol
443	TCP	https	HTTP-Secure (Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

445	TCP	smb	Server Message Block over TCP/IP
514	UDP	syslog	Syslog
546	UDP	dhcpv6-client	DHCPv6 Client
547	TCP	dhcpv6-server	DHCPv6 Server
587	TCP	smtps	SMTP-Secure
636	TCP	ldaps	LDAP-Secure
993	TCP	imaps	IMAP-Secure
995	TCP	pop3s	POP3-Secure
1433	TCP	sql-server	MS Structured Query Language (SQL) Server
1521	TCP	sqlnet	Oracle SQL*Net
3306	TCP	mysql	MySQL/MariaDB

3389	TCP	rdp	Remote Desktop Protocol
5004	UDP	rtp	Real-Time Protocol
5005	UDP	rtcp	Real-Time Control Protocol
5060	TCP/UDP	sip	Session Initiation Protocol
5061	TCP/UDP	sips	SIP-Secure

USE APPROPRIATE TOOLS TO SCAN NETWORK PORTS

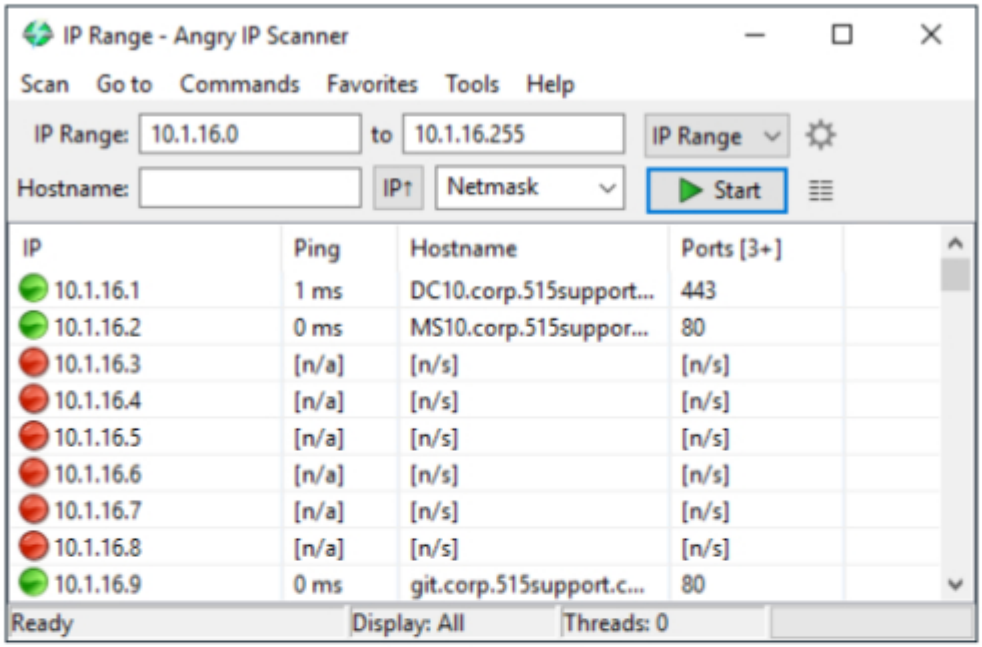
Pendahuluan: Gunakan Alat yang Tepat untuk Memindai Port Jaringan
Salah satu tugas penting bagi administrator jaringan adalah mengidentifikasi dan menganalisis lalu lintas yang melewati tautan jaringan. Informasi ini digunakan untuk memecahkan masalah layanan jaringan, dan untuk memverifikasi keamanan jaringan.

IP Scanners

Salah satu tugas manajemen yang dihadapi administrator jaringan adalah memverifikasi dengan tepat apa yang terhubung ke jaringan dan apa yang dikomunikasikan melaluinya. Ini biasanya digambarkan sebagai visibilitas jaringan. Visibilitas diperlukan untuk mengonfirmasi bahwa server dan klien berada di VLAN atau subnet yang benar dan untuk mencoba mengidentifikasi mesin yang tidak sah atau tidak sah. Pemindai IP adalah alat yang melakukan penemuan host dan dapat menetapkan topologi logis keseluruhan jaringan dalam hal subnet dan router.

Pemindaian IP dapat dilakukan menggunakan open source mandiri yang ringan atau alat komersial, seperti Nmap, AngryIP, atau PRTG. Suite manajemen jaringan perusahaan juga akan dapat melakukan pemindaian IP dan menggabungkannya dengan informasi aset atau inventaris tentang setiap host. Fungsi ini sering disebut sebagai IP Address Management (IPAM). Suite yang terintegrasi dengan DHCP dan server DNS dapat disebut sebagai DHCP,

DNS, dan IPAM (DDI). Windows Server dibundel dengan produk DDI. Vendor dan solusi terkenal lainnya termasuk ManageEngine, Infoblox, SolarWinds, Bluecat, dan Men -and- Mice.



Angry IP Scanner.

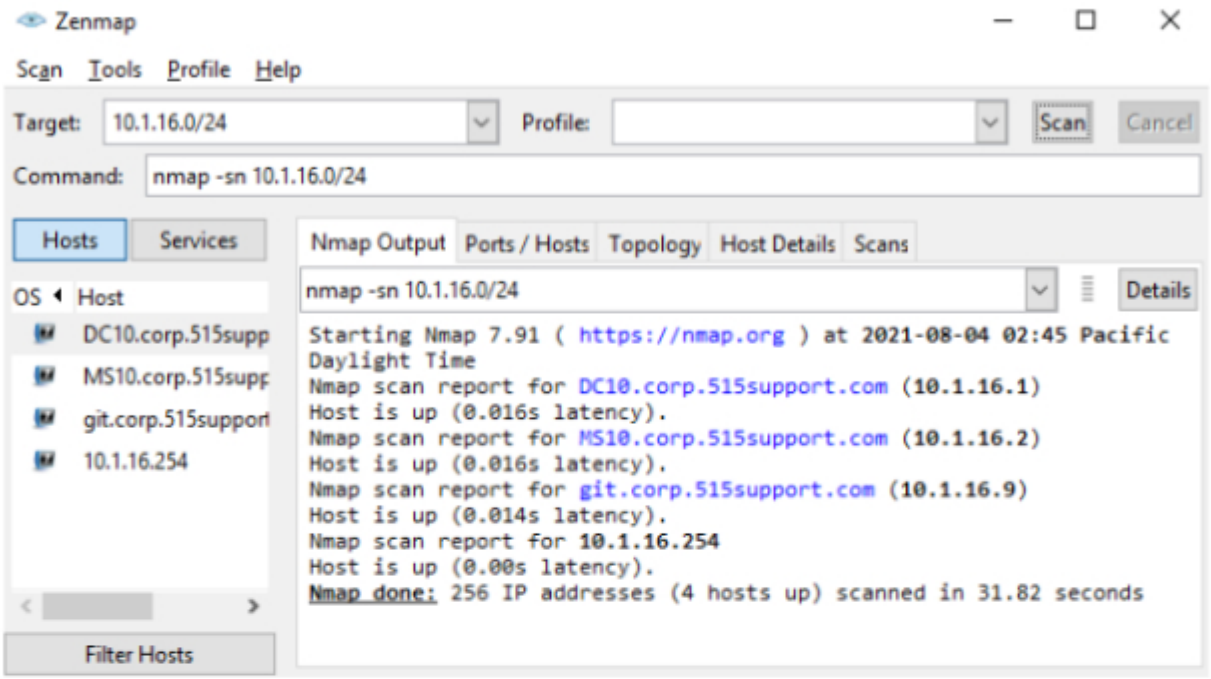
Penemuan host adalah tipe dasar pemindaian IP yang hanya mencoba menentukan apakah alamat IP "naik". Ada banyak teknik penemuan host yang berbeda. Beberapa yang terbaik dalam menemukan sejumlah besar host yang sah dengan cepat; yang lain dioptimalkan untuk mengidentifikasi host jahat yang mencoba untuk tetap tersembunyi. Teknik paling dasar menggunakan alat ping, arp, dan traceroute. Beberapa suite menggunakan kueri Simple Network Management Protocol (SNMP), yang juga dapat melaporkan informasi yang lebih detail tentang statistik antarmuka, sementara seperti disebutkan di atas, suite perusahaan dapat meminta informasi dari server DHCP dan DNS lokal. Pemindai berorientasi keamanan dapat menggunakan probe yang dibuat khusus untuk menemukan host yang mungkin dikonfigurasi untuk tidak menanggapi ping.

Nmap

Nmap Security Scanner (nmap.org) banyak digunakan untuk pemindaian IP, baik sebagai audit maupun sebagai alat pengujian penetrasi. Alat ini adalah perangkat lunak sumber terbuka dengan paket untuk sebagian besar versi Windows, Linux, dan macOS®. Ini dapat dioperasikan dengan baris perintah atau melalui GUI (Zenmap).

Sintaks dasar dari perintah Nmap adalah memberikan subnet IP (atau alamat IP) untuk dipindai. Saat digunakan tanpa sakelar seperti ini, perilaku default Nmap adalah melakukan ping dan mengirim paket TCP ACK ke port 80 dan 443 untuk menentukan apakah ada host. Pada segmen jaringan lokal, Nmap juga akan melakukan sweep ARP dan Neighbor Discovery (ND). Jika sebuah host terdeteksi, Nmap melakukan pemindaian port terhadap host tersebut untuk menentukan layanan mana yang dijalankannya. Sidik jari OS ini dapat memakan waktu pada

lingkup IP yang besar. Jika Anda hanya ingin melakukan penemuan host, Anda dapat menggunakan Nmap dengan sakelar -sn untuk menekan pemindaian port. Alat ini juga dapat menghitung jumlah lompatan dengan menentukan sakelar --traceroute.



Pemindaian penemuan Nmap. (Screenshot digunakan dengan izin dari Nmap.)

Berbagai opsi tersedia untuk pemindaian khusus untuk mencoba mendeteksi host tersembunyi (nmap.org/book/host-discovery-techniques.html).

Netstat

Selain menemukan host, satu tantangan visibilitas lainnya adalah menetapkan layanan apa yang dijalankan oleh host. Perintah netstat memungkinkan Anda untuk memeriksa status port pada host lokal. Anda dapat menggunakan netstat untuk memeriksa kesalahan konfigurasi layanan, seperti host yang menjalankan web atau server FTP yang diinstal pengguna tanpa izin. Anda mungkin juga dapat mengidentifikasi koneksi jarak jauh yang mencurigakan ke layanan di host lokal atau dari host ke alamat IP jarak jauh.

Pada Windows®, digunakan tanpa sakelar, perintah mengeluarkan koneksi TCP aktif, menunjukkan alamat dan port lokal dan asing. Menggunakan -a switch menampilkan semua port yang terbuka, termasuk koneksi TCP dan UDP yang aktif dan port dalam status mendengarkan.

Di Linux®, menjalankan netstat tanpa sakelar menunjukkan koneksi aktif jenis apa pun. Jika Anda ingin menampilkan jenis koneksi yang berbeda, Anda dapat menggunakan sakelar untuk koneksi Internet untuk TCP (-t) dan UDP (-u), koneksi mentah (-w), dan soket UNIX®/port server lokal (-x). Menggunakan sakelar -a menyertakan port dalam status mendengarkan di

output. -l hanya menampilkan port dalam status mendengarkan, menghilangkan koneksi yang sudah ada.

Misalnya, perintah berikut hanya menunjukkan mendengarkan dan membuat koneksi Internet (TCP dan UDP): netstat -tua

```
lamp@lamp:~$ netstat -tua
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 localhost:33060         0.0.0.0:*               LISTEN
tcp        0      1 172.16.0.201:52492      172.16.0.254:domain     SYN_SENT
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
udp        0      0 172.16.0.201:43367      172.16.0.254:domain     ESTABLISHED
udp        0      0 172.16.0.201:42410      172.16.0.254:domain     ESTABLISHED
udp        0      0 172.16.0.201:47084      172.16.0.254:domain     ESTABLISHED
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 172.16.0.201:bootpc     0.0.0.0:*
```

Linux netstat output showing active and listening TCP and UDP connections.

Pada Windows dan Linux, -n menampilkan port dan alamat dalam format numerik. Melewati resolusi nama akan mempercepat setiap kueri. Di Linux, masing-masing menggunakan -4 atau -6 menyaring soket berdasarkan alamat IPv4 atau IPv6. Di Windows, gunakan sakelar -p dengan tipe protokol (TCP , TCPv6 , UDP , atau UDPv6).

Tugas umum lainnya adalah mengidentifikasi proses perangkat lunak mana yang terikat ke soket. Pada Windows, -o menunjukkan nomor Process ID (PID) yang telah membuka port, sedangkan -b menunjukkan nama proses. Di Linux, gunakan -p untuk menampilkan PID dan nama proses.

netstat -s laporan per statistik protokol, seperti paket yang diterima, kesalahan, membuang, permintaan tidak dikenal, permintaan port, koneksi gagal, dan sebagainya. Alat ini akan melaporkan statistik Ethernet menggunakan -e (Windows) atau -I (Linux). netstat -r menampilkan tabel perutean.

```
lamp@lamp:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500     4069      0      0 0          8134      0      0      0 BMRU
lo       65536     5322      0      0 0          5322      0      0      0 LRU
```

Linux netstat interface statistics showing receive and transmit packets numbers plus errors and dropped packets.

netstat juga dapat diatur untuk berjalan terus menerus. Di Windows, jalankan netstat nn , di mana nn adalah interval penyegaran dalam hitungan detik (tekan Ctrl+C untuk berhenti); di Linux, jalankan netstat -c .

Tips: Perintah netstat Linux adalah bagian dari paket net-tools yang sudah tidak digunakan lagi. Paket pilihan iproute2 berisi sejumlah perintah berbeda untuk menggantikan fungsionalitas netstat. Sebagian besar fungsi pemindaian port dilakukan oleh ss, sedangkan statistik antarmuka dilaporkan oleh nstat.

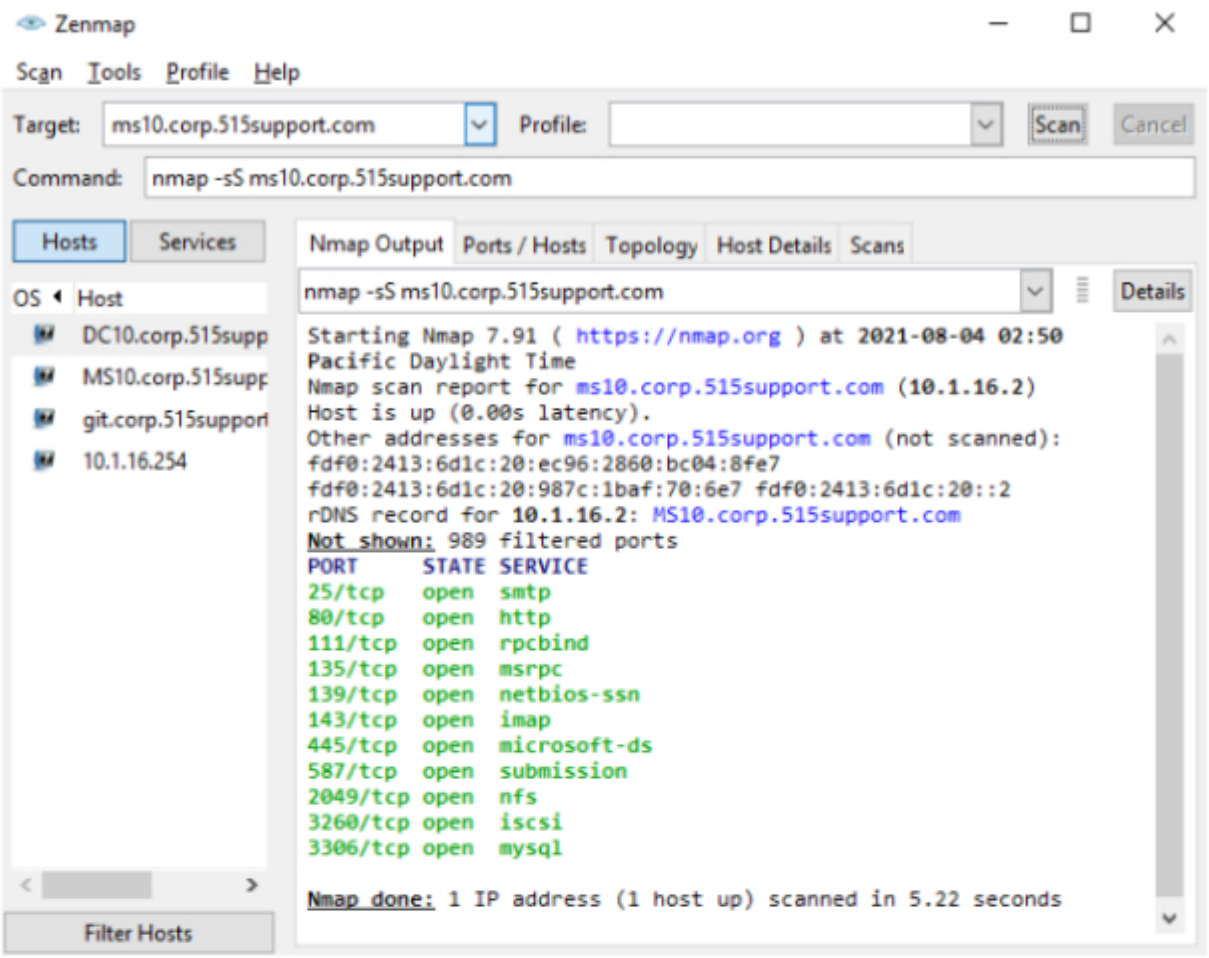
Remote Port Scanners

Di mana netstat melaporkan status port lokal, pemindai port jarak jauh melakukan pemeriksaan dari komputer lain, atau bahkan mesin di jaringan lain.

Banyak alat yang digunakan untuk penemuan host juga dapat melakukan pemindaian port jarak jauh. Seperti penemuan host, ada banyak teknik berbeda untuk melakukan pemindaian port. Beberapa teknik dirancang untuk penggunaan rahasia (untuk mencoba menghindari deteksi aktivitas pemindaian oleh target) dan beberapa dirancang untuk menyelidiki di luar hambatan keamanan, seperti firewall.

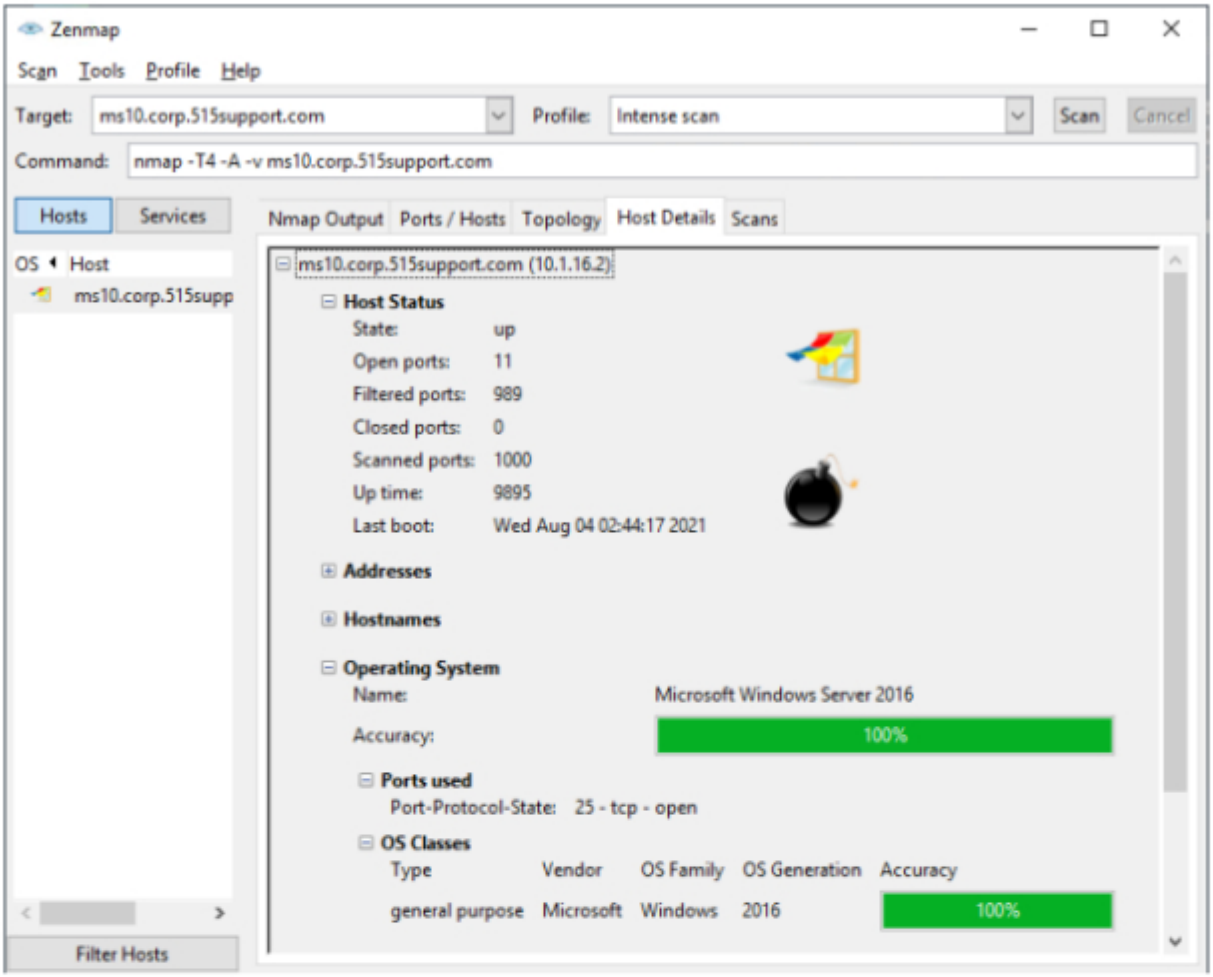
Sebagai contoh, berikut ini menunjukkan beberapa jenis pemindaian utama yang dapat dilakukan Nmap:

- TCP SYN (-sS)-Ini adalah teknik cepat (juga disebut sebagai pemindaian setengah terbuka) karena host pemindaian meminta koneksi tanpa mengakuinya. Respons target terhadap paket SYN pemindaian mengidentifikasi status port.
- TCP connect (-sT)-Pemindaian setengah terbuka membutuhkan Nmap untuk memiliki akses istimewa ke driver jaringan sehingga dapat membuat paket. Jika akses istimewa tidak tersedia, Nmap harus menggunakan OS untuk mencoba koneksi TCP penuh. Jenis pemindaian ini kurang tersembunyi.
- Pemindaian UDP (-sU) -Pindai port UDP. Karena ini tidak menggunakan ACK, Nmap perlu menunggu respons atau batas waktu untuk menentukan status port, sehingga pemindaian UDP bisa memakan waktu lama. Pemindaian UDP dapat digabungkan dengan pemindaian TCP.
- Rentang port (-p) -Secara default, Nmap memindai 1.000 port yang umum digunakan. Gunakan argumen -p untuk menentukan rentang port. Anda juga dapat menggunakan --top-ports n , di mana n adalah jumlah port yang umum digunakan untuk dipindai. Statistik frekuensi untuk menentukan seberapa sering port digunakan disimpan dalam file konfigurasi nmap-services.



Pemindaian setengah terbuka dengan Nmap. (Screenshot digunakan dengan izin dari Nmap.)

Ketika layanan ditemukan, Anda dapat menggunakan Nmap dengan sakelar -sV atau -A untuk menyelidiki host secara lebih intensif guna menemukan perangkat lunak atau versi perangkat lunak yang mengoperasikan setiap port. Proses mengidentifikasi OS atau aplikasi perangkat lunak dari tanggapannya terhadap probe disebut sidik jari.



Tanggapan terhadap probe jaringan dapat digunakan untuk mengidentifikasi jenis dan versi sistem operasi host. (Screenshot digunakan dengan izin dari Nmap.)

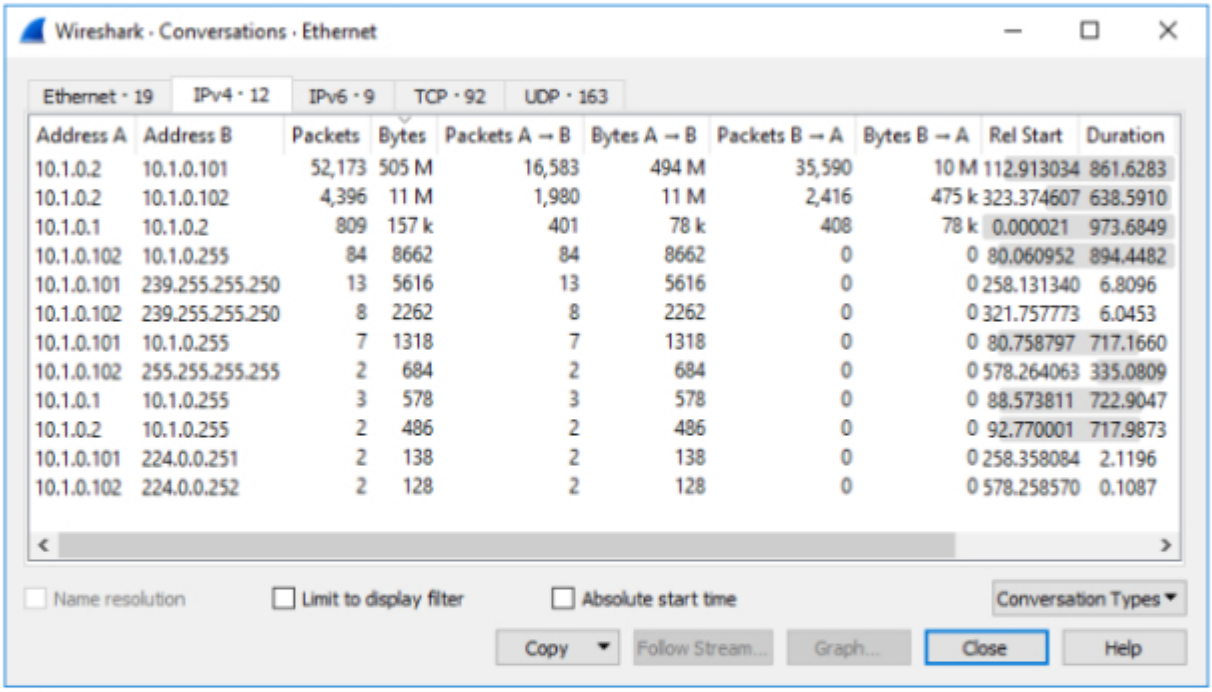
Penganalisis Protokol

Sebuah penganalisa protokol bekerja bersama dengan alat penangkap paket atau sniffer. Anda dapat menganalisis tangkapan langsung untuk menganalisis bingkai saat dibaca oleh sniffer atau membuka file tangkapan tersimpan (.pcap). Sebagian besar alat penganalisis protokol menggabungkan komponen sniffer dengan penganalisis dalam paket perangkat lunak yang sama.

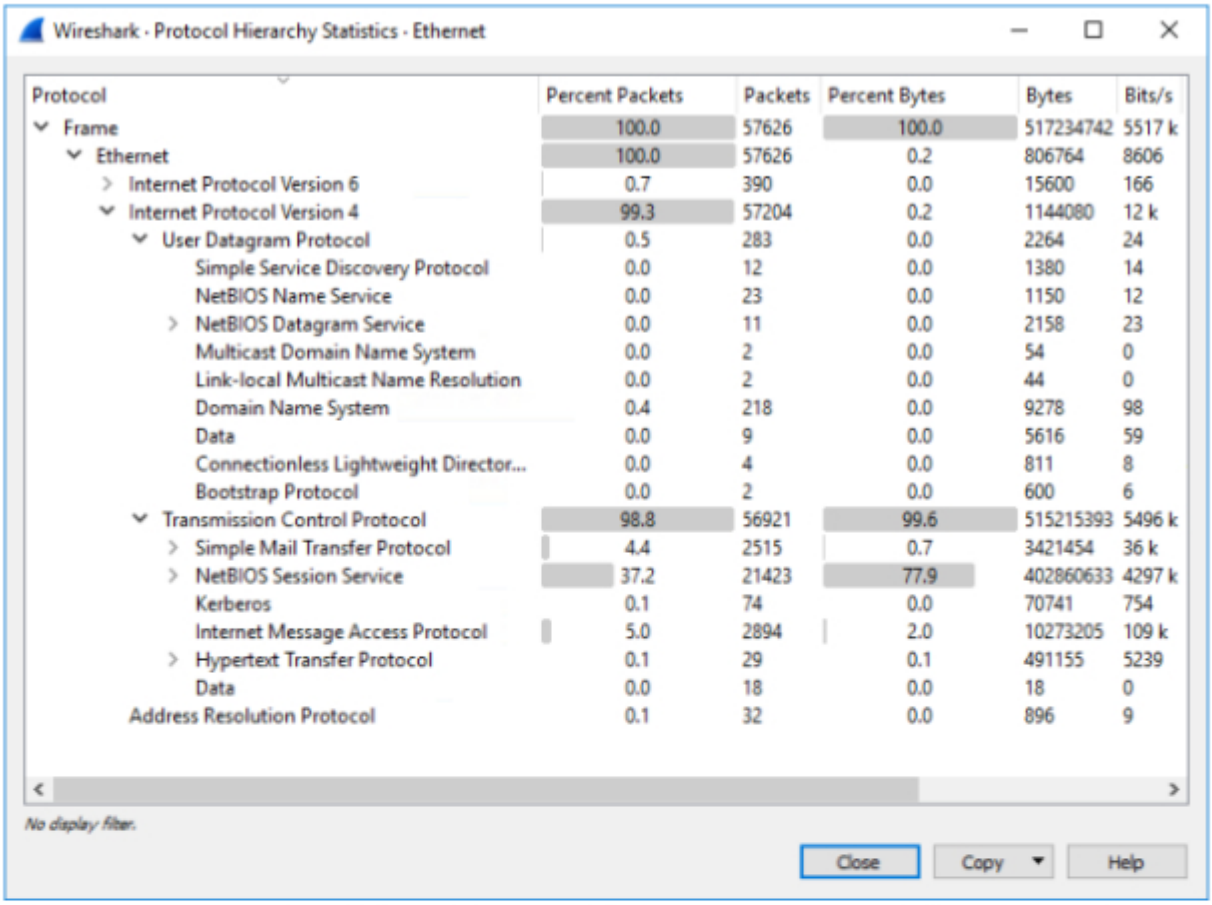
Salah satu fungsi dari penganalisis protokol adalah untuk mengurai setiap frame dalam aliran lalu lintas untuk mengungkapkan bidang header dan konten muatan dalam format yang dapat dibaca. Ini disebut sebagai analisis paket. Menganalisis data protokol pada tingkat bingkai atau paket akan membantu mengidentifikasi kesalahan konfigurasi protokol atau layanan. Karena streaming langsung atau file tangkapan dapat berisi ratusan atau ribuan bingkai, Anda dapat menggunakan filter tampilan untuk hanya menampilkan bingkai atau urutan bingkai tertentu.

Opsi berguna lainnya adalah menggunakan perintah konteks Ikuti TCP Stream untuk merekonstruksi konten paket untuk sesi TCP.

Fungsi lain dari penganalisis protokol adalah untuk melakukan analisis lalu lintas. Daripada membaca setiap frame satu per satu, Anda menggunakan alat untuk memantau statistik yang terkait dengan arus komunikasi, seperti bandwidth yang dikonsumsi oleh setiap protokol atau setiap host, mengidentifikasi host jaringan yang paling aktif, memantau pemanfaatan dan keandalan tautan, dan seterusnya. Di Wireshark, Anda dapat menggunakan menu Statistik untuk mengakses alat analisis lalu lintas.



Menggunakan opsi Percakapan dari alat Statistik Wireshark. (Tangkapan layar milik Wireshark.)



Menggunakan alat Hirarki Protokol di Wireshark untuk melihat protokol paling aktif pada tautan jaringan. Laporan semacam ini dapat digunakan untuk aktivitas jaringan dasar. (Tangkapan layar milik Wireshark.)

MODUL 10

Menjelaskan Layanan Jaringan

PENGANTAR PELAJARAN
Anda telah mengidentifikasi teknologi dan protokol lapisan Fisik, Data Link, Jaringan, dan Transport yang mendukung konektivitas dasar. Paket protokol TCP/IP juga mencakup protokol aplikasi yang mengimplementasikan layanan jaringan.

Pelajaran ini berfokus pada protokol aplikasi yang melakukan tugas operasi jaringan tingkat rendah, seperti menyediakan alamat dinamis atau layanan resolusi nama. Anda harus memahami fungsi protokol layanan jaringan dan port yang mereka andalkan untuk beroperasi.

TUJUAN PELAJARAN
Dalam pelajaran ini, Anda akan:

- Menjelaskan penggunaan layanan pengalamatan jaringan.
- Jelaskan penggunaan layanan resolusi nama.
- Konfigurasikan layanan DNS.

A. Jelaskan Penggunaan Layanan Pengalamatan Jaringan

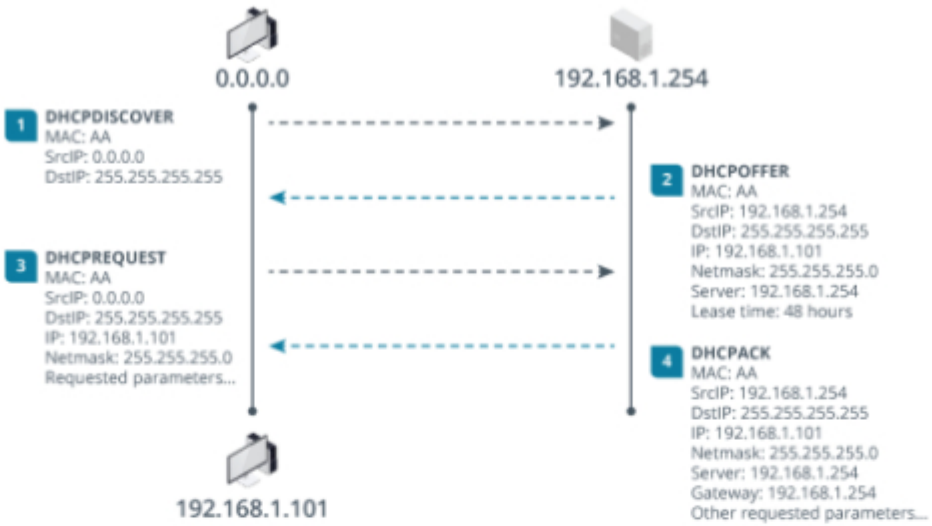
Pendahuluan: Menjelaskan Penggunaan Layanan Pengalamatan Jaringan

Setiap antarmuka host memerlukan konfigurasi IP untuk berkomunikasi pada jaringan TCP/IP. Administrator dapat secara manual menetapkan alamat IP ini, atau penetapan dapat dilakukan secara otomatis tanpa intervensi manual. Dengan memahami berbagai metode yang tersedia bagi Anda untuk menetapkan alamat IP, Anda dapat memilih metode yang paling sesuai dengan jaringan dan host yang berbeda.

Protokol Konfigurasi Host Dinamis

Dynamic Host Configuration Protocol (DHCP) menyediakan metode otomatis untuk mengalokasikan alamat IP, subnet mask, dan parameter opsional, seperti gateway default dan alamat server DNS, ketika host bergabung dengan jaringan. Semua sistem operasi utama menyediakan dukungan untuk klien dan server DHCP. Server DHCP juga tertanam di banyak router dan modem SOHO.

Sebuah host dikonfigurasikan untuk menggunakan DHCP dengan menetapkan dalam konfigurasi TCP/IP bahwa ia harus secara otomatis mendapatkan alamat IP.



DHCP Discover, Offer, Request, Ack process. (Images © 123RF.com.)

Ketika klien DHCP diinisialisasi, ia menyiarkan paket DHCPDISCOVER untuk menemukan server DHCP. Semua komunikasi dikirim menggunakan UDP, dengan server mendengarkan pada port 67 dan klien pada port 68.

Dengan asumsi itu memiliki alamat IP yang tersedia, server DHCP merespon klien dengan paket DHCPOFFER, yang berisi alamat dan informasi konfigurasi lainnya.

Tips: Meskipun klien belum memiliki alamat IP, DHCPOFFER biasanya dikirimkan sebagai unicast karena server mengetahui alamat MAC klien. Beberapa host tidak dapat menerima unicast tanpa alamat IP. Mereka harus mengatur bit siaran dalam paket DHCPDISCOVER.

Klien dapat memilih untuk menerima tawaran menggunakan paket DHCPREQUEST-juga disiarkan ke jaringan.

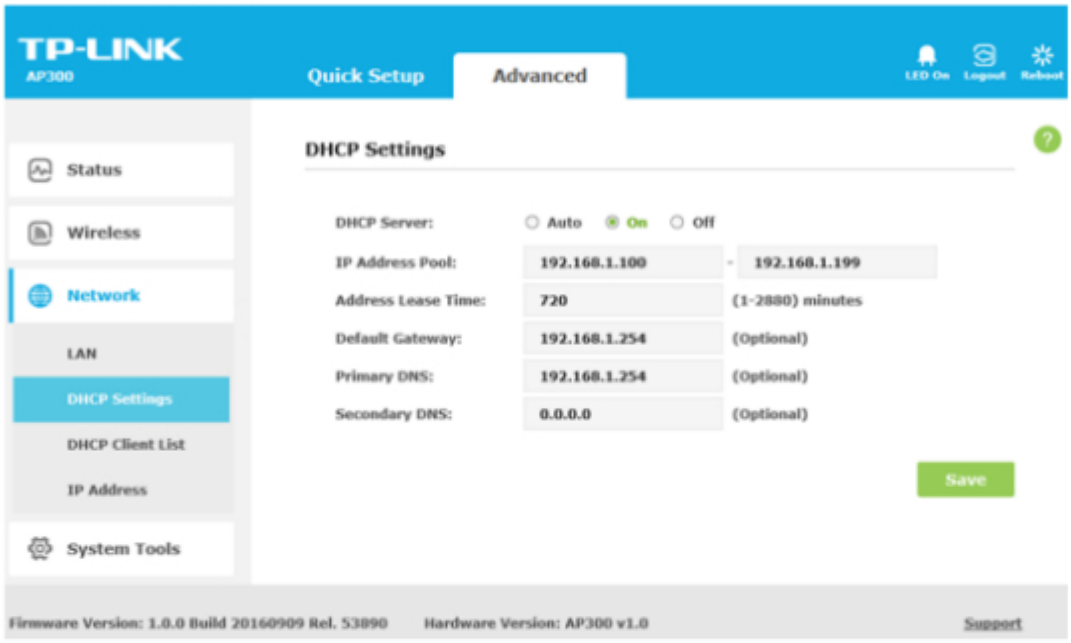
Dengan asumsi penawaran masih tersedia, server akan merespons dengan paket DHCPACK. Klien menyiarkan pesan ARP untuk memeriksa bahwa alamat tidak digunakan. Jika demikian, itu akan mulai menggunakan alamat dan opsi; jika tidak, itu menolak alamat dan meminta yang baru.

Alamat IP disewa oleh server untuk jangka waktu terbatas saja. Klien dapat mencoba untuk memperbarui atau mengikat kembali sewa sebelum berakhir. Jika sewa tidak dapat diperpanjang, klien harus melepaskan alamat IP dan memulai proses penemuan lagi.

Tips: Terkadang, proses penyewaan DHCP disebut proses DORA: Discover, Offer, Request, dan Ack(knowledge).

Konfigurasi DHCP Server

DHCP biasanya digunakan sebagai layanan sistem operasi jaringan atau melalui alat seperti sakelar atau router. Server DHCP harus dialokasikan alamat IP statis dan dikonfigurasi dengan rentang (atau kumpulan) alamat IP dan subnet mask ditambah nilai opsi untuk dialokasikan.



Mengkonfigurasi DHCP pada titik akses nirkabel TP-LINK. (Tangkapan layar milik TP-Link Technologies Co., Ltd.)

Rentang alamat dan opsi yang dikonfigurasi untuk satu subnet disebut sebagai ruang lingkup. Untuk menentukan cakupan, Anda harus memberikan alamat IP awal dan akhir bersama dengan subnet mask. Server mempertahankan pemetaan cakupan satu-ke-satu ke subnet. Artinya, tidak ada ruang lingkup yang dapat mencakup lebih dari satu subnet dan tidak ada subnet yang dapat berisi lebih dari satu ruang lingkup.

Perangkat multifungsi yang ditampilkan hanya mendukung satu cakupan. Server DHCP harus ditempatkan di subnet yang sama dengan kliennya. Server DHCP yang lebih canggih mungkin dikonfigurasi untuk mengelola beberapa cakupan. Jika server menyediakan konfigurasi IP untuk beberapa subnet/cakupan, server harus memilih kumpulan untuk melayani setiap permintaan berdasarkan subnet asal permintaan.

Tips: Tidak ada mekanisme bagi klien untuk memilih di antara beberapa server. Oleh karena itu, jika beberapa server DHCP dikerahkan-untuk toleransi kesalahan, misalnya-mereka harus dikonfigurasi dengan cakupan nonoverlapping atau split. DHCP untuk beberapa subnet biasanya ditangani dengan mengkonfigurasi agen relai untuk meneruskan permintaan ke server DHCP pusat.

Konfigurasi Opsi DHCP

Seiring dengan cakupan alamat, Anda juga perlu menentukan parameter lain, seperti waktu dan opsi sewa.

Waktu Sewa DHCP dan Sewa yang Tersedia
Klien dapat memperbarui sewa ketika setidaknya setengah periode sewa telah berlalu (pengatur waktu T1) sehingga menyimpan informasi pengalamatan IP yang sama. Jika server DHCP asli tidak menanggapi permintaan untuk memperbarui sewa, klien mencoba untuk mengikat ulang konfigurasi sewa yang sama dengan server DHCP yang tersedia. Secara default, ini terjadi setelah 87,5% dari durasi sewa habis (pengatur waktu T2). Jika ini gagal, klien melepaskan alamat IP dan terus menyiarkan untuk menemukan server.

Waktu sewa yang lama berarti klien tidak perlu sering memperbarui sewa, tetapi kumpulan alamat IP server DHCP yang tersedia tidak sering diisi ulang. Jika alamat IP kekurangan pasokan, periode sewa yang singkat memungkinkan server DHCP mengalokasikan alamat yang sebelumnya ditetapkan ke host yang sekarang tidak aktif di jaringan.

Tips: Klien Windows dapat dipaksa untuk melepaskan sewa dengan mengeluarkan perintah seperti ipconfig. Di Linux, utilitas dhclient sering digunakan untuk tugas ini, meskipun distribusi modern mungkin menggunakan NetworkManager atau systemd-networkd. Host Windows yang gagal mendapatkan sewa akan kembali ke alamat IP otomatis (APIPA) atau konfigurasi tautan-lokal dan memilih alamat dalam rentang 169.254.0.0/16. Linux mungkin menggunakan pengalamatan tautan-lokal, menyetel alamat ke tidak dikenal (0.0.0.0), atau membiarkan antarmuka tidak dikonfigurasi.

Opsi DHCP
Ketika server DHCP menawarkan konfigurasi ke klien, minimal harus menyediakan alamat IP dan subnet mask. Biasanya, itu juga akan menyediakan pengaturan terkait IP lainnya, yang dikenal sebagai opsi DHCP. Setiap opsi diidentifikasi dengan byte tag atau nilai desimal antara 0 dan 255 (meskipun 0 maupun 255 tidak dapat digunakan sebagai nilai opsi). Beberapa opsi yang banyak digunakan meliputi:

- Gateway default (alamat IP router).
- Alamat IP server DNS yang dapat bertindak sebagai resolver untuk kueri nama.
- Sufiks DNS (nama domain) yang akan digunakan oleh klien.
- Opsi server berguna lainnya, seperti sinkronisasi waktu (NTP), transfer file (TFTP), atau proxy VoIP.

Satu set opsi default (global) dapat dikonfigurasi di seluruh server. Opsi default dapat diganti dengan menyetel opsi khusus cakupan.

DHCP Reservations and Exclusions

Salah satu kelemahan metode penetapan dinamis standar adalah tidak menjamin bahwa klien tertentu akan mempertahankan alamat IP yang sama dari waktu ke waktu. Ada beberapa kasus di mana akan menguntungkan bagi host tertentu, seperti printer jaringan atau titik akses nirkabel, untuk mempertahankan alamat IP mereka.

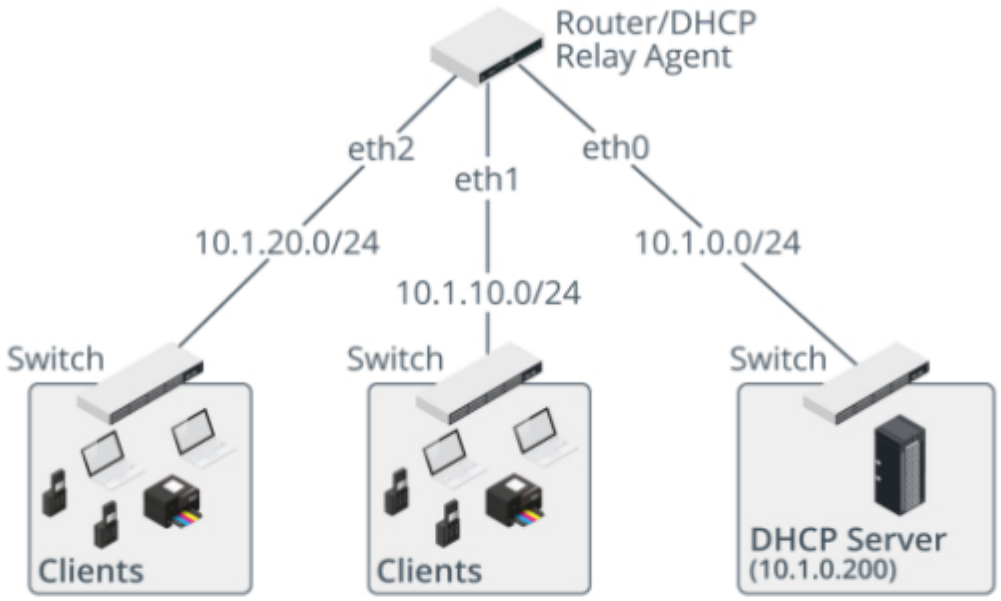
Salah satu solusinya adalah mengonfigurasi penetapan statis, menggunakan alamat IP di luar cakupan DHCP. Atau, alamat yang ditetapkan secara statis dapat ditetapkan dari rentang pengecualian yang dikonfigurasi secara khusus, jika ini didukung oleh server. Sementara solusi ini berfungsi, mereka kehilangan keuntungan dari manajemen konfigurasi terpusat.

Pendekatan alternatif adalah membuat reservasi. Reservasi adalah pemetaan alamat MAC atau ID antarmuka ke alamat IP tertentu dalam kumpulan alamat server DHCP. Ketika server DHCP menerima permintaan dari antarmuka yang diberikan, selalu memberikan alamat IP yang sama. Ini juga disebut sebagai penetapan alamat statis atau tetap. Reservasi yang dialokasikan secara otomatis mengacu pada alamat yang disewakan secara permanen kepada klien. Ini berbeda dari alokasi statis karena administrator tidak menentukan alamat IP spesifik mana yang akan disewa.

DHCP Relay and IP Helper

Biasanya, router tidak meneruskan lalu lintas siaran. Ini berarti bahwa setiap domain broadcast harus dilayani oleh server DHCP-nya sendiri. Pada jaringan besar dengan banyak subnet, ini berarti menyediakan dan mengonfigurasi banyak server DHCP. Untuk menghindari skenario ini, agen relai DHCP dapat dikonfigurasi untuk menyediakan penerusan lalu lintas DHCP antar subnet. Router yang dapat menyediakan jenis penerusan ini dideskripsikan sebagai sesuai dengan RFC 1542.

Relai DHCP memotong bingkai DHCP siaran, menerapkan alamat unicast untuk server DHCP yang sesuai, dan meneruskannya melalui antarmuka untuk subnet yang berisi server. Server DHCP dapat mengidentifikasi subnet IP asli dari paket dan menawarkan sewa dari cakupan yang sesuai. Relai DHCP juga melakukan proses kebalikan dari mengarahkan tanggapan dari server ke subnet klien yang sesuai.



Configuring a DHCP relay agent. (Images © 123RF.com)

Fungsionalitas pembantu IP ini dapat dikonfigurasi pada router untuk memungkinkan set jenis lalu lintas siaran (termasuk DHCP) untuk diteruskan ke antarmuka. Fungsi pembantu IP mendukung fungsi agen relai DHCP. Misalnya, dalam diagram, host di subnet 10.1.20.0/24 dan 10.1.10.0/24 perlu menggunakan server DHCP untuk konfigurasi otomatis, tetapi server DHCP terletak di subnet yang berbeda. Router dikonfigurasi sebagai agen relai DHCP, menggunakan perintah berikut untuk mengaktifkan penerusan siaran DHCP pada antarmuka yang melayani subnet klien:

antarmuka eth1

ip helper-address 10.1.0.200

antarmuka eth2

ip helper-address 10.1.0.200

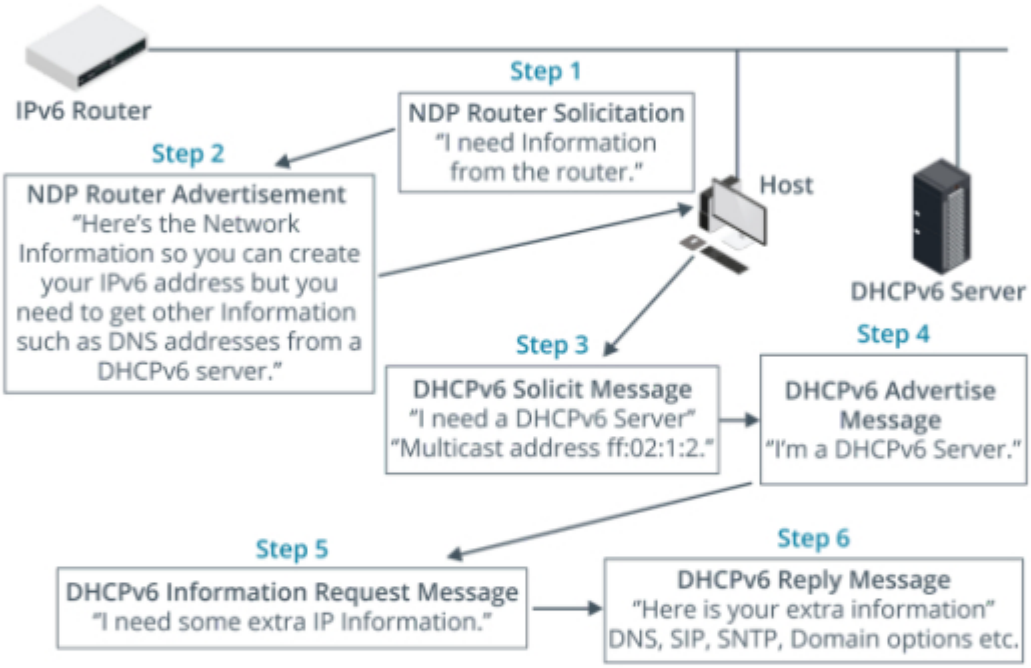
Penerusan UDP adalah aplikasi yang lebih umum dari prinsip yang sama. Selain DHCP, digunakan untuk Network Time Protocol (NTP) dan aplikasi berbasis siaran lainnya.

Konfigurasi Server DHCPv6

Proses Stateless Address Autoconfiguration (SLAAC) IPv6 dapat menemukan router (gerbang default) dan menghasilkan alamat host dengan awalan jaringan yang sesuai secara otomatis. Dalam konteks ini, peran server DHCP di IPv6 berbeda. DHCPv6 sering hanya digunakan untuk memberikan pengaturan opsi tambahan, daripada menyewakan alamat IP host. Format pesan

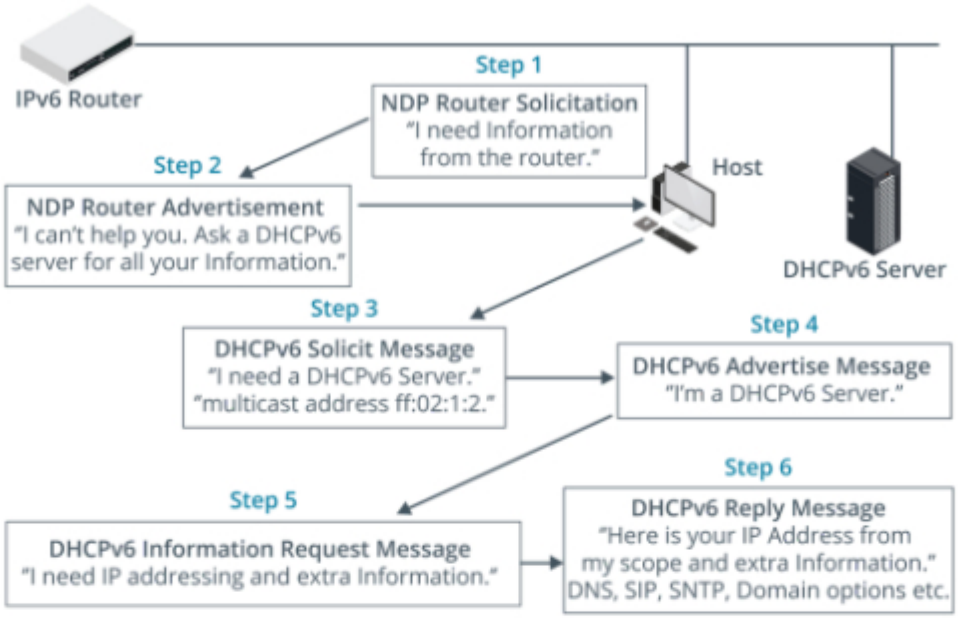
berbeda, tetapi proses penemuan server DHCP dan penyewaan alamat (jika ditawarkan) pada dasarnya sama. Karena IPv6 tidak mendukung siaran, klien menggunakan alamat multicast ff02::1:2 untuk menemukan server DHCP. DHCPv6 menggunakan port 546 (klien) dan 547 (server), bukan port 68 dan 67 seperti pada DHCPv4.

Dalam mode stateless, klien memperoleh awalan jaringan dari Iklan Router dan menggunakannya dengan ID antarmuka yang sesuai. Router juga dapat mengatur kombinasi flag untuk memberitahu klien bahwa server DHCP tersedia. Jika dikonfigurasi, klien meminta server DHCPv6 menggunakan alamat multicast ff02::1:2 dan meminta informasi konfigurasi tambahan.



DHCPv6 stateless mode. (Images © 123RF.com.)

Sebaliknya, mode stateful berarti bahwa sebuah host juga dapat memperoleh alamat IP yang dapat dirutekan dari lingkup DHCPv6, ditambah opsi lain (seperti dengan DHCP untuk IPv4).



DHCPv6 stateful mode. (Images © 123RF.com.)

Mengonfigurasi cakupan mengharuskan Anda untuk menentukan awalan jaringan dan kemudian alamat IP apa pun yang akan dikecualikan dari yang ditawarkan. Semua alamat lain yang tidak secara eksplisit dikecualikan dapat ditawarkan. Tuan rumah masih harus mendengarkan iklan router untuk mendapatkan awalan jaringan dan mengkonfigurasi gateway default. Tidak ada mekanisme di DHCPv6 untuk mengatur rute default.

B. Jelaskan Penggunaan Layanan Resolusi Nama

Pendahuluan: Jelaskan Penggunaan Layanan Resolusi Nama

Setiap host yang memiliki alamat IP yang ditetapkan juga dapat memiliki nama deskriptif. Ini memudahkan pengguna manusia untuk mengidentifikasi dan mengaksesnya di jaringan dan untuk layanan aplikasi dikonfigurasi dengan skema pengalamatan yang memungkinkan perubahan di jaringan yang mendasarinya. Hampir semua jaringan bergantung pada fungsi resolusi nama ini untuk beroperasi dengan lancar dan aman, jadi penting untuk memahami cara kerjanya. Dalam topik ini, Anda akan mengidentifikasi metode untuk resolusi nama host untuk jaringan TCP/IP.

Nama Host dan Nama Domain yang Memenuhi Syarat

Internet Protocol menggunakan alamat IP biner untuk menemukan host di internetwork. Representasi desimal bertitik (IPv4) atau hex (IPv6) dari alamat IP ini digunakan untuk tujuan konfigurasi, tetapi tidak mudah diingat orang. Untuk alasan ini, nama "ramah" juga biasanya diberikan untuk setiap host. Ada dua jenis nama: nama host dan Fully Qualified Domain Names (FQDNs).

Nama host diberikan ke komputer oleh administrator, biasanya saat OS diinstal. Nama host harus unik di jaringan lokal.

Untuk menghindari kemungkinan duplikasi nama host di Internet, nama domain yang sepenuhnya memenuhi syarat (FQDN) digunakan untuk memberikan identitas unik untuk host milik jaringan tertentu. Contoh FQDN mungkin nut.widget.example. FQDN terdiri dari nama host dan akhiran domain. Dalam contoh, nama host adalah nut dan akhiran domain adalah widget.example. Sufiks domain ini terdiri dari widget nama domain di dalam domain tingkat atas (TLD) .example . Sufiks domain juga dapat berisi subdomain antara host dan nama domain. Titik atau titik di akhir menunjukkan akar hierarki.

Tips: Saat Anda mengonfigurasi catatan nama, FQDN harus menyertakan periode akhir untuk mewakili root, tetapi ini dapat dihilangkan di sebagian besar kasus penggunaan lainnya.

Nama domain harus didaftarkan pada registrar untuk memastikan bahwa nama itu unik dalam domain tingkat atas. Setelah nama domain didaftarkan, tidak dapat digunakan oleh organisasi lain. Nama domain yang sama dapat didaftarkan dalam domain tingkat atas yang berbeda, namun-widget.example. dan widget.example.uk. adalah domain yang berbeda, misalnya.

Banyak host mungkin ada dalam satu domain. Misalnya: mur, baut , dan washer mungkin semuanya menjadi host dalam widget.example. domain. Mengingat itu, FQDN harus mengikuti aturan tertentu:

- Nama host harus unik di dalam domain.
-
- Panjang total FQDN tidak boleh melebihi 253 karakter, dengan setiap label (bagian dari nama yang ditentukan oleh titik) tidak lebih dari 63 karakter (tidak termasuk titik).
-
- Label DNS harus menggunakan karakter huruf, angka, dan tanda hubung saja. Label tidak boleh dimulai dengan tanda hubung. Karakter tanda baca seperti titik (.) atau garis miring (/) tidak boleh digunakan.
-
- Label DNS tidak peka huruf besar/kecil.

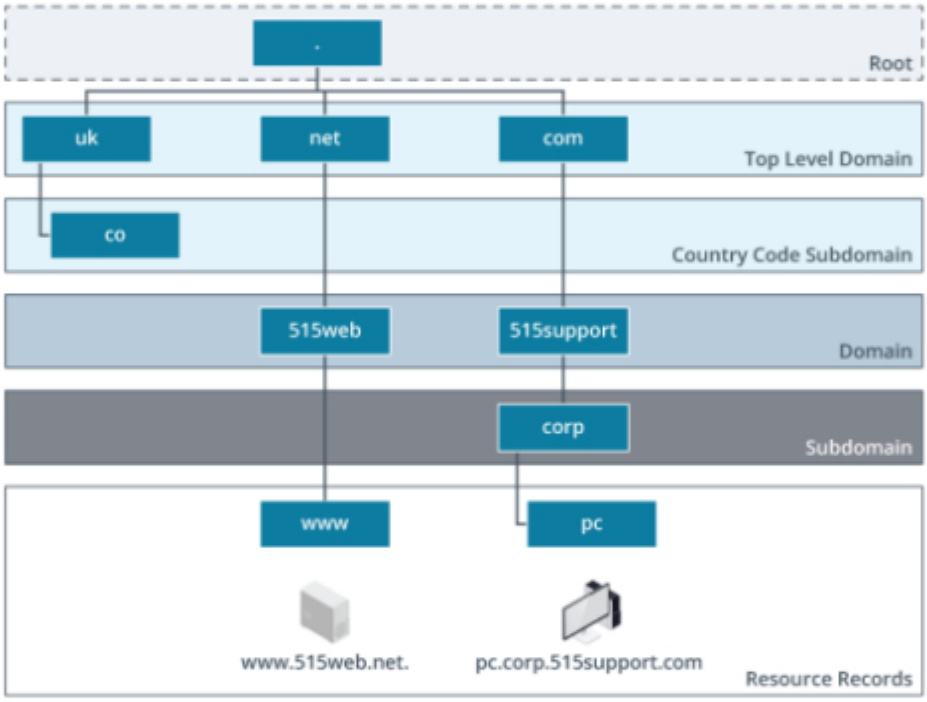
Selain itu, pendaftar Internet mungkin memiliki batasannya sendiri.

Sistem Nama Domain

Domain Name System (DNS) adalah hierarki global database server nama terdistribusi yang berisi informasi tentang domain dan host dalam domain tersebut. Di bagian atas hierarki DNS adalah root, yang diwakili oleh label nol, yang hanya terdiri dari titik (.). Ada 13 server tingkat root (A hingga M).

Tepat di bawah akar terletak domain tingkat atas (TLD). Ada beberapa jenis domain tingkat atas, tetapi yang paling umum adalah generik (seperti .com, .org, .net, .info, .biz), disponsori (seperti .gov, .edu), dan kode negara (seperti .uk, .ca, .de). DNS dioperasikan oleh ICANN (icann.org), yang juga mengelola TLD generik. Kode negara umumnya dikelola oleh organisasi yang ditunjuk oleh pemerintah terkait.

Informasi tentang domain ditemukan dengan menelusuri catatan dari akar ke bawah melalui hierarki. Server DNS root memiliki informasi lengkap tentang server domain tingkat atas. Pada gilirannya, server ini memiliki informasi yang berkaitan dengan server untuk domain tingkat kedua. Tidak ada server nama yang memiliki informasi lengkap tentang semua domain. Catatan dalam DNS memberi tahu mereka di mana server nama otoritatif untuk informasi yang hilang ditemukan.

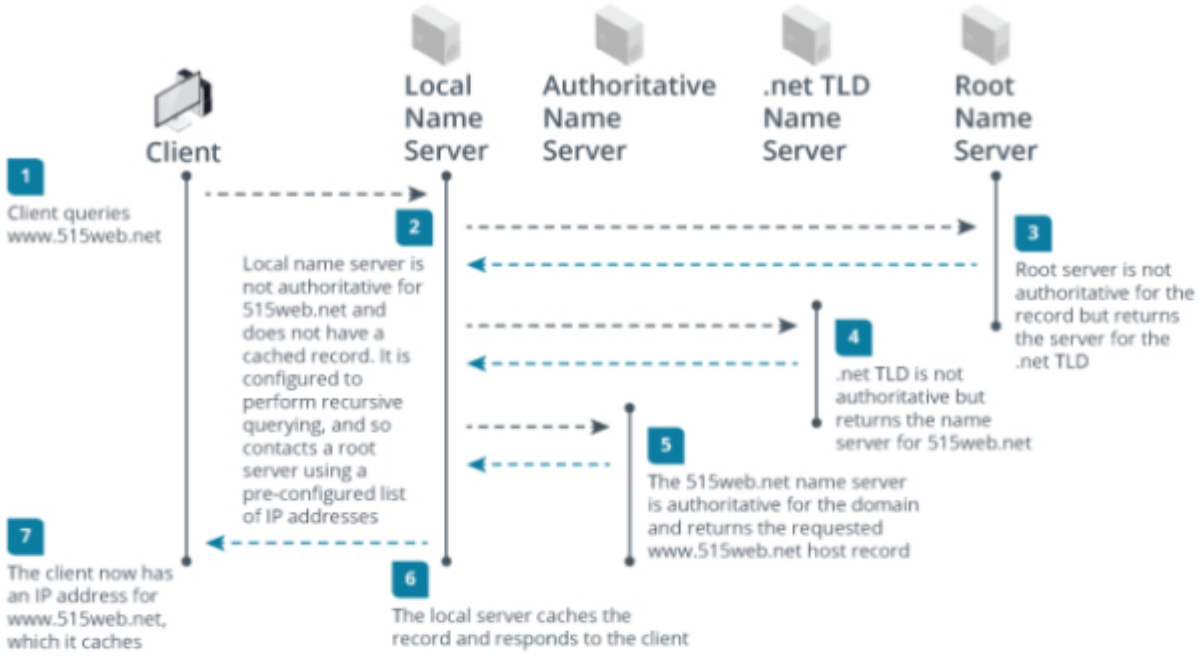


hierarki DNS. (Gambar © 123RF.com.)

FQDN mencerminkan hierarki ini, dari yang paling spesifik di sebelah kiri (catatan sumber daya host dengan namanya: pemetaan alamat IP) hingga yang paling tidak spesifik di sebelah kanan (TLD diikuti oleh root). Misalnya: pc.corp.515support.com.

Resolusi Nama Menggunakan DNS

Sinyal untuk memulai proses resolusi nama terjadi ketika pengguna menyajikan FQDN (seringkali dalam alamat web) ke program aplikasi, seperti browser web. Aplikasi klien, disebut sebagai stub resolver, memeriksa cache lokalnya untuk pemetaan. Jika tidak ada pemetaan yang ditemukan, kueri akan diteruskan ke server nama lokalnya. Alamat IP dari satu atau lebih server nama yang dapat bertindak sebagai resolver biasanya diatur dalam konfigurasi TCP/IP. Proses resolusi kemudian terjadi sebagai berikut:



DNS name resolution process. (Images © 123RF.com.)

Sebagian besar kueri antara server nama dilakukan sebagai pencarian berulang. Ini berarti bahwa server nama merespons kueri dengan catatan yang diminta atau alamat server nama di tingkat yang lebih rendah dalam hierarki yang otoritatif untuk namespace. Tidak ada upaya untuk mencoba membuat kueri tambahan untuk menemukan informasi yang tidak dimilikinya. Pada gambar, pada langkah 4 dan 5, server root dan server nama .net hanya melewati server kueri alamat server nama otoritatif. Mereka tidak mengambil tugas untuk menyelesaikan kueri asli untuk www.515web.net.

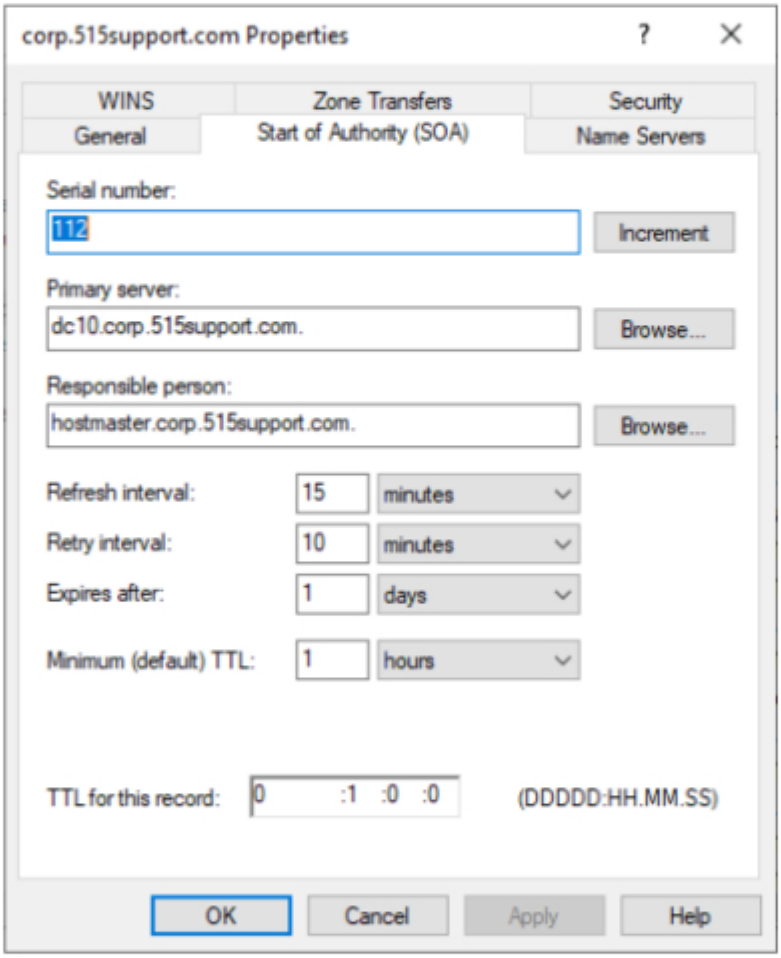
Pencarian rekursif berarti bahwa jika server yang ditanyakan tidak otoritatif, ia mengambil tugas untuk menanyakan server nama lain sampai menemukan catatan yang diminta atau waktu habis. Server nama yang tercantum dalam konfigurasi TCP/IP klien menerima kueri rekursif. Ini adalah jenis kueri yang dilakukan oleh server nama corp.515support.com.

Tips: Server DNS dapat dikonfigurasi untuk hanya melakukan kueri rekursif (penyelesai), atau mungkin melakukan kueri rekursif dan memelihara rekaman zona, atau mungkin hanya mempertahankan rekaman zona. Biasanya peran dibagi, terutama jika server terbuka ke Internet. Sebagian besar server DNS yang dapat diakses melalui Internet menonaktifkan kueri rekursif. Penyelesai rekursif biasanya hanya dapat diakses oleh pelanggan-pelanggan resmi dalam jaringan ISP atau klien di LAN pribadi, misalnya.

Jenis Catatan Sumber Daya

Zona DNS akan berisi banyak catatan sumber daya. Catatan ini memungkinkan server nama DNS untuk menyelesaikan kueri untuk nama dan layanan yang dihosting di domain menjadi alamat IP. Catatan sumber daya dapat dibuat dan diperbarui secara manual (statis), atau dapat dihasilkan secara dinamis dari informasi yang diterima dari komputer klien dan server di jaringan.

Catatan Mulai Otoritas (SOA) mengidentifikasi server nama otoritatif utama yang memelihara catatan sumber daya lengkap untuk zona tersebut. Server nama utama dapat digunakan untuk mengubah catatan sumber daya. SOA juga mencakup informasi kontak untuk zona dan nomor seri untuk kontrol versi.



Configuring a Start of Authority record in Windows DNS. (Screenshot courtesy of Microsoft.)

Catatan Name Server (NS) mengidentifikasi server nama DNS otoritatif untuk zona tersebut. Selain server nama utama, sebagian besar zona dikonfigurasi dengan server nama sekunder untuk redundansi dan penyeimbangan beban. Server nama sekunder

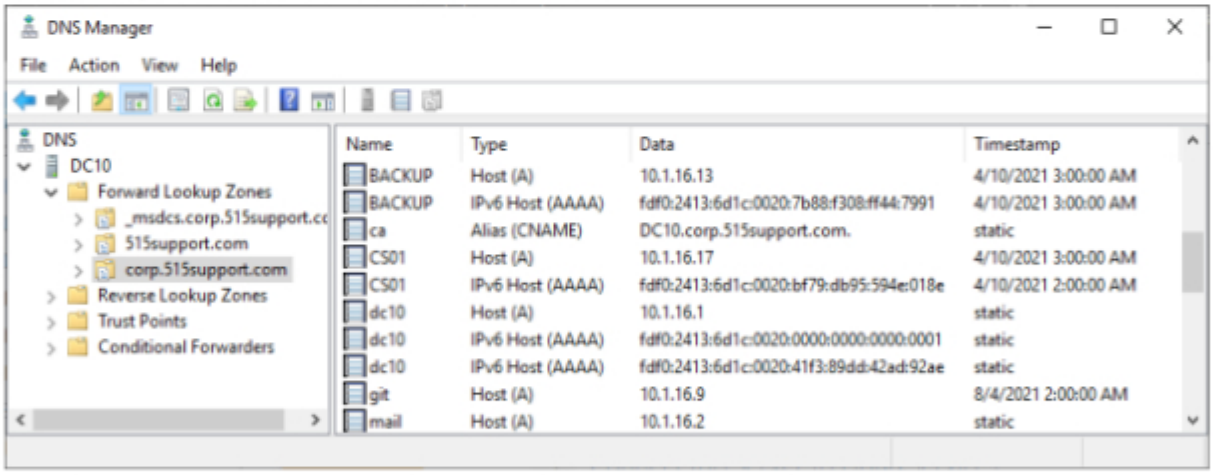
menyimpan salinan catatan sumber daya hanya-baca tetapi masih dapat menjadi otoritatif untuk zona tersebut.

```
;
; BIND data file for 515support.com
;
$TTL    604800
@       IN      SOA     ns1.515support.com. hostmaster.515support.com. (
                              2012080402         ; Serial
                                   3600         ; Refresh
                                   1800         ; Retry
                                 604800         ; Expire
                                  86400         ; Negative Cache TTL
)
        IN      NS      ns1.515support.com.
        IN      A       203.0.113.33
        IN      MX 10   mail.515support.com.
ns1     IN      A       203.0.113.33
www     IN      A       198.51.100.29
mail    IN      A       198.51.100.29
dvwa    IN      CNAME   www
```

Resource records configured on a BIND DNS server.

Host Address and Canonical Name Records

Catatan alamat (A) digunakan untuk menyelesaikan nama host ke alamat IPv4. Catatan AAAA menyelesaikan nama host ke alamat IPv6.



Both types of host records (A and AAAA) plus a CNAME record in Windows Server DNS. (Screenshot courtesy of Microsoft.)

Tips: DNS menggunakan protokol transport UDP melalui port 53 secara default, dan UDP memiliki ukuran paket maksimum 512 byte. Karena ukuran alamat IPv6 yang jauh lebih besar, catatan AAAA dapat melebihi ukuran ini. Hal ini dapat mengakibatkan paket UDP terfragmentasi menjadi beberapa paket yang lebih kecil. Ini dapat mengakibatkan

paket-paket ini diblokir oleh firewall jika tidak dikonfigurasi untuk mengharapkannya. Administrator jaringan harus memeriksa apakah server DNS mereka dapat menerima transmisi ini dan bahwa komponen perantara tidak memblokirnya.

Catatan Nama Kanonik (CNAME) (atau alias) digunakan untuk mengonfigurasi alias untuk catatan alamat yang ada (A atau AAAA). Misalnya, alamat IP server web dengan lampu catatan host juga dapat diselesaikan dengan alias www . Catatan CNAME juga sering digunakan untuk mempermudah administrasi DNS. Misalnya, alias dapat dialihkan ke host yang sama sekali berbeda untuk sementara selama pemeliharaan sistem.

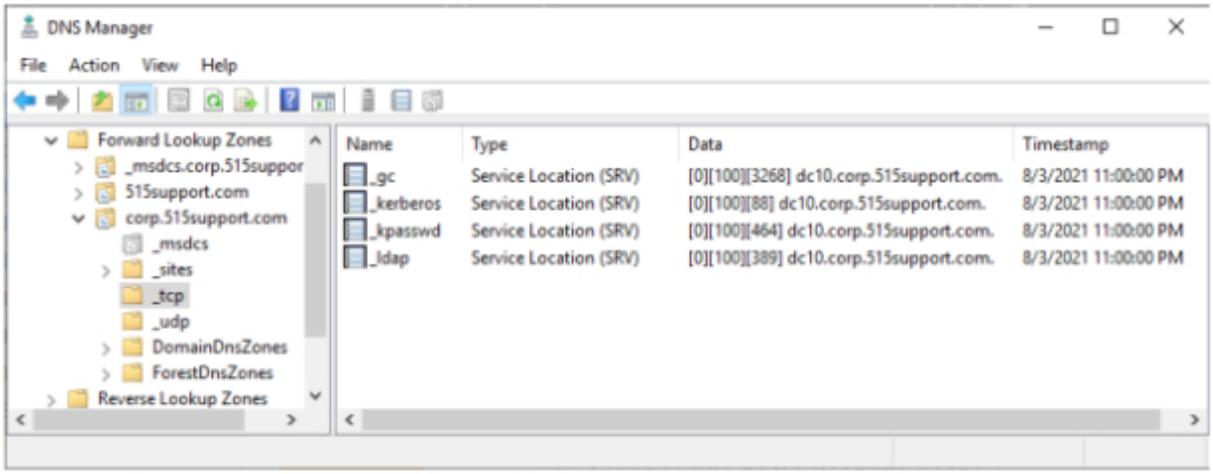
Beberapa catatan sumber daya bernama berbeda dapat merujuk ke alamat IP yang sama (dan sebaliknya dalam kasus penyeimbangan beban).

Tips: Tidak ada yang dapat menghentikan administrator mengonfigurasi beberapa catatan alamat untuk mengarahkan nama host yang berbeda ke alamat IP yang sama. Namun, menggunakan catatan CNAME biasanya dianggap sebagai praktik yang lebih baik. Dimungkinkan juga untuk mengonfigurasi beberapa catatan A atau AAAA dengan nama host yang sama tetapi alamat IP yang berbeda. Ini biasanya dilakukan sebagai teknik penyeimbangan beban dasar, yang disebut sebagai DNS round robin.

Pertukaran Surat, Layanan, dan Rekaman Teks

Data Mail Exchange (MX) digunakan untuk mengidentifikasi server email untuk domain. Dalam jaringan biasa, beberapa server dipasang untuk menyediakan redundansi, dan masing-masing akan diwakili dengan data MX. Setiap catatan server diberikan nilai preferensi dengan entri bernomor terendah lebih disukai. Host yang diidentifikasi dalam data MX harus memiliki data A atau AAAA terkait. Data MX tidak boleh mengarah ke data CNAME.

Sementara sebagian besar catatan DNS digunakan untuk menyelesaikan nama menjadi alamat IP, catatan Layanan (SRV) berisi nama layanan dan port tempat aplikasi tertentu di-host. Catatan SRV sering digunakan untuk mencari VoIP atau server media. Catatan SRV juga merupakan bagian penting dari infrastruktur yang mendukung Direktori Aktif Microsoft; mereka digunakan oleh klien untuk menemukan pengontrol domain, misalnya. Seperti halnya MX, data SRV dapat dikonfigurasi dengan nilai prioritas.

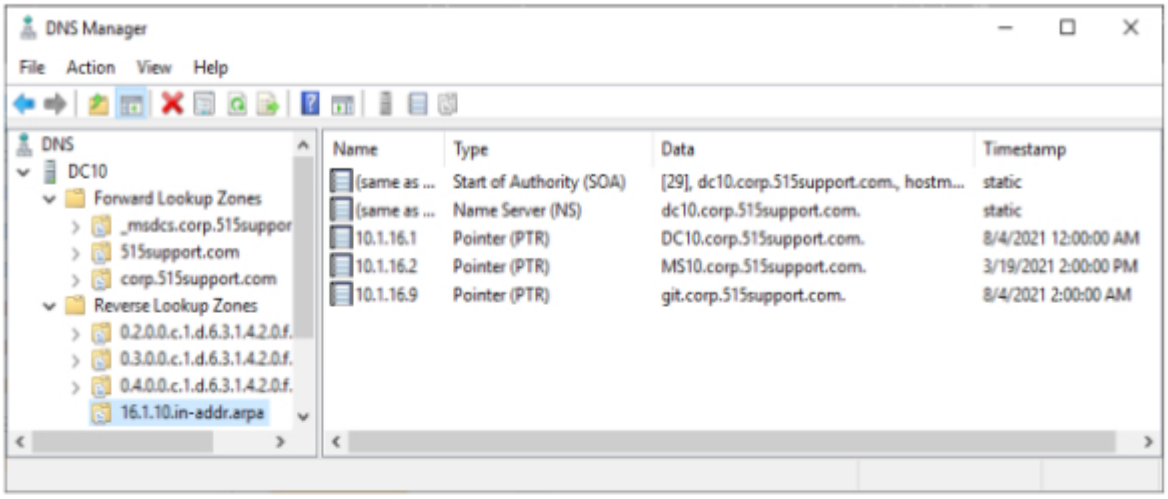


SRV records in Windows Server DNS. (Screenshot courtesy of Microsoft.)

Data TXT digunakan untuk menyimpan teks bentuk bebas apa pun yang mungkin diperlukan untuk mendukung layanan jaringan lainnya. Satu nama domain mungkin memiliki banyak data TXT, tetapi yang paling umum digunakan sebagai bagian dari Sender Policy Framework (SPF) dan DomainKeys Identified Mail (DKIM). Catatan SPF digunakan untuk mencantumkan alamat IP atau nama server yang diizinkan untuk mengirim email dari domain tertentu dan digunakan untuk memerangi pengiriman spam. Data DKIM digunakan untuk memutuskan apakah Anda harus mengizinkan email yang diterima dari sumber tertentu, mencegah spam dan spoofing email. DKIM dapat menggunakan tanda tangan terenkripsi untuk membuktikan bahwa pesan benar-benar berasal dari domain yang diklaimnya.

Pointer Records

Server DNS mungkin memiliki dua jenis zona: pencarian maju dan pencarian terbalik. Zona pencarian maju berisi catatan sumber daya yang terdaftar sebelumnya. Misalnya, mengingat catatan nama, pencarian ke depan mengembalikan alamat IP; data MX mengembalikan catatan host yang terkait dengan layanan email domain. Sebaliknya, permintaan DNS terbalik mengembalikan nama host yang terkait dengan alamat IP yang diberikan. Informasi ini disimpan di zona pencarian terbalik sebagai catatan penunjuk (PTR).



Reverse lookup zone and pointer records in Windows Server DNS. (Screenshot courtesy of Microsoft.)

Permintaan DNS terbalik menggunakan domain khusus yang diberi nama oleh tiga oktet pertama alamat IP di zona dalam urutan terbalik dan ditambahkan dengan in-addr.arpa. Server nama dikonfigurasi dengan zona pencarian terbalik. Zona ini berisi catatan PTR yang terdiri dari oktet akhir dari setiap catatan host. Misalnya, pencarian terbalik untuk catatan host yang berisi alamat IP 198.51.100.1 adalah:

1.100.51.198.in-addr.arpa

IPv6 menggunakan domain ip6.arpa; masing-masing dari 32 karakter hex dalam alamat IPv6 dinyatakan dalam urutan terbalik sebagai subdomain. Misalnya, alamat IPv6:

2001:0db8:0000:0000:0bcd:abcd:ef12:1234

diwakili oleh catatan pointer berikut:

4.3.2.1.2.1.f.e.d.c.b.a.d.c.b.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa

Zona pencarian terbalik tidak wajib dan sering dihilangkan dari server DNS, karena dapat digunakan oleh peretas untuk bekerja secara berurutan melalui berbagai alamat IP untuk menemukan nama perangkat yang berguna atau menarik, yang kemudian dapat ditargetkan oleh mekanisme peretasan lainnya.

Modul 11

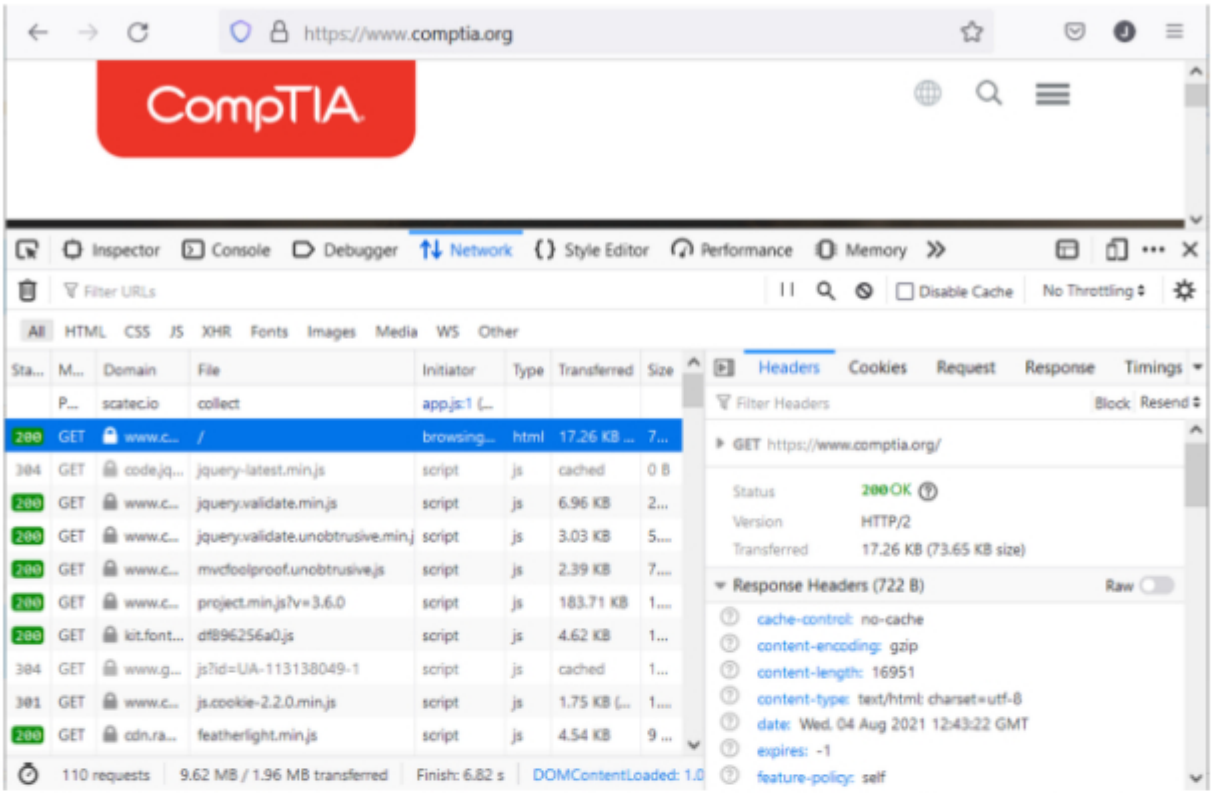
Explaining Network Applications

EXPLAIN THE USE OF WEB, FILE/PRINT, AND DATABASE SERVICES

Pendahuluan: Menjelaskan Penggunaan Web, File/Print, and Database Services
Sejauh ini, Anda telah mempelajari layanan lapisan bawah yang memungkinkan konektivitas dasar antar node. Di atas ini adalah layanan yang menyediakan fungsi yang berguna bagi pengguna, seperti penjelajahan web, berbagi file/cetak, dan basis data. Layanan yang merupakan bagian dari paket protokol TCP/IP sebagian besar adalah protokol dan aplikasi client-server. Aplikasi client-server didasarkan pada server terpusat yang menyimpan informasi dan menunggu permintaan dari klien. Anda memerlukan pemahaman yang baik tentang bagaimana protokol ini digunakan sehingga Anda dapat mendukungnya di jaringan Anda.

Transfer Hypertext Protocol
Situs web dan aplikasi web mungkin merupakan layanan jaringan yang paling berguna dan ada di mana-mana. Teknologi web dapat digunakan untuk berbagai macam fungsi dan aplikasi, sama sekali tidak terbatas pada halaman statis informasi yang menjadi ciri situs web pertama. Dasar dari teknologi web adalah HyperText Transfer Protocol (HTTP). HTTP memungkinkan klien (biasanya browser web) untuk meminta sumber daya dari server HTTP. Seorang klien terhubung ke server HTTP menggunakan port TCP yang sesuai (TCP/80, secara default) dan mengirimkan permintaan untuk sumber daya, menggunakan pencari sumber daya seragam (URL). Server mengakui permintaan dan merespon dengan data atau dengan pesan kesalahan.

HTTP Headers and Payload
Format respons dan permintaan ditentukan di header HTTP. Payload HTTP biasanya digunakan untuk melayani halaman web HyperText Markup Language (HTML), yang merupakan file teks biasa dengan tag kode yang menjelaskan bagaimana halaman harus diformat. Browser web dapat menginterpretasikan tag dan menampilkan teks dan sumber daya lain yang terkait dengan halaman, seperti gambar biner atau file suara yang ditautkan ke halaman HTML.



Using Firefox's web developer tools to inspect the HTTP requests and response headers involved in serving a typical modern web page. (Screenshot courtesy of Mozilla Foundation.)

HTTP juga dilengkapi mekanisme formulir (POST) yang memungkinkan pengguna untuk mengirimkan data dari klien ke server. HTTP secara nominal adalah protokol tanpa kewarganegaraan; ini berarti bahwa server tidak diharuskan untuk menyimpan informasi tentang klien selama sesi. Namun, fungsionalitas dasar server HTTP juga sering diperluas dengan dukungan untuk skrip dan fitur yang dapat diprogram (aplikasi web). Server juga dapat mengatur cookie file teks untuk menyimpan informasi sesi. Fitur pengkodean ini, ditambah integrasi dengan database, meningkatkan fleksibilitas dan interaktivitas, tetapi juga meningkatkan permukaan serangan dan mengekspos lebih banyak kerentanan.

Tips: Banyak yang berpendapat bahwa HTTP adalah protokol stateful. Versi 2 HTTP menambahkan lebih banyak fitur pelestarian negara (blog.zamicol.com/2017/05/is-http2-stateful-protocol-application.html).

Web Servers

Sebagian besar organisasi memiliki kehadiran online, diwakili oleh situs web. Untuk menjalankan situs web, itu harus di-host di server HTTP yang terhubung ke Internet. Organisasi yang lebih besar atau UKM dengan keahlian yang relevan dapat meng-host situs web itu sendiri, tetapi biasanya, sebuah organisasi akan menyewa server atau ruang di server dari ISP. Jenis paket hosting berikut ini umum:

- **Dedicated Serve**r - ISP mengalokasikan komputer server pribadi Anda sendiri. Jenis layanan ini biasanya tidak dikelola (atau manajemen dikenakan biaya tambahan).
- **Virtual Private Server (VPS)** - ISP mengalokasikan Anda mesin virtual (VM) di server fisik. Ini diisolasi dari contoh pelanggan lain oleh hypervisor.
- **Cloud Hosting** - Situs web Anda dijalankan di awan melalui beberapa komputer perangkat keras, memungkinkan lebih banyak skalabilitas jika pola permintaan berubah.
- **Shared Hosting** - Situs web Anda di-host dalam direktori pribadi di server bersama. Kinerja dapat sangat dipengaruhi oleh situs lain yang dihosting di server, karena semua situs bersaing untuk mendapatkan sumber daya yang sama. Platform server web utama adalah Apache®, Microsoft Internet Information Server (IIS), dan nginx.

Secure Sockets Layer/Transport Layer Security
Salah satu masalah kritis untuk penyediaan situs web awal adalah kurangnya keamanan di HTTP. Di bawah HTTP, semua data dikirim tidak terenkripsi, dan tidak ada otentikasi klien atau server. *Secure Sockets Layer* (SSL) dikembangkan oleh Netscape pada 1990-an untuk mengatasi masalah ini. SSL terbukti sangat populer di kalangan industri. *Transport Layer Security* (TLS) dikembangkan dari SSL dan diratifikasi sebagai standar oleh IETF.

SSL/TLS bekerja sebagai lapisan antara lapisan Aplikasi dan Transport dari tumpukan TCP/IP, atau, dalam istilah OSI, pada lapisan Sesi. Biasanya digunakan untuk mengenkripsi koneksi TCP. Ketika digunakan dengan aplikasi HTTP, ini disebut sebagai HTTP Secure (HTTPS). TLS juga dapat digunakan untuk mengamankan protokol aplikasi TCP lainnya, seperti FTP, POP3/IMAP, SMTP, dan LDAP.

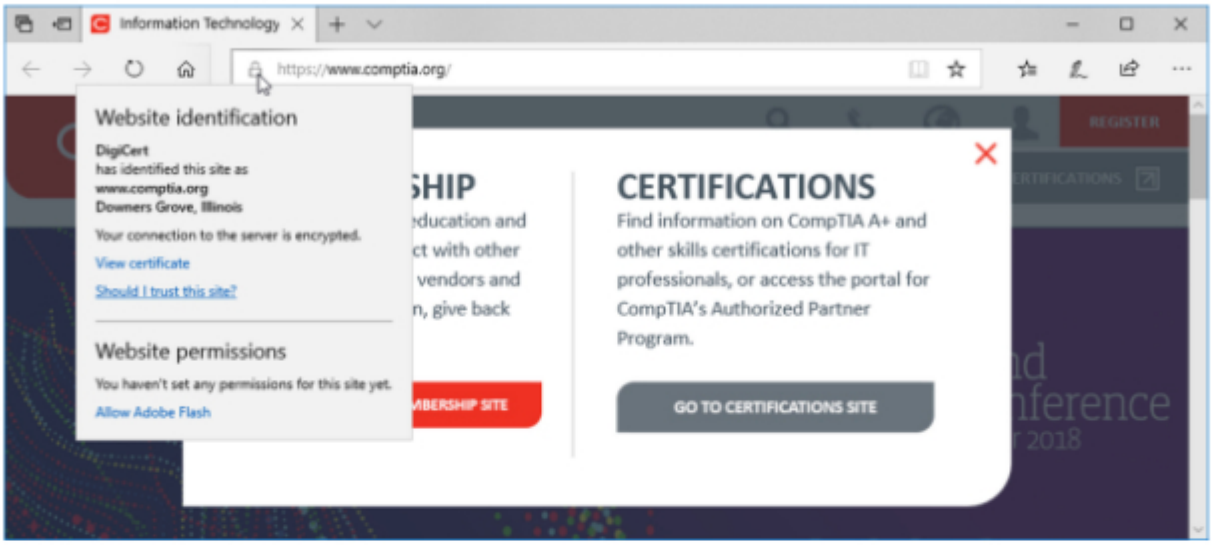
Tips: TLS juga dapat digunakan dengan UDP, disebut sebagai *Datagram Transport Layer Security* (DTLS), paling sering dalam solusi *virtual private networking* (VPN).

Untuk mengimplementasikan HTTPS, server web diinstal dengan sertifikat digital yang dikeluarkan oleh beberapa otoritas *certificate authority* (CA). Sertifikat menggunakan data terenkripsi untuk membuktikan identitas server, dengan asumsi bahwa klien juga mempercayai CA. Sertifikat adalah pembungkus untuk pasangan kunci enkripsi publik/pribadi. Kunci pribadi disimpan sebagai rahasia yang hanya diketahui oleh server; kunci publik diberikan kepada klien melalui sertifikat digital.

Server dan klien menggunakan pasangan kunci dalam sertifikat digital dan rangkaian sandi yang dipilih dalam protokol SSL/TLS untuk menyiapkan terowongan terenkripsi. Meskipun orang lain mungkin mengetahui kunci publik, mereka tidak dapat mendekripsi konten terowongan tanpa memperoleh kunci pribadi server. Ini berarti bahwa komunikasi tidak dapat dibaca atau diubah oleh pihak ketiga.

Lalu lintas terenkripsi antara klien dan server dikirim melalui port TCP 443 (secara default), daripada port terbuka dan tidak terenkripsi 80. Browser web akan membuka sesi aman ke server yang menyediakan layanan ini dengan menggunakan URL yang dimulai dengan https:/ /

dan itu juga akan menampilkan ikon gembok di bilah alamat untuk menunjukkan bahwa koneksi aman. Situs web dapat dikonfigurasi untuk meminta sesi aman dan menolak atau mengalihkan permintaan HTTP biasa.



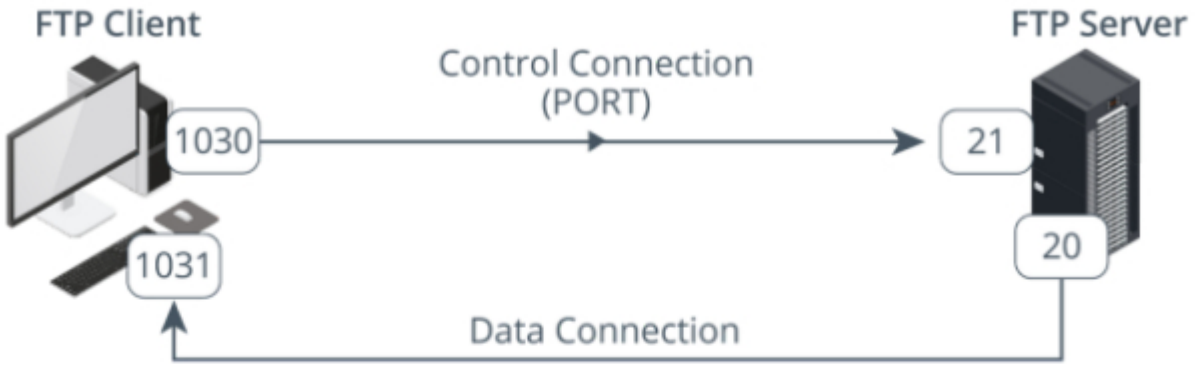
HTTPS padlock icon. (Screenshot courtesy of Microsoft.)

File Transfer Protocol

Seringkali diperlukan untuk mentransfer file ke dan dari peralatan atau server dari host jarak jauh. Banyak metode akses file jarak jauh menggunakan beberapa bentuk *File Transfer Protocol* (FTP). Sementara layanan web dan aplikasi web berbasis HTTPS sekarang dapat menawarkan unduhan file kepada pengguna akhir, FTP masih sering digunakan untuk melakukan pengunggahan/pengunduhan file administratif ke dan dari server dan peralatan. Untuk penggunaan ini, penting untuk mengamankan sesi FTP.

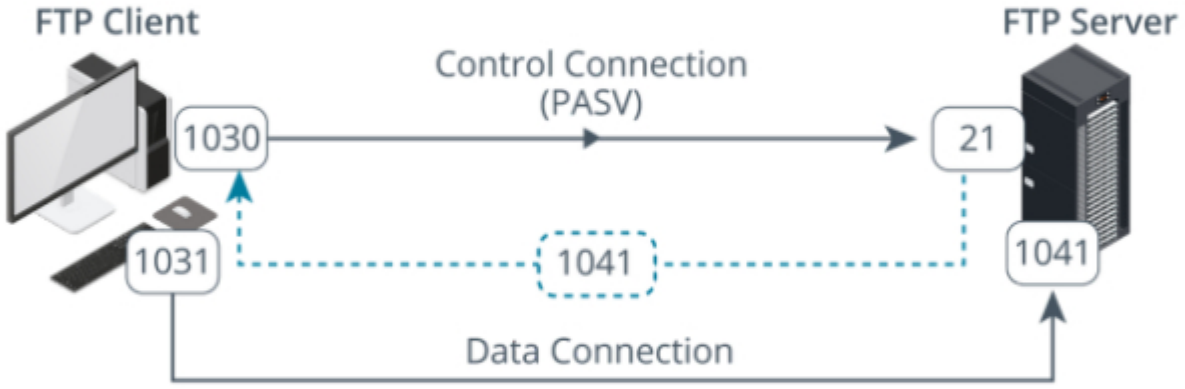
Active versus Passive FTP

Klien FTP terhubung ke port TCP 21 pada server FTP dan membuka nomor port klien dinamis yang dipilih (n). Port kontrol port 21 TCP digunakan untuk mentransfer perintah dan informasi status, tetapi tidak untuk transfer data. Transfer data dapat beroperasi dalam salah satu dari dua mode: aktif atau pasif. Dalam mode aktif, klien mengirimkan perintah PORT yang menentukan nomor port koneksi data yang dipilihnya (biasanya n+1), dan server membuka koneksi data antara port klien yang dipilih dan port TCP 20 di server.



FTP dalam mode aktif. (Gambar © 123RF.com.)

Dalam mode pasif, klien membuka port data (sekali lagi, biasanya n+1) dan mengirimkan perintah PASV ke port kontrol server. Server kemudian membuka nomor port tinggi secara acak dan mengirimkannya ke klien menggunakan perintah PORT. Klien kemudian memulai koneksi antara dua port.



FTP dalam mode pasif. (Gambar © 123RF.com.)

FTP aktif menimbulkan masalah konfigurasi untuk beberapa firewall, karena server memulai koneksi masuk, tetapi tidak ada cara untuk memprediksi nomor port mana yang akan digunakan. Namun, tidak semua server dan klien FTP dapat beroperasi dalam mode pasif. Jika demikian, periksa apakah firewall yang dipasang antara klien dan server dapat mendukung FTP aktif (firewall inspeksi stateful).

Tips: Masalah lainnya adalah koneksi kontrol dapat tetap idle saat koneksi data sedang digunakan, artinya koneksi dapat "dihabiskan" oleh firewall (atau perangkat perutean lainnya).

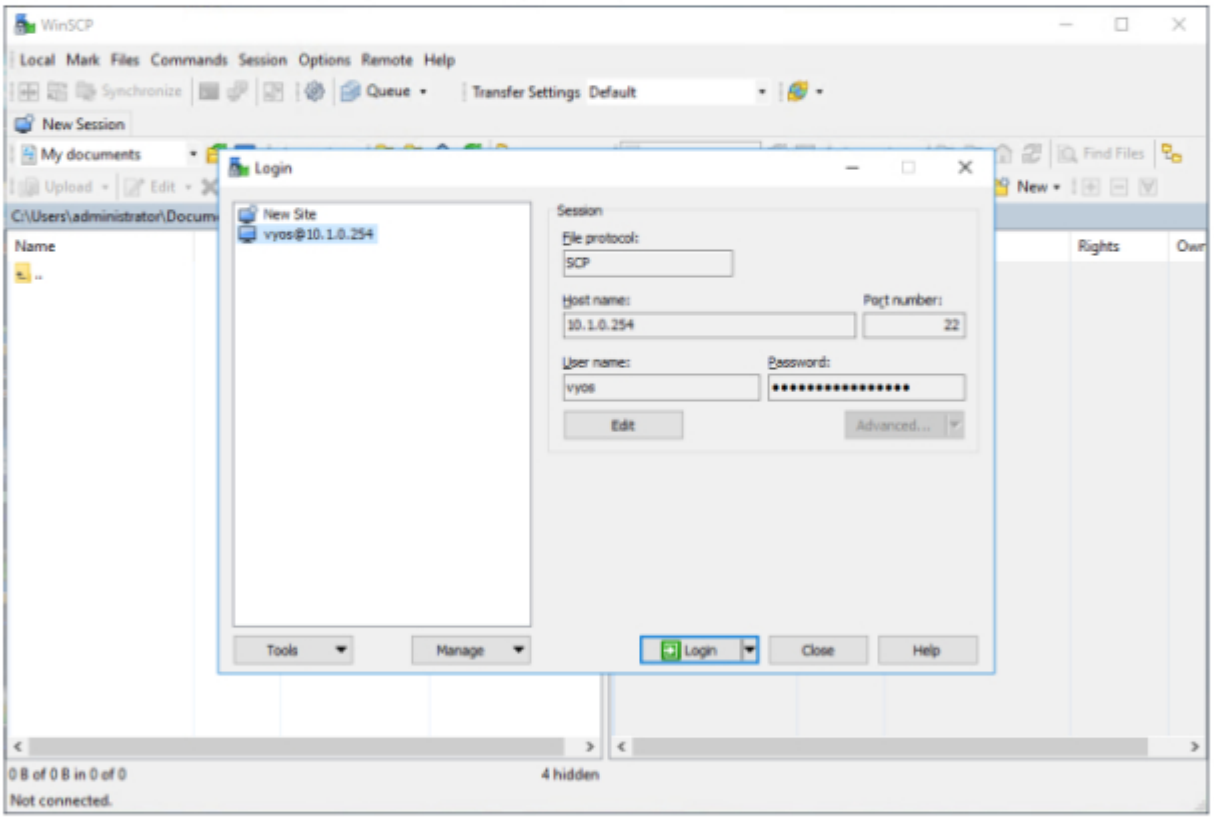
Trivial File Transfer Protocol

*Trivial File Transfer Protoco*l (TFTP) adalah protokol tanpa koneksi yang berjalan di atas port UDP 69. Akibatnya, TFTP tidak memberikan jaminan pengiriman yang ditawarkan oleh FTP dan hanya cocok untuk mentransfer file kecil. Juga, ini hanya mendukung membaca (GET) dan

menulis (PUT) file, bukan penjelajahan direktori, penghapusan file, atau fitur FTP lainnya. Server TFTP paling sering digunakan oleh peralatan jaringan lama (switch, router, workstation tanpa disk, dan printer) untuk mengunduh file konfigurasi. Ini juga dapat digunakan sebagai metode pencadangan dan pemulihan untuk file konfigurasi. Namun, TFTP tidak memiliki mekanisme keamanan dan peralatan tidak lagi dibatasi sumber dayanya seperti pada masa-masa awal jaringan. Akibatnya, protokol aman sekarang lebih disukai untuk fungsi-fungsi ini.

Secure File Transfer Protocol

Secure FTP (SFTP) mengatasi masalah privasi dan integritas FTP dengan mengenkripsi otentikasi dan transfer data antara klien dan server. Di SFTP, tautan aman dibuat antara klien dan server menggunakan Secure Shell (SSH) melalui port TCP 22. Perintah FTP biasa dan transfer data kemudian dapat dikirim melalui tautan aman tanpa risiko penyadapan. Solusi ini memerlukan server SSH yang mendukung perangkat lunak klien SFTP plus SFTP.



WinSCP SFTP client. (Screenshot courtesy of WinSCP.)

Cara lain untuk mengamankan FTP adalah dengan menggunakan protokol keamanan koneksi SSL/TLS. Ada dua cara untuk mengonfigurasi FTP melalui TLS:

Explicit TLS (FTPES)-Gunakan perintah AUTH TLS untuk meningkatkan koneksi tidak aman yang dibuat melalui port 21 ke koneksi yang aman. Ini melindungi kredensial otentikasi. Koneksi data untuk transfer file yang sebenarnya juga dapat dienkripsi (menggunakan perintah PROT).

TLS implisit (FTPS)-Negosiasikan terowongan SSL/TLS sebelum pertukaran perintah FTP apa pun. Mode ini menggunakan port aman 990 untuk koneksi kontrol. FTPS sulit untuk dikonfigurasi ketika ada firewall antara klien dan server. Akibatnya, FTPES biasanya merupakan metode yang disukai.

File and Print Services

File and Print Services memungkinkan klien jaringan untuk berbagi akses ke disk dan sumber daya printer.

Server Message Block

Pada jaringan Windows®, Layanan Berbagi File/Cetak disediakan oleh protokol Server Message Block (SMB). SMB memungkinkan host untuk membagikan direktori/file dan printernya agar tersedia untuk digunakan mesin lain. Dukungan untuk SMB di mesin berbasis UNIX atau Linux dan peralatan penyimpanan terpasang jaringan (NAS) disediakan dengan menggunakan rangkaian perangkat lunak Samba (samba.org/samba/what_is_samba.html), yang memungkinkan klien Windows mengakses host Linux sebagai meskipun itu adalah file Windows atau server cetak.

Pada jaringan lama, SMB dijalankan sebagai bagian dari protokol layanan jaringan lama yang disebut NetBIOS pada port TCP 139. Namun, jika tidak diperlukan dukungan klien lama, SMB biasanya dijalankan langsung melalui port TCP 445. SMB harus dibatasi untuk digunakan hanya pada jaringan lokal. Adalah penting bahwa setiap lalu lintas pada kisaran port NetBIOS (137-139) dan port 445 diblokir oleh firewall perimeter.

SMB versi 3 mendukung enkripsi pesan, yang dapat diaktifkan pada server file atau pada basis per-share. Berbagi terenkripsi hanya dapat diakses oleh klien SMB 3.0 atau lebih tinggi.

Tips: SMB telah melalui beberapa pembaruan, dengan SMB3 sebagai versi saat ini. SMB1 memiliki kerentanan keamanan yang sangat serius dan sekarang dinonaktifkan secara default pada versi Windows saat ini (docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2 -v3).

Remote Print Protocols

Printer dapat dihubungkan ke jaringan menggunakan tautan kabel atau nirkabel dan dikonfigurasi dengan alamat IP dan FQDN. Host harus dapat terhubung ke printer, mengonfigurasi opsi dan pengaturan cetak, mengirim pekerjaan cetak, dan menerima pesan status, seperti kesalahan kertas habis. Fungsi-fungsi ini diimplementasikan menggunakan protokol cetak jarak jauh untuk berkomunikasi antara proses monitor cetak yang berjalan di host dan perangkat cetak:

- Port 9100-Ini dapat disebut sebagai port TCP/IP standar, AppSocket, atau JetDirect. Port ini hanya membuat koneksi TCP untuk mentransfer data pekerjaan cetak Page Description Language (PDL) mentah serta konfigurasi dan data manajemen Bahasa Pekerjaan Printer (PJL). Dua PDL yang paling umum adalah PostScript (PS) dan Printer Command Language (PCL). Sebagian besar printer mendukung pesan status dua arah untuk menginformasikan monitor cetak host tentang kondisi kesalahan, seperti kertas habis atau kertas macet.
- *Internet Printing Protocol* (IPP)-Ini adalah bentuk adaptasi dari HTTP yang menggunakan TCP port 631 dan dapat diimplementasikan sebagai protokol aman (IPPS). Ini memberikan dukungan yang lebih baik untuk pesan status daripada port 9100.
- Layanan Web untuk Perangkat (WSD)/AirPrint-Teknologi ini memungkinkan perangkat cetak untuk mengiklankan kemampuan layanan melalui jaringan dan untuk host Windows dan MacOS/iOS masing-masing untuk menambahkan perangkat menggunakan plug-and-play dan mengelolanya menggunakan pesan status dua arah. Mereka juga memungkinkan koneksi aman ke perangkat cetak.
- Berbagi printer-Ini berarti bahwa sebuah host terhubung ke printer (menggunakan koneksi lokal atau jaringan) dan kemudian berbagi objek printer dengan host lain menggunakan SMB. Pekerjaan cetak dan pesan status dikirim melalui host yang berbagi printer.

Databases Services

Basis data menyediakan informasi dalam format yang dapat dibaca dan diperbarui melalui beberapa jenis bahasa kueri. Ada dua jenis utama database. Database relasional menyimpan informasi dalam tabel dengan baris (catatan) dan kolom (bidang). Hubungan antara bidang data dalam tabel yang berbeda dibuat menggunakan bidang kunci yang secara unik mengidentifikasi setiap catatan. Basis data relasional dioperasikan menggunakan bahasa kueri terstruktur (SQL). SQL mendefinisikan perintah seperti SELECT untuk mengambil informasi atau UPDATE untuk mengubahnya.

SQL telah diimplementasikan dalam platform sistem manajemen basis data relasional (RDBMS) oleh beberapa vendor yang berbeda. Selain menyediakan implementasi SQL, RDBMS juga menyediakan alat manajemen dan sering kali GUI yang digunakan untuk mengoperasikan database. Protokol akses jarak jauh memungkinkan klien untuk terhubung ke server database melalui jaringan dan memungkinkan lalu lintas replikasi untuk berpindah antar server database. Replikasi adalah sarana sinkronisasi data yang diadakan di setiap server. Setiap RDBMS menggunakan port TCP yang berbeda untuk membedakannya sebagai layanan aplikasi:

- Protokol akses data jarak jauh Oracle SQL*Net menggunakan TCP/1521.
- Microsoft SQL Server menggunakan TCP/1433.
- Platform MySQL open-source menggunakan TCP/3306. Platform MariaDB bercabang dari MySQL menggunakan port yang sama.
- Platform PostgreSQL open-source menggunakan TCP/5432.

Tips: Ini adalah port utama. RDBMS kemungkinan akan menggunakan port TCP atau UDP lain untuk fungsi tambahan.

Secara default, port ini tidak aman. Namun, server RDBMS dapat diinstal dengan sertifikat dan dikonfigurasi untuk mengaktifkan enkripsi transport TLS. Koneksi masih dilakukan melalui port yang sama. Server atau klien dapat dikonfigurasi untuk meminta enkripsi dan memutuskan sambungan jika profil keamanan yang valid tidak tersedia. Opsional, klien juga dapat diinstal dengan sertifikat dan server dikonfigurasi untuk menolak koneksi dari klien tanpa sertifikat yang valid.

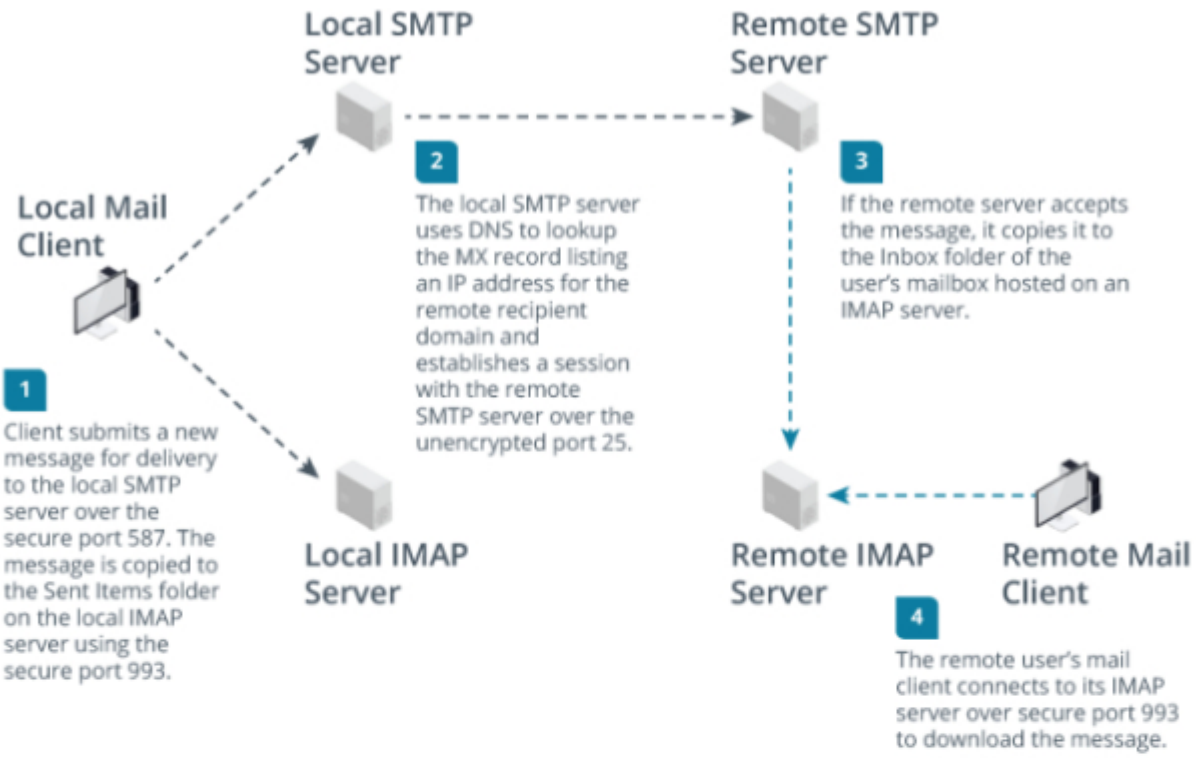
Jenis database lainnya disebut sebagai NoSQL atau "tidak hanya SQL." Daripada tabel relasional yang sangat terstruktur, data NoSQL dapat menggunakan berbagai format, seperti pasangan nilai kunci atau kolom lebar (di mana baris tidak harus memiliki kumpulan bidang yang sama). Basis data NoSQL biasanya diakses menggunakan antarmuka pemrograman aplikasi (API) melalui HTTPS.
Tips: Semua platform RDBMS juga menyediakan dukungan untuk penyimpanan data NoSQL. Ada juga platform NoSQL khusus, seperti MongoDB, DynamoDB Amazon, dan CouchDB.

EXPLAIN THE USE OF EMAIL AND VOICE SERVICES

Pendahuluan: Penggunaan Layanan Email dan Suara
Penggunaan layanan pesan, suara, dan video sekarang umum di rumah dan di banyak tempat kerja. Aplikasi real-time ini membawa tantangannya sendiri untuk arsitektur jaringan, dan Anda perlu memahami tuntutan kinerja ini untuk membangun jaringan yang dapat mendukungnya.

Simple Mail Transfer Protocol

Surat elektronik memungkinkan seseorang untuk menulis pesan dan mengirimkannya ke pengguna lain di jaringan mereka sendiri (intranet) atau di mana saja di dunia melalui Internet. Email menggunakan transfer surat dan protokol akses kotak surat yang terpisah:



Operation of delivery and mailbox email protocols. (Images © 123RF.com.)

Simple Mail Transfer Protocol (SMTP) menentukan bagaimana email dikirim dari satu sistem ke sistem lainnya. Server SMTP pengirim menemukan alamat IP server SMTP penerima dengan menggunakan bagian nama domain dari alamat email penerima. Server SMTP untuk domain terdaftar di DNS menggunakan data *Mail Exchange* (MX) dan host (A/AAAA).

SMTP tidak mengantri pesan tanpa batas. Jika ada masalah komunikasi, server SMTP mencoba ulang secara berkala sebelum waktu habis dan mengembalikan *non-delivery report* (NDR) ke pengirim. NDR akan berisi kode kesalahan yang menunjukkan alasan item tidak dapat dikirim. SMTP tidak menyediakan mekanisme untuk penyimpanan pesan yang persisten.

Komunikasi SMTP dapat diamankan menggunakan protokol versi TLS (SMTPS). Ini berfungsi seperti HTTPS dengan sertifikat di server SMTP dan negosiasi antara klien dan server tentang suite sandi mana yang akan digunakan. Ada dua cara bagi SMTP untuk menggunakan TLS:

- **STARTTLS**-Ini adalah perintah yang meningkatkan koneksi tidak aman yang ada untuk menggunakan TLS. Ini juga disebut sebagai TLS eksplisit atau TLS oportunistik.
- **SMTPS**-Ini membuat koneksi aman sebelum perintah SMTP (HELO, misalnya) dipertukarkan. Ini juga disebut sebagai TLS implisit.

Metode STARTTLS umumnya lebih banyak diterapkan daripada SMTPS. Konfigurasi SMTP tipikal menggunakan port dan layanan aman berikut:

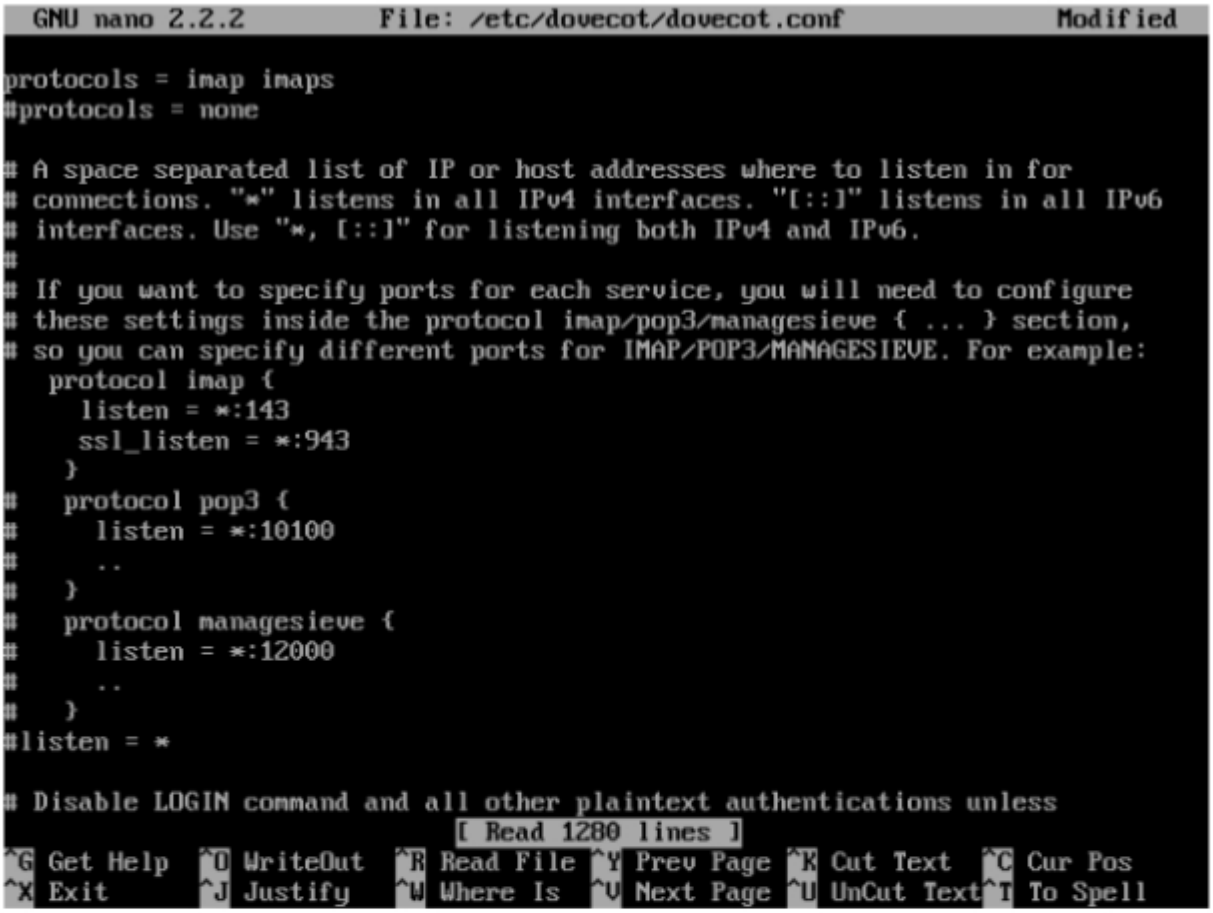
- **Port 25**-Digunakan untuk relai pesan antara server SMTP, atau agen transfer pesan (MTA). Jika keamanan diperlukan dan didukung oleh kedua server, perintah STARTTLS dapat digunakan untuk mengatur koneksi aman.
- **Port 587**-Digunakan oleh klien email atau agen pengiriman pesan (MSA) untuk mengirimkan pesan untuk pengiriman oleh server SMTP. Server yang dikonfigurasi untuk mendukung port 587 harus menggunakan STARTTLS dan memerlukan otentikasi sebelum pengiriman pesan.

Tips: Klien email dapat menggunakan port 25 untuk mengirimkan pesan ke server untuk pengiriman, tetapi ini bukan praktik terbaik. Penggunaan port 25 biasanya dicadangkan untuk relai antar server.

Mailbox Access Protocols
SMTP hanya berguna untuk mengirimkan email ke host yang tersedia secara permanen. Saat pesan diterima oleh server SMTP, pesan tersebut dikirimkan ke server kotak surat. Ini bisa berupa mesin terpisah atau proses terpisah yang berjalan di server yang sama. Protokol akses kotak surat memungkinkan perangkat lunak email klien pengguna untuk mengoperasikan kotak surat.

Post Office Protocol

Post Office Protocol (POP) adalah contoh awal dari protokol akses kotak surat. POP sering disebut sebagai POP3 karena versi protokol yang aktif adalah versi 3. Aplikasi klien POP, seperti Microsoft Outlook® atau Mozilla Thunderbird®, membuat sambungan ke server POP pada port TCP 110. Pengguna diautentikasi (dengan nama pengguna dan kata sandi), dan isi kotak suratnya diunduh untuk diproses di PC lokal. Secara umum, pesan dihapus dari server kotak surat saat diunduh, meskipun beberapa klien memiliki opsi untuk meninggalkan pesan di server.



Configuring mailbox access protocols on a server. (Screenshot courtesy of Mozilla Foundation.)

Seperti protokol aplikasi TCP lainnya, POP mentransfer semua informasi sebagai teks yang jelas. Ini berarti siapa pun yang dapat memantau sesi akan dapat memperoleh kredensial pengguna dan mengintip pesan. POP dapat diamankan dengan menggunakan enkripsi TLS. Port TCP default untuk POP (POP3S) aman adalah port 995.

Internet Message Access Protocol

POP memiliki beberapa batasan signifikan, beberapa di antaranya ditangani oleh *Internet Message Access Protocol* (IMAP). Seperti POP, IMAP adalah protokol pengambilan surat, tetapi dengan fitur manajemen kotak surat yang kurang di POP. POP terutama dirancang untuk akses dial-up; klien menghubungi server untuk mengunduh pesannya, dan kemudian memutuskan sambungan. IMAP mendukung koneksi permanen ke server dan menghubungkan beberapa klien ke kotak surat yang sama secara bersamaan. Hal ini juga memungkinkan klien untuk mengelola kotak surat di server (untuk mengatur pesan dalam folder dan untuk mengontrol ketika mereka dihapus, misalnya) dan untuk membuat beberapa kotak surat.

Klien terhubung ke server IMAP melalui port TCP 143, tetapi port ini tidak aman. Keamanan koneksi dapat dibuat menggunakan TLS. Port default untuk IMAPS adalah TCP/993.

Tips: Di lingkungan Windows, protokol *Messaging Application Programming Interface* (MAPI) berpemilik biasanya digunakan untuk mengakses kotak surat Microsoft Exchange. MAPI menggunakan HTTPS sebagai protokol transport yang aman.

Voice and Video Services

Solusi Voice over IP (VoIP), web conferencing, dan video teleconferencing (VTC) telah menjadi metode standar untuk penyediaan komunikasi bisnis dan sosial. Banyak jaringan yang ditingkatkan dari layanan suara lama ke protokol dan produk berbasis IP.

Private Branch Exchange

Layanan suara lama menggunakan *public switched telephone network* (PSTN). Instalasi telepon perumahan akan dilayani oleh kotak sederhana yang menyediakan antarmuka analog satu atau dua saluran ke pertukaran lokal. Antarmuka analog ini juga disebut sebagai *plain old telephone service* (POTS). Setiap saluran menyediakan satu saluran untuk panggilan masuk atau keluar. Bisnis tipikal membutuhkan puluhan atau ratusan saluran untuk komunikasi suara, apalagi kapasitas untuk komunikasi data. Secara historis, persyaratan ini akan difasilitasi oleh saluran trunk digital, juga disebut sebagai sirkuit *Time Division Multiplexing* (TDM). TDM dapat memisahkan saluran suara dan data untuk transmisi melalui satu kabel.

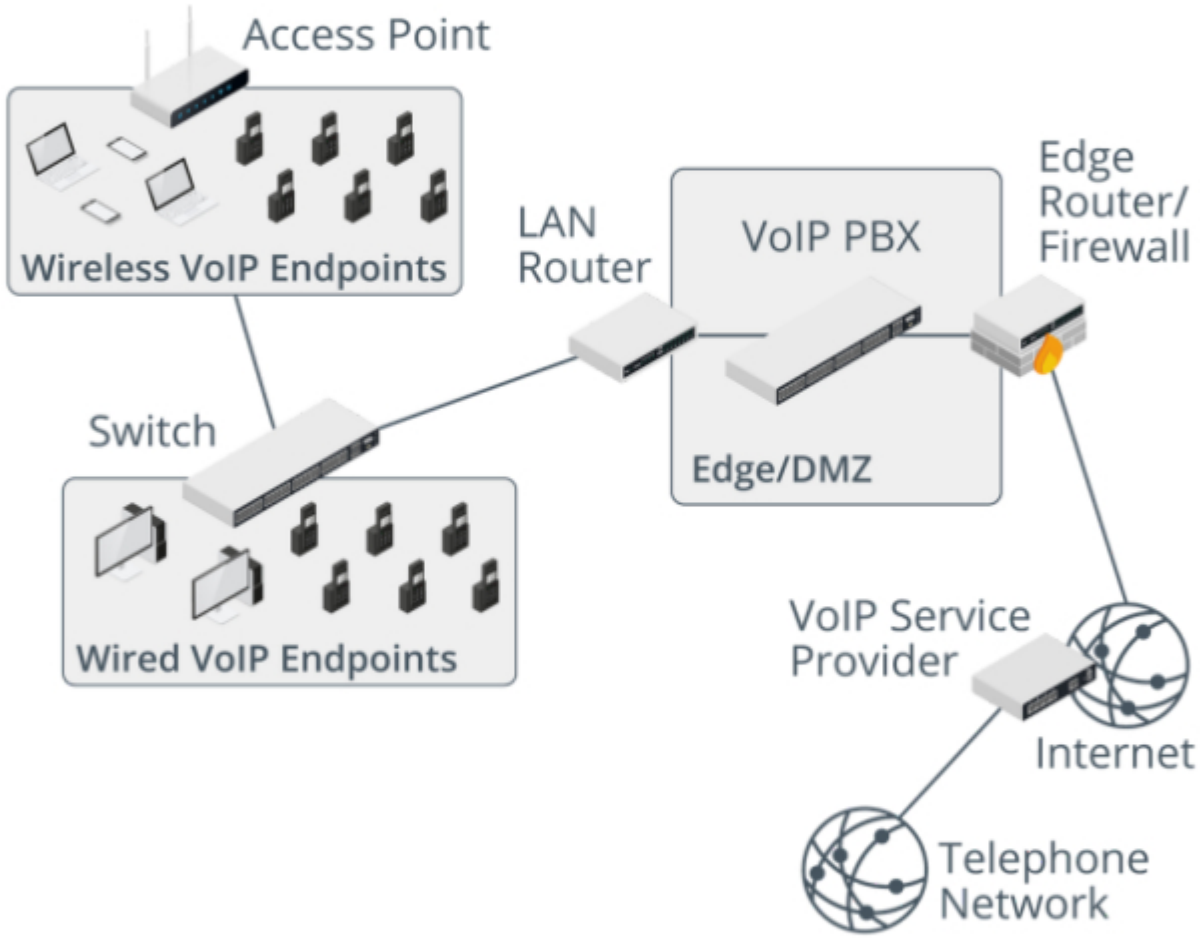
*A private branch exchang*e (PBX) adalah switchboard otomatis yang menyediakan titik koneksi tunggal untuk saluran suara organisasi. PBX berbasis TDM terhubung ke operator telekomunikasi melalui saluran utama digital, yang akan mendukung banyak saluran (panggilan masuk dan keluar). PBX memungkinkan konfigurasi sistem telepon internal untuk mengarahkan dan mengarahkan panggilan ke ekstensi lokal, dan menyediakan fitur telepon lain seperti panggilan tunggu, musik ditahan, dan pesan suara.

PBX TDM berbasis VoIP-Diaktifkan PBX digantikan oleh hybrid dan sepenuhnya IP/VoIP PBX. Untuk panggilan dan konferensi internal, PBX VoIP membuat koneksi antara titik akhir VoIP lokal dengan data yang dikirimkan melalui jaringan Ethernet lokal. VoIP PBX juga dapat merutekan panggilan masuk dan keluar dari dan ke jaringan eksternal. Ini mungkin melibatkan panggilan antara titik akhir VoIP internal dan eksternal, atau dengan penelepon dan penerima jaringan telepon suara. VoIP PBX juga akan mendukung fitur seperti musik yang ditahan dan pesan suara.

PBX TDM disediakan sebagai perangkat keras khusus vendor. VoIP PBX dapat diimplementasikan sebagai perangkat lunak yang berjalan di server Windows atau Linux. Contoh solusi berbasis perangkat lunak termasuk 3CX (3cx.com) dan Asterisk (asterisk.org). Ada juga solusi perangkat keras, di mana PBX VoIP berjalan pada router, seperti Cisco Unified

Communications Manager (cisco.com/c/en/us/products/unified-communications/unified-communications-manager-callmanager/index.html) .

VoIP PBX biasanya ditempatkan di tepi jaringan dan dilindungi oleh firewall. Klien internal terhubung ke PBX melalui kabel data Ethernet dan infrastruktur switching, menggunakan *Internet Protocol* (IP) pada lapisan Jaringan untuk pengalamatan. VoIP PBX menggunakan tautan Internet organisasi untuk terhubung ke penyedia layanan VoIP, yang memfasilitasi panggilan masuk dan keluar ke jaringan telepon berbasis suara.



A VoIP PBX facilitates internal IP calls and calls to and from external VoIP networks and the landline and cellular telephone networks. (Images © 123RF.com)

Protokol VoIP

Layanan suara dan video mungkin sulit untuk didukung karena memerlukan waktu respons yang diukur dalam milidetik (md). Respons yang tertunda akan menghasilkan kualitas panggilan

atau video yang buruk. Jenis data ini bisa satu arah, seperti halnya dengan media streaming, atau dua arah, seperti halnya dengan VoIP dan VTC.

Protokol yang dirancang untuk mendukung layanan waktu nyata mencakup satu atau beberapa fungsi berikut:

- **Session control** - Digunakan untuk menetapkan, mengelola, dan menghentikan sesi komunikasi. Mereka menangani tugas-tugas seperti penemuan pengguna (menemukan pengguna di jaringan), iklan ketersediaan (apakah pengguna siap menerima panggilan), menegosiasikan parameter sesi (seperti penggunaan audio/video), dan manajemen dan penghentian sesi.
- **Data Transport** - Menangani pengiriman informasi video atau suara yang sebenarnya.
- **Quality of Service (QoS)** - Menyediakan informasi tentang koneksi ke sistem QoS, yang pada gilirannya memastikan bahwa komunikasi suara atau video bebas dari masalah, seperti paket yang jatuh, penundaan, atau jitter.

Session Initiation Protocol
Session Initiation Protocol (SIP) adalah salah satu protokol kontrol sesi yang paling banyak digunakan. Titik akhir SIP adalah perangkat pengguna akhir (juga dikenal sebagai agen pengguna), seperti handset berkemampuan IP atau perangkat lunak konferensi web klien dan server. Setiap perangkat, konferensi, atau pengguna telepon diberi alamat SIP unik yang dikenal sebagai SIP Uniform Resource Indicator (URI). Contoh SIP URI meliputi:

sip:jaime@515support.com
sip:2622136227@515support.com
sip:jaime@2622136227
meet:sip:organizer@515support.com;ms-app=conf;ms-conf-id=subg42

Tips: Ada juga skema tel: URI yang memungkinkan titik akhir SIP untuk menghubungi telepon rumah atau ponsel. Tel: URI dapat menggunakan format global (E.164) (seperti tel:+1-866-8358020) atau format lokal (untuk ekstensi internal).

SIP biasanya berjalan melalui port UDP atau TCP 5060 (tidak aman) dan 5061 (SIP-TLS). SIP memiliki keandalan dan mekanisme transmisi ulangnya sendiri dan dengan demikian dapat terlihat paling diuntungkan dari overhead yang lebih rendah dan pengurangan latensi dan jitter UDP. Beberapa produk SIP perusahaan tetap menggunakan TCP.

Real-Time Transport Protocol and RTP Control Protocol
Sementara SIP menyediakan manajemen sesi, pengiriman data real-time yang sebenarnya menggunakan protokol yang berbeda. Yang utama adalah *Real-time Transport Protocol* (RTP). RTP memungkinkan pengiriman aliran data media melalui UDP, sambil menerapkan beberapa fitur keandalan yang biasanya terkait dengan komunikasi TCP. RTP bekerja sama dengan *RTP Control Protocol* (RTCP). Setiap aliran RTP menggunakan sesi RTCP yang sesuai untuk

memantau kualitas koneksi dan untuk memberikan laporan ke titik akhir. Laporan ini kemudian dapat digunakan oleh aplikasi untuk memodifikasi parameter codec atau oleh tumpukan jaringan untuk menyesuaikan parameter *Quality of Service* (QoS).

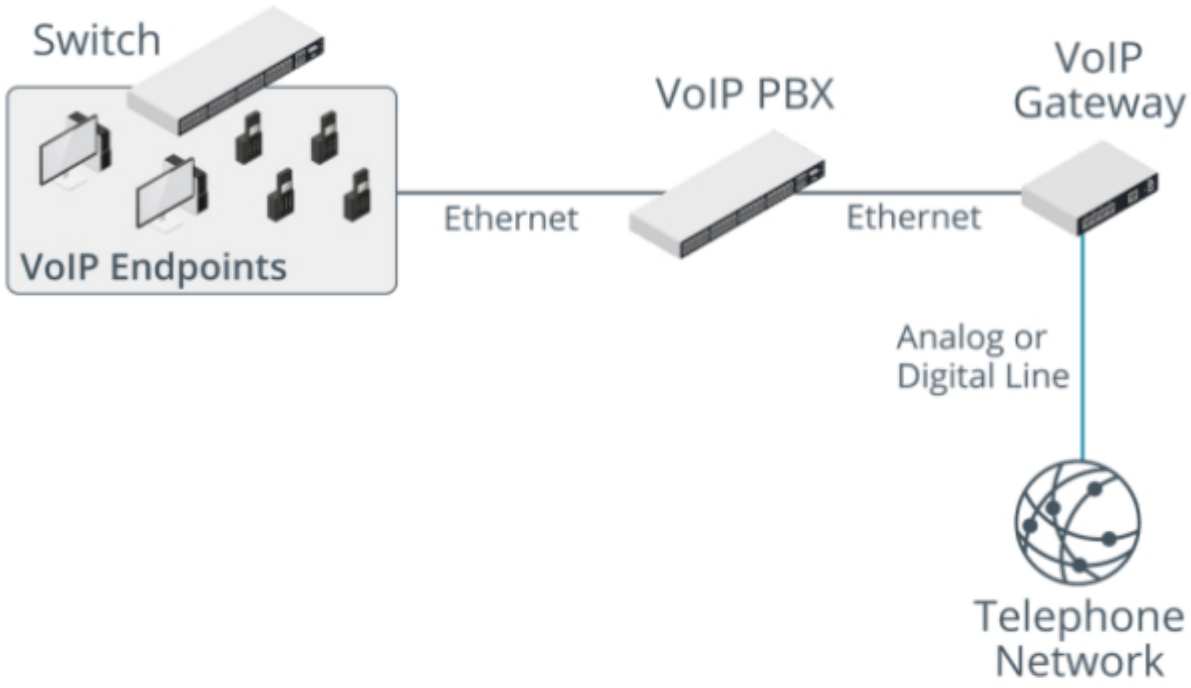
VoIP Phones

Titik akhir VoIP/SIP dapat diimplementasikan sebagai perangkat lunak yang berjalan di komputer atau ponsel cerdas atau sebagai handset perangkat keras khusus. Telepon VoIP menggunakan penandaan VLAN untuk memastikan bahwa kontrol SIP dan protokol media RTP dapat dipisahkan dari lalu lintas data normal. Dalam konfigurasi VLAN suara biasa, port LAN pada handset terhubung ke port dinding, sedangkan PC terhubung ke port PC pada handset. Kedua perangkat berbagi tautan fisik yang sama, tetapi lalu lintas data dibedakan dari lalu lintas suara dengan mengonfigurasi ID VLAN yang terpisah.

Handset dapat menggunakan *Power over Ethernet* (PoE), jika tersedia, untuk menghindari kebutuhan akan kabel daya atau baterai yang terpisah. Ada juga handset nirkabel yang bekerja melalui jaringan Wi-Fi 802.11.
Keamanan koneksi untuk VoIP bekerja dengan cara yang mirip dengan HTTPS. Untuk memulai panggilan, versi aman SIP (SIPS) menggunakan sertifikat digital untuk mengotentikasi titik akhir dan membuat terowongan SSL/TLS. Koneksi aman yang dibuat oleh SIPS juga dapat digunakan untuk menghasilkan kunci master untuk digunakan dengan versi aman dari protokol transport dan kontrol.
Saat Anda memasang handset baru, Anda juga harus menguji apakah koneksi berfungsi dan tautan menyediakan kualitas panggilan yang memadai. Sebagian besar penyedia layanan memiliki nomor uji untuk memverifikasi konektivitas dasar dan melakukan panggilan uji gema, yang memutar ulang pesan yang Anda rekam sehingga Anda dapat mengonfirmasi kualitas suara.

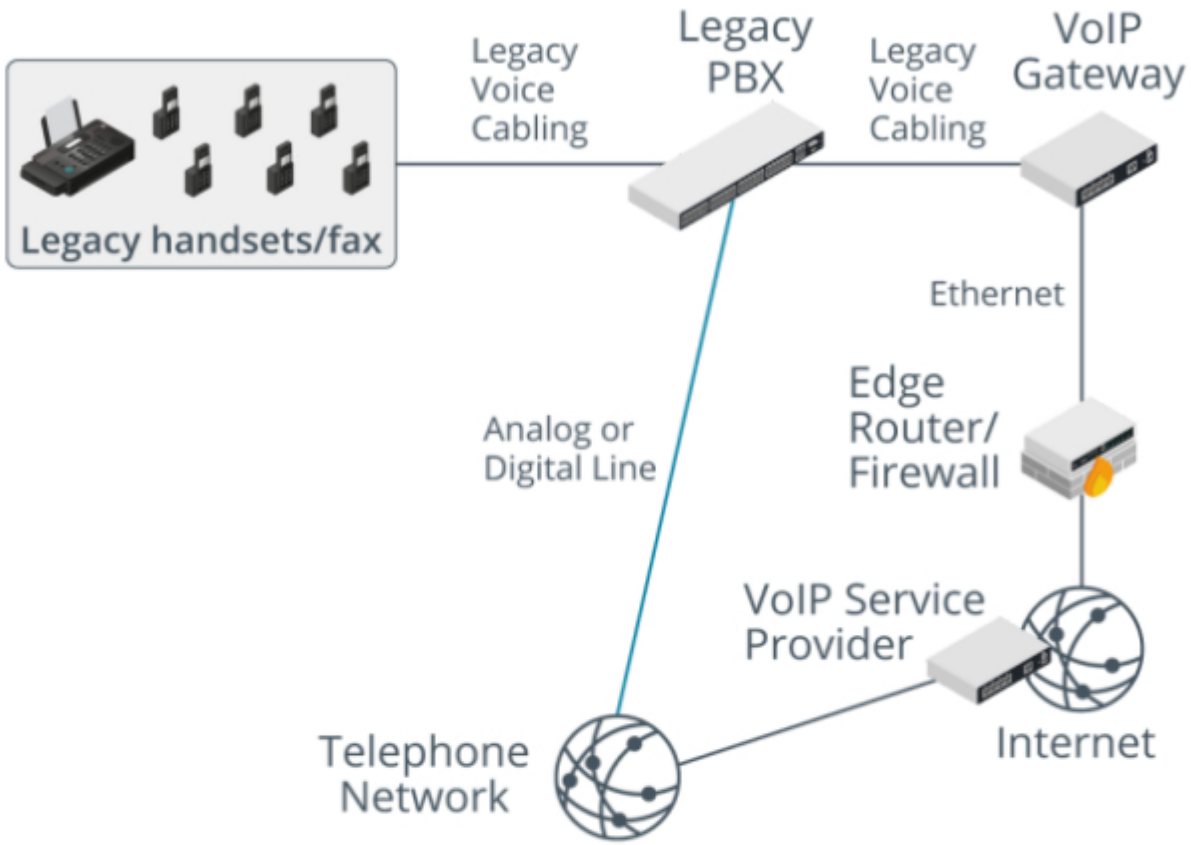
Voice Gateways

Titik akhir SIP dapat membangun komunikasi secara langsung dalam arsitektur peer-to-peer, tetapi lebih umum menggunakan server perantara, server direktori, dan gateway VoIP. Mungkin juga ada persyaratan untuk integrasi lokal antara jaringan dan peralatan data dan suara. Sebuah gateway suara adalah sarana menerjemahkan antara sistem VoIP dan peralatan suara warisan dan jaringan, seperti saluran POTS dan handset. Ada banyak jenis gateway VoIP, melayani fungsi yang berbeda. Misalnya, perusahaan mungkin menggunakan VoIP secara internal, tetapi terhubung ke jaringan telepon melalui gateway. Untuk memfasilitasi ini, Anda dapat menggunakan PBX VoIP hybrid atau berbasis perangkat keras dengan plug-in atau gateway VoIP terintegrasi, atau Anda dapat menggunakan perangkat gateway terpisah. Ada tipe analog dan digital yang sesuai dengan tipe telepon rumah yang masuk. Versi analog dari jenis gateway ini juga disebut sebagai gerbang *Foreign Exchange Office* (FXO).



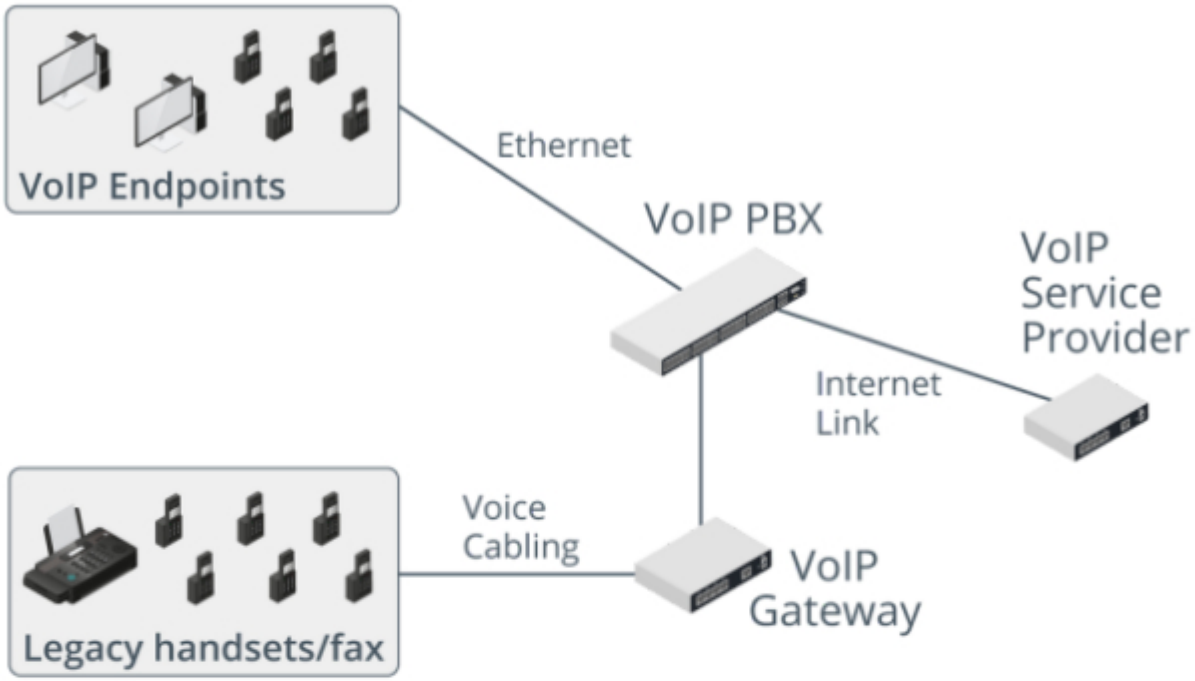
VoIP gateway connecting a local network using VoIP calling to the ordinary telephone network. (Images © 123RF.com)

Gateway VoIP juga dapat digunakan untuk memungkinkan sistem telepon internal analog atau digital lama menggunakan penyedia layanan VoIP untuk melakukan panggilan. Dalam jenis pengaturan ini, panggilan lokal dan nasional tarif rendah dapat dilakukan secara langsung, sedangkan panggilan internasional yang akan dikenakan biaya tinggi jika dilakukan secara langsung dirutekan melalui penyedia layanan VoIP.



VoIP gateway connecting a local network using legacy PBX and handsets to a VoIP service provider. (Images © 123RF.com)

Terakhir, gateway atau adaptor VoIP dapat digunakan untuk menghubungkan handset POTS dan mesin faks ke VoIP PBX. Jenis perangkat ini juga disebut gerbang *Foreign Exchange Subscriber* (FXS).



VoIP gateway connecting legacy handsets to a VoIP PBX. (Images © 123RF.com).

MODUL 12

Memastikan Ketersediaan Jaringan

PENGANTAR PELAJARAN
Sejauh ini dalam kursus ini, Anda telah belajar tentang semua media dan topologi jaringan yang berbeda ditambah protokol aplikasi yang digunakan untuk membangun konektivitas dan layanan jaringan. Dalam pelajaran ini, Anda akan menyelidiki beberapa alat dan metode manajemen yang akan membantu Anda menentukan baseline jaringan Anda dan mengoptimalkan kinerja jaringan Anda.

TUJUAN PELAJARAN
Dalam pelajaran ini, Anda akan:

- Jelaskan penggunaan layanan manajemen jaringan.
- Gunakan manajemen acara untuk memastikan ketersediaan jaringan.
- Gunakan metrik kinerja untuk memastikan ketersediaan jaringan

A. Jelaskan Penggunaan Layanan Manajemen Jaringan

Pendahuluan: Menjelaskan Penggunaan Layanan Manajemen Jaringan

Alat manajemen jarak jauh memungkinkan Anda mengonfigurasi server dan perangkat melalui jaringan. Harus melakukan konfigurasi dan aktivitas pemecahan masalah di konsol lokal akan sangat memakan waktu. Administrasi jaringan yang efisien tergantung pada alat akses jarak jauh. Namun, sangat penting untuk mengonfigurasi alat-alat ini dengan aman.

Server Shell Aman dan Emulator Terminal

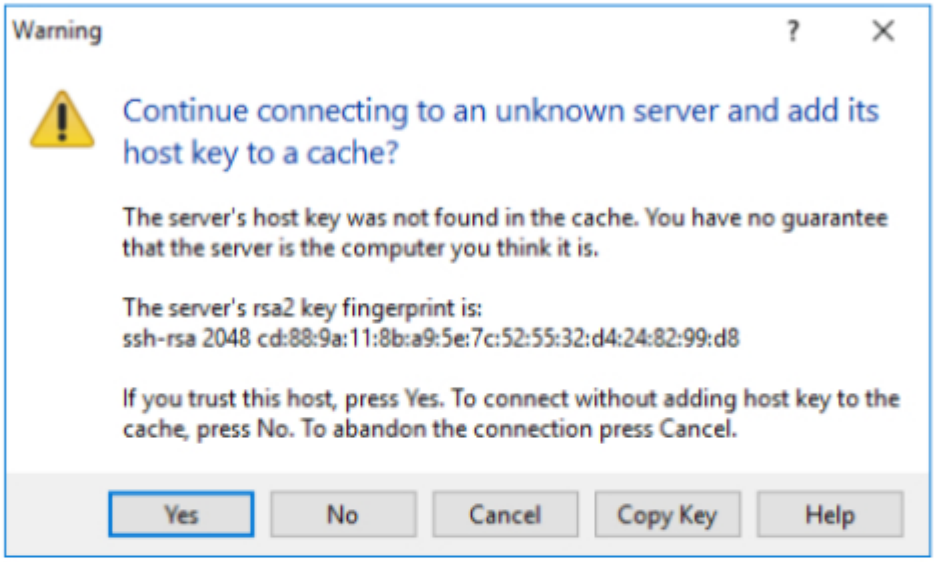
Nama "terminal" berasal dari hari-hari awal komputasi di mana konfigurasi dilakukan oleh perangkat teletype (TTY). TTY adalah terminal atau titik akhir untuk komunikasi antara komputer dan pengguna. TTY menangani input dan output teks antara pengguna dan shell, atau lingkungan perintah. Di mana terminal menerima input dan menampilkan output, shell melakukan pemrosesan yang sebenarnya.

Emulator terminal adalah perangkat lunak apa pun yang mereplikasi fungsi input/output TTY ini. Aplikasi emulator terminal tertentu mungkin mendukung koneksi ke beberapa jenis shell. Emulator terminal jarak jauh memungkinkan Anda terhubung ke shell host yang berbeda melalui jaringan.

Secure Shell (SSH) adalah sarana utama untuk mendapatkan akses jarak jauh yang aman ke server UNIX dan Linux dan ke sebagian besar jenis peralatan jaringan (switch, router, dan firewall). Selain emulasi terminal, SSH dapat digunakan sebagai protokol transfer file aman (SFTP). Ada banyak server SSH komersial dan open source serta

klien emulasi terminal yang tersedia untuk semua platform NOS utama (UNIX®, Linux®, Windows®, dan macOS®). Yang paling banyak digunakan adalah OpenSSH (openssh.com). Server SSH mendengarkan pada port TCP 22 secara default.

Kunci Host SSH Sebuah server SSH diidentifikasi oleh pasangan kunci publik/pribadi, yang disebut sebagai kunci host. Pemetaan nama host ke kunci publik dapat disimpan secara manual oleh setiap klien SSH, atau ada berbagai produk perangkat lunak perusahaan yang dirancang untuk manajemen kunci SSH.



Confirming the SSH server's host key using the SSH client. (Screenshot courtesy of Microsoft.)

Tips: Kunci host harus diubah jika ada dugaan kompromi dari host. Jika penyerang telah memperoleh kunci pribadi dari server atau alat, mereka dapat menyamar sebagai server atau alat itu dan melakukan serangan spoofing, biasanya dengan maksud untuk mendapatkan kredensial jaringan lainnya. Anda juga dapat mengubah kunci untuk menggunakan kekuatan bit yang lebih panjang.

SSH Client Authentication
Kunci host server digunakan untuk menyiapkan saluran aman yang digunakan klien untuk mengirimkan kredensial otentikasi. SSH memungkinkan berbagai metode untuk klien untuk mengotentikasi ke server SSH. Masing-masing metode ini dapat diaktifkan atau dinonaktifkan sesuai kebutuhan di server:

- Username/password : Klien mengirimkan kredensial yang diverifikasi oleh server SSH baik terhadap database pengguna lokal atau menggunakan server otentikasi jaringan.
- Public key authentication : Setiap kunci publik pengguna jarak jauh ditambahkan ke daftar kunci yang diotorisasi untuk setiap akun lokal di server SSH.

- Kerberos : Klien mengirimkan kredensial Kerberos (Tiket Pemberian Tiket) yang diperoleh saat pengguna masuk ke workstation ke server menggunakan Antarmuka Program Aplikasi Layanan Keamanan Generik (GSSAPI). Server SSH menghubungi Layanan Pemberian Tiket (di lingkungan Windows, ini akan menjadi pengontrol domain) untuk memvalidasi kredensial.

Tips: Mengelola kunci publik klien yang valid adalah tugas keamanan yang kritis. Banyak serangan baru-baru ini pada server web telah mengeksploitasi manajemen kunci yang buruk. Jika kunci pribadi pengguna disusupi, hapus kunci publik dari alat, lalu buat kembali pasangan kunci pada perangkat klien (yang dimediasi) pengguna dan salin kunci publik ke server SSH. Selalu hapus kunci publik jika izin akses pengguna telah dicabut.

Secure Shell Commands

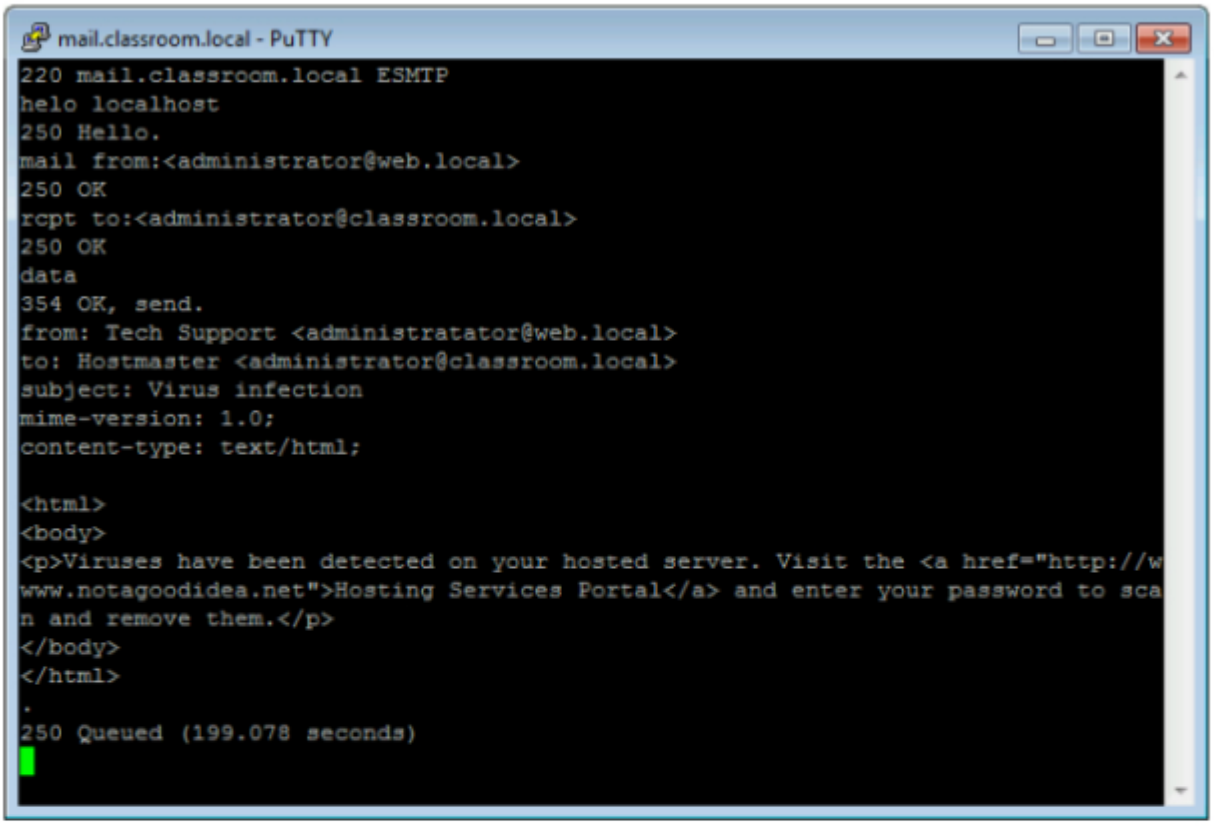
SSH menampilkan kumpulan perintah yang kaya, didokumentasikan sepenuhnya di situs web OpenSSH (openssh.com/manual.html). Beberapa perintah yang paling penting adalah:

- sshd-Mulai Daemon SSH (server). Parameter seperti file sertifikat host, port untuk mendengarkan, dan opsi logging dapat diatur melalui sakelar atau dalam file konfigurasi.
- ssh-keygen-Buat pasangan kunci yang akan digunakan untuk mengakses server. Kunci pribadi harus disimpan dengan aman di komputer lokal Anda. Kunci publik harus disalin ke server. Anda dapat menggunakan perintah ssh-copy-id untuk melakukan ini, atau Anda dapat menyalin file secara manual.
- ssh-agent-Konfigurasikan layanan yang akan digunakan untuk menyimpan kunci yang digunakan untuk mengakses banyak host. Agen menyimpan kunci pribadi untuk setiap kunci publik dengan aman dan mengurangi berapa kali penggunaan kunci pribadi harus dikonfirmasi dengan frasa sandi. Ini menyediakan mekanisme masuk tunggal (SSO) untuk beberapa server SSH. Perintah ssh-add digunakan untuk menambahkan kunci ke agen.
- ssh Host -Gunakan klien SSH untuk terhubung ke server yang berjalan di Host . Host dapat berupa FQDN atau alamat IP. Anda juga dapat membuat file konfigurasi klien.
- ssh Username@Host -Gunakan klien SSH untuk terhubung ke server yang berjalan di Host dengan Username yang berbeda.
- ssh Host "Command or Script" -Gunakan klien SSH untuk menjalankan perintah atau skrip di server jauh yang berjalan di Host tanpa memulai shell.
- scp Username@Host:RemoteFile /Local/Destination -Klien transfer file dengan antarmuka perintah copy/rcp-like jarak jauh
- sftp-A klien transfer file dengan antarmuka perintah seperti FTP.

Telnet

Telnet adalah protokol dan perangkat lunak emulasi terminal yang mengirimkan perintah shell dan output antara klien dan host jarak jauh. Untuk mendukung akses Telnet, komputer jarak

jauh harus menjalankan layanan yang dikenal sebagai Telnet Daemon. Telnet Daemon mendengarkan pada port TCP 23 secara default.



PuTTY Telnet client. (Screenshot courtesy of PuTTY.)

Antarmuka Telnet dapat dilindungi kata sandi tetapi kata sandi dan komunikasi lainnya tidak dienkripsi dan oleh karena itu rentan terhadap packet sniffing dan replay. Secara historis, Telnet menyediakan cara sederhana untuk mengkonfigurasi peralatan switch dan router, tetapi hanya metode akses aman yang harus digunakan untuk tugas-tugas ini sekarang. Pastikan layanan Telnet dicopot atau dinonaktifkan, dan blokir akses ke port 23.

Remote Desktop Protocol

Telnet dan SSH menyediakan emulasi terminal untuk shell baris perintah. Ini cukup untuk sebagian besar tugas administratif, tetapi di mana pengguna ingin terhubung ke desktop, mereka biasanya lebih suka bekerja dengan antarmuka grafis. Alat administrasi jarak jauh GUI mengirimkan data layar dan audio dari host jarak jauh ke klien dan mentransfer input mouse dan keyboard dari klien ke host jarak jauh. Remote Desktop Protocol (RDP) adalah protokol Microsoft untuk mengoperasikan koneksi GUI jarak jauh ke mesin Windows. RDP menggunakan port TCP 3389. Administrator dapat menentukan izin untuk menyambung ke server melalui RDP dan dapat mengkonfigurasi enkripsi pada sambungan.

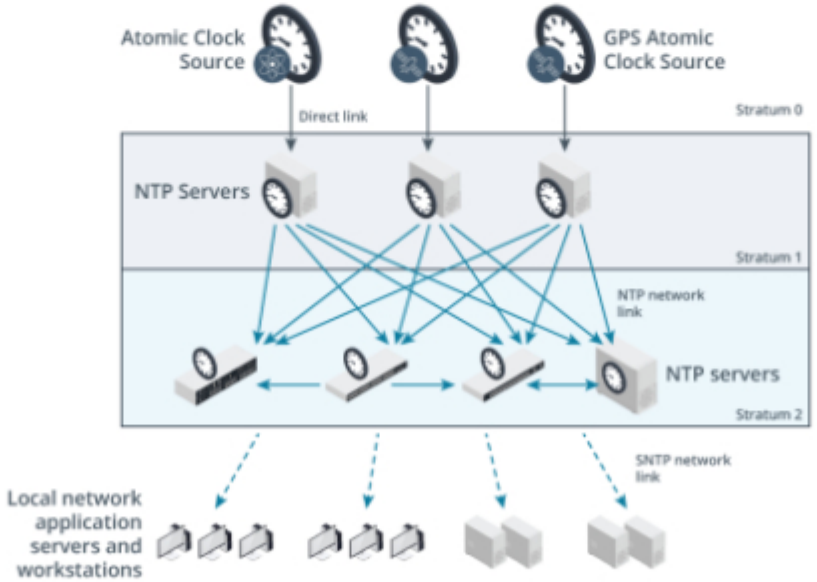
RDP terutama digunakan untuk administrasi jarak jauh dari server atau klien Windows, tetapi fungsi lainnya adalah untuk mempublikasikan aplikasi perangkat lunak di server, daripada menginstalnya secara lokal pada setiap klien (virtualisasi aplikasi).

Tips: Klien RDP tersedia untuk sistem operasi lain, termasuk Linux, macOS, iOS, dan Android sehingga Anda dapat terhubung ke desktop Windows dari jarak jauh menggunakan perangkat non-Windows. Ada juga produk server RDP open-source, seperti xrdp (xrdp.org).

Network Time Protocol

Banyak aplikasi di jaringan bergantung pada waktu dan kritis terhadap waktu, seperti mekanisme otentikasi dan keamanan, aplikasi penjadwalan, dan perangkat lunak pencadangan. Network Time Protocol (NTP) memungkinkan sinkronisasi aplikasi yang bergantung pada waktu ini. NTP bekerja melalui UDP pada port 123.

Server NTP tingkat atas (stratum 1) memperoleh Waktu Universal Terkoordinasi (UTC) melalui tautan fisik langsung ke sumber jam yang akurat, seperti jam atom yang diakses melalui Sistem Pemosisian Umum (GPS). Server NTP yang menyinkronkan waktunya dengan server strata 1 melalui jaringan beroperasi pada strata 2. Setiap level strata mewakili satu langkah menjauh dari sumber jam yang akurat melalui tautan jaringan. Server strata bawah ini bertindak sebagai klien dari server strata 1 dan sebagai server atau sumber waktu untuk server NTP strata bawah atau host klien. Kebanyakan switch dan router dapat dikonfigurasi untuk bertindak sebagai server waktu ke host klien lokal dan fungsi ini juga biasanya dilakukan oleh server direktori jaringan. Yang terbaik adalah mengonfigurasi masing-masing perangkat ini dengan beberapa sumber waktu referensi (setidaknya tiga) dan menjadikannya sebagai rekan untuk memungkinkan algoritme NTP mendeteksi penyimpangan atau nilai waktu yang jelas salah.



Stratum 1 NTP servers are directly connected to an accurate clock source. Each stratum level below one represents a network hop away from that accurate time source. (Images © 123RF.com.)

Host klien (server aplikasi dan workstation) biasanya memperoleh waktu dengan menggunakan bentuk protokol yang dimodifikasi yang disebut Simple NTP (SNTP). SNTP bekerja melalui port yang sama dengan NTP. Sebuah host yang hanya mendukung SNTP tidak dapat bertindak sebagai sumber waktu untuk host lain. Di Windows, Layanan Waktu dapat dikonfigurasi dengan menggunakan perintah w32tm. Di Linux, paket ntp dapat dikonfigurasi melalui /etc/ntp.conf.

Jika server atau host dikonfigurasi dengan waktu yang salah, mungkin tidak dapat mengakses layanan jaringan. Otentikasi, dan mekanisme keamanan lainnya akan sering gagal jika waktu tidak disinkronkan pada kedua perangkat yang berkomunikasi. Dalam situasi ini, kesalahan cenderung berupa pesan jenis token yang gagal atau tidak valid secara umum. Selalu mencoba untuk mengesampingkan sinkronisasi waktu sebagai masalah di awal proses pemecahan masalah.

Tips: Jika server stratum 1 lokal tidak dapat diimplementasikan pada jaringan lokal, sumber waktu dapat dikonfigurasi menggunakan satu atau lebih kumpulan server NTP publik, seperti time.google.com, time.windows.com, time.apple.com , time.nist.gov, atau pool.ntp.org.

B. Gunakan Manajemen Acara untuk Memastikan Ketersediaan Jaringan

Pendahuluan: Gunakan Manajemen Acara untuk Memastikan Ketersediaan Jaringan

Mengelola kinerja jaringan adalah tugas penting bagi teknisi jaringan. Dengan secara proaktif memantau status perangkat jaringan dan log peristiwa, Anda dapat memberikan layanan yang andal kepada pengguna Anda.

Metrik Kinerja, Kemacetan, dan Garis Dasar

Alat pemantauan jaringan memenuhi berbagai fungsi. Sebagai masukan, mereka dapat menangkap dan menganalisis lalu lintas, memantau antarmuka dan metrik perangkat, serta menggabungkan data log. Sebagai keluaran, mereka dapat mengingatkan Anda tentang peristiwa, membantu Anda menentukan garis dasar, menganalisis pola lalu lintas dan kemacetan, menentukan peningkatan dan perkiraan kebutuhan, dan menghasilkan laporan untuk manajemen.

Metrik Kinerja

Saat Anda memantau host jaringan atau sistem perantara, beberapa metrik kinerja dapat memberi tahu Anda apakah host beroperasi secara normal:

- Bandwidth/throughput : adalah kecepatan terukur dari semua antarmuka yang tersedia untuk perangkat, diukur dalam Mbps atau Gbps. Untuk tautan Ethernet kabel, ini biasanya tidak akan bervariasi, tetapi bandwidth WAN dan tautan nirkabel dapat berubah seiring waktu.
- CPU and memory : Perangkat seperti sakelar dan router melakukan banyak pemrosesan. Jika penggunaan CPU dan/atau memori sistem (diukur sebagai persentase) sangat tinggi, pemutakhiran mungkin diperlukan. Utilisasi CPU yang tinggi juga dapat menunjukkan masalah dengan lalu lintas jaringan.
- Storage : Beberapa perangkat jaringan memerlukan penyimpanan persisten (biasanya, satu atau lebih flash drive) untuk menyimpan informasi konfigurasi dan log. Penyimpanan diukur dalam MB atau GB. Jika perangkat kehabisan ruang penyimpanan, ini dapat menyebabkan kesalahan serius. Server juga bergantung pada input/output (I/O) yang cepat untuk menjalankan aplikasi secara efisien.

Bottlenecks

Kemacetan adalah titik kinerja buruk yang mengurangi produktivitas seluruh jaringan. Kemacetan dapat terjadi karena perangkat kurang bertenaga atau rusak. Ini juga dapat terjadi karena perilaku pengguna atau aplikasi. Untuk mengidentifikasi penyebab kemacetan, Anda perlu mengidentifikasi di mana dan kapan penggunaan jaringan yang berlebihan atau kesalahan yang berlebihan terjadi. Jika masalahnya terus-menerus, kemungkinan besar terkait dengan perangkat; jika masalah hanya terjadi pada waktu tertentu, kemungkinan besar masalah tersebut terkait dengan pengguna atau aplikasi.

Dasar Kinerja

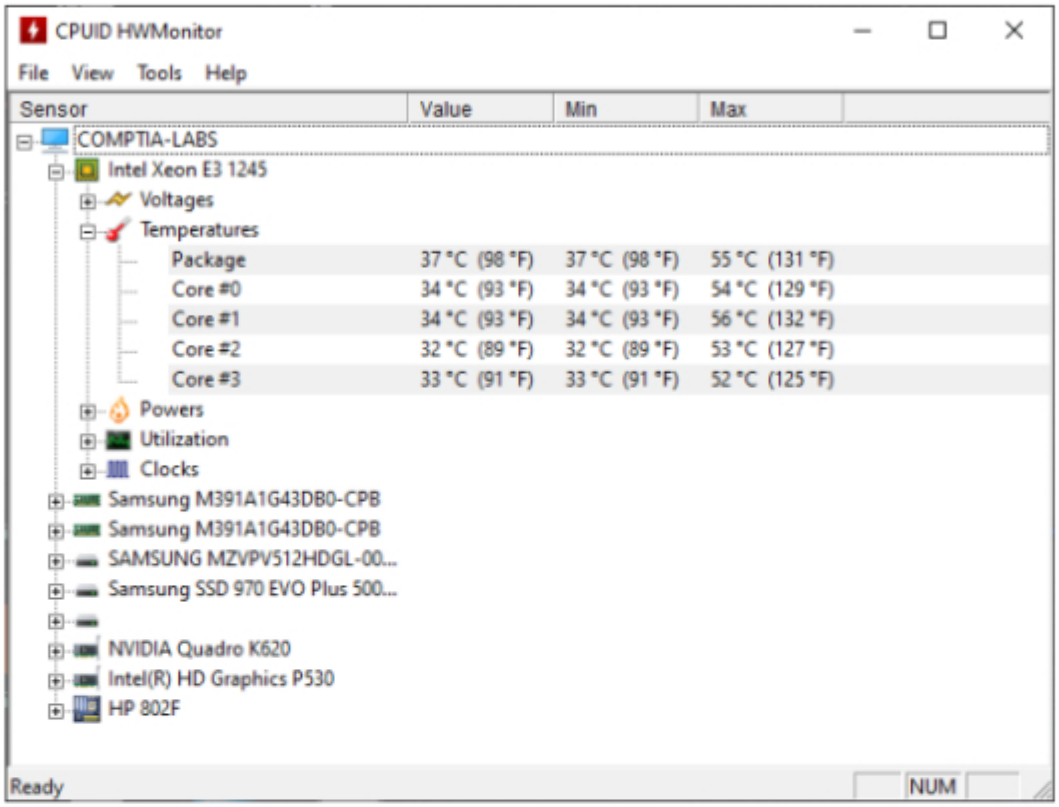
Garis dasar kinerja menetapkan metrik pemanfaatan sumber daya pada suatu titik waktu, seperti saat sistem pertama kali diinstal. Ini memberikan perbandingan untuk mengukur respons sistem nanti. Misalnya, jika perusahaan memperluas kantor jarak jauh yang terhubung ke kantor perusahaan dengan paket tingkat dasar ISP, garis dasar dapat membantu menentukan apakah ada cukup bandwidth cadangan untuk menangani beban pengguna tambahan, atau apakah paket dasar perlu ditingkatkan untuk mendukung bandwidth yang lebih tinggi.

Meninjau baseline adalah proses mengevaluasi apakah baseline masih sesuai dengan tujuan atau apakah baseline baru harus dibuat. Perubahan pada sistem biasanya memerlukan dasar baru untuk diambil.

Pemantauan Lingkungan

Berbeda dari monitor kinerja, sensor lingkungan digunakan untuk mendeteksi faktor-faktor yang dapat mengancam integritas atau ketersediaan alat atau fungsinya.

Server dan peralatan dilengkapi dengan sensor internal untuk memantau kondisi di dalam sasis perangkat. Ini dapat melaporkan masalah seperti suhu yang berlebihan di dalam sasis perangkat, kecepatan kipas, kegagalan komponen, dan intrusi sasis ke sistem pemantauan.



CPUID's HWMONITOR app can report temperatures from sensors installed on PC components. (Screenshot used by permission of CPUID.)

Sensor juga dapat dipasang untuk mengukur kondisi lingkungan sekitar untuk rak jaringan atau penutup atau di dalam ruang server atau lemari peralatan. Faktor lingkungan berikut ini perlu dipantau:

- Temperature : Suhu tinggi akan mempersulit perangkat dan sistem pendingin rak untuk membuang panas secara efektif. Hal ini meningkatkan risiko komponen yang terlalu panas di dalam sasis perangkat dan kesalahan yang diakibatkannya.
- Humidity : Lebih banyak uap air di udara berisiko membentuk kondensasi di dalam sasis perangkat, yang menyebabkan korosi dan gangguan hubung singkat. Sebaliknya, kelembaban yang sangat rendah meningkatkan risiko muatan statis yang menumpuk dan merusak komponen.
- Electrical : Sistem komputer membutuhkan catu daya yang stabil, bebas dari pemadaman (blackout), penurunan tegangan (brownout), dan lonjakan dan lonjakan tegangan. Sensor yang terpasang pada sistem distribusi daya dan sistem baterai cadangan dapat melaporkan penyimpangan dari catu daya normal.

- Flooding : Mungkin ada risiko banjir alami atau buatan manusia dari aliran air dan waduk terdekat atau risiko dari kebocoran pipa ledeng atau sistem pencegah kebakaran. Sistem kelistrikan harus segera dimatikan jika ada air dalam jumlah yang signifikan.

Protokol Manajemen Jaringan Sederhana

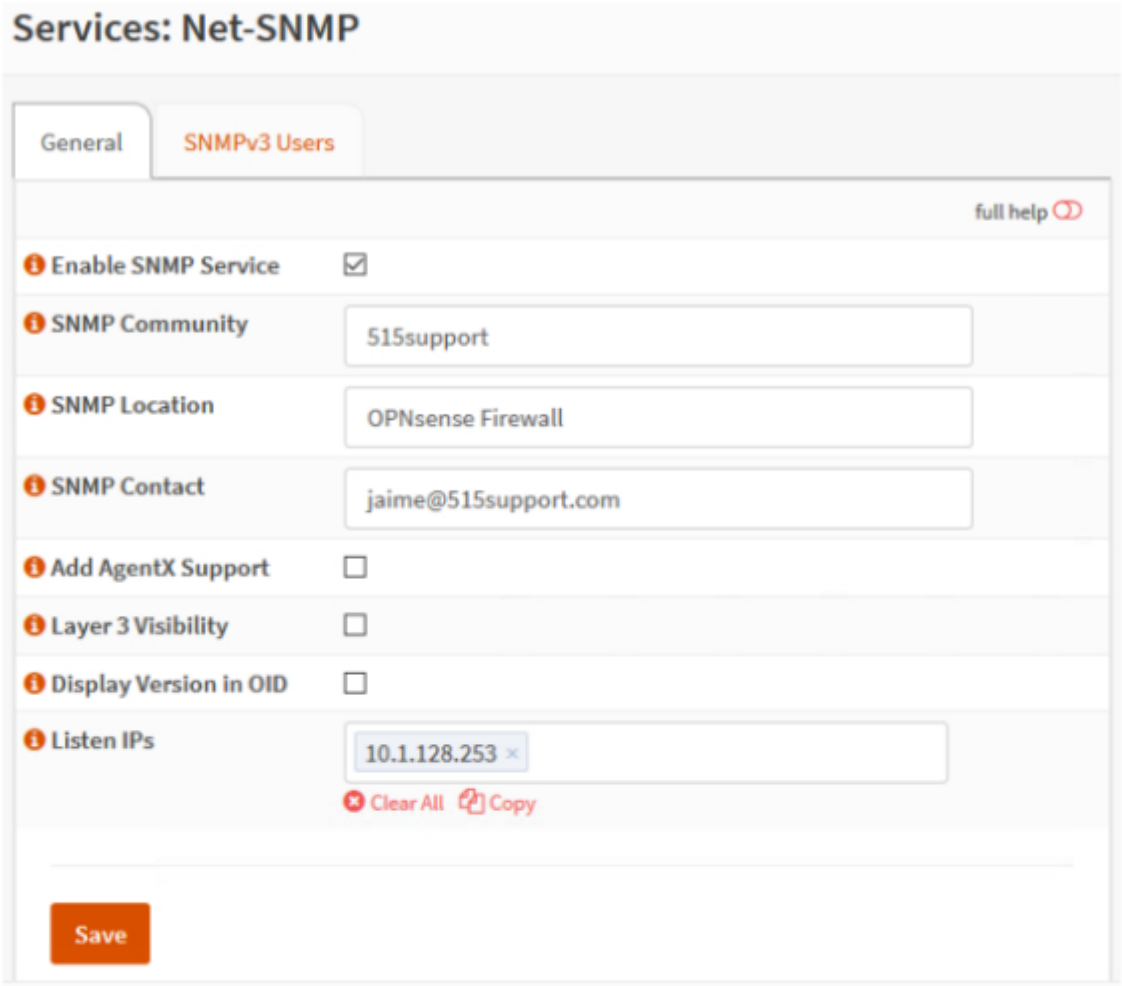
Perangkat yang berdiri sendiri mungkin memiliki konsol web untuk digunakan untuk kinerja dan pemantauan lingkungan. Namun, akses lokal tidak dapat diskalakan untuk mengelola puluhan atau ratusan perangkat.

Simple Network Management Protocol (SNMP) adalah kerangka kerja yang banyak digunakan untuk manajemen jarak jauh dan pemantauan server dan peralatan jaringan. SNMP terdiri dari agen dan sistem pemantauan.

- **SNMP Agents**

  Agen adalah proses (perangkat lunak atau firmware) yang berjalan pada sakelar, router, server, atau perangkat jaringan lain yang kompatibel dengan SNMP. Agen ini memelihara database yang disebut Management Information Base (MIB) yang menyimpan statistik yang berkaitan dengan aktivitas perangkat, seperti jumlah frame per detik yang ditangani oleh sakelar. Setiap parameter yang disimpan dalam MIB dirujuk oleh Object Identifier (OID) numerik. OID disimpan dalam struktur pohon. Bagian dari pohon adalah generik untuk SNMP, sedangkan bagian dapat ditentukan oleh vendor perangkat.

  Agen dikonfigurasi dengan Nama Komunitas komputer yang diizinkan untuk mengelola agen dan alamat IP atau nama host server yang menjalankan sistem manajemen. Nama komunitas bertindak sebagai jenis kata sandi yang belum sempurna. Agen hanya dapat meneruskan informasi ke sistem manajemen yang dikonfigurasi dengan nama komunitas yang sama. Biasanya ada dua nama komunitas; satu untuk akses baca-saja dan satu untuk akses baca-tulis (atau mode istimewa).



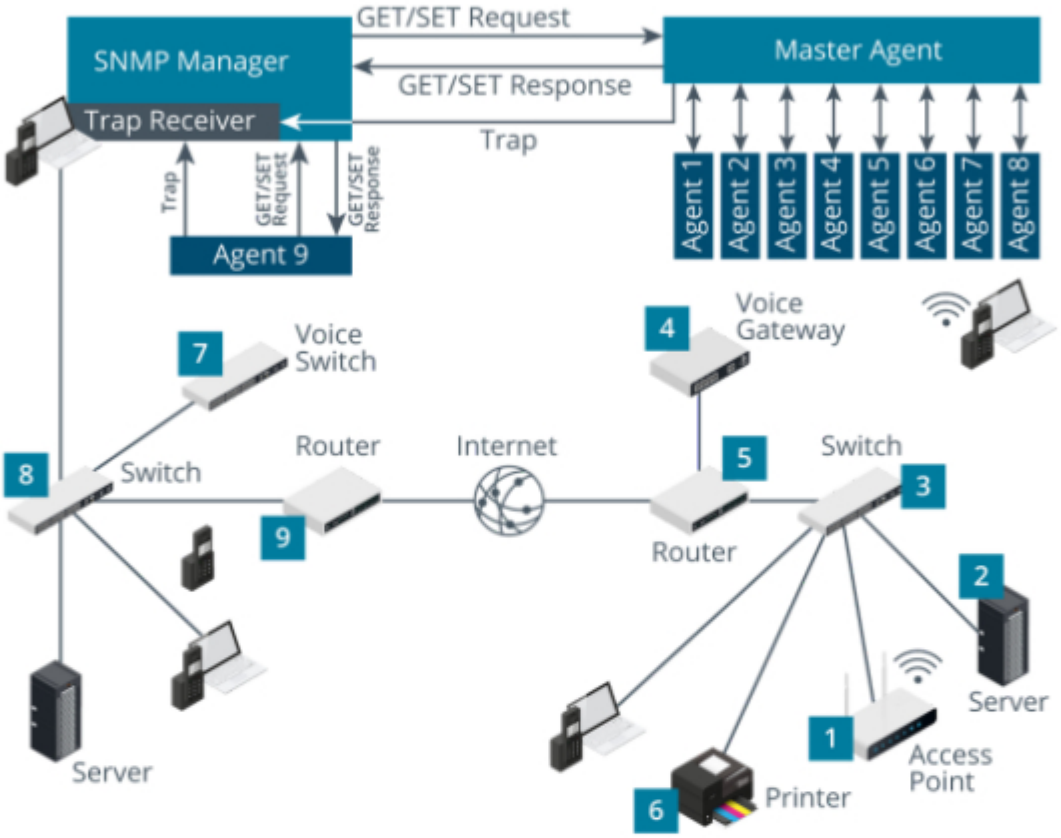
Configuring an SNMP agent on an OPNsense security appliance. (Screenshot courtesy of OPNsense.)

- **SNMP Monitor**

  Monitor SNMP adalah perangkat lunak manajemen yang menyediakan lokasi dari mana Anda dapat mengawasi aktivitas jaringan. Pemantau melakukan polling kepada agen secara berkala untuk mendapatkan informasi dari MIB mereka dan menampilkan informasi untuk ditinjau. Ini juga menampilkan operasi perangkap apa pun sebagai peringatan bagi administrator jaringan untuk menilai dan bertindak sesuai kebutuhan. Monitor dapat mengambil informasi dari perangkat dengan dua cara utama:

- ☐ Get : Perangkat lunak menanyakan agen untuk satu OID. Perintah ini digunakan oleh monitor untuk melakukan polling reguler (memperoleh informasi dari perangkat pada interval yang ditentukan).
- ☐ Trap : Agen memberi tahu monitor tentang peristiwa penting (kegagalan port, misalnya). Ambang batas untuk memicu jebakan dapat diatur untuk setiap nilai.

Monitor dapat digunakan untuk mengubah variabel tertentu menggunakan perintah Set. Itu juga dapat menjalankan subpohon MIB dengan menggunakan beberapa perintah Dapatkan dan Dapatkan Berikutnya. Ini digunakan untuk menemukan tata letak lengkap MIB. Kueri perangkat dilakukan melalui port UDP 161; perangkap dikomunikasikan melalui port UDP 162.



SNMP collects information from network devices for diagnostic purposes. (Images © 123RF.com)

- **Network Device Logs**

  Log perangkat jaringan adalah salah satu sumber informasi kinerja, pemecahan masalah, dan audit keamanan yang paling berharga. Satu peristiwa yang dicatat dalam log terdiri dari metadata, seperti tanggal dan waktu, kategori, dan ID peristiwa, ditambah deskripsi dan konten kesalahan atau keluaran informasi. Misalnya, Anda dapat menggunakan log sistem untuk memecahkan masalah konflik IP dengan mencari kejadian TCP/IP atau untuk menentukan kapan dan mengapa sistem dimatikan.

Meskipun spesifik tentang apa dan di mana peristiwa dicatat dapat sangat bervariasi dari platform ke platform, beberapa jenis log umum dapat dibedakan, termasuk sistem, keamanan, aplikasi, dan kinerja atau lalu lintas.

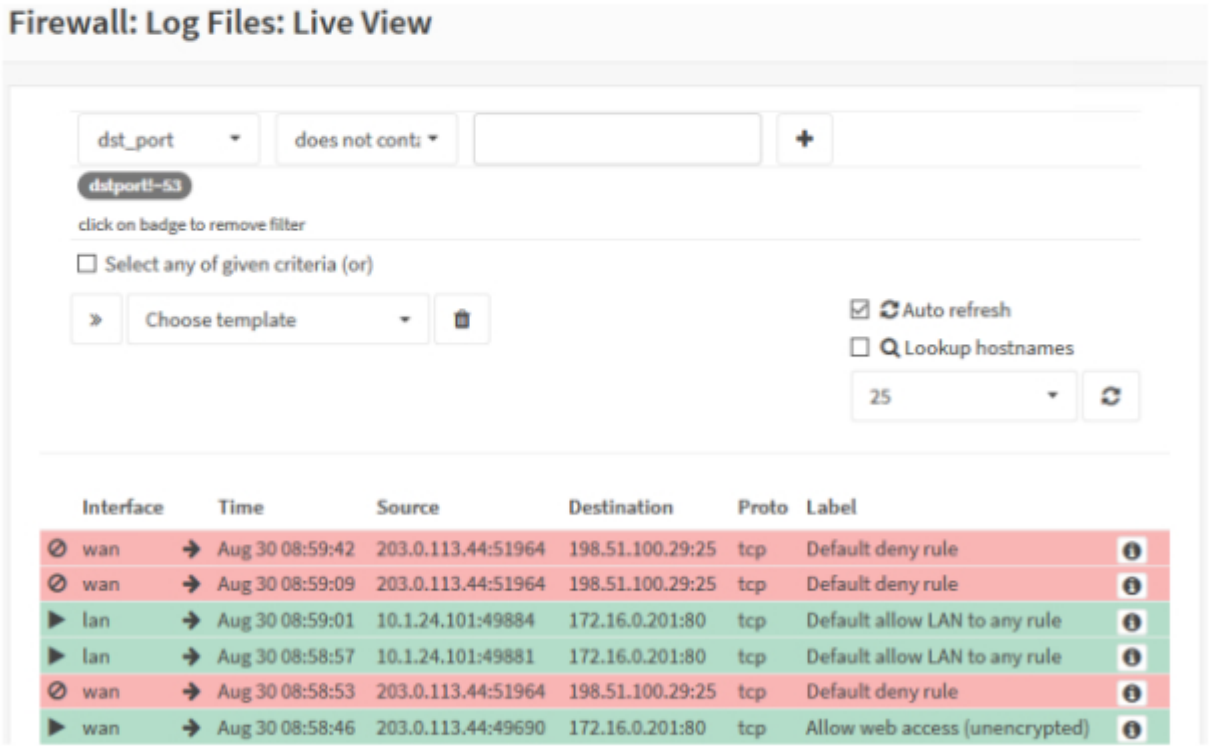
- **System and Application Logs**

  Log sistem mencatat peristiwa startup ditambah perubahan konfigurasi berikutnya pada tingkat OS. Ini pasti akan mencakup proses dan driver kernel tetapi juga dapat mencakup layanan inti.

  Sebaliknya, log aplikasi merekam data untuk satu layanan tertentu, seperti DNS, HTTP, atau RDBMS. Perhatikan bahwa aplikasi yang kompleks dapat menulis ke beberapa file log. Misalnya, server web Apache mencatat kesalahan ke satu file dan upaya akses ke file lain.

- **Audit Logs**

  Log audit mencatat penggunaan hak otentikasi dan otorisasi. Ini umumnya akan merekam acara jenis sukses/gagal. Log audit juga dapat digambarkan sebagai log akses atau log keamanan. Pencatatan log audit dapat dilakukan pada tingkat OS dan pada tingkat per aplikasi.



Tips: Log audit biasanya mengaitkan suatu tindakan dengan pengguna tertentu. Ini adalah salah satu alasan mengapa sangat penting bagi pengguna untuk tidak

membagikan detail login. Jika akun pengguna disusupi, tidak ada cara untuk mengikat peristiwa di log ke penyerang yang sebenarnya

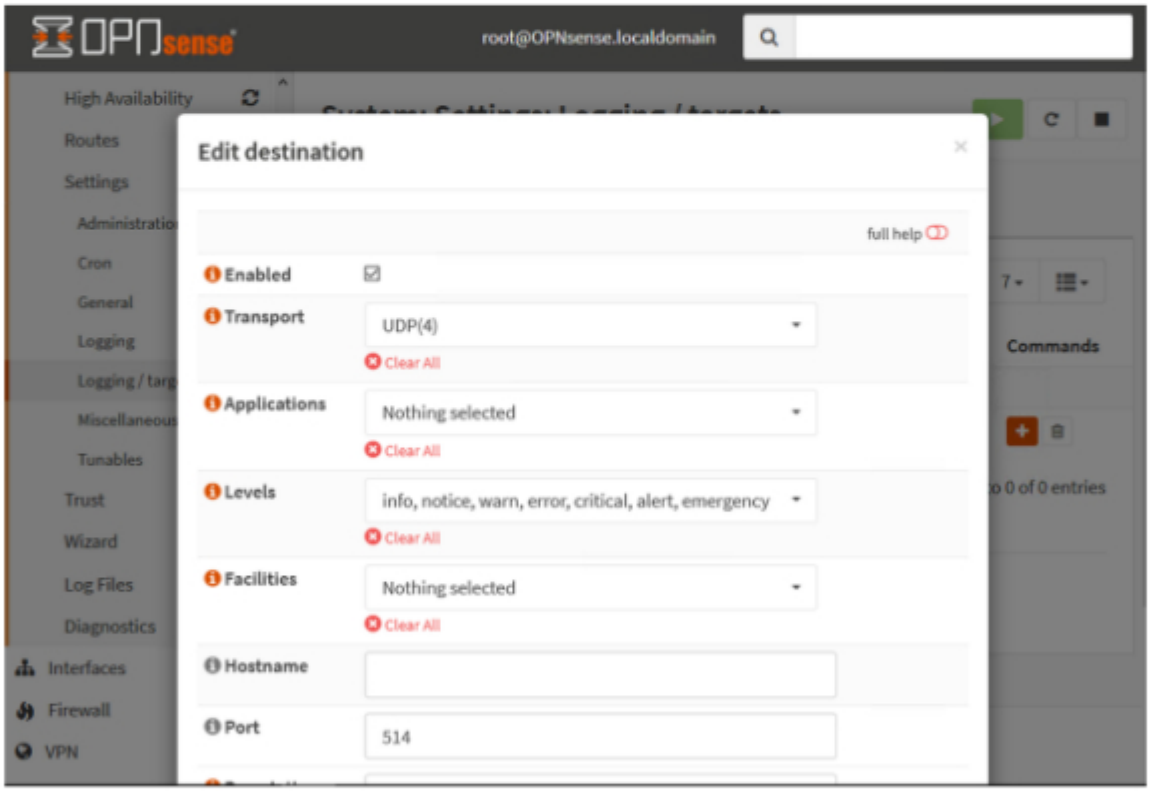
- **Performance/Traffic Logs**

  Log kinerja dan lalu lintas mencatat statistik untuk komputasi, penyimpanan, dan sumber daya jaringan selama periode yang ditentukan.

Log Collectors and Syslog

Pengumpul log mengumpulkan pesan peristiwa dari banyak perangkat ke satu lokasi penyimpanan. Selain menggabungkan log, sistem dapat dikonfigurasi untuk menjalankan satu atau lebih status dan dasbor peringatan.

Syslog adalah contoh protokol dan perangkat lunak pendukung yang memfasilitasi pengumpulan log. Ini telah menjadi standar de facto untuk mencatat peristiwa dari sistem terdistribusi. Misalnya, pesan syslog dapat dibuat oleh router dan switch Cisco®, serta server dan workstation UNIX atau Linux. Kolektor syslog biasanya mendengarkan pada port UDP 514.



Configuring an OPNsense security appliance to transmit logs to a remote syslog server. (Screenshot courtesy of OPNsense.)

Selain protokol untuk meneruskan pesan ke pengumpul log jarak jauh, Syslog menyediakan format terbuka untuk data peristiwa. Pesan syslog terdiri dari kode PRI, header yang berisi cap

waktu dan nama host, dan bagian pesan. Kode PRI dihitung dari fasilitas dan tingkat keparahan. Bagian pesan berisi tag yang menunjukkan proses sumber ditambah konten. Format konten bergantung pada aplikasi. Ini mungkin menggunakan bidang yang dipisahkan spasi atau koma atau pasangan nama/nilai, seperti data JavaScript Object Notation (JSON).

Event Management

Perangkat dapat menghasilkan ribuan acara per jam. Sistem untuk memprioritaskan mereka di antara yang membutuhkan respons segera atau jangka panjang sangat penting. Sebagian besar sistem pencatatan mengkategorikan setiap peristiwa. Misalnya, di Windows, peristiwa sistem dan aplikasi didefinisikan sebagai Informasional, Peringatan, atau Kritis, sedangkan peristiwa audit dikategorikan sebagai Sukses atau Gagal.

Tingkat keparahan syslog adalah sebagai berikut:

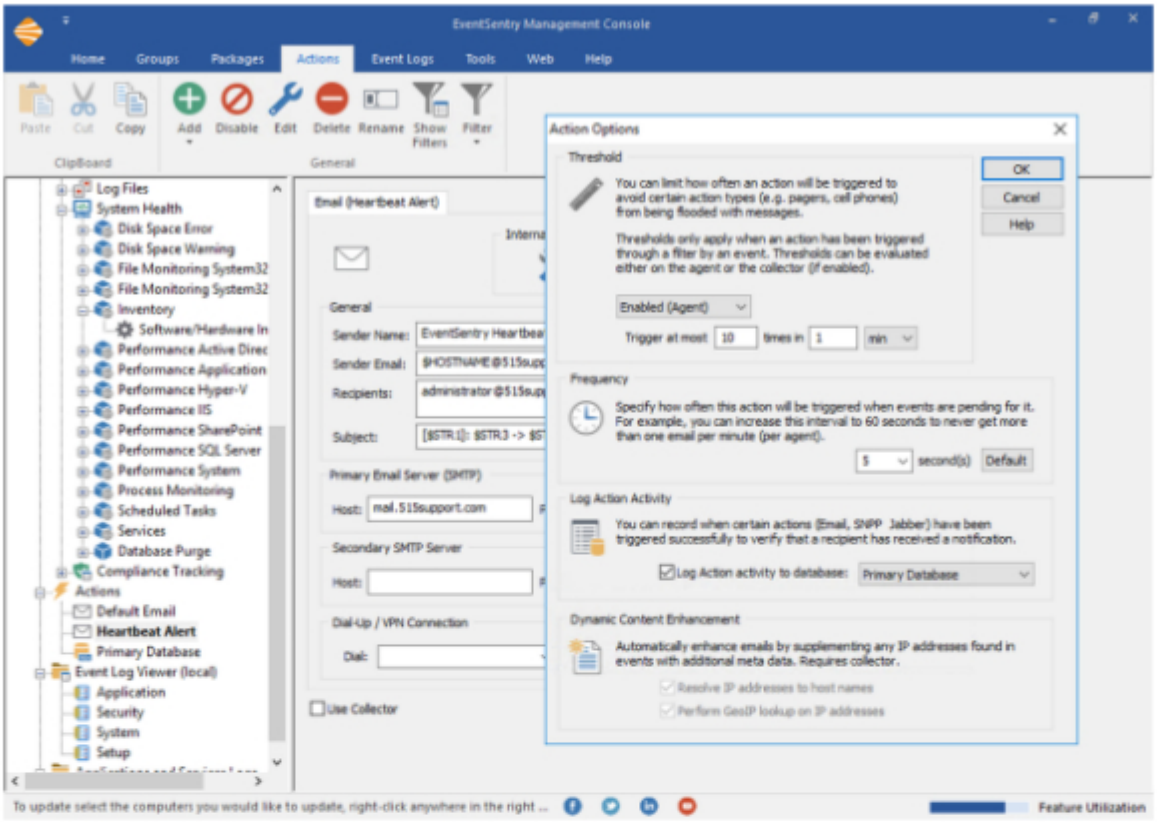
Code	Level	Interpretation
0	Emergency	The system is unusable (kernel panic)
1	Alert	A fault requiring immediate remediation has occurred
2	Critical	A fault that will require immediate remediation is likely to develop
3	Error	A nonurgent fault has developed
4	Warning	A nonurgent fault is likely to develop
5	Notice	A state that could potentially lead to an error condition has developed
6	Informational	A normal but reportable event has occurred
7	Debug	Verbose status conditions used during development and testing

Level logging yang dikonfigurasi pada setiap host menentukan level maksimum di mana peristiwa direkam atau diteruskan. Misalnya, jika level logging untuk penerusan jarak jauh diatur ke 4, peristiwa yang berada di level 5, 6, atau 7 tidak akan diteruskan.

Sistem manajemen peristiwa otomatis dapat dikonfigurasi untuk menghasilkan semacam peringatan ketika jenis peristiwa tertentu dengan tingkat keparahan tertentu ditemukan. Peringatan juga dapat dihasilkan dengan menetapkan ambang batas untuk penghitung kinerja. Contohnya termasuk kehilangan paket, penurunan bandwidth tautan, jumlah sesi yang dibuat, penundaan/jitter dalam aplikasi waktu nyata, dan sebagainya. Sebagian besar monitor jaringan juga mendukung tes detak jantung sehingga Anda dapat menerima peringatan jika perangkat atau server berhenti merespons pemeriksaan.

Mengatur peringatan adalah masalah keseimbangan. Di satu sisi, Anda tidak ingin kinerja menurun hingga memengaruhi aktivitas pengguna; di sisi lain, Anda tidak ingin kewalahan oleh peringatan.

Anda juga dapat membedakan antara lansiran dan pemberitahuan. Peringatan berarti bahwa sistem telah cocok dengan semacam pola atau filter yang harus direkam dan disorot. Notifikasi berarti bahwa sistem mengirimkan pesan untuk mengiklankan terjadinya peringatan. Peringatan prioritas rendah mungkin hanya ditampilkan di dasbor sistem. Peringatan prioritas tinggi mungkin menggunakan semacam pesan pemberitahuan aktif, seperti mengirim email ke administrator sistem, mengirim pesan teks (SMS) ke telepon, atau memicu sinyal alarm fisik.



Configuring alert and notification settings in EventSentry SIEM. (Screenshot courtesy of NETIKUS.NET Ltd.)

Harus ada beberapa proses untuk mengakui dan mengabaikan peringatan saat muncul. Peringatan serius mungkin perlu diproses sebagai insiden dan diberi tiket pekerjaan untuk penyelidikan formal. Jika peringatan adalah positif palsu, itu dapat diberhentikan. Jika sistem manajemen atau dasbor dibiarkan menjadi berantakan dengan peringatan lama, akan jauh lebih sulit untuk mengidentifikasi peringatan baru dan mengukur status keseluruhan jaringan.

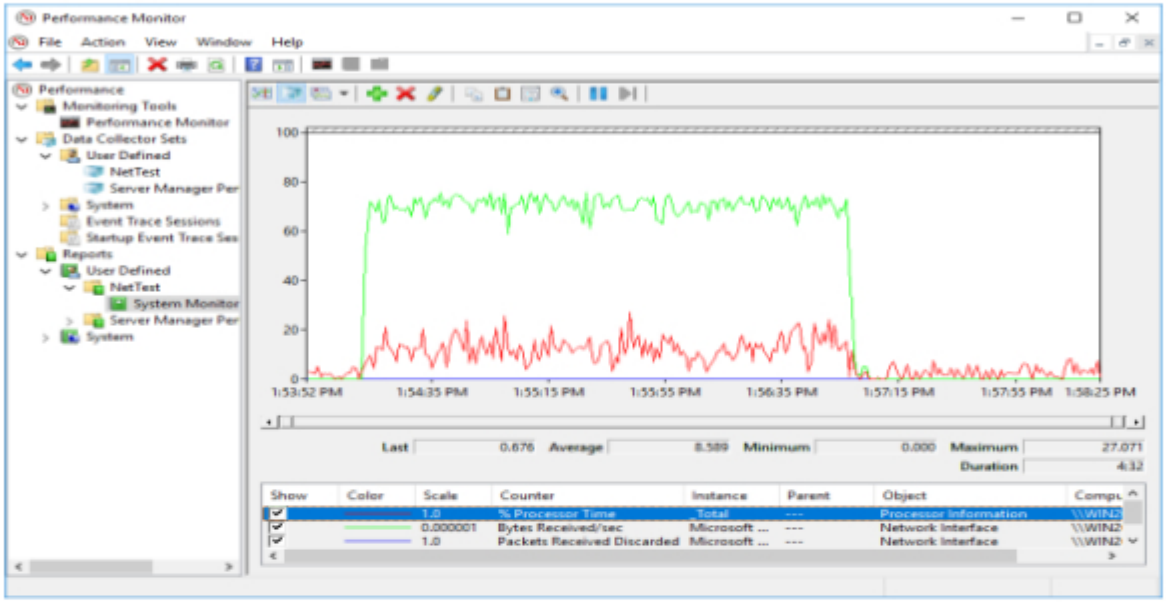
Log Reviews

Pemantauan melibatkan melihat lalu lintas, protokol, dan acara secara real time. Peninjauan jaringan dan log, atau analisis melibatkan pemeriksaan dan interpretasi selanjutnya dari data yang diambil untuk menentukan apa yang ditunjukkan oleh data yang terjadi di jaringan selama penangkapan. Pemantauan diselaraskan dengan respons insiden; analisis selaras dengan menyelidiki penyebab insiden atau mencegah insiden sejak awal. Penting untuk melakukan analisis kinerja dan tinjauan log secara terus-menerus. Mengacu pada log hanya setelah insiden besar kehilangan kesempatan untuk mengidentifikasi ancaman dan kerentanan atau masalah kinerja lebih awal dan untuk merespons secara proaktif.

Tidak semua insiden kinerja akan terungkap oleh satu acara. Salah satu fitur analisis log dan perangkat lunak pelaporan harus mengidentifikasi tren. Tren sulit dikenali dengan memeriksa setiap peristiwa dalam file log. Sebagai gantinya, Anda memerlukan perangkat lunak untuk

memetakan kejadian jenis peristiwa dan menunjukkan bagaimana jumlah atau frekuensi peristiwa tersebut berubah dari waktu ke waktu.

Memplot data sebagai grafik sangat membantu karena lebih mudah untuk melihat tren atau lonjakan atau palung dalam visualisasi peristiwa, daripada data mentah. Sebagian besar monitor kinerja dapat memplot metrik dalam grafik.



Data retrieved from a performance log file. (Screenshot courtesy of Microsoft.)

C. Gunakan Metrik Performa untuk Memastikan Ketersediaan Jaringan

Pendahuluan: Gunakan Metrik Performa untuk Memastikan Ketersediaan Jaringan

Jaringan modern menuntut persyaratan kinerja yang hanya dapat dievaluasi dan dipenuhi dengan menilai berbagai metrik kinerja. Memahami metrik ini dan cara merekam serta mengukurnya akan membantu Anda mengoptimalkan jaringan agar berkinerja pada tingkat puncaknya.

Metrik Jaringan

Protokol dan peralatan Quality of Service (QoS) dirancang untuk mendukung layanan real-time. Aplikasi seperti suara dan video yang membawa data waktu nyata memiliki persyaratan jaringan yang berbeda dengan jenis data yang diwakili oleh transfer file. Dengan data "biasa", mungkin bermanfaat untuk mentransfer file secepat mungkin, tetapi urutan pengiriman paket dan interval variabel antara paket yang tiba tidak mempengaruhi aplikasi secara material. Jenis transfer data ini digambarkan sebagai bursty.

Sementara aplikasi video streaming dapat memiliki kebutuhan bandwidth yang tinggi dalam hal jumlah data yang akan ditransfer, bandwidth pada jaringan modern biasanya lebih sedikit masalah daripada packet loss, latency, dan jitter.

Bandwidth

Bandwidth adalah jumlah informasi yang dapat ditransmisikan, diukur dalam bit per detik (bps), atau beberapa kelipatannya. Saat memantau, Anda perlu membedakan antara tautan data nominal/kecepatan bit Ethernet, throughput tautan di Layer 3, dan throughput yang tersedia untuk aplikasi.

Bandwidth untuk audio tergantung pada frekuensi sampling (Hertz) dan kedalaman bit setiap sampel. Misalnya, tautan telekomunikasi didasarkan pada saluran 64 Kbps. Ini diperoleh melalui perhitungan berikut:

- Rentang frekuensi suara adalah 4000 Hz. Ini harus diambil sampelnya dengan kecepatan dua kali lipat untuk memastikan representasi akurat dari bentuk gelombang analog asli.
- Ukuran sampel adalah 1 byte (atau 8 bit). Oleh karena itu, 8 KHz x 8 bit = 64 Kbps. Untuk VoIP, persyaratan bandwidth untuk panggilan suara dapat bervariasi, tetapi mengizinkan 100 Kbps per panggilan upstream dan downstream harus cukup dalam banyak kasus.

Bandwidth yang diperlukan untuk video ditentukan oleh resolusi gambar (jumlah piksel), kedalaman warna, dan kecepatan bingkai, diukur dalam bingkai per detik (fps).

Latency and Jitter

Masalah dengan waktu dan urutan pengiriman paket didefinisikan sebagai latency dan jitter. Latensi adalah waktu yang diperlukan transmisi untuk mencapai penerima, diukur dalam milidetik (ms). Jitter didefinisikan sebagai variasi dalam penundaan. Jitter memanifestasikan dirinya sebagai tingkat pengiriman paket yang tidak konsisten. Jitter juga diukur dalam milidetik, menggunakan algoritme untuk menghitung nilai dari sampel waktu transit.

Latensi dan jitter bukanlah masalah yang signifikan saat transfer data meledak, tetapi aplikasi waktu nyata jauh lebih sensitif terhadap efeknya karena bermanifestasi sebagai gema, penundaan, dan perlambatan video. Jika paket tertunda, tiba di luar urutan, atau hilang, maka host penerima harus menyangga paket yang diterima sampai paket yang tertunda diterima. Jika kehilangan atau penundaan paket sangat berlebihan sehingga buffer habis, maka masalah audio atau video (artefak) yang nyata dialami oleh pengguna.

Anda dapat menguji latensi tautan menggunakan alat seperti ping, jalur, dan mtr. Anda juga dapat menggunakan mtr untuk menghitung jitter. Saat menilai latensi, Anda perlu mempertimbangkan Waktu Pulang Pergi (RTT). VoIP umumnya diharapkan membutuhkan RTT

kurang dari 300 ms. Jitter harus 30 ms atau kurang. Tautan juga tidak boleh menunjukkan kehilangan paket lebih dari 1 persen.

Bandwidth Management

Latensi dan jitter di Internet sulit dikendalikan karena jumlah pihak yang terlibat berbeda (baik jaringan pemanggil plus jaringan transit ISP apa pun). Pada jaringan lokal, penundaan biasanya disebabkan oleh kemacetan. Artinya infrastruktur jaringan tidak mampu memenuhi tuntutan beban puncak.

Anda dapat menyediakan tautan bandwidth yang lebih tinggi dan/atau sakelar dan router yang lebih cepat, atau Anda dapat menggunakan semacam mekanisme manajemen bandwidth. Misalnya, jika Anda menjalankan VoIP melalui jaringan Anda dan seseorang memutuskan untuk menyalin file 40 GB dari server, transfer file berpotensi merusak kualitas panggilan VoIP. Tanpa QoS, switch dan router meneruskan lalu lintas berdasarkan upaya terbaik atau first-in, first-out, yang berarti bahwa frame atau paket diteruskan sesuai urutan kedatangannya. Sistem QoS mengidentifikasi paket atau aliran lalu lintas milik aplikasi tertentu, seperti VoIP, dan memprioritaskannya di atas aplikasi lain, seperti transfer file.

Differentiated Services

Kerangka kerja Differentiated Services (DiffServ) mengklasifikasikan setiap paket yang melewati perangkat. Kebijakan router kemudian dapat ditentukan untuk menggunakan klasifikasi paket untuk memprioritaskan pengiriman. DiffServ adalah mekanisme penandaan layanan IP (Layer 3). Ini menggunakan bidang Jenis Layanan di header IPv4 (Kelas Lalu Lintas di IPv6). Bidang diisi dengan DiffServ Code Point (DSCP) 6-byte oleh host pengirim atau oleh router. Paket dengan DSCP dan tujuan yang sama disebut sebagai Agregat Perilaku dan mengalokasikan Perilaku Per Hop (PHB) yang sama di setiap router yang kompatibel dengan DiffServ.

Kelas lalu lintas DiffServ biasanya dikelompokkan menjadi tiga jenis:

- Usaha terbaik.
- Penerusan Terjamin (yang dipecah menjadi sub-level).
- Expedited Forwarding (yang memiliki prioritas tertinggi).
- IEEE 802.1p

  Sementara DiffServ bekerja pada lapisan 3, IEEE 802.1p dapat digunakan pada Lapisan 2 (secara independen atau bersama dengan DiffServ) untuk mengklasifikasikan dan memprioritaskan lalu lintas yang melewati sakelar atau titik akses nirkabel. 802.1p mendefinisikan mekanisme penandaan dalam bidang VLAN 802.1Q (juga sering disebut sebagai 802.1Q/p). Bidang prioritas 3-bit diatur ke nilai antara 0 dan 7. Sebagian besar vendor memetakan nilai DSCP ke nilai 802.1p. Misalnya, 7 dan 6 dapat dicadangkan untuk kontrol jaringan (seperti pembaruan tabel perutean), peta 5 dan 4 ke tingkat penerusan yang dipercepat untuk komunikasi 2 arah, peta 3 dan 2 untuk penerusan terjamin untuk streaming multimedia, dan 1 dan 0 untuk pengiriman upaya terbaik "biasa".

Tips: Selain menggunakan tag prioritas, infrastruktur VLAN sering digunakan untuk manajemen lalu lintas di jaringan lokal. Misalnya, lalu lintas suara mungkin dialokasikan ke VLAN yang berbeda dari lalu lintas data.

Traffic Shaping

Quality of Service (QoS) berbeda dari Class of Service (CoS). mekanisme CoS seperti DiffServ dan 802.1p hanya mengkategorikan protokol ke dalam grup yang memerlukan tingkat layanan yang berbeda dan menyediakan mekanisme penandaan untuk menentukan kelas bingkai atau paket. QoS memungkinkan kontrol halus atas parameter lalu lintas. Misalnya, tautan jaringan macet, tidak ada yang dapat dilakukan DiffServ dan 802.1p, tetapi protokol seperti Multiprotocol Label Switching (MPLS) dengan fungsionalitas QoS dapat mencadangkan bandwidth yang diperlukan dan statistik yang telah ditentukan sebelumnya seperti yang dapat diterima packet loss dan latency maksimum dan jitter saat mengatur link.

Dalam hal QoS, fungsi jaringan biasanya dibagi menjadi tiga bidang:

- Control plane-membuat keputusan tentang bagaimana lalu lintas harus diprioritaskan dan di mana harus dialihkan.
- Data plane-menangani download lalu lintas yang sebenarnya.
- Pesawat manajemen-memantau kondisi lalu lintas.

Protokol, peralatan, dan perangkat lunak yang dapat menerapkan ketiga fungsi ini dapat digambarkan sebagai pembentuk lalu lintas atau pembentuk bandwidth. Pembentuk lalu menunda jenis paket tertentu berdasarkan kontennya-untuk memastikan bahwa paket lain memiliki prioritas yang lebih tinggi. Ini dapat membantu memastikan bahwa latensi berkurang untuk aplikasi penting.

Perangkat yang lebih sederhana, yang melakukan pengaturan lalu lintas, tidak menawarkan fungsi manajemen lalu lintas yang disempurnakan dari pembentuk. Misalnya, perangkat pemolisian lalu lintas biasa akan gagal mengirimkan paket setelah ambang lalu lintas yang dikonfigurasi telah tercapai (ini sering disebut sebagai penurunan ekor). Akibatnya, akan ada saat-saat ketika paket hilang, sementara di waktu lain jaringan relatif tidak aktif, dan bandwidth kurang dimanfaatkan. Pembentuk lalu lintas akan menyimpan paket sampai ada bandwidth gratis yang tersedia. Mudah-mudahan, ini mengarah pada penggunaan bandwidth yang konsisten dan beberapa paket yang hilang.

Tips: Perangkat yang dipilih harus mampu menangani volume lalu lintas yang tinggi. Karena perangkat ini memiliki buffer terbatas, akan ada situasi ketika buffer meluap. Perangkat dapat menjatuhkan paket dan pada dasarnya menyediakan pengaturan lalu lintas, atau perangkat lain harus menerapkan algoritma penurunan. Random Early Detection (RED) adalah salah satu dari beberapa algoritma yang dapat diimplementasikan untuk membantu mengatur traffic overflow pada shaper.

Traffic Analysis Tools

Manajemen bandwidth yang efektif atau kebijakan pembentukan lalu lintas bergantung pada informasi terperinci tentang arus lalu lintas jaringan. Alat analisis jaringan akan membantu Anda melaporkan kondisi lalu lintas.

Throughput Testers

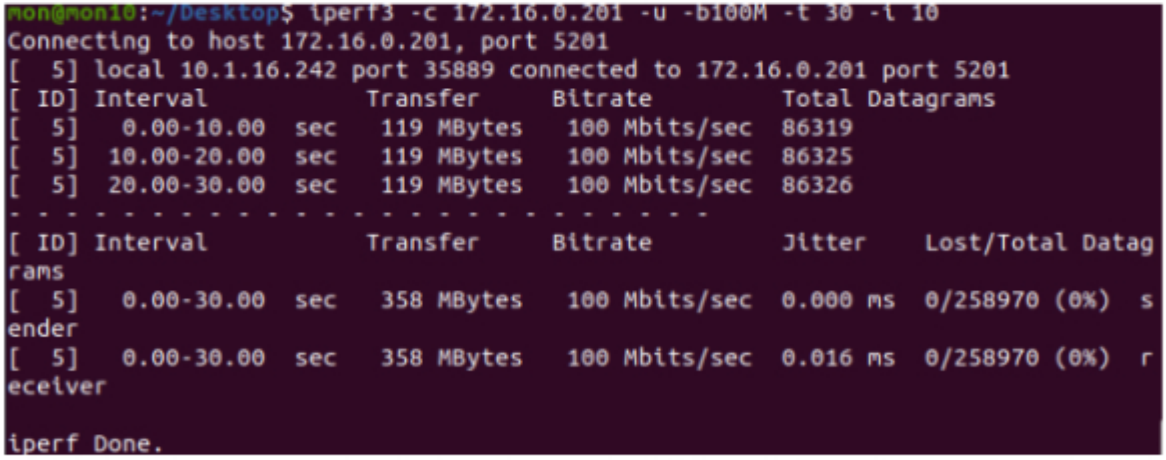
Salah satu cara yang cukup sederhana untuk mengukur throughput jaringan adalah dengan mentransfer file besar antara dua host yang sesuai. Sesuai dalam pengertian ini berarti subnet yang sesuai dan mewakili server dan workstation yang ingin Anda ukur. Penting juga untuk memilih waktu yang representatif. Tidak ada gunanya mengukur throughput ketika jaringan tidak membawa lalu lintas lain.

Untuk menentukan throughput jaringan Anda menggunakan metode ini, cukup bagi ukuran file dengan jumlah waktu yang dibutuhkan untuk menyalin file. Misalnya, jika Anda mentransfer file 1 GB dalam waktu setengah jam, throughput dapat dihitung sebagai berikut:

- 1 gigabyte is 1024 megabytes (1,073,741,824 bytes or 8,589,934,592 bits).
- 8,589,934,592 bits in 1,800 seconds is 4,772,186 bits per second or 4.55 Mbps.

Metode ini memperoleh nilai yang berbeda dari kecepatan data nominal. Karena dua host sedang mentransfer file antara satu sama lain, itu adalah lapisan Aplikasi yang menangani transfer file. Lapisan intervensi pada kedua host menambah kompleksitas (tajuk) dan memperkenalkan ketidakakuratan, seperti bingkai rusak yang harus ditransmisikan ulang.

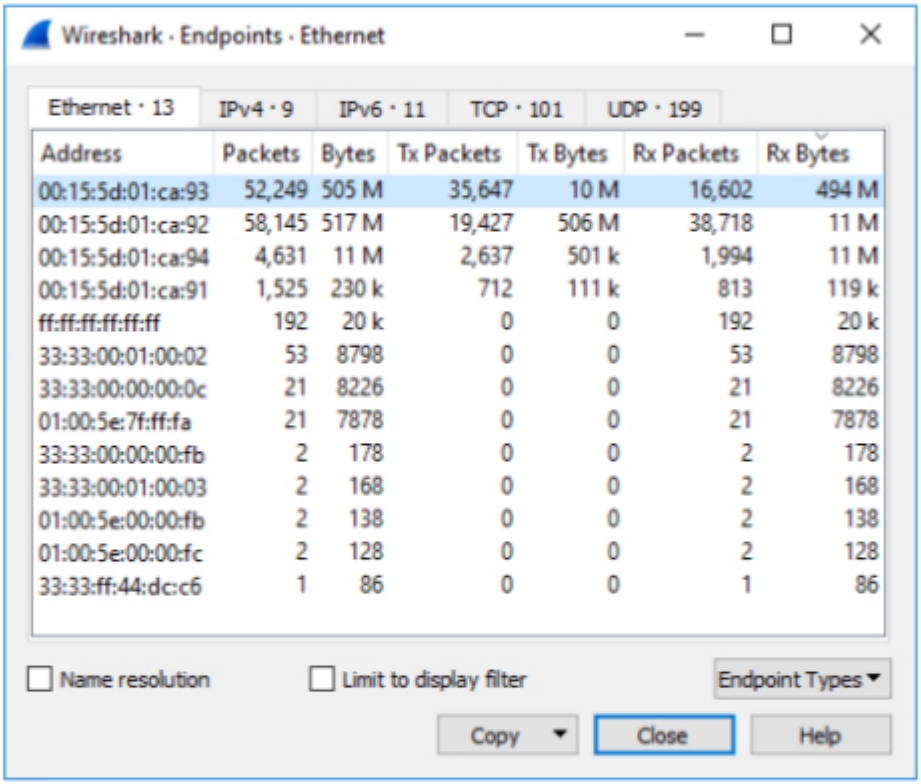
Beberapa utilitas perangkat lunak, seperti iperf (iperf.fr), Ttcp (linux.die.net/man/1/ttcp), dan bwping (bwping.sourceforge.io), dapat digunakan untuk mengukur throughput jaringan. Instance alat dikonfigurasi pada dua host jaringan dan alat mengukur throughput yang dicapai antara pengirim dan pendengar.



iperf3 transfer report showing bitrate, jitter, and packet loss. (Screenshot courtesy of iperf.)

Top Talkers/Listeners

Pembicara teratas adalah antarmuka yang menghasilkan lalu lintas keluar paling banyak (dalam hal bandwidth), sedangkan pendengar teratas adalah antarmuka yang menerima lalu lintas masuk paling banyak. Mengidentifikasi host ini dan rute yang mereka gunakan berguna dalam mengidentifikasi dan menghilangkan hambatan kinerja. Sebagian besar perangkat lunak penganalisis jaringan dilengkapi dengan filter atau pelaporan bawaan untuk mengidentifikasi pembicara teratas atau pendengar teratas.



The Endpoints report in Wireshark can be used to identify top talkers and top listeners. (Screenshot courtesy of Wireshark.)

Bandwidth Speed Testers

Selain menguji kinerja pada jaringan lokal, Anda mungkin juga ingin menguji tautan Internet menggunakan beberapa jenis penguji kecepatan bandwidth. Ada banyak alat Internet yang tersedia untuk memeriksa kinerja. Dua kelas utama adalah:

- Pemeriksa kecepatan broadband-Ini menguji seberapa cepat tautan broadband lokal ke Internet. Mereka sebagian besar dirancang untuk penggunaan SOHO. Alat ini akan menguji kecepatan downlink dan uplink, menguji latensi menggunakan ping, dan biasanya dapat membandingkan hasilnya dengan properti tetangga dan pengguna lain dari ISP yang sama.

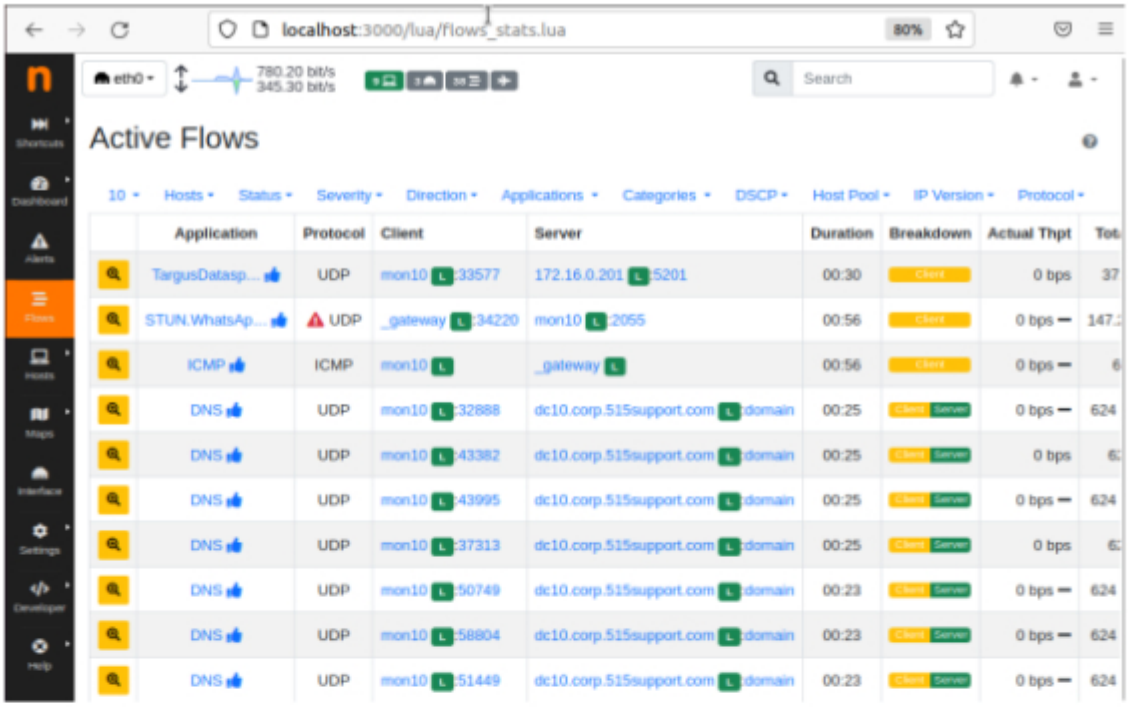
- Pemeriksa kinerja situs web-Ini meminta situs web yang dinominasikan untuk mengetahui seberapa cepat halaman dimuat. Salah satu keuntungan alat online adalah Anda dapat menguji waktu respons situs Anda dari perspektif pelanggan di berbagai negara.

NetFlow

Sebuah penganalisis paket dapat digunakan untuk mengukur statistik lalu lintas jaringan tetapi mencoba untuk merekam setiap frame membebankan overhead pemrosesan yang berat pada tap jaringan atau port cermin. Mengumpulkan hanya metadata paket, daripada seluruh muatan paket, mengurangi bandwidth yang dibutuhkan oleh sniffer. Teknologi seperti Cisco NetFlow (cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html) hanya mengumpulkan metadata lalu lintas dan melaporkannya ke database terstruktur. Teknologi ini juga dapat menggunakan pengambilan sampel untuk lebih mengurangi permintaan pemrosesan. NetFlow telah dikembangkan kembali sebagai standar IETF Ekspor Informasi Aliran IP (IPFIX) (tools.ietf.org/html/rfc7011).

Menggunakan NetFlow melibatkan penggelaran tiga jenis komponen:

- Eksportir NetFlow dikonfigurasi pada peralatan jaringan (switch, router, dan firewall). Setiap aliran didefinisikan pada eksportir. Aliran lalu lintas ditentukan oleh paket yang memiliki karakteristik yang sama, seperti sumber IP dan alamat tujuan serta jenis protokol. Lima bit informasi ini disebut sebagai 5-tuple. Aliran 7-tuple menambahkan antarmuka input dan jenis data layanan IP. Setiap eksportir menyimpan data untuk aliran yang baru terlihat dan menyetel timer untuk menentukan kedaluwarsa aliran. Ketika aliran kedaluwarsa atau menjadi tidak aktif, eksportir mengirimkan data ke kolektor.
- Kolektor NetFlow mengumpulkan aliran dari beberapa eksportir. Jaringan yang besar dapat menghasilkan volume lalu lintas aliran dan catatan data yang sangat besar, sehingga kolektor membutuhkan tautan jaringan bandwidth tinggi dan kapasitas penyimpanan yang besar. Eksportir dan kolektor harus mendukung versi NetFlow dan/atau IPFIX yang kompatibel. Versi NetFlow yang paling banyak digunakan adalah v5 dan v9.
- Penganalisis NetFlow melaporkan dan menafsirkan informasi dengan menanyakan kolektor dan dapat dikonfigurasi untuk menghasilkan peringatan dan pemberitahuan. Dalam istilah praktis, komponen pengumpul dan penganalisis sering diimplementasikan sebagai satu produk.



ntopng community edition being used to monitor NetFlow traffic data. (Screenshot used courtesy of ntop.)

Interface Monitoring Metrics

Anda dapat mengumpulkan data dan mengonfigurasi peringatan untuk statistik antarmuka, baik pada adaptor jaringan atau sakelar atau port router.

- Link state : Mengukur apakah antarmuka berfungsi (naik) atau tidak (bawah). Anda akan mengonfigurasi peringatan jika antarmuka turun sehingga dapat segera diselidiki. Anda mungkin juga ingin melacak persentase uptime atau downtime sehingga Anda dapat menilai keandalan tautan dari waktu ke waktu.
- Resets : Berapa kali antarmuka telah dimulai ulang selama periode kontra. Antarmuka dapat diatur ulang secara manual atau dapat dimulai ulang secara otomatis jika volume lalu lintas sangat tinggi, atau sejumlah besar kesalahan dialami. Apa pun kecuali reset sesekali harus dipantau dan diselidiki secara ketat. Antarmuka yang terus-menerus diatur ulang digambarkan sebagai mengepakkan.
- Speed : adalah kecepatan rated antarmuka, diukur dalam Mbps atau Gbps. Untuk tautan Ethernet kabel ini biasanya tidak akan bervariasi, tetapi bandwidth WAN dan tautan nirkabel dapat berubah seiring waktu. Untuk tautan Ethernet, kecepatan antarmuka harus sama pada port host dan switch.
- <>bDuplex-Most Ethernet beroperasi dalam mode full duplex. Jika antarmuka beroperasi dalam mode half duplex, kemungkinan akan ada semacam masalah, kecuali jika Anda mendukung perangkat lama.

- Utilization : data yang ditransfer selama periode tertentu. Ini dapat diukur sebagai jumlah lalu lintas data yang dikirim dan diterima (diukur dalam bit atau byte per detik atau kelipatannya) atau dihitung sebagai persentase dari bandwidth yang tersedia.

Tips: Anda juga perlu membedakan antara pemanfaatan rata-rata dan pemanfaatan puncak. Jika penggunaan rata-rata sekitar 80%, mungkin tampak bahwa ada bandwidth yang cukup. Namun, jika pemanfaatan puncak sering melonjak hingga 100%, maka itu akan bermanifestasi sebagai penundaan dan kehilangan paket dan mungkin mengharuskan Anda meningkatkan tautan. Memantau panjang antrean dapat membantu menentukan apakah tautan tersebut merupakan kemacetan.

- Per-protocol utilization: Paket atau byte dihitung untuk protokol tertentu. Hal ini sering berguna untuk memantau jumlah paket dan konsumsi bandwidth. Jumlah paket yang tinggi akan dikenakan beban pemrosesan pada CPU dan sumber daya memori sistem alat, bahkan jika ukuran setiap paket cukup kecil.
- Error rate : Jumlah paket per detik yang menyebabkan kesalahan. Kesalahan dapat terjadi sebagai akibat dari gangguan atau kualitas tautan yang buruk yang menyebabkan kerusakan data dalam bingkai. Secara umum, tingkat kesalahan harus di bawah 1 persen; Tingkat kesalahan yang tinggi dapat mengindikasikan masalah driver, jika masalah media jaringan dapat dikesampingkan.
- Discards/drops : Antarmuka dapat membuang frame masuk dan / atau keluar karena beberapa alasan, termasuk kesalahan checksum, MTUs yang tidak serasi, paket yang terlalu kecil (runt) atau terlalu besar (raksasa), beban tinggi, atau izin - pengirim tidak ada dalam daftar kontrol akses antarmuka (ACL) atau ada semacam masalah konfigurasi VLAN, misalnya. Setiap antarmuka cenderung mengklasifikasikan jenis buang atau jatuhkan secara terpisah untuk membantu pemecahan masalah penyebab pastinya.

Tips: Beberapa vendor dapat menggunakan istilah buang untuk frame yang ditolak karena kesalahan atau kebijakan keamanan dan drop untuk frame yang hilang karena beban tinggi, tetapi sering istilah yang digunakan secara bergantian.

- Retransmissions : Kesalahan dan buang / tetes berarti bahwa frame data hilang selama transmisi antara dua perangkat. Akibatnya, komunikasi tidak akan lengkap, dan data akan, oleh karena itu, harus dikirim kembali untuk memastikan integritas data aplikasi. Jika Anda mengamati tingkat transmisi ulang yang tinggi (sebagai persentase dari keseluruhan lalu lintas), Anda harus menganalisis dan memecahkan masalah penyebab spesifik dari kehilangan paket yang mendasarinya, yang dapat melibatkan beberapa aspek konfigurasi dan konektivitas jaringan.

Troubleshooting Interface Errors

Serta pemantauan untuk kemacetan lalu lintas dan masalah kinerja lainnya, kesalahan antarmuka mungkin menunjukkan masalah kesalahan konfigurasi pada lapisan tautan data atau gangguan pada lapisan fisik.

Cyclic Redundancy Check Errors

Pemeriksaan redundansi siklik (CRC) dihitung oleh antarmuka saat mengirim bingkai. Nilai CRC dihitung dari konten bingkai untuk mendapatkan nilai 32-bit. Ini ditambahkan ke header sebagai urutan pemeriksaan bingkai. Antarmuka penerima menggunakan perhitungan yang sama. Jika mendapatkan nilai yang berbeda, frame ditolak. Jumlah kesalahan CRC dapat dipantau per antarmuka.

Kesalahan CRC biasanya disebabkan oleh gangguan. Gangguan ini mungkin disebabkan oleh kabel atau pemutusan kualitas yang buruk, redaman, ketidakcocokan antara transceiver optik atau jenis kabel, atau karena beberapa faktor eksternal.

Encapsulation Errors

Enkapsulasi adalah format bingkai yang diharapkan pada antarmuka. Kesalahan enkapsulasi akan mencegah transmisi dan penerimaan. Jika Anda memeriksa status antarmuka, tautan fisik akan terdaftar sebagai naik, tetapi protokol jalur akan terdaftar sebagai bawah. Jenis kesalahan ini dapat muncul dalam beberapa keadaan:

- Ethernet frame type : Ethernet dapat menggunakan berbagai jenis bingkai. Yang paling umum adalah Ethernet II, tetapi jika host dikonfigurasi untuk menggunakan tipe yang berbeda, seperti SNAP, maka kesalahan akan dilaporkan pada tautan.
- Ethernet trunks : Ketika sebuah trunk link dibuat antara dua switch, biasanya akan menggunakan format frame Ethernet 802.1Q. 802.1Q menentukan header bingkai tambahan untuk membawa ID VLAN dan jenis data layanan. Jika satu antarmuka sakelar menggunakan 802.1Q tetapi yang lain tidak, ini dapat dilaporkan sebagai kesalahan enkapsulasi.
- WAN framing : Antarmuka router ke jaringan penyedia dapat menggunakan berbagai format bingkai. Seringkali ini adalah protokol serial sederhana, seperti High-level Data Link Control (HDLC) atau Point-to-Point Protocol (PPP). Atau, antarmuka dapat menggunakan Ethernet yang dienkapsulasi melalui Asynchronous Transfer Mode (ATM) atau Virtual Private LAN Service (VPLS) atau protokol yang lebih lama, seperti Frame Relay. Antarmuka pada router Customer Edge (CE) harus dikonfigurasi untuk jenis pembingkaian yang sama dengan router Provider Edge (PE).

Runt Frame Errors

Kerdil adalah bingkai yang lebih kecil dari ukuran minimum (64 byte untuk Ethernet). Bingkai kerdil biasanya disebabkan oleh tabrakan. Dalam lingkungan yang diaktifkan, tabrakan hanya boleh dialami pada antarmuka yang terhubung ke perangkat hub lama dan ada ketidakcocokan

dupleks dalam konfigurasi antarmuka (atau mungkin pada tautan yang salah konfigurasi ke platform virtualisasi). Jika kerdil dihasilkan dalam kondisi lain, curigai masalah driver pada host transmisi.

Giant Frame Errors

Raksasa adalah bingkai yang lebih besar dari ukuran maksimum yang diizinkan (1518 byte untuk Ethernet II). Ada dua kemungkinan penyebab bingkai raksasa:

- **Ethernet trunks** : Seperti di atas, jika satu antarmuka sakelar dikonfigurasi untuk pembingkaian 802.1Q, tetapi yang lainnya tidak, bingkai akan tampak terlalu besar bagi penerima, karena 802.1Q menambahkan 4 byte ke header, membuat ukuran bingkai maksimum 1522 byte.

Tips: Bingkai Ethernet yang sedikit lebih besar (hingga 1600 byte) sering disebut sebagai bayi raksasa.

- **Jumbo frames** : Sebuah host mungkin dikonfigurasi untuk menggunakan frame jumbo, tetapi antarmuka switch tidak dikonfigurasi untuk menerimanya. Jenis masalah ini sering terjadi saat mengonfigurasi jaringan area penyimpanan (SAN) atau tautan antara SAN dan jaringan data.

Modul 13

Menjelaskan konsep keamanan umum

JELASKAN KONSEP KEAMANAN UMUM

Pendahuluan: Jelaskan Konsep Keamanan Umum

Dalam pelajaran ini, Anda akan menjelaskan konsep dasar yang terkait dengan penilaian keamanan jaringan. Sangat penting untuk memiliki dasar yang kuat dan kesadaran akan terminologi industri yang digunakan saat Anda mendiskusikan keamanan jaringan.

Konsep Keamanan

Membangun keamanan komputer dan jaringan berarti mengembangkan proses dan kontrol yang melindungi aset data dan memastikan kelangsungan bisnis dengan membuat sistem jaringan dan host tahan terhadap berbagai jenis serangan.

The Confidentiality, Integrity, and Availability (CIA) Triad

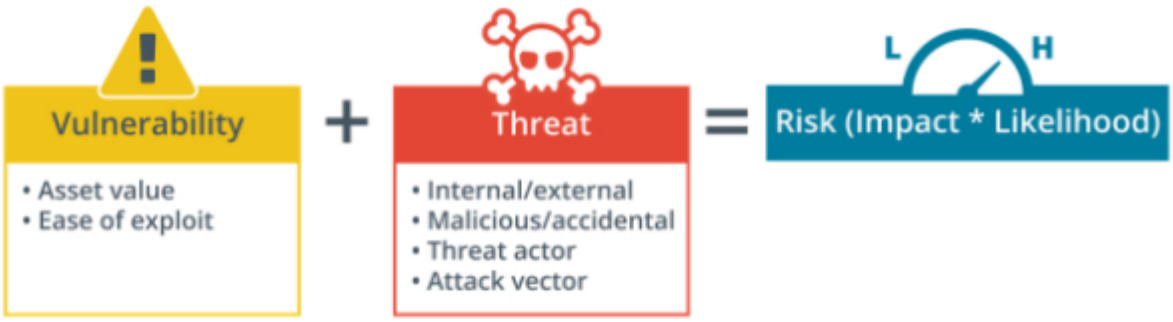
Salah satu prinsip dasar keamanan komputer adalah bahwa sistem yang digunakan untuk menyimpan, mengirimkan, dan memproses data harus menunjukkan tiga sifat, sering disebut sebagai CIA Triad:

- Kerahasiaan berarti bahwa informasi tertentu hanya boleh diketahui oleh orang-orang tertentu.
- Integritas berarti bahwa data disimpan dan ditransfer sebagaimana dimaksud dan bahwa modifikasi apa pun diizinkan.
- Ketersediaan berarti bahwa informasi dapat diakses oleh mereka yang berwenang untuk melihat atau memodifikasinya.

Kerentanan, Ancaman, dan Risiko

Untuk melakukan penilaian dan pemantauan, tim keamanan harus mengidentifikasi cara di mana sistem mereka dapat diserang. Penilaian ini melibatkan kerentanan, ancaman, dan risiko:

- **Kerentanan** -Kelemahan yang dapat dipicu secara tidak sengaja atau sengaja dieksploitasi untuk menyebabkan pelanggaran keamanan.
- **Ancaman** - Potensi seseorang atau sesuatu untuk mengeksploitasi kerentanan dan melanggar keamanan. Ancaman mungkin disengaja atau tidak disengaja. Orang atau hal yang menimbulkan ancaman disebut sebagai aktor ancaman atau agen ancaman. Jalur atau alat yang digunakan oleh aktor ancaman jahat dapat disebut sebagai vektor serangan. Risiko-Kemungkinan dan dampak (atau konsekuensi) dari aktor ancaman yang menjalankan kerentanan.



Hubungan antara kerentanan, ancaman, dan risiko.

Penilaian Risiko Keamanan

Banyak alat dan teknik yang tersedia untuk memastikan bahwa sistem jaringan menunjukkan tiga sifat dari triad CIA. Pemilihan dan penerapan alat ini dipandu oleh kebijakan keamanan. Kebijakan keamanan memastikan bahwa organisasi telah mengevaluasi risiko yang dihadapinya dan telah menerapkan kontrol keamanan untuk mengurangi risiko tersebut. Membuat sistem lebih aman juga disebut sebagai pengerasan. Kebijakan keamanan yang berbeda harus mencakup setiap aspek penggunaan teknologi komputer dan jaringan organisasi, mulai dari pengadaan dan kontrol perubahan hingga penggunaan yang dapat diterima.

Manajemen risiko adalah proses untuk mengidentifikasi, menilai, dan mengurangi kerentanan dan ancaman terhadap fungsi penting yang harus dilakukan bisnis untuk melayani pelanggannya. Manajemen risiko itu kompleks dan diperlakukan sangat berbeda di perusahaan dan institusi dengan ukuran berbeda, dan dengan persyaratan peraturan dan kepatuhan yang berbeda. Sebagian besar perusahaan akan melembagakan kebijakan dan prosedur manajemen risiko perusahaan (enterprise risk management/ERM), berdasarkan kerangka kerja yang diterbitkan.

Penilaian risiko adalah bagian dari manajemen risiko di mana sistem dan prosedur perusahaan dievaluasi untuk faktor risiko. Penilaian terpisah dapat dirancang untuk melakukan evaluasi awal dan pemantauan berkelanjutan terhadap ancaman, kerentanan, dan postur keamanan.

Penilaian Postur

Ada banyak cara berpikir yang berbeda tentang bagaimana layanan TI harus diatur untuk memenuhi kebutuhan bisnis secara keseluruhan. Beberapa organisasi telah mengembangkan kerangka kerja layanan TI untuk memberikan panduan praktik terbaik untuk menerapkan TI dan keamanan siber. Kerangka kerja ini dapat membentuk kebijakan perusahaan dan menyediakan daftar prosedur, aktivitas, dan teknologi yang idealnya harus ada.

Secara kolektif, prosedur, aktivitas, dan alat ini dapat disebut sebagai kontrol keamanan. Kontrol keamanan adalah sesuatu yang dirancang untuk memberikan sistem atau aset data sifat kerahasiaan, integritas, ketersediaan, dan non-penolakan.

Secara teori, kontrol keamanan atau tindakan pencegahan dapat diperkenalkan untuk mengatasi setiap faktor risiko. Kesulitannya adalah bahwa kontrol keamanan bisa mahal, jadi Anda harus menyeimbangkan biaya kontrol dengan biaya yang terkait dengan risiko. Tidak mungkin untuk menghilangkan risiko; melainkan, tujuannya adalah untuk memitigasi faktor risiko ke titik di mana organisasi hanya terpapar pada tingkat risiko yang mampu ditanggungnya. Status keseluruhan manajemen risiko disebut sebagai postur risiko. Postur risiko menunjukkan opsi respons risiko mana yang dapat diidentifikasi dan diprioritaskan. Penilaian postur sering dilakukan dengan mengacu pada kerangka kerja TI atau keamanan. Kerangka kerja tersebut dapat digunakan untuk menilai tingkat kematangan organisasi dalam penggunaan kebijakan dan kontrol keamanannya.

Penilaian Proses Mengurangi risiko dapat melibatkan sejumlah besar pengeluaran sehingga penting untuk memfokuskan upaya. Manajemen risiko yang efektif harus fokus pada fungsi-fungsi penting misi yang dapat menyebabkan seluruh bisnis gagal jika tidak dilakukan. Bagian dari proses ini melibatkan pengidentifikasian sistem dan aset penting yang mendukung fungsi-fungsi ini. Fungsi esensial misi (MEF) adalah fungsi yang tidak dapat ditunda. Artinya organisasi harus dapat menjalankan fungsi sedekat mungkin secara terus menerus, dan jika ada gangguan layanan, fungsi esensial misi harus dipulihkan terlebih dahulu.

Analisis dampak bisnis (BIA) adalah proses menilai kerugian apa yang mungkin terjadi untuk berbagai skenario ancaman. Misalnya, jika serangan penolakan layanan (DoS) menangguhkan portal e-niaga selama lima jam, analisis dampak bisnis akan dapat mengukur kerugian dari pesanan yang tidak dibuat dan pelanggan pindah secara permanen ke pemasok lain berdasarkan data historis. Kemungkinan serangan DoS dapat dinilai secara tahunan untuk menentukan dampak tahunan, dalam hal biaya. Anda kemudian memiliki informasi yang diperlukan untuk menilai apakah kontrol keamanan, seperti penyeimbangan beban atau mitigasi serangan terkelola, bernilai investasi.

Dimana BIA mengidentifikasi risiko, perencanaan kelangsungan bisnis (BCP) mengidentifikasi kontrol dan proses yang memungkinkan organisasi untuk mempertahankan alur kerja kritis dalam menghadapi beberapa peristiwa yang merugikan.

Jenis Kerentanan dan Eksploitasi

Kerentanan dapat terjadi karena kesalahan konfigurasi atau praktik yang buruk, tetapi banyak orang memahami istilah tersebut sebagai kesalahan dalam perangkat lunak secara khusus. Kerentanan perangkat lunak adalah cacat desain yang dapat menyebabkan sistem keamanan aplikasi dielakkan atau yang akan menyebabkan aplikasi mogok. Kerentanan yang paling serius memungkinkan penyerang untuk mengeksekusi kode arbitrer pada sistem, yang dapat memungkinkan instalasi malware atau memungkinkan aktor ancaman untuk menonaktifkan

atau melemahkan konfigurasi yang aman. Biasanya, aplikasi seperti server web, browser web, plug-in browser web, klien email, dan database menjadi sasaran.

Eksploitasi adalah kode atau metode khusus untuk menggunakan kerentanan untuk mendapatkan kendali atas suatu sistem atau merusaknya dengan cara tertentu. Biasanya, kerentanan perangkat lunak dapat dieksploitasi hanya dalam keadaan yang cukup spesifik, tetapi karena kompleksitas perangkat lunak modern dan kecepatan rilis versi baru ke pasar, hampir tidak ada perangkat lunak yang bebas dari kerentanan.

Kerentanan dan Eksploitasi Zero-Day
Sebagian besar kerentanan perangkat lunak ditemukan oleh peneliti perangkat lunak dan keamanan, yang memberi tahu vendor untuk memberi mereka waktu untuk menambal kerentanan sebelum merilis detailnya ke publik yang lebih luas. Kerentanan yang dieksploitasi sebelum pengembang mengetahuinya atau dapat merilis patch disebut zero-day. Ini bisa sangat merusak, karena vendor membutuhkan banyak waktu untuk mengembangkan tambalan, membuat sistem rentan selama berhari-hari, berminggu-minggu, atau bahkan bertahun-tahun.

Tips: Istilah zero-day biasanya diterapkan pada kerentanan itu sendiri tetapi juga dapat merujuk pada serangan atau malware yang mengeksploitasinya.

Sistem yang Belum Ditambal dan Lama
Meskipun eksploitasi untuk kerentanan zero-day bisa sangat merusak, itu adalah kejadian yang relatif jarang terjadi. Ancaman yang lebih besar adalah banyaknya sistem yang belum ditambal atau sistem lama yang digunakan. Sistem yang belum ditambal adalah sistem yang belum diperbarui oleh pemiliknya dengan OS dan patch aplikasi; sistem warisan adalah sistem di mana vendor perangkat lunak tidak lagi memberikan dukungan atau perbaikan untuk masalah.
Tips: Masalah ini tidak hanya memengaruhi PC. Peralatan jaringan juga bisa rentan terhadap eksploitasi. Risiko terhadap sistem tertanam telah menjadi lebih jelas selama beberapa tahun terakhir, dan risiko yang ditimbulkan oleh perangkat seluler yang belum ditambal dan Internet of Things kemungkinan akan meningkat.

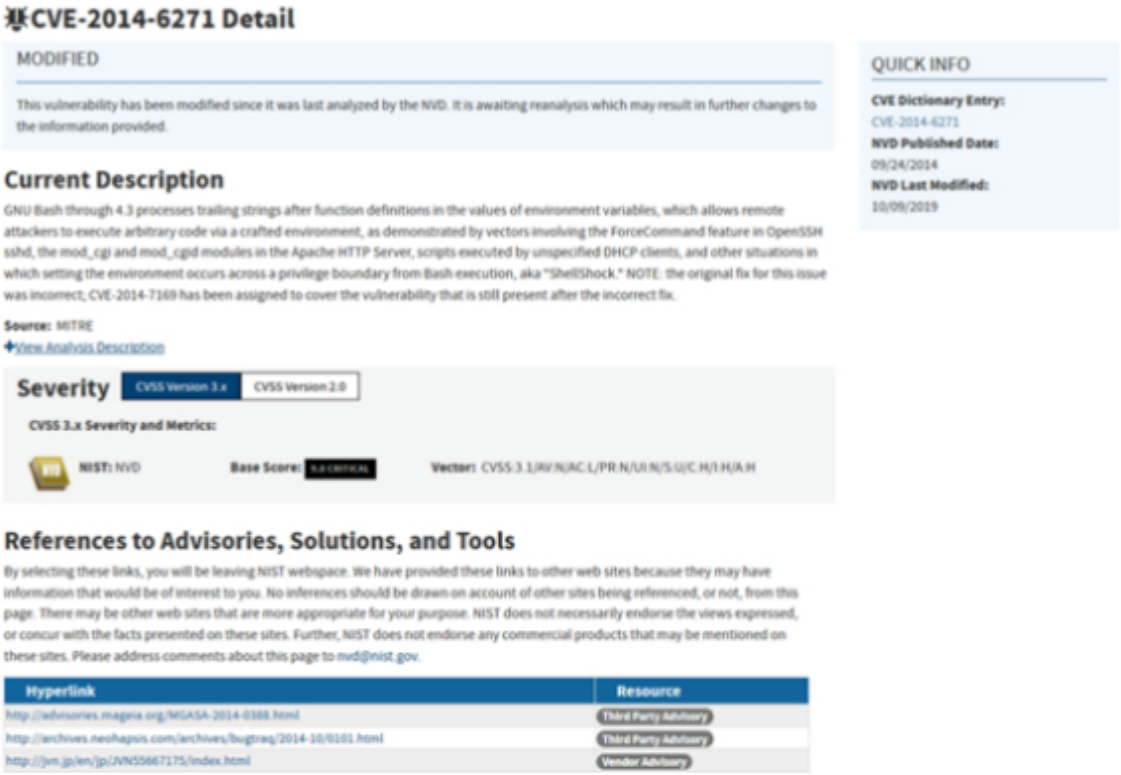
Penilaian Kerentanan Penilaian
kerentanan adalah evaluasi keamanan sistem dan kemampuan untuk memenuhi persyaratan kepatuhan berdasarkan status konfigurasi sistem. Pada dasarnya, penilaian kerentanan menentukan apakah konfigurasi saat ini cocok dengan konfigurasi ideal (baseline). Penilaian kerentanan mungkin melibatkan pemeriksaan manual terhadap kontrol keamanan tetapi lebih sering dilakukan melalui pemindai kerentanan otomatis.

Kerentanan dan Eksposur

Umum Kerentanan dan Eksposur Umum (CVE) adalah kamus kerentanan dalam sistem operasi dan perangkat lunak aplikasi yang diterbitkan (cve.mitre.org). Perangkat lunak pemindaian kerentanan otomatis menggunakan kamus ini untuk mengembangkan pengujian guna

menemukan kerentanan pada sistem langsung. Ada beberapa elemen yang membentuk entri kerentanan di CVE:

- Pengidentifikasi dalam format: CVE-YYYY-####, di mana YYYY adalah tahun kerentanan ditemukan, dan #### setidaknya empat digit yang menunjukkan urutan kerentanan ditemukan.
- Deskripsi singkat tentang kerentanan.
- Daftar referensi URL yang menyediakan lebih banyak informasi tentang kerentanan.
- Tanggal entri kerentanan dibuat.



CVE-2014-6271 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.

Source: MITRE

View Analysis Description

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry: CVE-2014-6271

NVD Published Date: 09/24/2014

NVD Last Modified: 10/09/2019

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://advisories.mageia.org/MGASA-2014-0388.html	Third Party Advisory
http://archives.neohapsis.com/archives/bugtraq/2014-10/0101.html	Third Party Advisory
http://jvn.jp/en/jp/JVN55667175/index.html	Vendor Advisory

Contoh CV.

Jenis dan Penilaian Ancaman

Eksploitasi untuk kerentanan dikembangkan oleh aktor ancaman atau diekspos oleh kelemahan prosedur yang tidak disengaja. Penilaian ancaman adalah proses mengidentifikasi sumber ancaman dan membuat profil jenis dan kemampuan aktor ancaman.

Ancaman Eksternal versus Internal

Aktor atau agen ancaman eksternal adalah orang yang tidak memiliki akun atau akses resmi ke sistem target. Ancaman eksternal yang berbahaya harus menyusup ke sistem keamanan menggunakan malware dan/atau rekayasa sosial. Perhatikan bahwa aktor eksternal dapat

melakukan serangan dari jarak jauh atau di tempat (dengan membobol kantor pusat perusahaan, misalnya). Ini adalah aktor ancaman yang didefinisikan sebagai eksternal, bukan metode serangan.

Sebaliknya, aktor ancaman internal (atau orang dalam) adalah orang yang telah diberikan izin pada sistem. Ini biasanya berarti seorang karyawan, tetapi ancaman orang dalam juga dapat muncul dari kontraktor dan mitra bisnis.

Penelitian

Ancaman Penelitian ancaman adalah upaya pengumpulan kontra intelijen di mana perusahaan keamanan dan peneliti berusaha menemukan taktik, teknik, dan prosedur (TTP) aktor ancaman.

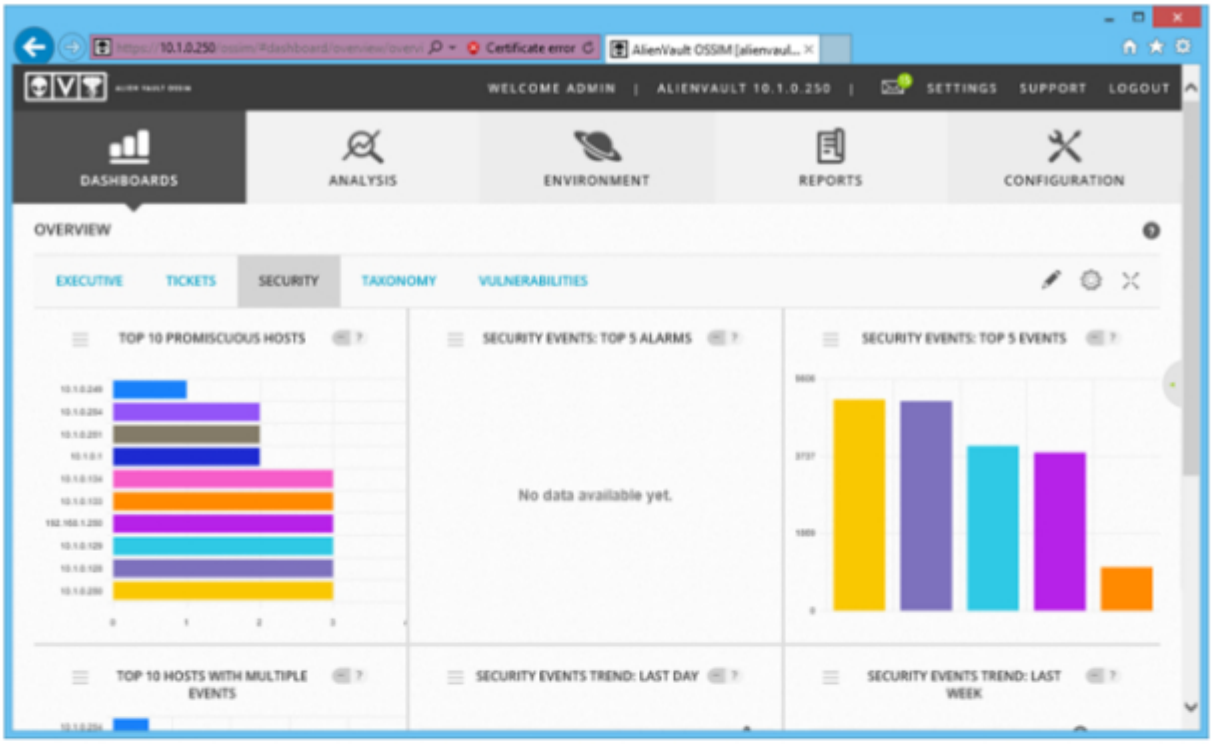
Keluaran dari penelitian utama yang dilakukan oleh penyedia solusi keamanan dan akademisi dapat mengambil tiga bentuk utama:

- **Penelitian ancaman perilaku** -komentar naratif yang menjelaskan contoh serangan dan TTP yang dikumpulkan melalui sumber penelitian utama.
- **Intelijen ancaman reputasi** -daftar alamat IP dan domain yang terkait dengan perilaku jahat, ditambah tanda tangan malware berbasis file yang diketahui.
- **Data ancaman** -data komputer yang dapat menghubungkan peristiwa yang diamati pada jaringan dan log pelanggan sendiri dengan indikator TTP dan aktor ancaman yang diketahui.

Informasi Keamanan dan Manajemen Acara

Informasi Keamanan dan Manajemen Peristiwa (SIEM) adalah kontrol keamanan yang dirancang untuk mengintegrasikan upaya penilaian kerentanan dan ancaman melalui pengumpulan, agregasi, dan analisis data log otomatis. Fungsi inti dari alat SIEM adalah untuk mengumpulkan log dari berbagai sumber. Selain log dari host berbasis Windows dan Linux, ini dapat mencakup sakelar, router, firewall, sensor deteksi intrusi, pemindai kerentanan, pemindai malware, dan basis data.

Fungsi kritis kedua dari SIEM (dan faktor utama yang membedakannya dari manajemen log dasar) adalah korelasi. Ini berarti bahwa perangkat lunak SIEM dapat menghubungkan peristiwa individu atau titik data (dapat diamati) menjadi indikator risiko yang berarti, atau indikator kompromi (IOC). Korelasi kemudian dapat digunakan untuk menggerakkan sistem peringatan. Akhirnya, SIEM dapat memberikan fungsi retensi jangka panjang dan digunakan untuk menunjukkan kepatuhan terhadap peraturan.



Dasbor OSSIM SIEM. Dasbor yang dapat dikonfigurasi memberikan tampilan status tingkat tinggi dari metrik keamanan jaringan. (Tangkapan layar digunakan dengan izin dari AT-and-T Cybersecurity.)

Pengujian Penetrasi

Jika pengujian kerentanan menggunakan sebagian besar alat pemindaian otomatis dan sebagian besar merupakan aktivitas penilaian pasif atau non-intrusif, pengujian penetrasi bertujuan untuk memodelkan seberapa terbuka organisasi terhadap kerentanan yang dapat dieksploitasi oleh pelaku ancaman.

Uji penetrasi-sering disingkat menjadi uji pena-menggunakan teknik peretasan resmi untuk menemukan kelemahan yang dapat dieksploitasi dalam sistem keamanan target. Pengujian pena juga disebut sebagai peretasan etis.

Perbedaan utama dari pemindaian kerentanan pasif adalah bahwa upaya dilakukan untuk menguji kontrol keamanan secara aktif dan mengeksploitasi setiap kerentanan yang ditemukan. Pengujian pena adalah teknik penilaian yang mengganggu. Misalnya, pemindaian kerentanan dapat mengungkapkan bahwa SQL Server belum ditambal untuk melindungi dari eksploitasi yang diketahui. Tes penetrasi akan mencoba menggunakan eksploit untuk melakukan injeksi kode dan membahayakan server. Ini menyediakan pengujian aktif kontrol keamanan. Meskipun ada potensi eksploitasi, dalam praktiknya izin di server mungkin mencegah penyerang menggunakannya. Ini tidak akan diidentifikasi oleh pemindaian kerentanan tetapi harus dibuktikan atau tidak terbukti dengan pengujian penetrasi.

Manajemen Akses Istimewa

Akun dengan hak istimewa adalah akun yang dapat membuat perubahan konfigurasi yang signifikan pada sebuah host, seperti menginstal perangkat lunak atau menonaktifkan firewall atau sistem keamanan lainnya. Akun istimewa juga memiliki hak untuk masuk ke peralatan jaringan dan server aplikasi.

Manajemen akses istimewa (PAM) mengacu pada kebijakan, prosedur, dan kontrol teknis untuk mencegah penyalahgunaan akun istimewa oleh pelaku ancaman internal dan untuk mengurangi risiko dari kontrol konfigurasi yang lemah atas hak istimewa. Kontrol ini mengidentifikasi dan mendokumentasikan akun istimewa, memberikan visibilitas ke dalam penggunaannya, dan mengelola kredensial yang digunakan untuk mengaksesnya.

Beberapa prinsip umum PAM lainnya termasuk hak istimewa paling rendah, akses berbasis peran, dan kepercayaan nol:

- **Hak istimewa terkecil** berarti bahwa pengguna diberikan hak yang cukup untuk melakukan pekerjaannya dan tidak lebih. Ini mengurangi risiko jika akun harus disusupi dan berada di bawah kendali aktor ancaman. Authorization creep mengacu pada situasi di mana pengguna memperoleh lebih banyak hak, baik secara langsung atau dengan ditambahkan ke grup dan peran keamanan. Hak istimewa terkecil harus dipastikan dengan menganalisis alur kerja bisnis secara cermat untuk menilai hak istimewa apa yang diperlukan dan dengan melakukan audit akun reguler.
- **Akses berbasis peran** berarti bahwa seperangkat peran organisasi ditentukan, dan subjek dialokasikan untuk peran tersebut. Di bawah sistem ini, hak untuk mengubah peran disediakan untuk pemilik sistem. Oleh karena itu, sistem ini nondiscretionary, karena setiap akun subjek tidak memiliki hak untuk mengubah ACL sumber daya, meskipun mereka mungkin dapat mengubah sumber daya dengan cara lain. Pengguna dikatakan mendapatkan hak secara implisit (melalui ditugaskan ke suatu peran) daripada secara eksplisit (diberikan hak secara langsung).
- **Kepercayaan nol** didasarkan pada gagasan bahwa keamanan perimeter tidak mungkin sepenuhnya kuat. Pada jaringan modern, ada terlalu banyak peluang bagi lalu lintas untuk lolos dari pemantauan/pemfilteran oleh perangkat perimeter. Zero trust menggunakan sistem seperti otentikasi berkelanjutan dan akses bersyarat untuk mengurangi eskalasi hak istimewa dan kompromi akun oleh aktor ancaman. Teknik zero-trust lainnya adalah dengan menerapkan microsegmentation. Mikrosegmentasi adalah proses keamanan yang mampu menerapkan kebijakan ke satu node, seolah-olah berada di zonanya sendiri.

Penilaian Vendor

Pelanggaran profil tinggi telah menyebabkan apresiasi yang lebih besar akan pentingnya rantai pasokan dalam manajemen kerentanan. Sebuah produk, atau bahkan layanan, mungkin memiliki komponen yang dibuat dan dipelihara oleh rantai panjang perusahaan yang berbeda. Setiap perusahaan dalam rantai bergantung pada pemasok atau vendornya yang melakukan uji

tuntas pada vendor mereka. Tautan yang lemah dalam rantai dapat menyebabkan dampak pada ketersediaan dan kinerja layanan, atau dalam kasus terburuk menyebabkan pelanggaran data.

Manajemen vendor adalah proses untuk memilih perusahaan pemasok dan mengevaluasi risiko yang melekat dalam mengandalkan produk atau layanan pihak ketiga. Dalam hal data dan keamanan siber, Anda harus memahami bahwa risiko tidak dapat sepenuhnya dialihkan ke vendor. Jika vendor penyimpanan data mengalami pelanggaran data, Anda mungkin dapat menuntut biaya dari mereka, tetapi perusahaan Anda akan tetap bertanggung jawab dalam hal hukuman hukum dan kerusakan reputasi. Jika toko web Anda sering mengalami pemadaman karena kegagalan pada penyedia hosting, reputasi perusahaan Anda yang akan menderita dan perusahaan Anda yang akan kehilangan pesanan karena pelanggan mencari di tempat lain.

Vendor dapat menyediakan dokumentasi dan sertifikasi untuk membuktikan bahwa ia telah menerapkan kebijakan keamanan dengan kuat. Anda mungkin dapat melihat bukti kemampuan keamanan, seperti riwayat manajemen kerentanan yang efektif dan dukungan produk. Perusahaan yang lebih besar biasanya akan meminta vendor untuk menyelesaikan proses audit terperinci untuk memastikan bahwa mereka memenuhi standar yang dipersyaratkan.

JELASKAN METODE OTENTIKASI

Pendahuluan: Jelaskan Metode Otentikasi

Dalam topik ini, Anda akan mengidentifikasi metode otentikasi jaringan. Otentikasi yang kuat adalah garis pertahanan pertama untuk mengamankan sumber daya jaringan. Sebagai profesional jaringan, untuk mengelola autentikasi secara efektif di jaringan Anda, Anda perlu memahami sistem yang berbeda ini dan apa yang masing-masing dapat berikan untuk organisasi Anda.

Metode Otentikasi dan Kontrol Akses

Sistem kontrol akses adalah seperangkat kontrol keamanan teknis yang mengatur bagaimana subjek diizinkan untuk berinteraksi dengan objek. Subjek dalam pengertian ini adalah pengguna, perangkat, atau proses perangkat lunak, atau apa pun yang dapat meminta dan diberikan akses ke sumber daya. Objek adalah sumber daya; ini bisa berupa jaringan, server, database, file, dan sebagainya.

Dalam keamanan komputer, dasar dari kontrol akses biasanya adalah daftar kontrol akses (ACL). Ini adalah daftar subjek dan hak atau izin yang telah diberikan pada objek tersebut.

Sistem manajemen identitas dan akses (IAM) untuk menengahi penggunaan objek oleh subjek biasanya dijelaskan dalam empat proses utama:

- **Identifikasi** -Membuat akun atau ID yang mengidentifikasi pengguna, perangkat, atau proses di jaringan.
- **Otentikasi** -Membuktikan bahwa subjek adalah siapa atau apa yang diklaimnya ketika mencoba mengakses sumber daya.
- **Otorisasi** -Menentukan hak apa yang harus dimiliki subjek pada setiap sumber daya dan menegakkan hak-hak tersebut.
- **Akuntansi** -Melacak penggunaan sumber daya yang sah atau penggunaan hak oleh subjek dan memperingatkan ketika penggunaan yang tidak sah terdeteksi atau dicoba.

Otentikasi Multifaktor dan Dua Faktor

Akun mendefinisikan subjek pada komputer atau sistem jaringan. Dengan asumsi bahwa akun telah dibuat dengan aman (identitas pemegang akun telah diverifikasi), otentikasi memverifikasi bahwa hanya pemegang akun yang dapat menggunakan akun, dan bahwa sistem hanya dapat digunakan oleh pemegang akun. Otentikasi dilakukan ketika pemegang akun mengirimkan kredensial ke sistem untuk meminta akses. Ini dibandingkan dengan kredensial yang disimpan di sistem. Jika cocok, akun tersebut diautentikasi.

Jenis data yang digunakan untuk membuat kredensial disebut faktor otentikasi. Faktor otentikasi termasuk dalam kategori berikut:

- **Faktor pengetahuan** -sesuatu yang Anda ketahui (seperti kata sandi).
- **Faktor kepemilikan** -sesuatu yang Anda miliki (seperti kartu pintar).
- **Faktor manusia atau biometrik** -sesuatu tentang Anda (seperti sidik jari).
- **Faktor perilaku** -sesuatu yang Anda lakukan (seperti membuat tanda tangan).
- **Faktor lokasi** -di suatu tempat Anda berada (seperti menggunakan perangkat seluler dengan layanan lokasi).

Suatu teknologi atau mekanisme otentikasi dianggap kuat jika menggabungkan penggunaan lebih dari satu tipe data otentikasi (multifaktor). Sistem otentikasi satu faktor dapat dengan mudah dikompromikan: kata sandi dapat ditulis atau dibagikan, atau disusupi oleh serangan rekayasa sosial, kartu pintar dapat hilang atau dicuri, dan sistem biometrik dapat mengalami tingkat kesalahan yang tinggi.

Otentikasi dua faktor menggabungkan sesuatu seperti kartu pintar atau mekanisme biometrik dengan faktor pengetahuan, seperti kata sandi atau nomor identitas pribadi (PIN). Otentikasi tiga faktor menggabungkan tiga kemungkinan teknologi. Contohnya adalah kartu pintar dengan pembaca sidik jari terintegrasi. Artinya, untuk otentikasi, pengguna harus memiliki kartu, sidik jari pengguna harus sesuai dengan template yang tersimpan di kartu, dan pengguna harus memasukkan PIN.

Tips: Otentikasi multifaktor memerlukan kombinasi teknologi yang berbeda. Misalnya, meminta PIN bersama dengan tanggal lahir mungkin lebih kuat daripada memasukkan PIN saja, tetapi ini bukan multifaktor.

Otentikasi Lokal dan Sistem Masuk Tunggal

Salah satu fitur terpenting dari sistem operasi adalah penyedia otentikasi. Penyedia otentikasi lokal adalah arsitektur perangkat lunak dan kode yang mendukung mekanisme di mana pengguna diautentikasi sebelum memulai shell. Ini biasanya digambarkan sebagai masuk (Linux) atau masuk atau masuk (Microsoft). Otentikasi berbasis pengetahuan, menggunakan kata sandi atau PIN, adalah penyedia otentikasi default untuk sebagian besar sistem operasi.

Otentikasi berbasis pengetahuan bergantung pada hash kriptografi. Hash kriptografi adalah fungsi yang mengubah string apa pun menjadi kode unik dengan panjang tetap. Fungsi harus memastikan bahwa kode tidak dapat diubah kembali menjadi string teks biasa.

```
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Type........: NetNTLMv2
Hash.Target......: ADMINISTRATOR::515support:2f8cbd19fd1bfac9:881c5503...000000
Time.Started.....: Mon Jan  6 11:25:16 2020 (1 min, 38 secs)
Time.Estimated...: Sat Jan 11 07:49:57 2020 (4 days, 20 hours)
Guess.Mask.......: ?1?1?1?1?1?1?1?1 [8]
Guess.Charset....: -1 pPaAsSwWoOrRdD0123456789$, -2 Undefined, -3 Undefined, -4
Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   364.1 kH/s (11.09ms) @ Accel:128 Loops:32 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 34233472/152587890625 (0.02%)
Rejected.........: 0/34233472 (0.00%)
Restore.Point....: 2176/9765625 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:1824-1856 Iteration:0-32
Candidates.#1....: $87r8678 -> dSDoRS12
```

Kredensial kata sandi disimpan sebagai hash kriptografis (seperti nilai Hash.Target yang ditampilkan di tangkapan layar) yang biasanya tidak dapat dikonversi kembali ke string teks biasa. Utilitas hashcat mencoba memulihkan kata sandi dengan mencocokkan hash melalui kamus atau metode brute force.

Kata sandi biasanya tidak dikirimkan atau disimpan dalam basis data kredensial sebagai teks biasa karena risiko kompromi. Sebaliknya, kata sandi disimpan sebagai hash kriptografis. Ketika pengguna memasukkan kata sandi untuk masuk, autentikator mengubah apa yang diketik menjadi hash dan mengirimkannya ke otoritas. Otoritas membandingkan hash yang dikirimkan dengan yang ada di database dan mengotentikasi subjek hanya jika cocok.

Otentikasi Windows Otentikasi

Windows melibatkan arsitektur komponen yang kompleks (docs.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication), tetapi tiga skenario berikut adalah tipikal:

- **Masuk lokal Windows** - Otoritas Keamanan Lokal (LSA) membandingkan kredensial yang dikirimkan dengan hash yang disimpan di database Manajer Akun Keamanan (SAM), yang merupakan bagian dari registri. Ini juga disebut sebagai logon interaktif.
- **Masuk jaringan Windows** - LSA dapat meneruskan kredensial untuk otentikasi ke layanan jaringan. Sistem yang disukai untuk otentikasi jaringan didasarkan pada Kerberos, tetapi aplikasi jaringan lama mungkin menggunakan otentikasi NT LAN Manager (NTLM).
- **Masuk jarak jauh** -jika perangkat pengguna tidak terhubung ke jaringan lokal, otentikasi dapat dilakukan melalui beberapa jenis jaringan pribadi virtual (VPN) atau portal web.

Otentikasi Linux

Di Linux, nama akun pengguna lokal disimpan di /etc/passwd. Saat pengguna masuk ke shell interaktif lokal, kata sandi diperiksa terhadap hash yang disimpan di /etc/shadow. Login interaktif melalui jaringan biasanya dilakukan dengan menggunakan Secure Shell (SSH). Dengan SSH, pengguna dapat diautentikasi menggunakan kunci kriptografis alih-alih kata sandi.

Modul otentikasi pluggable (PAM) adalah paket untuk mengaktifkan penyedia otentikasi yang berbeda, seperti login kartu pintar (tecmint.com/configure-pam-in-centos-ubuntu-linux). Kerangka kerja PAM juga dapat digunakan untuk mengimplementasikan otentikasi ke server jaringan.

Sistem Masuk Tunggal

Sistem masuk tunggal (SSO) memungkinkan pengguna untuk mengautentikasi sekali ke perangkat lokal dan diberi otorisasi untuk mengakses server aplikasi yang kompatibel tanpa harus memasukkan kredensial lagi. Di Windows, SSO disediakan oleh kerangka kerja Kerberos.

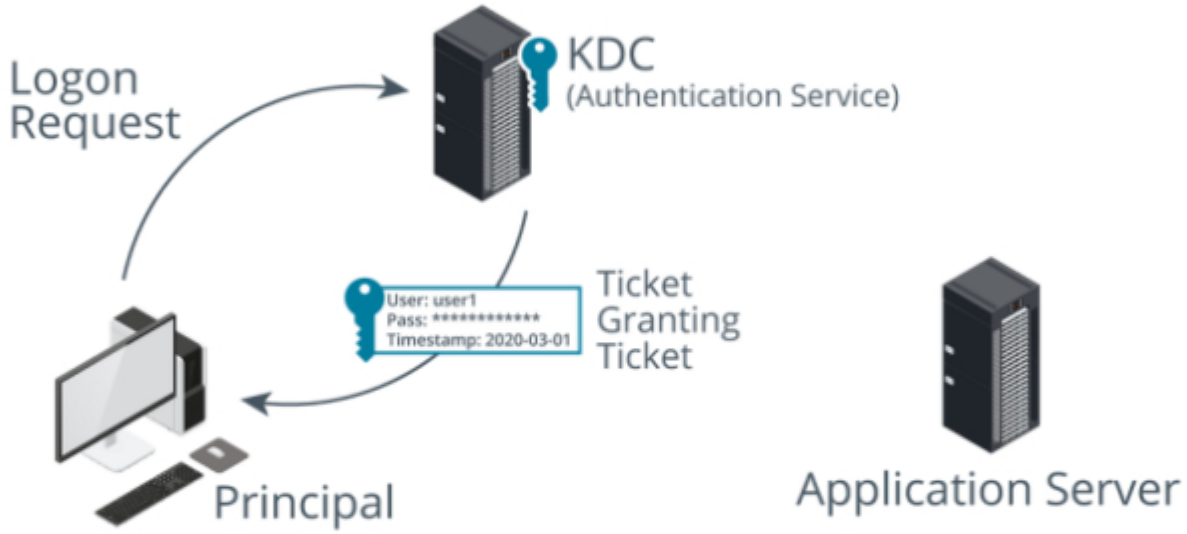
Kerberos

Kerberos menyediakan autentikasi SSO ke Active Directory®, serta kompatibilitas dengan sistem operasi non-Windows lainnya. Kerberos dinamai anjing penjaga berkepala tiga dari Hades (Cerberus) karena terdiri dari tiga bagian. Klien meminta

layanan dari server, yang keduanya mengandalkan perantara - Pusat Distribusi Kunci (KDC) - untuk menjamin identitas mereka.

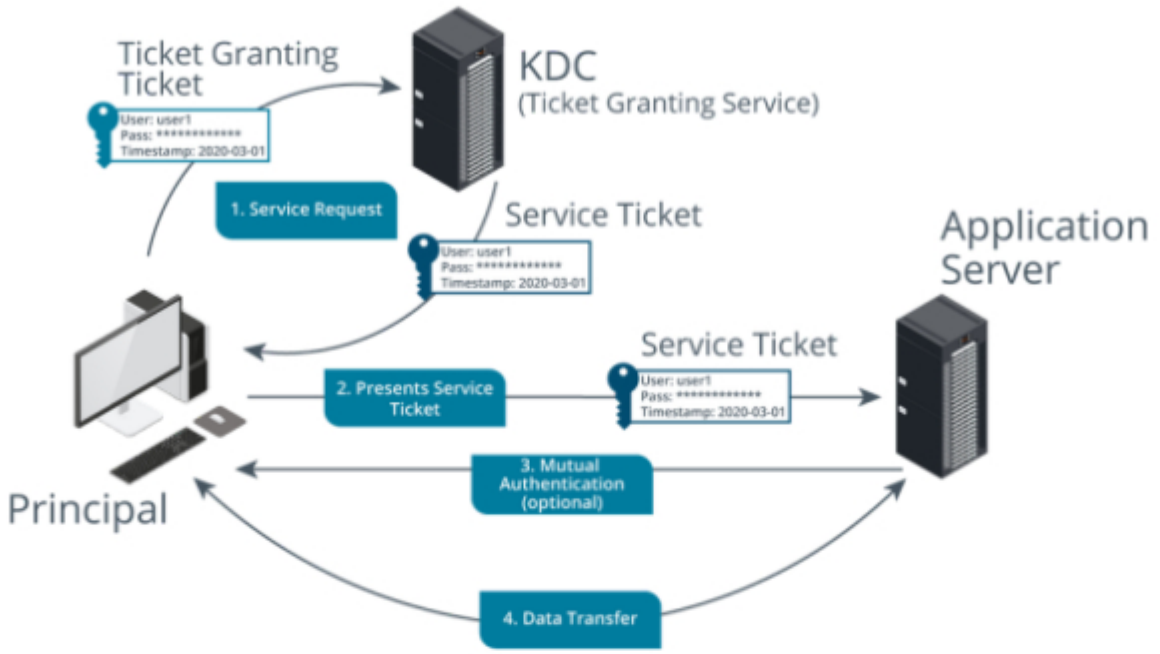
Ada dua layanan yang membentuk KDC: Layanan Otentikasi dan Layanan Pemberian Tiket.

Layanan Otentikasi bertanggung jawab untuk mengautentikasi permintaan masuk pengguna. Secara lebih umum, pengguna dan layanan dapat diautentikasi; ini secara kolektif disebut sebagai prinsipal. Misalnya, ketika Anda duduk di workstation domain Windows dan masuk ke domain (dokumentasi Kerberos merujuk ke ranah daripada domain, yang merupakan terminologi Microsoft), langkah pertama masuk adalah mengautentikasi dengan server KDC (diimplementasikan sebagai domain pengontrol).



Layanan Otentikasi Kerberos. (Gambar © 123RF.com.)

Saat diautentikasi, server KDC memberikan Tiket Pemberian Tiket kepada pengguna. Untuk mengakses sumber daya dalam domain, klien meminta Tiket Layanan (token yang memberikan akses ke server aplikasi target) dengan menyediakan Tiket Pemberian Tiket ke Layanan Pemberian Tiket (TGS).



Layanan Pemberian Tiket Kerberos. (Gambar © 123RF.com.)

Sertifikat Digital dan PKI

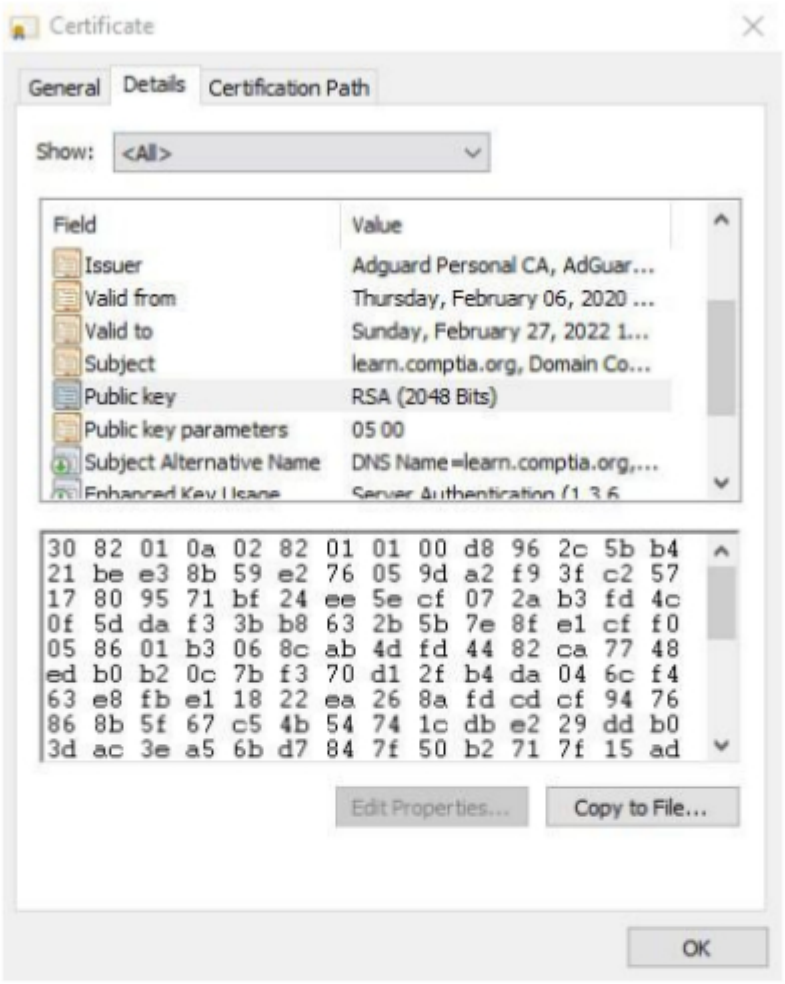
Protokol seperti Kerberos juga dapat digunakan dengan kartu pintar. Kartu pintar diprogram dengan pasangan kunci enkripsi dan sertifikat digital, yang dikeluarkan oleh domain otentikasi. Sertifikat digital juga digunakan untuk mengautentikasi mesin server saat menggunakan Transport Layer Security (TLS). Sertifikat dapat diinstal pada server web atau server email untuk memvalidasi identitasnya dan membuat saluran transmisi yang aman.

Sertifikat digital bergantung pada konsep kriptografi kunci publik. Kriptografi kunci publik, juga disebut sebagai enkripsi asimetris, memecahkan masalah pendistribusian kunci enkripsi saat Anda ingin berkomunikasi secara aman dengan orang lain, mengotentikasi pesan yang Anda kirim ke orang lain, atau mengotentikasi diri Anda sendiri ke sistem kontrol akses. Dengan enkripsi asimetris, Anda menghasilkan pasangan kunci. Kunci pribadi dalam pasangan tetap menjadi rahasia yang hanya Anda yang tahu. Kunci publik dapat ditransmisikan ke subjek lain. Kunci pribadi tidak dapat diturunkan dari kunci publik. Pasangan kunci dapat digunakan dengan cara berikut:

- Saat Anda ingin orang lain mengirimi Anda pesan rahasia, Anda memberi mereka kunci publik untuk digunakan mengenkripsi pesan. Pesan tersebut kemudian hanya dapat didekripsi oleh kunci pribadi Anda, yang hanya Anda ketahui sendiri. Karena cara kerja enkripsi asimetris, kunci publik tidak dapat digunakan untuk mendekripsi pesan, meskipun itu digunakan untuk mengenkripsinya sejak awal.

Tips: Karena enkripsi menggunakan kunci publik relatif lambat; daripada mengenkripsi seluruh pesan menggunakan kunci publik, lebih umum lagi, kunci publik digunakan untuk mengenkripsi kunci enkripsi simetris untuk digunakan dalam satu sesi dan menukarnya dengan aman. Kunci sesi simetris kemudian digunakan untuk mengenkripsi pesan yang sebenarnya. Kunci simetris dapat melakukan enkripsi dan dekripsi.

- Saat Anda ingin mengautentikasi diri Anda kepada orang lain, Anda membuat tanda tangan dan menandatanganinya dengan mengenkripsi tanda tangan dengan kunci pribadi Anda. Anda memberi orang lain kunci publik Anda untuk digunakan untuk mendekripsi tanda tangan. Karena hanya Anda yang mengetahui kunci pribadi, setiap orang dapat diyakinkan bahwa hanya Anda yang dapat membuat tanda tangan. Masalah dasar kriptografi kunci publik terletak pada pembuktian identitas pemilik kunci publik. Sistem ini rentan terhadap serangan on-path di mana aktor ancaman mengganti kunci publik Anda dengan kunci mereka sendiri. Infrastruktur kunci publik (PKI) bertujuan untuk membuktikan bahwa pemilik kunci publik adalah seperti yang mereka katakan. Di bawah PKI, siapa pun yang mengeluarkan kunci publik harus mendapatkan sertifikat digital. Validitas sertifikat dijamin oleh otoritas sertifikat (CA). Sertifikat digital pada dasarnya adalah pembungkus untuk suatu subjek. kunci publik s (atau entitas akhir). Selain kunci publik, ini berisi informasi tentang subjek dan penerbit atau penjamin sertifikat. Sertifikat ditandatangani secara digital untuk membuktikan bahwa sertifikat tersebut dikeluarkan untuk subjek oleh CA tertentu.



Detail sertifikat digital. (Tangkapan layar digunakan dengan izin dari Microsoft.)

Protokol Otentikasi yang Dapat Diperluas dan IEEE 802.1X

Otentikasi kartu pintar digunakan untuk otentikasi Kerberos di mana komputer terhubung ke jaringan lokal dan pengguna masuk ke Windows. Jenis otentikasi multifaktor ini mungkin juga diperlukan dalam konteks lain:

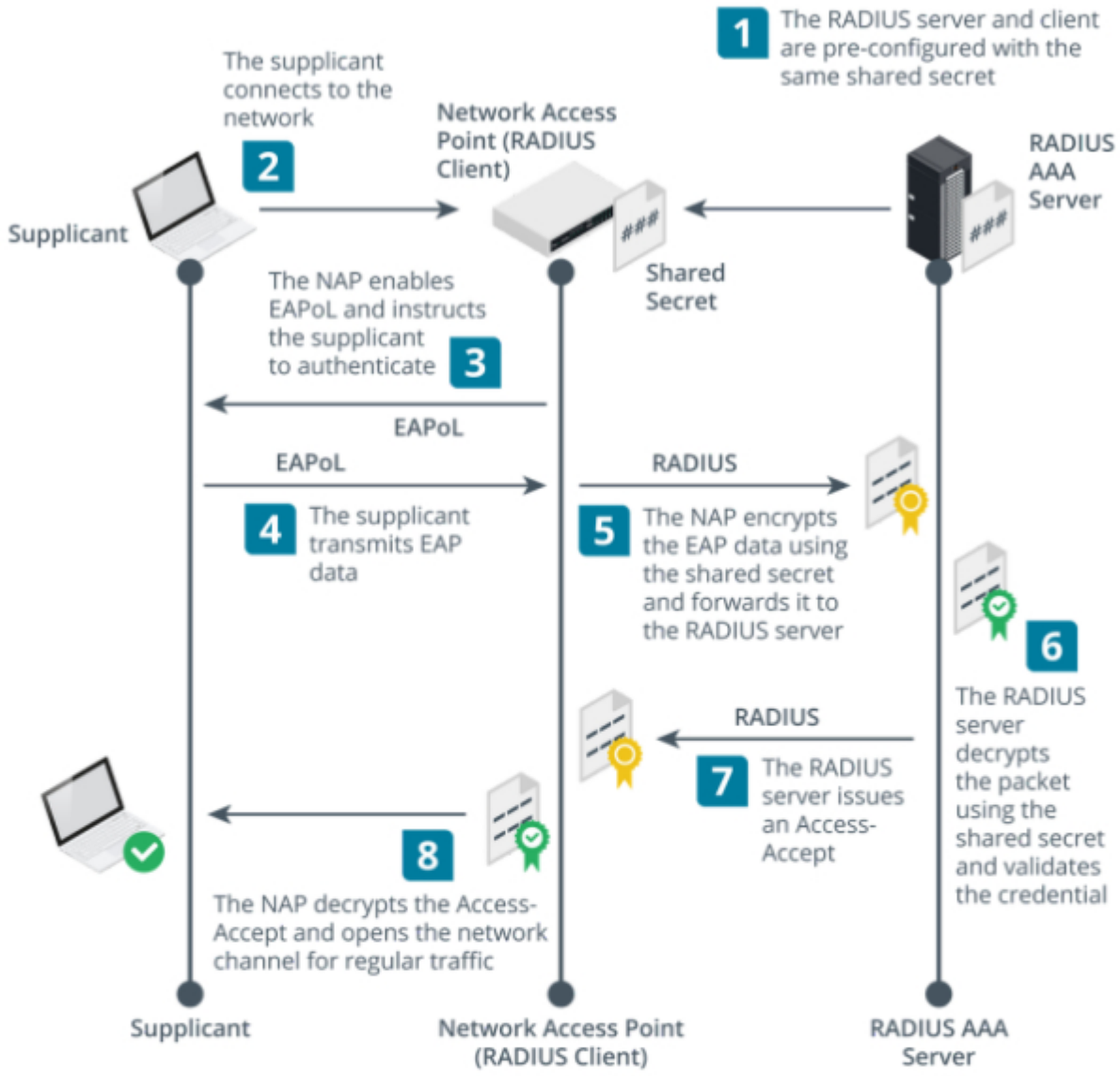
- Saat pengguna mengakses jaringan nirkabel dan perlu mengautentikasi dengan database jaringan.
- Saat perangkat terhubung ke jaringan melalui sakelar dan kebijakan jaringan mengharuskan pengguna untuk diautentikasi sebelum perangkat diizinkan untuk berkomunikasi.
- Ketika pengguna terhubung ke jaringan melalui jaringan publik melalui jaringan pribadi virtual (VPN).

Dalam skenario ini, Extensible Authentication Protocol (EAP) menyediakan kerangka kerja untuk menyebarkan beberapa jenis protokol dan teknologi otentikasi. EAP memungkinkan banyak metode otentikasi yang berbeda, tetapi banyak dari mereka menggunakan sertifikat digital di server dan/atau mesin klien. Sertifikat ini memungkinkan mesin untuk membangun hubungan kepercayaan dan membuat terowongan aman untuk mengirimkan kredensial pengguna atau untuk melakukan otentikasi kartu pintar tanpa kata sandi pengguna.

Di mana EAP mengimplementasikan faktor dan mekanisme otentikasi tertentu, protokol IEEE 802.1X Port-based Network Access Control (NAC) menyediakan sarana untuk menggunakan metode EAP ketika perangkat terhubung ke port switch Ethernet, titik akses nirkabel, atau gateway VPN. 802.1X menggunakan arsitektur otentikasi, otorisasi, dan akuntansi (AAA). AAA menggunakan komponen berikut:

- **Supplicant** -perangkat yang meminta akses, seperti PC atau laptop pengguna.
- **Server akses jaringan (NAS) atau titik akses jaringan (NAP)** -peralatan jaringan tepi, seperti sakelar, titik akses, dan gateway VPN. Ini juga disebut sebagai klien AAA atau autentikator.
- **Server AAA** -server otentikasi, diposisikan dalam jaringan lokal. Ada dua jenis utama server AAA: RADIUS dan TACACS+.

Dengan AAA, perangkat NAS tidak perlu menyimpan kredensial autentikasi apa pun. Mereka meneruskan data ini antara server AAA dan pemohon.

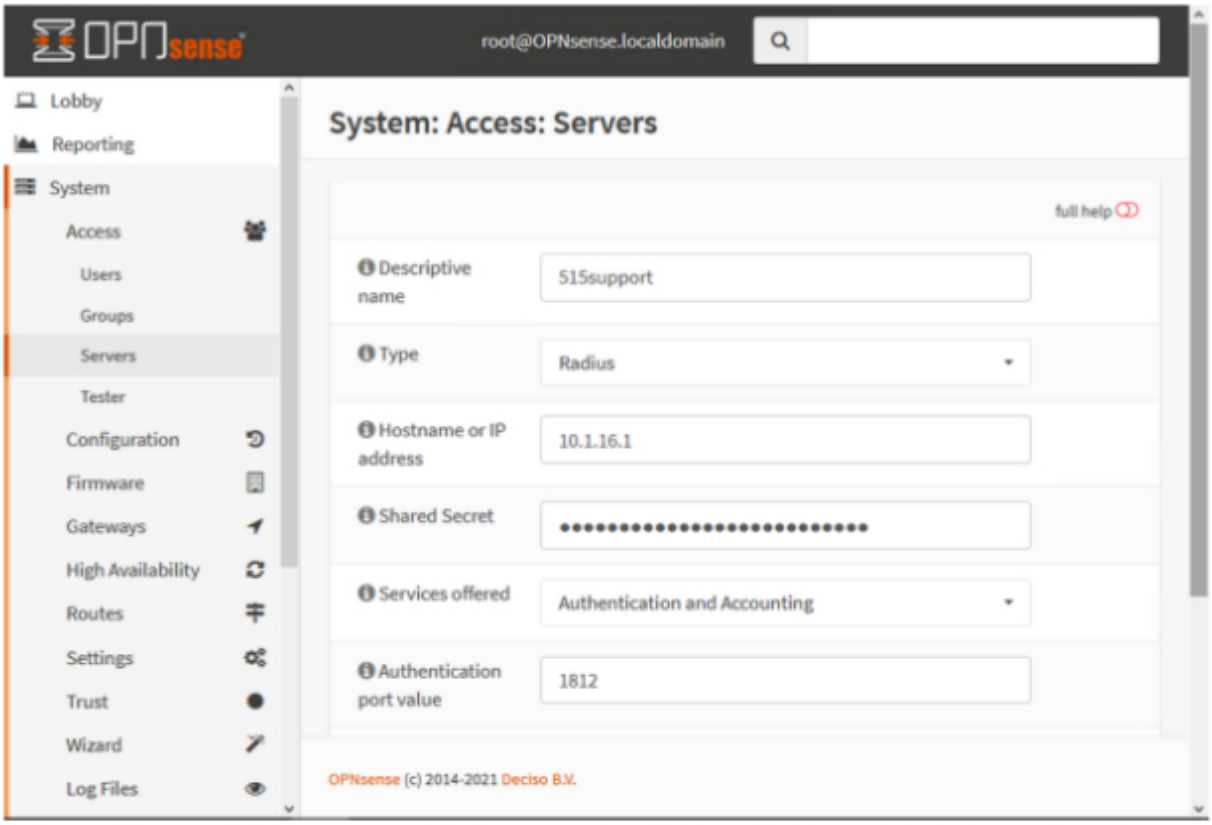


Otentikasi RADIUS dengan gambaran umum EAP. (Gambar © 123RF.com.)

RADIUS dan TACACS+

Remote Authentication Dial-in User Service (RADIUS) sangat banyak digunakan untuk akses perangkat klien melalui switch, jaringan nirkabel, dan VPN. Ada beberapa produk server dan klien RADIUS. Microsoft memiliki Network Policy Server (NPS) untuk platform Windows, dan ada implementasi open-source untuk UNIX dan Linux, seperti FreeRADIUS, serta produk komersial pihak ketiga, seperti Cisco's Secure Access Control Server, OSC Radiator, dan Juniper Networks Steel-Belted RADIUS.

RADIUS biasanya menggunakan port UDP 1812 dan 1813. Setiap klien RADIUS harus dikonfigurasi dengan alamat IP server RADIUS ditambah rahasia bersama yang sama.



Mengonfigurasi alat keamanan OPNsense sebagai klien RADIUS. Alat OPNsense berfungsi sebagai server akses jaringan pribadi virtual (VPN). Ini menggunakan server RADIUS di 10.1.16.1 untuk mengotentikasi pengguna VPN. Klien harus dikonfigurasi dengan rahasia bersama yang sama dengan server. (Tangkapan layar digunakan dengan izin dari OPNsense.)

Terminal Access Controller Access Control System (TACACS+) adalah protokol yang mirip dengan RADIUS tetapi dirancang agar lebih fleksibel dan andal. TACACS+ dikembangkan oleh Cisco tetapi juga didukung pada banyak implementasi server RADIUS pihak ketiga dan open-source lainnya. Dimana RADIUS sering digunakan untuk kontrol akses jaringan atas perangkat pengguna akhir, TACACS+ sering digunakan dalam mengautentikasi akses administratif ke router dan switch. Ini menggunakan TCP melalui port 49 dan pengiriman andal yang ditawarkan oleh TCP membuatnya lebih mudah untuk dideteksi saat server sedang down.

Juga, fungsi otentikasi, otorisasi, dan akuntansi bersifat diskrit. Banyak tugas pengelolaan perangkat memerlukan autentikasi ulang (mirip dengan keharusan memasukkan kembali kata sandi untuk sudo atau UAC) dan otorisasi dan hak istimewa per perintah untuk pengguna, grup, dan peran. TACACS+ mendukung alur kerja ini lebih baik daripada RADIUS.

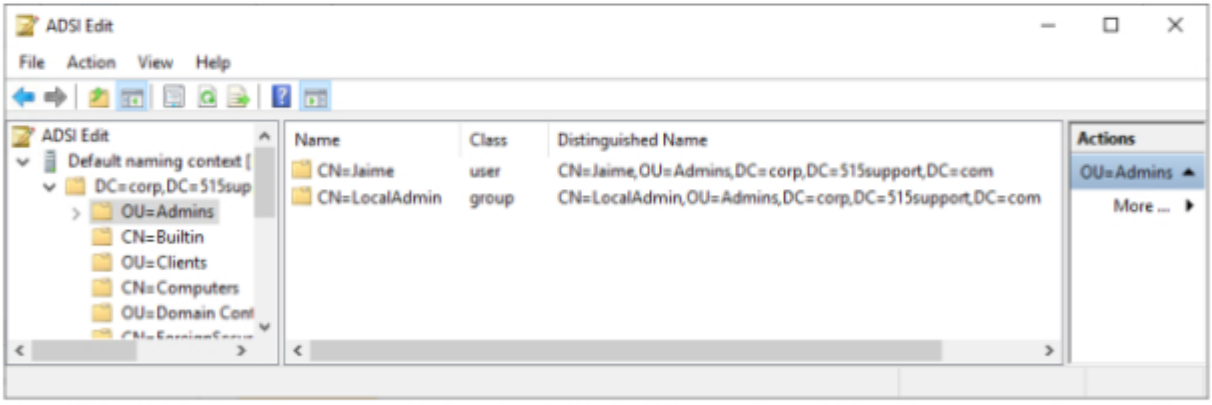
Protokol Akses Direktori Ringan

Layanan direktori adalah sarana utama untuk menyediakan manajemen hak istimewa dan otorisasi pada jaringan perusahaan.

Ketika pengguna yang diautentikasi masuk ke jaringan, layanan keamanan server menghasilkan kunci akses untuk pengguna. Ini berisi nama pengguna dan keanggotaan grup dari pengguna yang diautentikasi. Setiap kali pengguna mencoba mengakses sumber daya, kunci aksesnya diberikan sebagai identifikasi. Layanan keamanan server mencocokkan nama pengguna dan keanggotaan grup dari kunci akses dengan entri dalam daftar akses, dan dari sini, ia menghitung hak akses pengguna.

Semua informasi ini disimpan dalam direktori. Direktori seperti database, di mana objek seperti catatan, dan hal-hal yang Anda ketahui tentang objek (atribut) seperti bidang. Agar produk dari vendor yang berbeda dapat dioperasikan, sebagian besar direktori didasarkan pada standar yang sama. Standar direktori utama adalah seri standar X.500. Karena X.500 kompleks, sebagian besar layanan direktori adalah implementasi dari Lightweight Directory Access Protocol (LDAP). LDAP bukan standar direktori, tetapi protokol yang digunakan untuk melakukan kueri dan memperbarui direktori mirip X.500. LDAP didukung secara luas dalam produk direktori saat ini (Windows Active Directory®, NetIQ eDirectory, atau open source OpenLDAP). Pesan LDAP menggunakan port TCP dan UDP 389 secara default.

Dalam X.500, setiap objek memiliki pengidentifikasi unik yang disebut nama yang dibedakan. Nama yang dibedakan terdiri dari pasangan atribut=nilai, dipisahkan dengan koma. Atribut yang paling spesifik dicantumkan terlebih dahulu, dan atribut yang berurutan menjadi semakin luas. Atribut paling spesifik ini juga disebut sebagai nama pembeda relatif, karena atribut tersebut secara unik mengidentifikasi objek dalam konteks nilai atribut (induk) yang berurutan.



Menjelajahi objek dalam skema LDAP Direktori Aktif. (Tangkapan layar digunakan dengan izin dari Microsoft.)

Jenis atribut, informasi apa yang dikandungnya, dan cara tipe objek didefinisikan melalui atribut (beberapa di antaranya mungkin diperlukan dan beberapa opsional) dijelaskan oleh skema

direktori. Misalnya, nama khusus server web yang dioperasikan oleh Widget di London mungkin adalah:

CN=WIDGETWEB, OU=Pemasaran, O=Widget, L=London, ST=London, C=UK, DC=widget, DC=contoh

LDAP Aman

Seperti banyak protokol TCP/IP, LDAP tidak memberikan keamanan, dan semua transmisi dalam teks biasa, sehingga rentan terhadap serangan sniffing dan spoofing. Selain itu, server yang tidak mengharuskan klien untuk mengautentikasi rentan terhadap kelebihan beban oleh serangan penolakan layanan. Otentikasi, yang disebut sebagai pengikatan ke server, dapat diimplementasikan dengan cara berikut:

- **Tidak ada otentikasi** -Akses anonim diberikan ke direktori.
- **Ikatan sederhana** - klien harus memberikan nama khusus (DN) dan kata sandinya, tetapi ini diteruskan sebagai teks biasa.
- **Simple Authentication and Security Layer (SASL)** -klien dan server menegosiasikan penggunaan mekanisme otentikasi yang didukung, seperti Kerberos. Perintah STARTTLS dapat digunakan untuk meminta enkripsi (penyegelan) dan integritas pesan (penandatanganan). Ini adalah mekanisme yang lebih disukai untuk implementasi LDAP Microsoft Active Directory (AD).
- **LDAP Secure (LDAPS)** -server diinstal dengan sertifikat digital, yang digunakan untuk menyiapkan terowongan aman untuk pertukaran kredensial pengguna. LDAPS menggunakan port 636.

Jika akses aman diperlukan, metode akses otentikasi anonim dan sederhana harus dinonaktifkan di server.

Umumnya, dua tingkat akses perlu diberikan pada direktori: akses baca-saja (kueri) dan akses baca/tulis (pembaruan). Ini diimplementasikan menggunakan kebijakan kontrol akses, tetapi mekanisme yang tepat adalah khusus vendor dan tidak ditentukan oleh dokumentasi standar LDAP.

Kecuali jika hosting layanan publik, server direktori LDAP juga hanya dapat diakses dari jaringan pribadi. Ini berarti bahwa port LDAP (389 melalui TCP dan UDP) harus diblokir oleh firewall dari akses melalui antarmuka publik.

Modul 14

Supporting and Troubleshouting Secure Networks

Compare and Contrast Security Appliances

- Pendahuluan: Bandingkan dan Kontraskan Peralatan Keamanan
  Peralatan keamanan seperti firewall, server proxy, dan sistem deteksi/pencegahan intrusi menerapkan kontrol akses untuk memastikan penggunaan jaringan yang sah. Mereka melakukan fungsi penyaringan untuk menganalisis properti permintaan koneksi dan kemudian mengizinkan, menolak, dan/atau mencatatnya sebagaimana mestinya. Meskipun Anda mungkin tidak menginstal dan mengkonfigurasi perangkat ini pada tahap ini dalam karier Anda, penting bagi Anda untuk memahami penggunaannya di jaringan.

- Penegakan Segmentasi Jaringan
  Penempatan peralatan keamanan yang efektif tergantung pada segmentasi jaringan ke dalam area yang ditentukan dengan jelas. Pada lapisan dua dan tiga, penegakan segmentasi jaringan diterapkan menggunakan kombinasi LAN virtual dan subnet. Setiap segmen adalah domain siaran yang terpisah. Setiap lalu lintas antar segmen harus dirutekan. Dalam istilah keamanan, unit utama dari jaringan yang tersegmentasi secara logis adalah zona. Zona adalah area jaringan di mana konfigurasi keamanannya sama untuk semua host di dalamnya. Lalu lintas jaringan antar zona harus dikontrol secara ketat menggunakan perangkat keamanan-biasanya firewall.

  Zona ini biasanya akan dikonfigurasi untuk melindungi integritas dan kerahasiaan kelompok aset yang berbeda dalam organisasi. Misalnya, server yang menyimpan catatan keuangan dapat berupa VLAN mereka sendiri, dan server pemasaran dapat berupa VLAN lain. Jika sesuatu seperti Trojan akses jarak jauh diperkenalkan di satu VLAN, itu seharusnya tidak dapat menyebar ke VLAN lain tanpa juga dapat melewati firewall yang melindungi setiap zona.

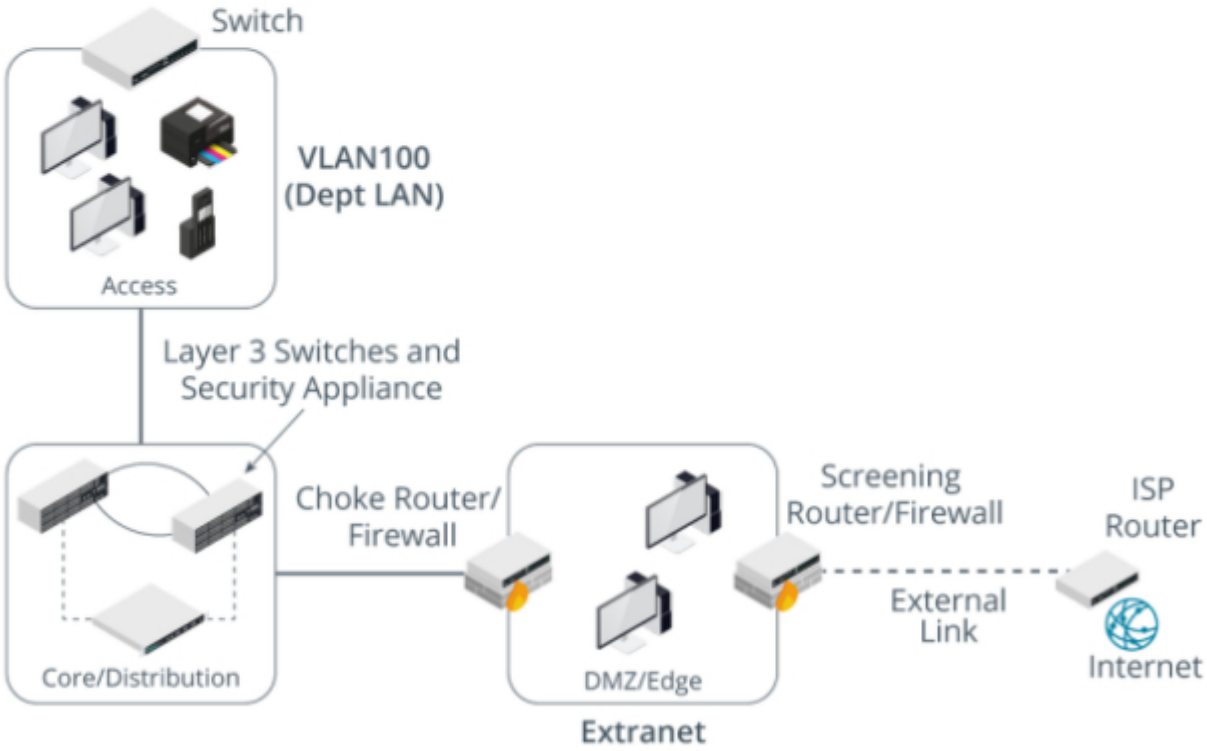
  Satu perbedaan penting antara zona keamanan yang berbeda adalah apakah host menghadap ke Internet. Host yang menghadap ke Internet menerima koneksi masuk dari Internet. Host yang menghadap internet ditempatkan di zona jaringan perimeter. Prinsip dasar dari zona jaringan perimeter adalah bahwa lalu lintas tidak dapat melewatinya secara langsung. Jaringan perimeter memungkinkan klien eksternal untuk mengakses data pada sistem pribadi, seperti server web, tanpa mengorbankan keamanan jaringan internal.

  Jika komunikasi diperlukan antara host di kedua sisi jaringan perimeter, host di dalamnya dapat dikonfigurasi untuk bertindak sebagai proxy. Misalnya, jika sebuah host di jaringan lokal meminta koneksi dengan server web di Internet, proxy di perimeter jaringan menerima permintaan tersebut dan memeriksanya. Jika permintaan itu valid, itu

mentransmisikannya kembali ke tujuan. Host eksternal tidak tahu tentang apa (jika ada) di belakang perimeter.

Server yang menyediakan layanan akses publik harus ditempatkan dalam jaringan perimeter. Ini biasanya akan mencakup server web, email dan server komunikasi lainnya, server proxy, dan server akses jarak jauh. Host di perimeter tidak sepenuhnya dipercaya oleh jaringan internal karena kemungkinan mereka dapat disusupi dari Internet. Mereka disebut sebagai bastion host.

- Subnet yang Disaring
  Untuk mengkonfigurasi jaringan perimeter, dua konfigurasi keamanan yang berbeda harus diaktifkan: satu di antarmuka eksternal dan satu di antarmuka internal.
  Subnet yang disaring menggunakan dua firewall yang ditempatkan di kedua sisi zona jaringan perimeter. Edge firewall membatasi lalu lintas pada antarmuka eksternal/publik dan mengizinkan lalu lintas yang diizinkan ke host di subnet zona perimeter. Firewall tepi dapat disebut sebagai firewall penyaringan atau router. Firewall internal menyaring komunikasi antara host di perimeter dan host di LAN. Firewall ini sering digambarkan sebagai choke firewall. Titik tersedak adalah gerbang yang sengaja dibuat sempit yang memfasilitasi kontrol akses yang lebih baik dan pemantauan yang lebih mudah.



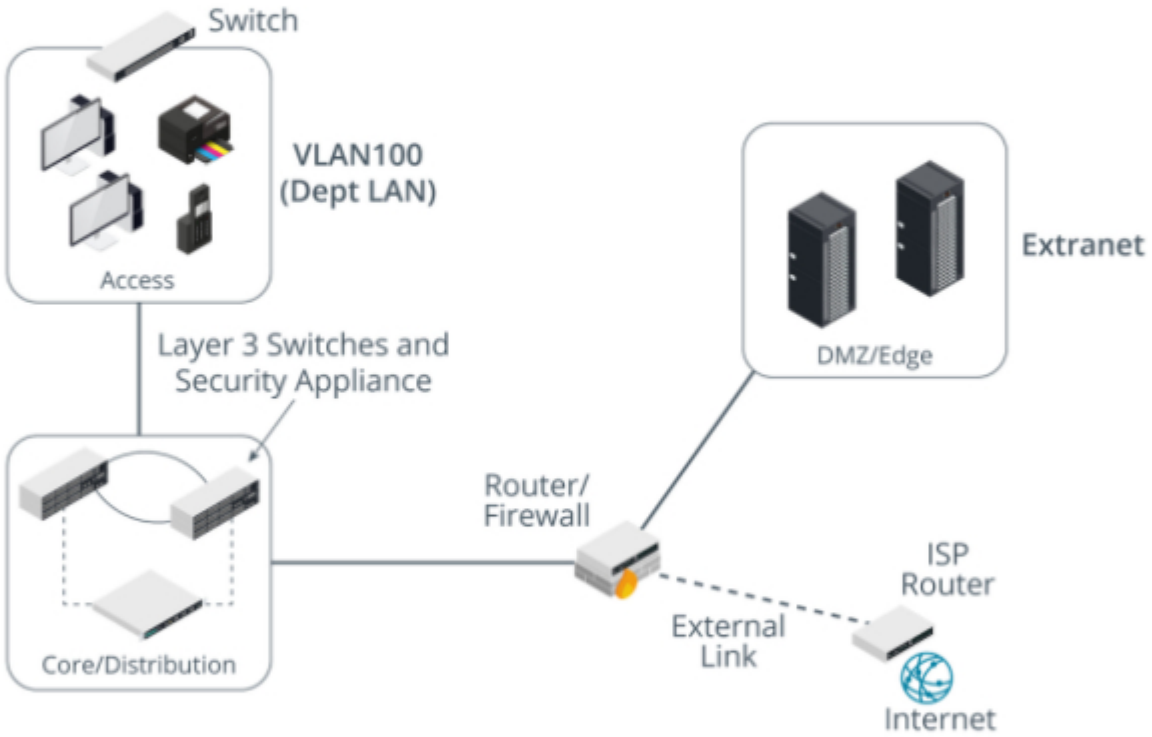
Subnet yang disaring. (Images © 123RF.com.)

Jaringan perimeter juga dapat dibuat menggunakan satu alat router/firewall dengan tiga antarmuka jaringan, yang disebut sebagai triple homed. Satu antarmuka adalah antarmuka publik, yang lain adalah subnet perimeter, dan yang ketiga terhubung ke

LAN. Aturan perutean dan pemfilteran menentukan penerusan apa yang diizinkan di antara antarmuka ini. Ini dapat mencapai konfigurasi yang sama seperti subnet yang disaring.

Tips: Topologi subnet yang disaring sebelumnya disebut sebagai *demilitarized zone* (DMZ). Terminologi DMZ sekarang tidak digunakan lagi.

Jaringan perimeter juga dapat dibuat menggunakan satu alat router/firewall dengan tiga antarmuka jaringan, yang disebut sebagai triple homed. Satu antarmuka adalah antarmuka publik, yang lain adalah subnet perimeter, dan yang ketiga terhubung ke LAN. Aturan perutean dan pemfilteran menentukan penerusan apa yang diizinkan di antara antarmuka ini. Ini dapat mencapai konfigurasi yang sama seperti subnet yang disaring.



Firewall dengan tiga rumah. (Images © 123RF.com.)

- Subnet yang Disaring
  Fungsi dasar dari firewall adalah penyaringan lalu lintas. Firewall memproses lalu lintas menurut aturan; lalu lintas yang tidak sesuai dengan aturan yang memungkinkan aksesnya diblokir.

  Ada banyak jenis firewall dan banyak cara untuk mengimplementasikan firewall. Satu perbedaan dapat dibuat antara firewall yang melindungi seluruh jaringan (yang ditempatkan inline dalam jaringan dan memeriksa semua lalu lintas yang melewatinya) dan firewall yang melindungi satu host saja (yang diinstal pada host dan hanya

memeriksa lalu lintas itu). ditujukan kepada tuan rumah itu). Perbedaan lebih lanjut dapat dibuat tentang bagian paket mana yang dapat diperiksa dan dioperasikan oleh teknologi firewall tertentu.

- Firewall Penyaringan Paket
  Pemfilteran paket menggambarkan jenis firewall paling awal. Semua firewall masih dapat menjalankan fungsi dasar ini. Firewall pemfilteran paket dikonfigurasi dengan menetapkan aturan dalam access control list(ACL). Setiap aturan mendefinisikan jenis paket data tertentu dan tindakan yang tepat untuk diambil ketika sebuah paket cocok dengan aturan. Suatu tindakan dapat berupa menolak (memblokir atau menjatuhkan paket, dan secara opsional mencatat suatu peristiwa) atau menerima (membiarkan paket melewati firewall). Firewall pemfilteran paket bekerja di Layer 3 model OSI untuk memeriksa header paket IP. Ini berarti bahwa aturan dapat didasarkan pada informasi yang ditemukan di header tersebut:

    - Penyaringan IP-Menerima atau menolak lalu lintas berdasarkan sumber dan/atau alamat IP tujuan.

    - ID/jenis protokol (TCP, UDP, ICMP, protokol perutean, dan sebagainya).

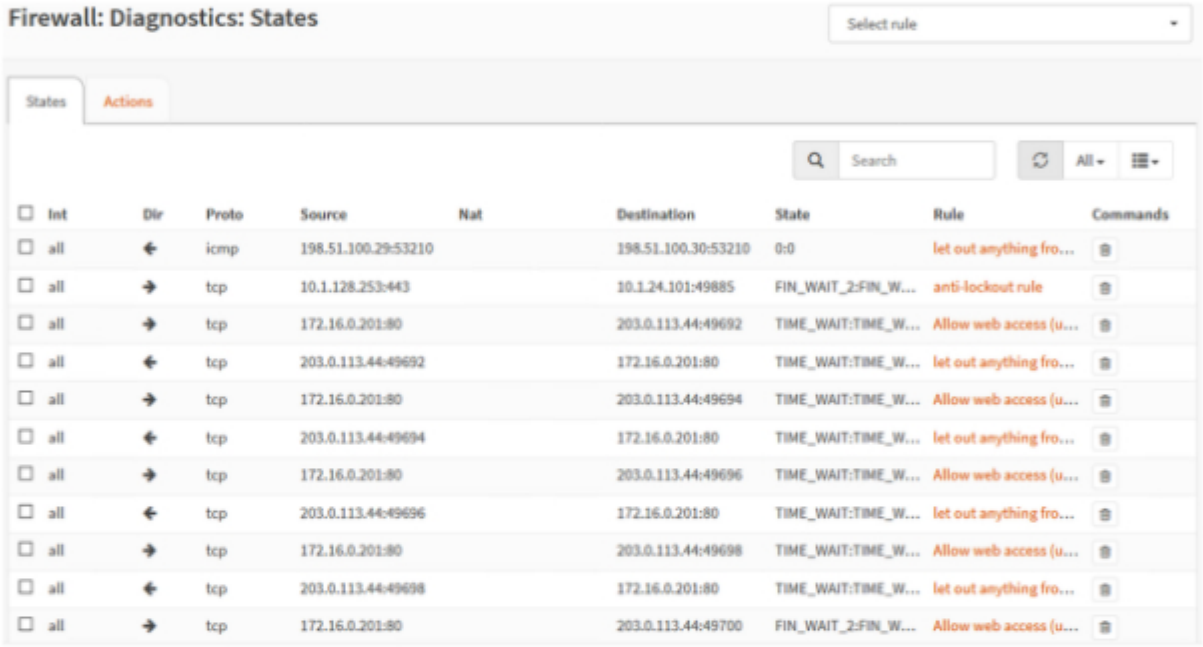
    - Penyaringan/keamanan port-Menerima atau menolak paket berdasarkan nomor port sumber dan tujuan (jenis aplikasi TCP atau UDP).

  Tips: Nomor port terdapat dalam header TCP atau UDP (layer 4), daripada header datagram IP, tetapi firewall penyaringan paket hampir selalu digambarkan bekerja pada layer 3. Mereka hanya dapat memeriksa nomor port dan bukan layer 4 lainnya informasi tajuk.

  ACL mungkin dirancang untuk mengontrol hanya lalu lintas masuk atau lalu lintas masuk dan keluar. Ini juga sering disebut sebagai lalu lintas atau penyaringan "masuk" dan "keluar". Mengontrol lalu lintas keluar berguna karena dapat memblokir aplikasi yang belum diotorisasi untuk berjalan di jaringan dan mengalahkan malware, seperti backdoors. Lalu lintas masuk dan keluar di filter menggunakan ACL terpisah.

  Firewall pemfilteran paket tidak memiliki kewarganegaraan. Ini berarti bahwa itu tidak menyimpan informasi tentang koneksi antara dua host. Setiap paket dianalisis secara independen tanpa catatan paket yang diproses sebelumnya. Jenis pemfilteran ini membutuhkan upaya pemrosesan paling sedikit, tetapi dapat rentan terhadap serangan yang tersebar di urutan paket. Firewall stateless juga dapat menimbulkan masalah dalam arus lalu lintas, terutama ketika semacam penyeimbangan beban sedang digunakan atau ketika klien atau server perlu menggunakan port yang ditetapkan secara dinamis.

- Firewall Inspeksi Stateful
  Firewall inspeksi stateful tingkat sirkuit mengatasi masalah ini dengan mempertahankan informasi stateful tentang sesi yang dibuat antara dua host (termasuk upaya jahat untuk memulai sesi palsu). Informasi tentang setiap sesi disimpan dalam tabel status yang diperbarui secara dinamis. Firewall stateful beroperasi pada Layer 5 (Session) dari model OSI. Ketika sebuah paket tiba, firewall memeriksanya untuk memastikan apakah paket tersebut milik koneksi yang ada. Jika tidak, itu menerapkan aturan penyaringan paket biasa untuk menentukan apakah akan mengizinkannya. Setelah koneksi diizinkan, firewall mengizinkan lalu lintas lewat tanpa pengawasan, untuk menghemat upaya pemrosesan.



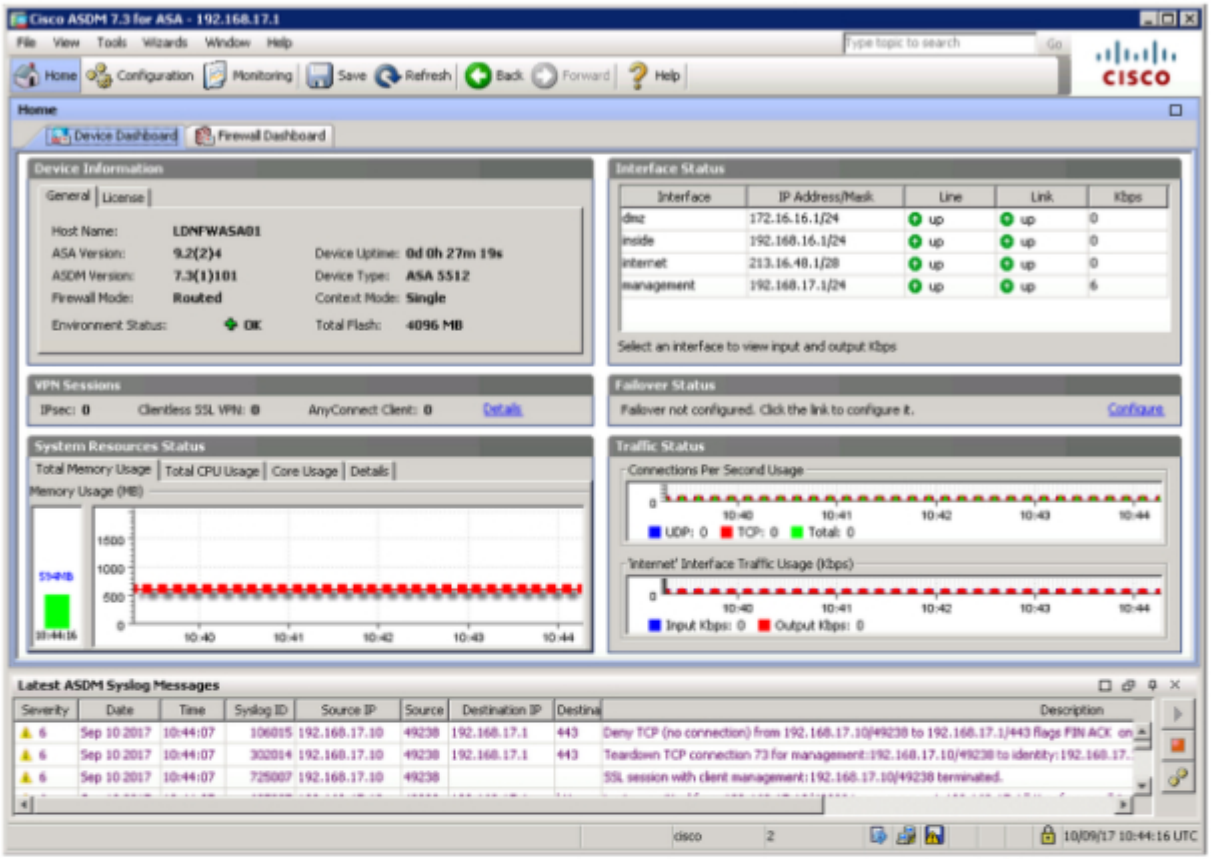
Int	Dir	Proto	Source	Nat	Destination	State	Rule	Commands
all	←	icmp	198.51.100.29:53210		198.51.100.30:53210	0:0	let out anything fro...	
all	→	tcp	10.1.128.253:443		10.1.24.101:49885	FIN_WAIT_2:FIN_W...	anti-lockout rule	
all	→	tcp	172.16.0.201:80		203.0.113.44:49692	TIME_WAIT:TIME_W...	Allow web access (u...	
all	←	tcp	203.0.113.44:49692		172.16.0.201:80	TIME_WAIT:TIME_W...	let out anything fro...	
all	→	tcp	172.16.0.201:80		203.0.113.44:49694	TIME_WAIT:TIME_W...	Allow web access (u...	
all	←	tcp	203.0.113.44:49694		172.16.0.201:80	TIME_WAIT:TIME_W...	let out anything fro...	
all	→	tcp	172.16.0.201:80		203.0.113.44:49696	TIME_WAIT:TIME_W...	Allow web access (u...	
all	←	tcp	203.0.113.44:49696		172.16.0.201:80	TIME_WAIT:TIME_W...	let out anything fro...	
all	→	tcp	172.16.0.201:80		203.0.113.44:49698	TIME_WAIT:TIME_W...	Allow web access (u...	
all	←	tcp	203.0.113.44:49698		172.16.0.201:80	TIME_WAIT:TIME_W...	let out anything fro...	
all	→	tcp	172.16.0.201:80		203.0.113.44:49700	FIN_WAIT_2:FIN_W...	Allow web access (u...	

Status tabel di alat firewall OPNsense. (Tangkapan layar digunakan dengan izin dari OPNsense.)

- Pemilihan dan Penempatan Firewall
  Anda harus mempertimbangkan bagaimana firewall diimplementasikan (sebagai perangkat keras atau perangkat lunak, misalnya) untuk mencakup penempatan atau penggunaan tertentu di jaringan. Beberapa jenis firewall lebih cocok untuk ditempatkan pada batas jaringan atau segmen; lain dirancang untuk melindungi host individu. Pemilihan model firewall jaringan akan sangat bergantung pada volume lalu lintas yang harus diproses. Firewall tunggal dapat mewakili kemacetan jaringan jika tidak mampu menangani volume lalu lintas yang diperlukan.

  Firewall alat adalah firewall perangkat keras yang berdiri sendiri yang hanya menjalankan fungsi firewall. Fungsi firewall diimplementasikan pada firmware alat. Ini juga merupakan jenis firewall berbasis jaringan dan memantau semua lalu lintas yang

masuk dan keluar dari segmen jaringan. Jenis alat ini dapat diimplementasikan dengan antarmuka yang dirutekan atau sebagai firewall "transparan" Layer 2/kawat virtual.



Antarmuka Cisco ASA (*Adaptive Security Appliance*) ASDM (*Adaptive Security Device Manager*). (Gambar © dan Courtesy of Cisco Systems, Inc. Penggunaan tidak sah tidak diizinkan.)

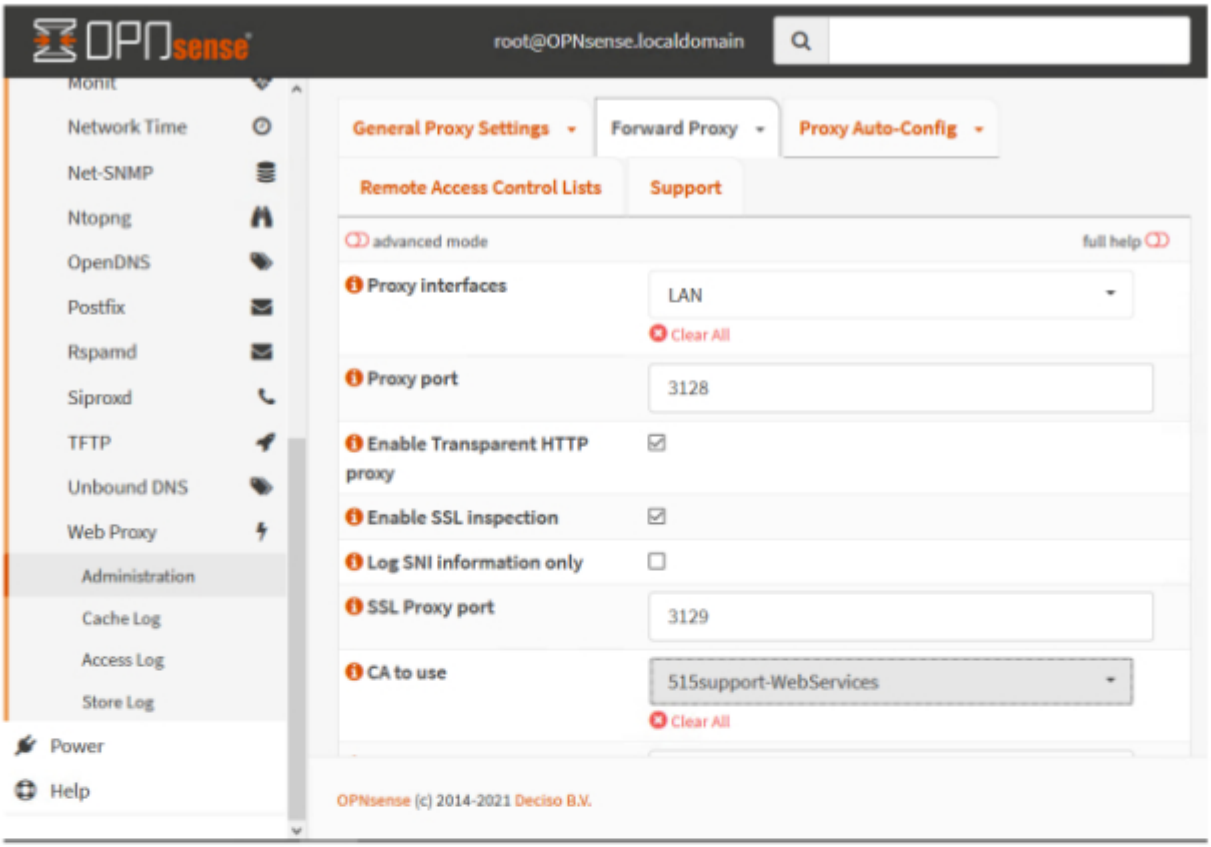
Firewall router serupa, kecuali bahwa fungsinya dibangun ke dalam firmware router. Sebagian besar router/modem Internet SOHO memiliki fungsi firewall jenis ini, meskipun biasanya terbatas untuk mendukung satu subnet dalam jaringan rumah. Firewall router kelas perusahaan akan dapat mendukung lebih banyak sesi daripada SOHO. Selain itu, beberapa switch Layer 3 dapat melakukan penyaringan paket.

- Server Proxy
  Fungsi dasar firewall jaringan adalah untuk memeriksa paket dan menentukan apakah akan memblokirnya atau mengizinkannya lewat. Sebaliknya, server proxy meneruskan permintaan dan tanggapan atas nama kliennya. Alih-alih memeriksa lalu lintas saat melewati, proxy mendekonstruksi setiap paket, melakukan analisis, kemudian membangun kembali paket dan meneruskannya, asalkan sesuai dengan aturan. Perangkat jenis ini ditempatkan di jaringan perimeter.

- Forward Proxies
  Server proxy penerusan menyediakan lalu lintas keluar khusus protokol. Misalnya, Anda mungkin menggunakan proxy web yang memungkinkan host klien terhubung ke situs web dan mengamankan situs web di Internet. Server proxy harus memahami aplikasi yang dilayaninya. Proxy web harus dapat menguraikan dan memodifikasi perintah HTTP dan HTTPS (dan berpotensi HTML juga). Beberapa server proxy khusus untuk aplikasi; lainnya multiguna. Proxy multiguna adalah proxy yang dikonfigurasi dengan filter untuk beberapa jenis protokol, seperti HTTP, FTP, dan SMTP.

  Manfaat utama dari server proxy adalah bahwa klien terhubung ke titik tertentu dalam jaringan perimeter untuk akses web. Ini memberikan tingkat manajemen lalu lintas dan keamanan. Selain itu, sebagian besar server proxy web menyediakan mesin caching, di mana halaman web yang sering diminta disimpan di proxy, meniadakan kebutuhan untuk mengambil kembali halaman tersebut untuk permintaan berikutnya.

  Server proxy umumnya dapat digolongkan sebagai non-transparan atau transparan. Server non transparan berarti bahwa klien harus dikonfigurasi dengan alamat server proxy dan nomor port untuk menggunakannya. Port dimana server proxy menerima koneksi klien sering dikonfigurasi sebagai port 8080. Proxy transparan (atau "dipaksa" atau "mencegat") memotong lalu lintas klien tanpa klien harus dikonfigurasi ulang. Proxy transparan harus diimplementasikan pada switch atau router atau perangkat jaringan inline lainnya.



Mengkonfigurasi pengaturan proxy transparan untuk server proxy yang berjalan pada alat keamanan OPNsense. (Tangkapan layar digunakan dengan izin dari OPNsense.)

- *Reverse Proxies*
  Server proxy terbalik menyediakan lalu lintas masuk khusus protokol. Untuk tujuan keamanan, tidak disarankan untuk menempatkan server aplikasi, seperti server perpesanan dan VoIP, di jaringan perimeter, di mana mereka langsung terhubung ke Internet. Sebagai gantinya, Anda dapat menggunakan proxy terbalik dan mengkonfigurasinya untuk mendengarkan permintaan klien dari jaringan publik (Internet) dan membuat permintaan yang sesuai ke server internal di jaringan perusahaan.

  Reverse Proxies dapat mempublikasikan aplikasi dari jaringan perusahaan ke Internet dengan cara ini. Selain itu, beberapa server proxy terbalik dapat menangani masalah enkripsi/dekripsi dan otentikasi yang muncul saat pengguna jarak jauh mencoba menyambung ke server perusahaan, mengurangi overhead pada server tersebut. Aplikasi umum untuk server proxy terbalik termasuk memublikasikan server web, memublikasikan aplikasi perpesanan atau konferensi, dan mengaktifkan pengambilan email POP/IMAP.

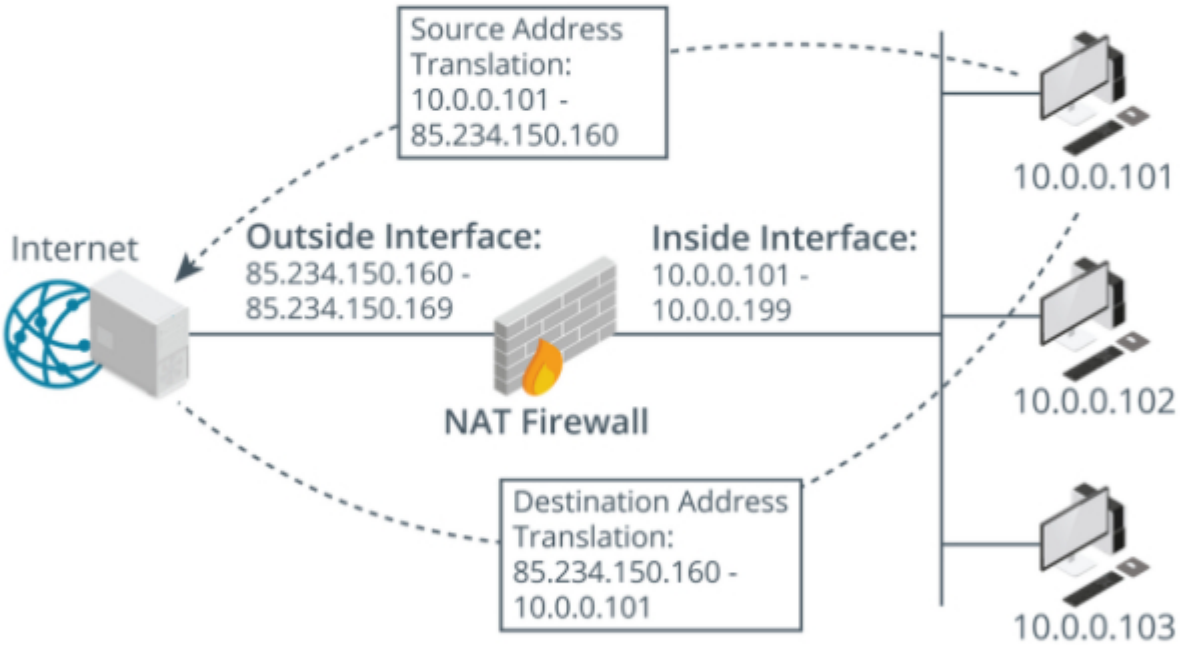
- *Network Address Translation*

Network Address Translation (NAT) dirancang sebagai cara untuk membebaskan alamat IP yang langka untuk host yang membutuhkan akses Internet. NAT adalah layanan yang menerjemahkan antara skema pengalamatan pribadi (atau lokal) yang digunakan oleh host di LAN dan skema pengalamatan publik (atau global) yang digunakan oleh perangkat yang terhubung ke Internet. NAT dikonfigurasi pada perangkat perbatasan, seperti router, server proxy, atau firewall. NAT bukanlah mekanisme keamanan; keamanan disediakan oleh ACL router/firewall.

Dalam konfigurasi static NAT dasar, pemetaan 1:1 sederhana dibuat antara alamat jaringan pribadi (di dalam lokal) dan alamat publik (di dalam global). Jika jaringan tujuan menggunakan NAT, itu digambarkan memiliki skema pengalamatan global dan luar lokal.

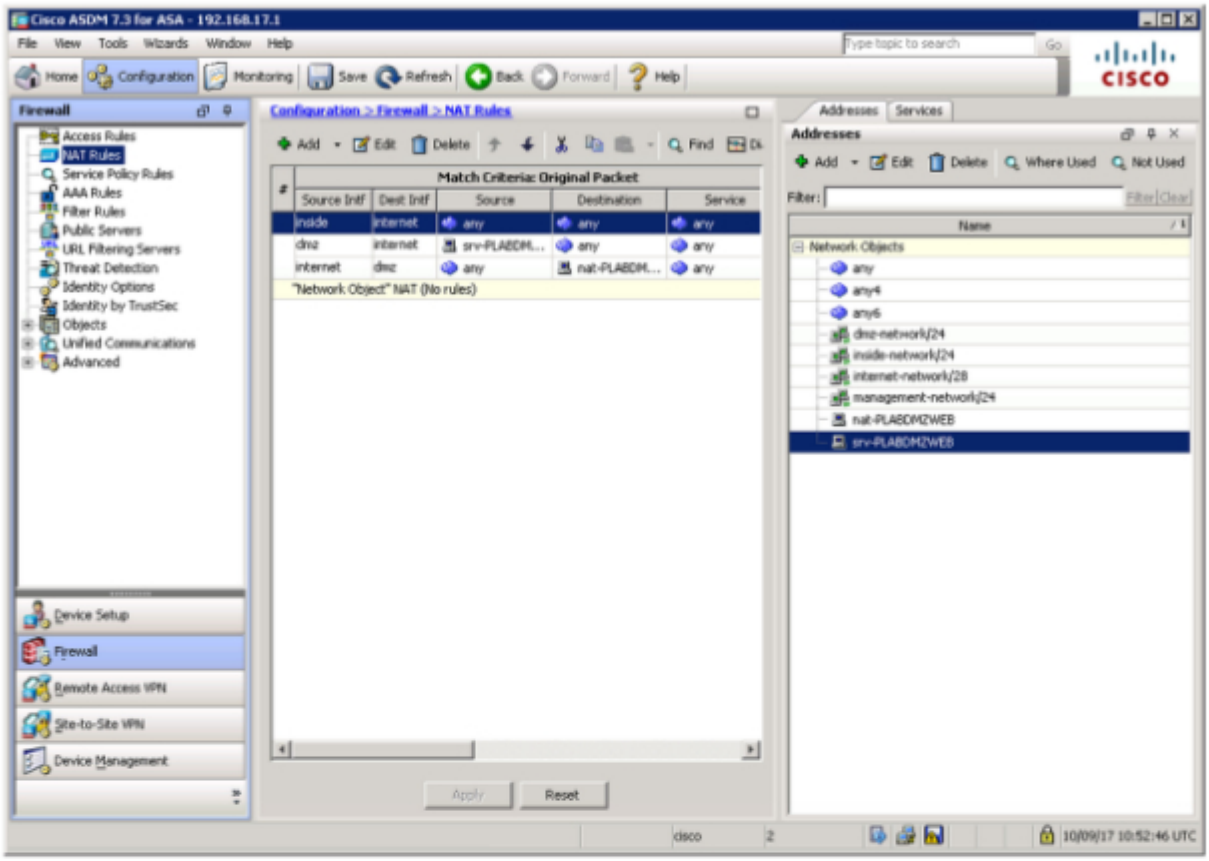
NAT dasar berguna dalam skenario di mana koneksi masuk ke host harus didukung. Misalnya, Anda mungkin memposisikan server web di belakang firewall yang menjalankan NAT. Firewall melakukan terjemahan alamat 1:1 pada alamat IP server web. Ini berarti bahwa host eksternal tidak mengetahui alamat IP server web yang sebenarnya, tetapi mereka dapat berkomunikasi dengannya dengan sukses

.



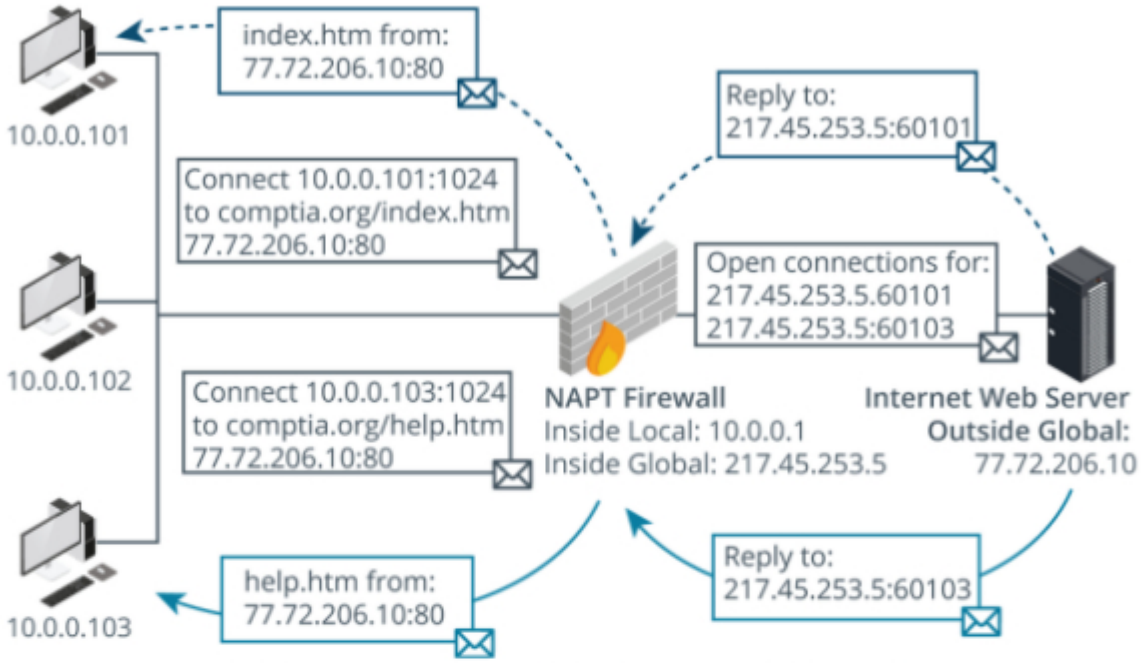
Network Address Translation (NAT). (Images © 123RF.com.)

- Pemetaan statis tunggal tidak terlalu berguna di sebagian besar skenario. Di bawah NAT dinamis, perangkat NAT memperlihatkan kumpulan alamat IP publik. Untuk mendukung koneksi masuk dan keluar antara jaringan pribadi dan Internet, layanan NAT membuat tabel pemetaan alamat publik ke pribadi. Setiap sesi baru membuat pengikatan alamat publik-swasta baru di tabel. Ketika sesi berakhir atau waktu habis, pengikatan dilepaskan untuk digunakan oleh host lain.



Mendefinisikan aturan NAT di Cisco *Adaptive Security Appliance* (ASA). (Tangkapan layar digunakan dengan izin dari Cisco.)

- Port Address Translation
  Basic NAT mendukung beberapa koneksi simultan tetapi masih dibatasi oleh jumlah alamat IP publik yang tersedia. Perusahaan yang lebih kecil hanya dapat dialokasikan satu atau blok kecil alamat oleh ISP mereka. Dalam kasus seperti itu, sarana untuk beberapa alamat IP pribadi untuk dipetakan ke satu alamat publik akan berguna. Fungsi ini disediakan oleh *Port Address Translation* (PAT). Ini dapat disebut sebagai *Network Address Port Translation* (NAPT) atau NAT overloading atau NAT satu-ke-banyak.



Port Address Translation (PAT). (Images ©123RF.com.)

PAT bekerja dengan mengalokasikan setiap koneksi baru sebuah port TCP atau UDP sementara. Misalnya, katakanlah dua host (10.0.0.101 dan 10.0.0.102) memulai koneksi web pada saat yang sama. Layanan PAT membuat dua pemetaan port baru untuk permintaan ini (10.0.0.101:61101 dan 10.0.0.102:61102) di tabel statusnya. Ini kemudian menggantikan IP pribadi untuk IP publik dan meneruskan permintaan ke Internet publik. Ia melakukan pemetaan terbalik pada setiap lalu lintas yang dikembalikan menggunakan port tersebut, memasukkan alamat IP asli dan nomor port, dan meneruskan paket ke host internal.

- Pertahanan di Kedalaman
  Firewall, subnet yang disaring, dan server proxy mencoba membangun penghalang aman di tepi jaringan. Ini disebut sebagai keamanan perimeter. Proliferasi perangkat seluler dengan akses data nirkabel atau seluler dan layanan cloud, ditambah pengenalan yang lebih baik terhadap ancaman orang dalam dan kerentanan terhadap malware, telah mengikis kepercayaan pada model keamanan berbasis perimeter semata. Desain keamanan jaringan harus membahas konsep pertahanan secara mendalam. Ini mengacu pada penempatan kontrol keamanan di seluruh jaringan, sehingga semua upaya akses diautentikasi, diotorisasi, dan diaudit. Beberapa contoh kontrol keamanan yang memberikan pertahanan secara mendalam tambahan untuk segmentasi jaringan dan subnet yang disaring termasuk Kontrol Akses Jaringan, honeypots, pemisahan tugas, dan deteksi intrusi.

- *Network Access Control*
  Network Access Control (NAC) adalah sistem untuk mengautentikasi titik akhir pada titik yang mereka hubungkan ke jaringan. NAC menggunakan mekanisme keamanan port 802.1X, EAP, dan model pemohon AAA, klien AAA perangkat akses jaringan, dan server AAA. NAC memungkinkan perangkat untuk diautentikasi ketika mereka terhubung ke port switch, jaringan nirkabel, atau server akses jarak jauh *virtual private network* (VPN).

  Solusi NAC dasar dapat mengautentikasi klien berdasarkan sertifikat mesin dan/atau kata sandi pengguna. Solusi yang lebih canggih dapat menegakkan kebijakan kesehatan. Kebijakan kesehatan berarti bahwa klien harus menyerahkan laporan pengesahan. Laporan aman ini membuktikan bahwa klien menjalankan OS resmi dan memiliki patch terbaru dan konfigurasi pemindai keamanan.

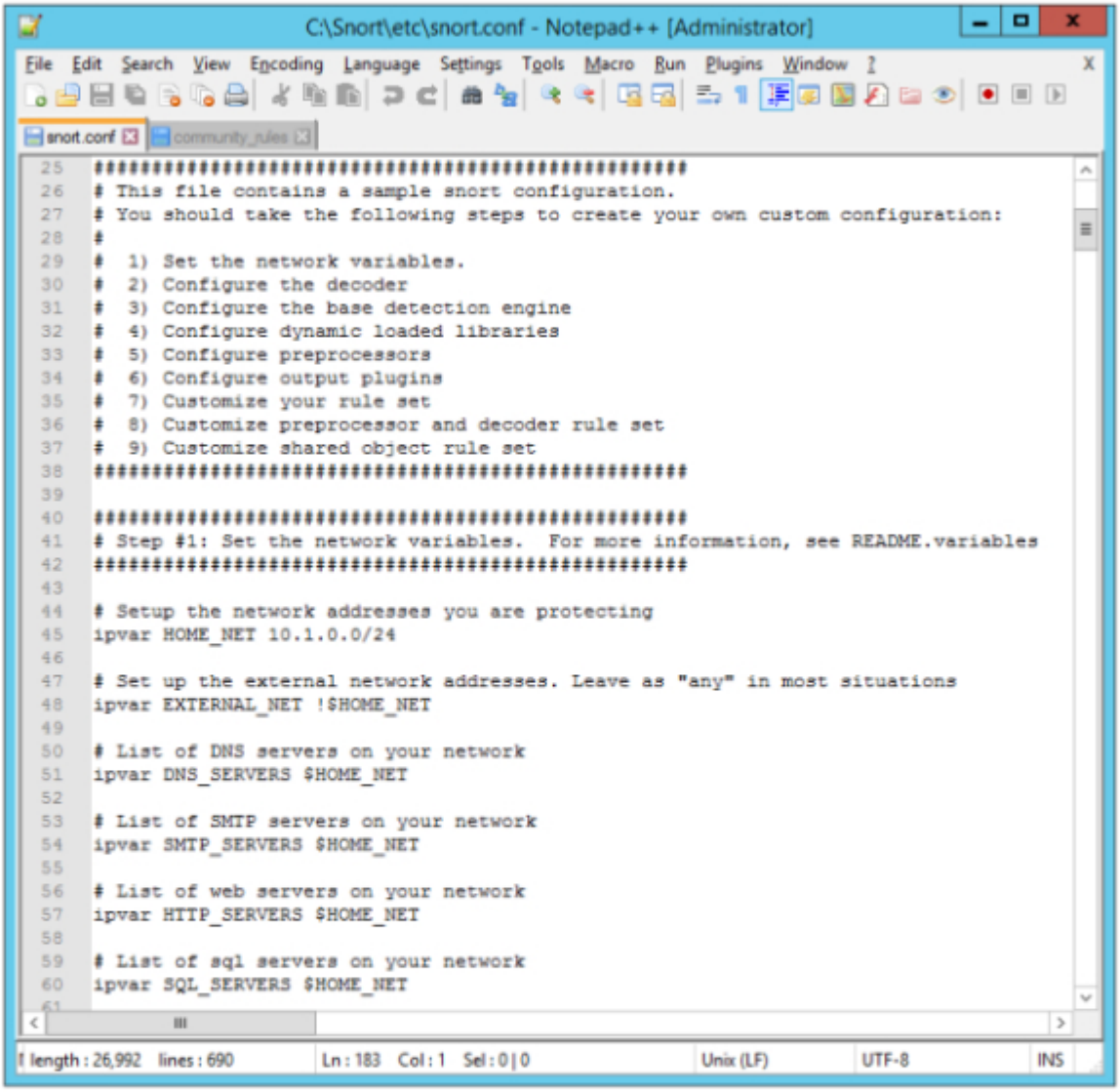
- *Honeypot*
  Honeypot adalah sistem komputer yang dibuat untuk menarik penyerang, dengan tujuan menganalisis strategi dan alat serangan, untuk memberikan peringatan dini upaya serangan, atau mungkin sebagai umpan untuk mengalihkan perhatian dari sistem komputer yang sebenarnya. Kegunaan lainnya adalah untuk mendeteksi internal fraud, snooping, dan malpraktek. Honeynet adalah seluruh jaringan umpan. Ini dapat diatur sebagai jaringan aktual atau disimulasikan menggunakan emulator.

  Pada jaringan produksi, honeypot lebih mungkin ditempatkan di area yang dilindungi tetapi tidak dipercaya antara Internet dan jaringan pribadi atau pada segmen yang dipantau dan disaring secara ketat di dalam jaringan pribadi itu sendiri. Ini memberikan peringatan dini dan bukti apakah aktor ancaman telah mampu menembus zona keamanan tertentu.

- Pemisahan Tugas
  Pemisahan tugas adalah sarana untuk menetapkan pemeriksaan dan keseimbangan terhadap kemungkinan bahwa sistem atau prosedur penting dapat dikompromikan oleh ancaman orang dalam. Tugas dan tanggung jawab harus dibagi di antara individu untuk mencegah konflik etika atau penyalahgunaan kekuasaan.

- *Intrusion Detection and Prevention Systems*
  An intrusion detection system (IDS) melakukan analisis real-time baik lalu lintas jaringan atau sistem dan log aplikasi. Dimana firewall menerapkan aturan dari ACL, IDS dikonfigurasi dengan pola tanda tangan. Setiap pola mewakili jenis aktivitas berbahaya yang diketahui. Jika pola dicocokkan dalam arus lalu lintas, IDS memunculkan peringatan. Seperti perangkat lunak antivirus, IDS harus selalu diperbarui dengan pola tanda tangan terbaru. IDS sering juga dikonfigurasi dengan data ancaman otomatis, seperti daftar alamat IP dan domain yang terkait dengan aktor ancaman.
-
  Seperti penganalisa paket, IDS harus dikonfigurasi dengan sniffer untuk membaca frame dari port cermin atau TAP. Penempatan sniffer harus dipertimbangkan dengan cermat

untuk memenuhi tujuan keamanan. Biasanya, IDS diposisikan di belakang firewall. Tujuannya adalah untuk mendeteksi lalu lintas mencurigakan yang tidak diblokir oleh firewall, memberikan pertahanan yang mendalam. Jenis sensor pasif ini tidak memperlambat lalu lintas dan tidak terdeteksi oleh penyerang (tidak memiliki alamat IP pada segmen jaringan yang dipantau).



File konfigurasi untuk Snort IDS.

Dibandingkan dengan fungsi logging/peringatan pasif dari IDS, sistem pencegahan intrusi (IPS) dapat memberikan respons aktif terhadap ancaman jaringan apa pun yang cocok. Salah satu tindakan pencegahan tipikal adalah mengakhiri sesi dengan mengirimkan paket reset TCP ke host yang menyerang. Pilihan lainnya adalah sensor menerapkan filter sementara pada firewall untuk memblokir alamat IP penyerang (menghindar). Langkah-langkah lanjutan lainnya termasuk membatasi bandwidth untuk menyerang host, menerapkan filter firewall yang kompleks, dan bahkan memodifikasi

paket yang dicurigai agar tidak berbahaya. Terakhir, alat mungkin dapat menjalankan skrip atau program pihak ketiga untuk melakukan tindakan lain yang tidak didukung oleh perangkat lunak IPS itu sendiri.

Fungsionalitas IPS sekarang sangat umum dibangun ke dalam peralatan firewall dan server proxy. Firewall berkemampuan IPS sejajar dengan jaringan, artinya semua lalu lintas melewatinya (juga menjadikannya satu titik kegagalan jika tidak ada mekanisme toleransi kesalahan). Ini jelas berarti bahwa mereka harus mampu mengatasi bandwidth tinggi dan memproses setiap paket dengan sangat cepat untuk menghindari memperlambat jaringan.

Tips: IDS/IPS Jaringan dapat digabungkan dengan IDS/IPS berbasis host. Ini berjalan sebagai agen pada sistem akhir untuk memantau proses aplikasi, file data, dan file log untuk aktivitas yang mencurigakan. Rangkaian IDS/IPS tingkat lanjut menganalisis informasi dari berbagai sensor untuk mengidentifikasi arus lalu lintas yang mencurigakan dan aktivitas host.

Troubleshoot Service and Security Issues

- Pendahuluan: Memecahkan Masalah Layanan dan Keamanan
  Masalah pada lapisan aplikasi atau layanan dapat menjadi masalah yang paling rumit untuk didiagnosis dan dipecahkan. Baik opsi konfigurasi yang kompleks maupun masalah keamanan dapat menjadi faktor dalam masalah terkait layanan. Dalam topik ini, Anda akan bekerja melalui beberapa skenario umum untuk mengidentifikasi gejala khas dan penyebab masalah dengan keamanan dan layanan jaringan.

- Masalah DHCP
  Dynamic Host Configuration Protocol (DHCP) menyediakan konfigurasi otomatis pengalamatan IP ke host tanpa parameter IP statis. Jika klien Windows gagal mendapatkan sewa DHCP, defaultnya adalah menggunakan alamat dalam rentang Pengalamatan IP Pribadi Otomatis (APIPA) dari 169.254.0.0/16. Ini akan dibatasi untuk komunikasi dengan host APIPA lain di segmen jaringan yang sama (domain siaran). Host Linux akan menggunakan rentang 169.254.0.0/16 jika mereka memiliki dukungan Zeroconf, biarkan alamat IP disetel ke 0.0.0.0, atau nonaktifkan IPv4 pada antarmuka.

  Tips: APIPA adalah terminologi Microsoft. Dokumentasi standar mengacu pada rentang alamat ini sebagai IPv4 Link-local (IPV4LL).

- Server DHCP dan Masalah Kehabisan Cakupan
  Kemungkinan alasan klien gagal mendapatkan sewa meliputi:

  - Server DHCP sedang offline. Jika server DHCP Anda offline, pengguna akan terus terhubung ke jaringan selama beberapa waktu dan setelah itu mulai kehilangan kontak dengan layanan jaringan dan server saat mereka datang untuk mencoba memperbarui sewa.

    - Tidak ada lagi alamat yang tersedia (cakupan DHCP habis). Buat ruang lingkup baru dengan alamat yang cukup atau kurangi masa sewa. Ingatlah bahwa rangkaian perangkat lunak Manajemen Alamat IP (IPAM) dapat digunakan untuk melacak penggunaan alamat di seluruh infrastruktur DHCP yang kompleks.

    - Router antara klien dan server DHCP tidak mendukung penerusan BOOTP. Instal router yang sesuai dengan RFC 1542 atau tambahkan jenis agen relai DHCP lainnya ke setiap subnet atau VLAN.

  Jika Anda mengkonfigurasi ulang server DHCP dan cakupannya, klien secara bertahap akan dikonfigurasi ulang. Anda perlu memastikan bahwa Anda merencanakan fakta bahwa tidak semua konfigurasi IP klien akan diperbarui ketika cakupan server diedit dan dapat dibiarkan dengan IP yang kedaluwarsa, gateway default, atau alamat server DNS. Anda dapat melakukan ini dengan menurunkan durasi sewa sebelum perubahan, memaksa semua klien untuk memperbarui, atau menjalankan pengaturan paralel untuk suatu periode.

- Masalah Server DHCP Rogue
  Klien tidak memiliki sarana untuk memilih server DHCP. Jika dua server DHCP berjalan pada subnet yang sama, klien dapat berakhir dengan konfigurasi IP yang salah karena mereka telah memperoleh sewa dari server jahat. Server DHCP jahat dapat digunakan secara tidak sengaja (lupa untuk menonaktifkan server DHCP di titik akses atau router, misalnya) atau dapat digunakan oleh penyerang jahat untuk menumbangkan jaringan. Penyerang biasanya akan menggunakan server jahat untuk mengubah gateway default dan/atau alamat DNS resolver untuk subnet dan merutekan komunikasi melalui mesinnya (serangan on-path).

- Masalah Resolusi Nama
  Saat Anda melakukan tes konektivitas yang berhasil berdasarkan alamat IP, langkah berikutnya mungkin mencoba melakukan ping berdasarkan nama, sehingga menguji resolusi nama.

- Metode Resolusi Nama
  Untuk memecahkan masalah resolusi nama, Anda harus menetapkan persis bagaimana proses bekerja pada host tertentu. Sebuah host dapat menggunakan berbagai metode untuk menyelesaikan nama atau FQDN ke alamat IP. Dalam istilah yang sangat umum, ini akan menjadi sebagai berikut:

    - Periksa cache lokal. Salah satu komplikasi di sini adalah bahwa ada berbagai jenis cache dan cache terpisah untuk aplikasi individual, seperti browser web. Di Windows, Anda dapat menggunakan ipconfig /displaydns dan ipconfig /flushdns untuk memantau dan menghapus cache sistem.

- Periksa HOSTS. File HOSTS adalah daftar statis nama host ke pemetaan alamat IP. Lokasi default di Windows adalah %SystemRoot%\system32\drivers\etc\, sedangkan di Linux biasanya ditempatkan di direktori /etc. Dalam kebanyakan kasus, HOSTS tidak boleh berisi entri apa pun (selain alamat loopback). Entri statis apa pun di HOSTS dapat menjadi penyebab masalah resolusi nama. File juga dapat digunakan untuk pemecahan masalah.

- DNS permintaan. Sebuah host menggunakan server nama yang ditentukan dalam konfigurasi IP-nya untuk menyelesaikan query.

Tips: Teks apa pun yang diawali dengan simbol # dalam file HOSTS adalah komentar dan tidak akan diproses.

Tips: Saat kami berfokus pada resolusi nama melalui DNS di sini, perhatikan bahwa host dapat menggunakan beberapa metode, terutama pada jaringan grup kerja Windows. *Link Local Multicast Name Resolution* (LLMNR) dan *multicast DNS* (mDNS) adalah bentuk modifikasi DNS yang memungkinkan klien untuk melakukan resolusi nama pada link lokal tanpa memerlukan server.

- Masalah Konfigurasi DNS
Sistem Linux dan Windows biasanya mengandalkan infrastruktur server DNS untuk resolusi nama dan penemuan layanan. Dengan tidak adanya server DNS, mesin klien jaringan tidak akan dapat masuk atau terhubung ke layanan atau server.

  Jika host Anda mengalami masalah DNS, gejalanya akan mencakup ketidakmampuan untuk terhubung ke server dengan nama, meskipun dapat diakses dengan alamat IP. Untuk memverifikasi masalah resolusi nama, edit file HOSTS dan tempatkan nama dan catatan alamat IP yang benar dalam file untuk host uji. Saat Anda melakukan ping, jika berhasil, ini menunjukkan masalah resolusi nama.

  Jika satu klien tidak dapat menyelesaikan nama, masalahnya mungkin terletak pada konfigurasi klien.

  - Klien telah dikonfigurasi baik tanpa alamat server DNS atau alamat server DNS yang salah. Konfigurasi ulang alamat server DNS.

  - Klien memiliki akhiran DNS yang salah. Verifikasi domain DNS tempat klien seharusnya berada dan verifikasi kecocokan konfigurasi host.

  Ingatlah bahwa dalam kedua situasi ini, DHCP mungkin salah mengkonfigurasi pengaturan ini. Oleh karena itu, periksa juga opsi server atau konfigurasi opsi cakupan pada server DHCP.

Jika beberapa klien terpengaruh, masalahnya mungkin terletak pada layanan server (atau cara subnet mengakses layanan server). Periksa apakah server yang dikonfigurasi sebagai DNS resolver online dan tersedia (bahwa Anda dapat melakukan ping ke server dari klien).

Jika beberapa query DNS bekerja dari klien dan yang lainnya tidak, maka masalahnya lebih kompleks. Gunakan utilitas nslookup atau dig untuk memeriksa catatan apa yang dikembalikan oleh resolver. Jika mencoba menyambung ke sumber daya Internet, bandingkan catatan ini dengan catatan yang dikembalikan oleh resolver publik (seperti server Google di 8.8.8.8). Pertimbangkan apakah klien telah men-cache catatan yang telah diubah baru-baru ini. Konfigurasi ulang catatan DNS harus direncanakan dan diterapkan dengan hati-hati untuk menghindari masalah caching.

- Masalah Penugasan VLAN
  Saat Anda mempartisi jaringan menjadi VLAN terpisah, karena setiap VLAN adalah domain siaran diskrit, Anda harus memastikan bahwa layanan, seperti DHCP dan DNS, tersedia dengan benar untuk semua VLAN. Jika tidak, pengguna akan mengeluh bahwa "Internet sedang tidak aktif", ketika ternyata tidak ada server DNS lokal yang tersedia untuk menangani permintaan resolusi nama mereka.

  Jika perangkat tidak berada dalam VLAN yang sama dan harus berkomunikasi, pastikan bahwa perutean telah dikonfigurasi untuk mengaktifkan komunikasi VLAN-ke-VLAN. Anda mungkin juga perlu mengkonfigurasi layanan seperti relay DHCP agar host dapat menghubungi server DHCP. Juga, jika perangkat ditempatkan di VLAN yang ditunjuk, konfigurasi IP-nya harus sesuai dalam hal alamat IP, subnet mask, gateway default, dan server DNS.

  Masalah lain adalah bahwa host telah ditempatkan di VLAN yang salah. Pastikan semua perangkat ditempatkan ke VLAN yang sesuai sesuai dengan konfigurasi dasar. Penetapan VLAN dapat dikonfigurasi secara manual, dan administrator mungkin telah membuat kesalahan, jadi periksa konfigurasi antarmuka untuk port switch. Penetapan VLAN juga dapat dikonfigurasi secara otomatis, menggunakan parameter seperti alamat MAC host atau kredensial otentikasi, dan proses ini mungkin gagal, atau database yang digunakan untuk memetakan data dinamis ke ID VLAN mungkin salah dikonfigurasi.

- Masalah Kinerja Jaringan dan Layanan Tidak Responsif
  Jika Anda dapat mengesampingkan masalah konektivitas dengan klien atau subnet lokal, masalahnya mungkin pada server aplikasi, bukan klien. Masalah layanan yang tidak responsif seperti itu biasanya akan bermanifestasi dengan beberapa klien tidak dapat terhubung. Mungkin ada sejumlah penyebab yang mendasarinya, tetapi pertimbangkan beberapa hal berikut:

  - Aplikasi atau OS yang menghosting layanan mogok (atau ada masalah perangkat keras atau daya).

- Server yang menghosting layanan kelebihan beban (penggunaan CPU/memory/disk I/O/penggunaan ruang disk yang tinggi). Cobalah membatasi koneksi klien hingga sumber daya server dapat ditingkatkan.

- Ada kemacetan di jaringan, baik di ujung klien atau server (atau keduanya). Gunakan ping atau traceroute untuk memeriksa latensi yang dialami melalui tautan dan membandingkannya dengan garis dasar kinerja jaringan. Sekali lagi, pembatasan koneksi atau bandwidth dapat membantu mengurangi kemacetan hingga tautan bandwidth yang lebih tinggi dapat disediakan.

- Badai siaran menyebabkan hilangnya bandwidth jaringan. Pengalihan loop menyebabkan siaran dan bingkai unicast yang tidak dikenal untuk mengedarkan jaringan terus-menerus, karena setiap switch berulang kali membanjiri setiap bingkai. Badai siaran dapat dengan cepat menghabiskan semua bandwidth tautan dan peralatan jaringan mogok (periksa penggunaan CPU yang berlebihan pada switch dan host). *Spanning Tree Protocol* (STP) seharusnya mencegah loop seperti itu, tetapi ini bisa gagal jika komunikasi STP antar switch tidak berfungsi dengan benar, baik karena kesalahan dalam pengkabelan atau port/transceiver atau karena kesalahan konfigurasi.

-

- Kemacetan jaringan juga dapat menjadi tanda bahwa layanan tersebut terkena serangan *Denial of Service* (DoS). Cari pola akses yang tidak biasa (misalnya, gunakan GeoIP untuk membuat grafik alamat IP sumber menurut negara dan bandingkan dengan pola akses dasar).

Tips: Jika pengguna di LAN tidak dapat terhubung ke layanan eksternal, seperti aplikasi cloud, Anda dapat menggunakan situs seperti isitdownrightnow.com untuk menguji apakah masalah tersebut lokal ke jaringan Anda atau masalah dengan situs penyedia layanan.

Tips: Bersikaplah proaktif dalam memantau ketersediaan layanan sehingga Anda dapat menyelesaikan masalah sebelum mempengaruhi sejumlah besar klien.

- Masalah Firewall dan ACL yang Salah Konfigurasi
Salah satu jenis firewall, ACL, atau kesalahan konfigurasi filter konten menyebabkan layanan, port, atau alamat yang diblokir yang seharusnya diizinkan untuk dilewati. Ini akan menyebabkan aplikasi atau protokol gagal berfungsi dengan benar. Misalnya, firewall mungkin memblokir port TCP atau UDP yang seharusnya terbuka, atau mungkin mengizinkan port tetapi menolak akses ke jaringan IP atau alamat host yang seharusnya dapat terhubung. Juga pertimbangkan bahwa firewall tingkat lanjut mampu menerapkan kriteria pemfilteran tambahan, seperti mengevaluasi nama/lokasi yang dapat dieksekusi proses/layanan atau otorisasi berdasarkan akun pengguna atau keanggotaan grup.

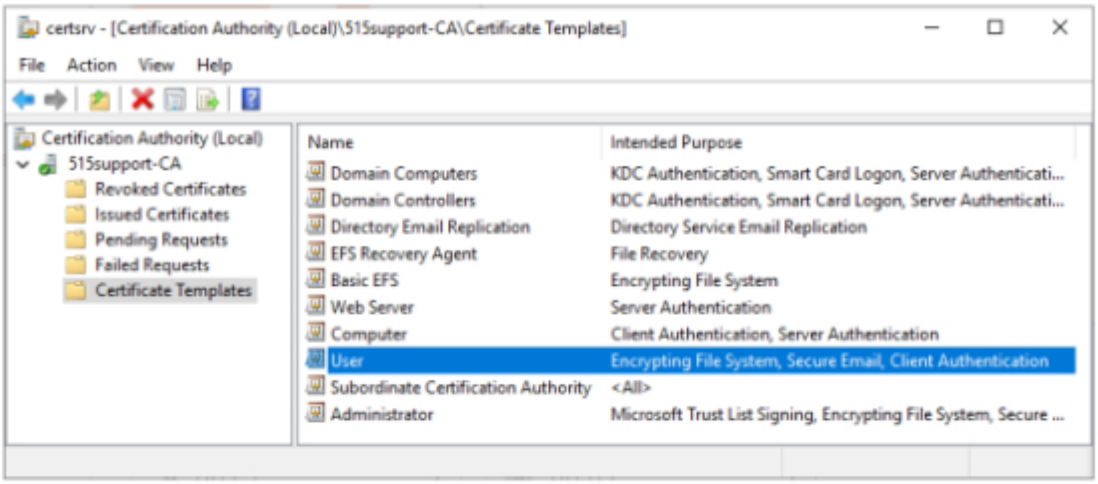
Jenis kesalahan penolakan biasanya akan mudah diidentifikasi, karena pengguna akan melaporkan insiden yang terkait dengan kegagalan lalu lintas data. Dengan insiden seperti itu, konfigurasi firewall akan selalu menjadi penyebab yang mungkin, sehingga akan menjadi prioritas utama untuk diselidiki. Diagnosis dapat dikonfirmasi dengan mencoba membuat koneksi dari dalam dan luar firewall. Jika terhubung dari luar firewall tetapi tidak dari dalam, ini akan mengkonfirmasi bahwa firewall menjadi penyebab masalah.

Masalah potensial lainnya adalah di mana ada pengaturan firewall berbasis jaringan dan berbasis host untuk bernavigasi di jalur komunikasi. Mungkin ada firewall host yang berjalan di klien, di server, atau di keduanya. Untuk mendiagnosis masalah dengan firewall host, coba sambungan dengan firewall host dinonaktifkan. Jika upaya koneksi berhasil, maka ACL firewall jaringan mengizinkan paket, tetapi firewall host dikonfigurasi untuk memblokirnya. Jika upaya koneksi gagal, selidiki ACL firewall jaringan terlebih dahulu. Anda juga dapat memeriksa file log firewall untuk menemukan aturan apa yang telah diterapkan untuk memblokir lalu lintas pada waktu tertentu.

Hasil lain yang mungkin dari firewall yang dikonfigurasi dengan buruk adalah bahwa paket dapat diizinkan melalui yang harus diblokir. Ini adalah hasil yang lebih serius, karena hasilnya adalah membuka sistem untuk kerentanan keamanan. Itu juga tidak selalu mudah dideteksi, karena biasanya tidak menyebabkan apa pun berhenti berfungsi. Karena tidak ada insiden yang biasanya muncul dari hasil ini (kecuali dalam kasus kerentanan dieksploitasi), ini bukan skenario yang tunduk pada pemecahan masalah. Sebaliknya, ini menggarisbawahi perlunya audit firewall reguler dan proses kontrol perubahan menyeluruh untuk menangani permintaan perubahan firewall.

- Masalah Sertifikat Tidak Terpercaya
  Jika sertifikat digital yang disajikan oleh subjek (server atau pengguna) tidak dipercaya oleh aplikasi klien (seperti browser), klien akan memberitahu pengguna. Alasan paling umum untuk sertifikat tidak dipercaya adalah bahwa penerbit sertifikat tidak dipercaya. Misalnya, server web Widget menerima sertifikat yang ditandatangani oleh MyCA. Kecuali jika sertifikat MyCA sendiri disimpan di toko akar terpercaya browser, aplikasi klien tidak akan mempercayai server Widget. Pengguna biasanya dapat memilih untuk mengabaikan peringatan ini dan menambahkan pengecualian, tetapi ini harus dilakukan hanya jika penyebab kurangnya hubungan kepercayaan dipahami.

  Jika Anda mempercayai penerbitnya, Anda dapat menambahkan sertifikat mereka ke penyimpanan sertifikat root perangkat klien. Di Windows, Anda dapat menggunakan konsol certmgr.msc untuk mengelola sertifikat pengguna dan konsol certlm.msc untuk mengelola sertifikat mesin. Anda juga menggunakan konsol ini untuk mengelola sertifikat yang digunakan oleh komputer atau akun penggunanya.



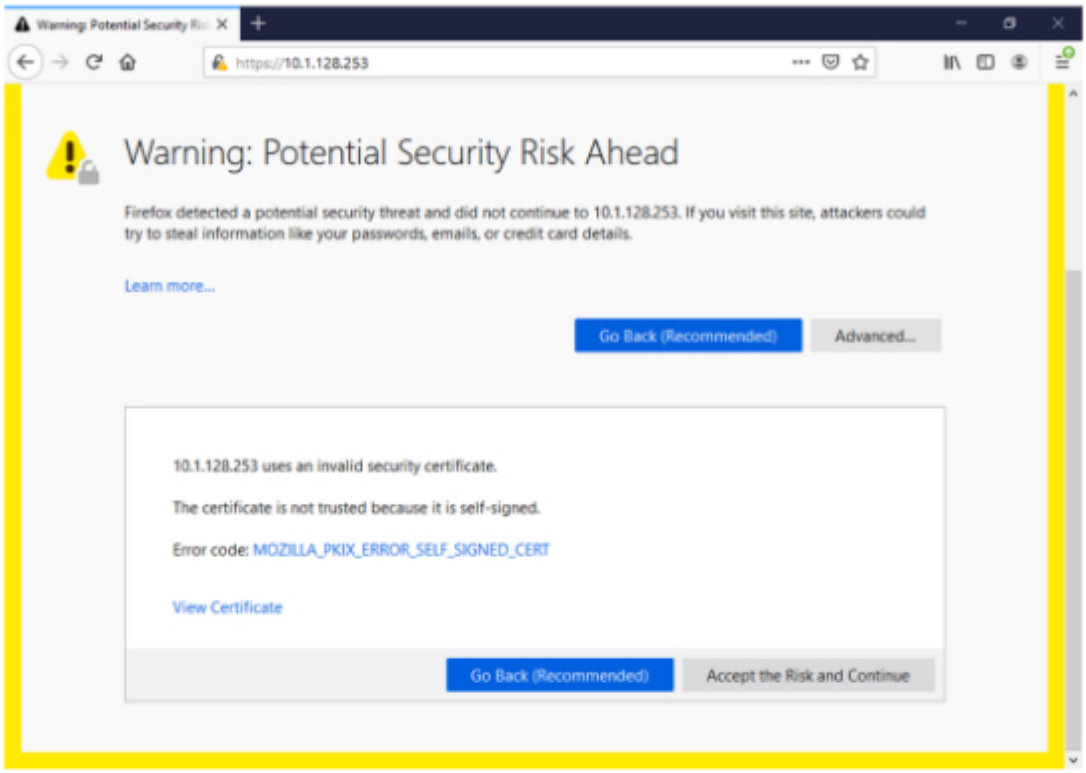
Konsol Manajemen Sertifikat. Root CA Terpercaya berisi semua perwalian Microsoft dan perusahaan, ditambah perwalian CA pihak ketiga. (Tangkapan layar digunakan dengan izin dari Microsoft.)

Satu komplikasi di sini adalah bahwa aplikasi yang berbeda mungkin memiliki penyimpanan sertifikat terpercaya yang berbeda. Misalnya, ada penyimpanan sertifikat Windows, tetapi browser Firefox® tidak mempercayainya secara default dan mengelola penyimpanan sertifikatnya sendiri. Berbagai distribusi Linux menyimpan sertifikat root terpercaya di beberapa lokasi berbeda.

Seringkali, sertifikat tidak dipercaya karena ditandatangani sendiri (pemegang sertifikat adalah penerbit dan subjek sertifikat). Hal ini sering terjadi pada sertifikat yang digunakan untuk melindungi antarmuka manajemen web dari peralatan tingkat konsumen dan aplikasi server. Anda mungkin dapat mengganti sertifikat default dengan yang dipercaya oleh perusahaan.

Beberapa penyebab lain dari sertifikat tidak terpercaya adalah:

- Nama subjek sertifikat tidak cocok dengan URL. Ini biasanya merupakan kesalahan konfigurasi dari pengelola server web, tetapi ini dapat mengindikasikan aktivitas jahat. Anda harus mengkonfirmasi nama umum sertifikat dan mengakses situs web dengan menggunakan URL tersebut.



Sertifikat ini tidak dipercaya karena ditandatangani sendiri dan karena tidak cocok dengan nama subjek (karena host diakses melalui alamat IP, bukan FQDN). (Tangkapan layar milik Mozilla Foundation.)

- Sertifikat tidak digunakan untuk tujuan yang dinyatakan. Misalnya, sertifikat yang dikeluarkan untuk menandatangani email sedang digunakan di server web. Dalam keadaan ini, Anda tidak boleh menambahkan pengecualian. Pemilik atau subjek layanan harus mendapatkan sertifikat yang diformat dengan benar.

- Sertifikat kadaluarsa atau dicabut. Sekali lagi, kecuali ada keadaan yang dapat dijelaskan, Anda tidak boleh mengizinkan pengecualian. Jika Anda mengelola peralatan lama (router SOHO atau drive NAS, misalnya), kemungkinan sertifikat yang diinstal di dalamnya akan kedaluwarsa. Jika Anda tahu bahwa alat tersebut belum dirusak, Anda dapat melanjutkan.

- Waktu tidak disinkronkan dengan benar antara server dan klien.

Tips: Browser dan aplikasi email biasanya menampilkan pesan error yang informatif. Dalam konteks lain, seperti otentikasi EAP, mungkin tidak begitu jelas bahwa sertifikat adalah penyebab kegagalan atau mengapa sertifikat ditolak. Periksa log yang merekam koneksi untuk mencari petunjuk.

- Masalah Umum Lainnya
  Ketika datang ke pemecahan masalah lapisan aplikasi, Anda biasanya perlu menggunakan referensi yang khusus untuk lingkungan atau aplikasi untuk memecahkan masalah. Beberapa masalah umum lainnya yang mungkin Anda temui termasuk sinkronisasi waktu, perangkat seluler, dan lisensi.

- Masalah NTP
  Sebagian besar layanan jaringan, dan terutama mekanisme otentikasi dan otorisasi, bergantung pada setiap host yang menggunakan sumber waktu yang disinkronkan. Sumber waktu yang tidak akurat juga mempengaruhi keandalan dan kegunaan data log, yang dapat berimplikasi pada kepatuhan terhadap peraturan.

  Sinkronisasi waktu biasanya dilakukan melalui Network Time Protocol (NTP). Klien harus dapat mengakses sumber waktu melalui port UDP 123. Dalam lingkungan Windows, sumber waktu untuk klien biasanya berupa pengontrol domain. Pengontrol domain dapat menggunakan sumber waktu berbasis GPS perangkat keras atau mengandalkan server Internet, tergantung pada tingkat akurasi yang diperlukan. Di Windows, perintah w32tm /query /configuration dapat digunakan untuk memeriksa konfigurasi saat ini.

- Tantangan BYOD
  Bring Your Own Device (BYOD) adalah model penyediaan smartphone/tablet yang memungkinkan pengguna memilih perangkat pribadi yang akan digunakan untuk berinteraksi dengan layanan jaringan perusahaan dan aplikasi cloud. Mengizinkan pemilihan perangkat oleh pengguna memperkenalkan berbagai tantangan kompatibilitas, dukungan, dan keamanan:

  - **Kompatibilitas/dukungan**-Berbagai perangkat, versi OS seluler, dan dukungan vendor untuk patch membuat tugas memastikan bahwa setiap perangkat dapat terhubung ke aplikasi jaringan perusahaan dan sumber daya data menjadi sangat kompleks.

  - **Keamanan**-Keragaman perangkat ini juga menyebabkan masalah keamanan, terutama dalam hal perangkat yang tidak ditambal. Masalah lainnya adalah perangkat tidak sepenuhnya berada di bawah kendali administratif departemen TI. Pelaku ancaman orang dalam dapat menginstal aplikasi yang dapat menimbulkan risiko terhadap data perusahaan atau menyalahgunakan perangkat untuk mengekstrak data.

  Beberapa dampak dari masalah ini dapat dikurangi melalui penggunaan suite *enterprise mobility management* (EMM) dan ruang kerja perusahaan. EMM (atau manajemen perangkat seluler) adalah jenis solusi kontrol akses jaringan yang mendaftarkan perangkat saat mereka terhubung ke jaringan. Kemudian dapat menerapkan kebijakan keamanan saat perangkat terhubung. Ini mungkin membatasi penggunaan fungsi

perangkat atau aplikasi pribadi. Ruang kerja perusahaan adalah aplikasi yang tersegmentasi dari perangkat lainnya dan memungkinkan kontrol yang lebih terpusat atas data perusahaan. Pengguna juga harus menyetujui kebijakan penggunaan yang dapat diterima, yang mungkin melarang penginstalan aplikasi non store dan rooting/jailbreak perangkat dan memperbarui perangkat dengan patch. Pengguna juga biasanya harus tunduk pada pemeriksaan perangkat untuk melindungi data perusahaan.

- Masalah Fitur Berlisensi
  Lisensi untuk server dan peralatan jaringan dapat menjadi rumit dan mudah untuk membuat kesalahan konfigurasi. Ketika dihadapkan dengan masalah yang tidak terduga, sering kali perlu dipertimbangkan apakah masalah lisensi atau aktivasi fitur dapat menjadi penyebabnya. Pada switch atau router, kegagalan lisensi dapat membatasi jumlah port yang tersedia, jumlah rute yang diizinkan dalam tabel perutean, atau ketersediaan protokol perutean. Fitur keamanan dan manajemen mungkin telah dikonfigurasi dalam periode uji coba atau evaluasi dan tiba-tiba berhenti berfungsi saat masa tenggang berakhir.

  Titik awal untuk memecahkan masalah lisensi adalah log. Ini harus menunjukkan apakah periode evaluasi/percobaan baru saja kedaluwarsa atau ketika jumlah kursi/contoh telah terlampaui. Pastikan perangkat memiliki lisensi atau kunci aktivasi yang benar terpasang. Jika relevan, pastikan alat dapat terhubung ke server lisensi atau aktivasinya.

Modul 15

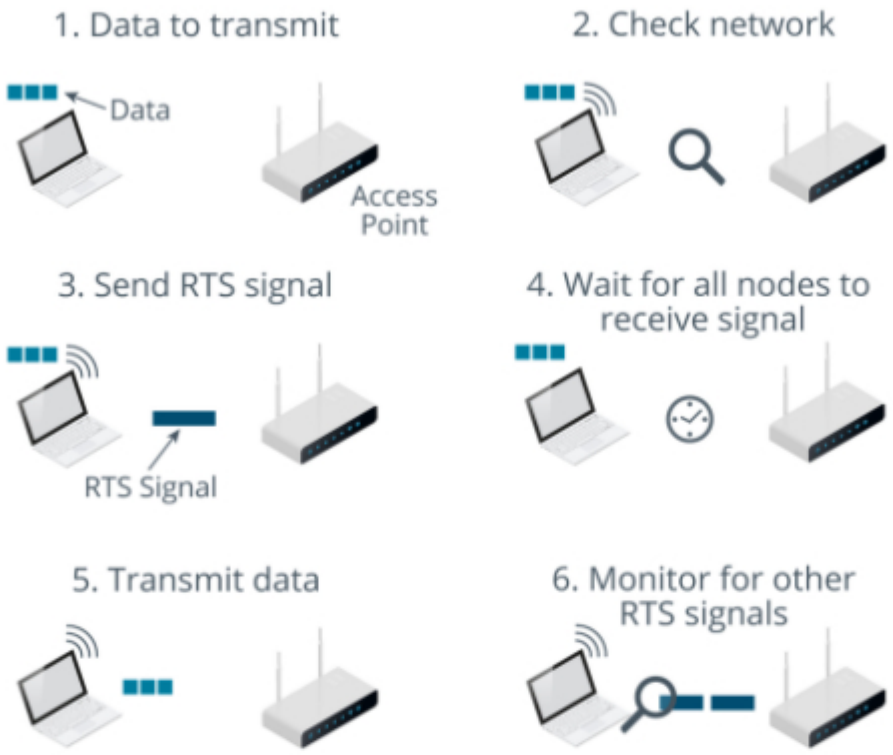
Deploying and Troubleshouting Wireless Network

Summarize Wireless Standards

- Pendahuluan: Ringkasan Standar Nirkabel
  Konektivitas nirkabel adalah fitur inti dari sebagian besar lingkungan jaringan saat ini karena mendukung kebutuhan pengguna akan mobilitas menggunakan perangkat yang berbeda. Untuk mendukung jaringan nirkabel, Anda harus dapat merangkum fitur standar *Wi-Fi* dan seluler.

- Standar Nirkabel IEEE 802.11
  Sebagian besar LAN nirkabel (WLAN) didasarkan pada standar IEEE 802.11, lebih dikenal dengan nama merek *Wi-Fi*. Standar 802.11 mendefinisikan media lapisan fisik dimana data dikodekan menjadi sinyal pembawa radio dengan menggunakan skema modulasi. Sifat gelombang radio meliputi amplitudo (ketinggian puncak dan lembah), frekuensi (jumlah puncak per satuan waktu), dan fase (sudut gelombang pada suatu titik waktu). Modulasi mengubah satu atau lebih properti tersebut untuk mengkodekan sinyal. Selain skema modulasi, standar *Wi-Fi* menggunakan metode pembawa yang berbeda untuk memberikan ketahanan yang cukup terhadap interferensi dari kebisingan dan sumber radio lainnya.

  Sebuah transmisi dan penerimaan radio nirkabel dalam rentang frekuensi tertentu dengan skema modulasi yang sama adalah media akses bersama setengah dupleks (bus fisik). 802.11 menggunakan *Carrier Sense Multiple Access* dengan *Collision Avoidance* (CSMA/CA) untuk mengatasi pertentangan. Di bawah CSMA/CA, ketika sebuah stasiun menerima sebuah frame, ia melakukan pengecekan kesalahan. Jika frame utuh, stasiun merespon dengan *acknowledgmen*t (ACK). Jika ACK tidak diterima, stasiun pemancar mengirim ulang frame sampai waktu habis. 802.11 juga mendefinisikan mekanisme kontrol aliran Virtual Carrier Sense untuk lebih mengurangi insiden tabrakan. Sebuah stasiun menyiarkan *Request to Send* (RTS) dengan sumber dan tujuan serta waktu yang diperlukan untuk mengirim. Stasiun penerima merespons dengan *Clear To Send* (CTS) dan semua stasiun lain dalam jangkauan tidak berusaha mengirimkan dalam periode itu.



Metode akses media CSMA/CA. (Images © 123RF.com.)

Standar *Wi-Fi* 802.11 yang asli hanya bekerja pada 1 Mbps, tetapi seperti standar Ethernet 802.3, standar ini telah direvisi berkali-kali, dengan setiap iterasi menentukan mekanisme pensinyalan dan transmisi yang berbeda. Produk yang memenuhi berbagai standar dapat disertifikasi oleh *Wi-Fi* Alliance (wi-fi.org).

- IEEE 802.11a dan Bandwidth Saluran 5 GHz
  Setiap perangkat nirkabel beroperasi pada rentang frekuensi radio tertentu dalam pita frekuensi keseluruhan. Rentang frekuensi tertentu disebut sebagai saluran. Penting untuk memahami perbedaan antara dua pita frekuensi yang digunakan oleh standar IEEE 802.11:

  - 2,4 GHz lebih baik dalam propagasi melalui permukaan padat, sehingga ideal untuk menyediakan jangkauan sinyal terpanjang. Namun, pita 2,4 GHz tidak mendukung sejumlah besar saluran individual dan sering macet, baik dengan jaringan Wi-Fi lain maupun jenis teknologi nirkabel lainnya, seperti Bluetooth®. Akibatnya, dengan pita 2,4 GHz, ada peningkatan risiko interferensi, dan kecepatan data maksimum yang dapat dicapai biasanya lebih rendah dibandingkan dengan 5 GHz.

  - 5 GHz kurang efektif dalam menembus permukaan padat sehingga tidak mendukung rentang maksimum yang dicapai dengan standar 2,4 GHz, tetapi pita ini mendukung lebih banyak saluran individual dan lebih sedikit mengalami

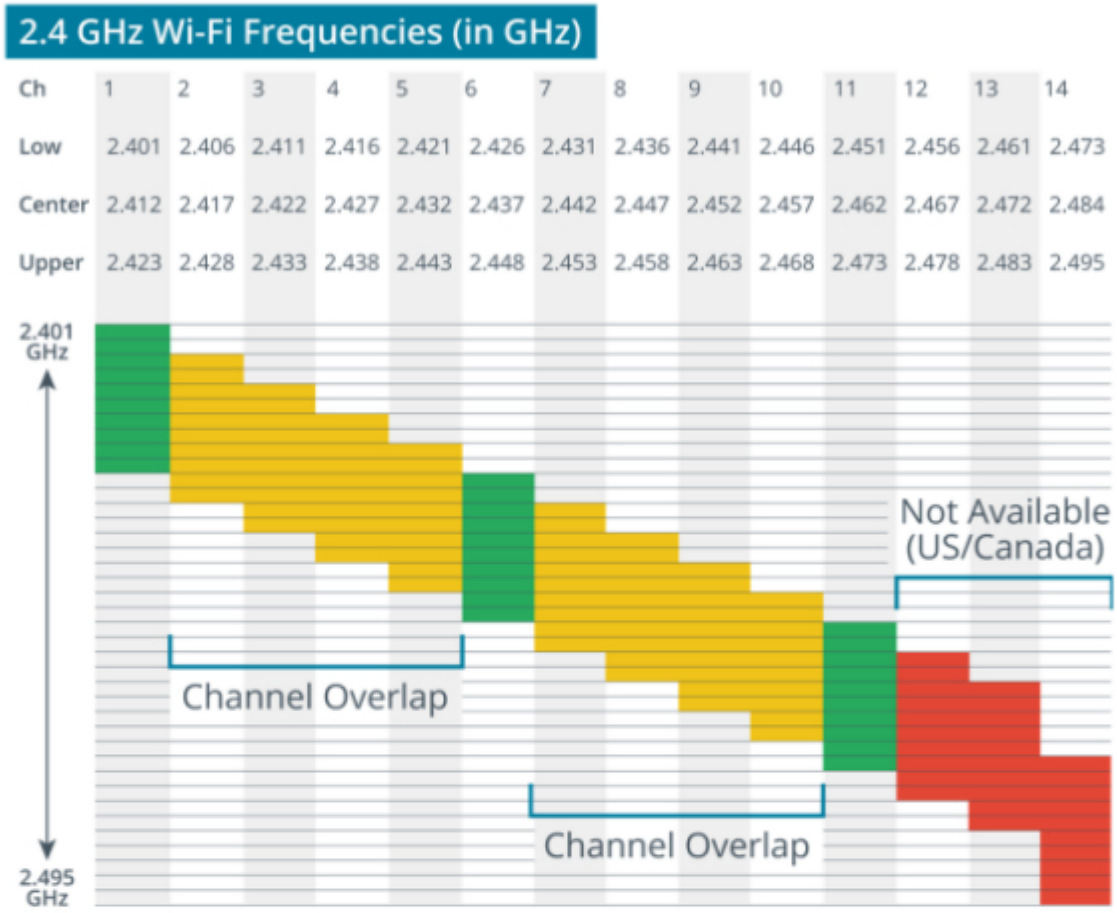
kemacetan dan gangguan, yang berarti mendukung kecepatan data yang lebih tinggi pada rentang yang lebih pendek.

Standar IEEE 802.11a menetapkan penggunaan pita frekuensi 5 GHz dan skema pembawa multipleks yang disebut *Orthogonal Frequency Division Multiplexing* (OFDM). 802.11a memiliki kecepatan data nominal 54 Mbps.

The 5 GHz band dibagi lagi menjadi 23 saluran yang tidak tumpang tindih, yang masing-masing memiliki lebar 20 MHz. Awalnya, ada 11 saluran, tetapi standar 802.11h berikutnya menambahkan 12 saluran lagi. 802.11h juga menambahkan metode *Dynamic Frequency Selection* (DFS) untuk mencegah *access points* (AP) yang bekerja di 5 GHz band agar tidak mengganggu sinyal radar dan satelit. Penggunaan saluran yang tepat dapat tunduk pada peraturan yang berbeda di negara yang berbeda. Dampak regulasi juga mencakup batasan ketat pada keluaran daya, yang membatasi jangkauan perangkat *Wi-Fi*.

- IEEE 802.11b/g dan Bandwidth Saluran 2,4 GHz
  Standar 802.11b menggunakan pita frekuensi 2,4 GHz dan dirilis secara paralel dengan 802.11a. Ini menstandarisasi penggunaan metode pembawa *Direct Sequence Spread Spectrum* (DSSS), bersama dengan pengkodean sinyal *Complementary Code Keying* (CCK). Sementara dalam beberapa hal, DSSS adalah teknologi yang lebih rendah daripada OFDM-dengan kecepatan data nominal hanya 11 Mbps-802.11b, produk lebih cepat dipasarkan dan menjadi lebih mapan daripada 802.11a.

  The 2.4 GHz band dibagi lagi menjadi hingga 14 saluran, dengan interval 5 MHz dari 2412 MHz hingga 2484 MHz. Karena jaraknya hanya 5 MHz dan *Wi-Fi* membutuhkan bandwidth saluran ~20 MHz, saluran 802.11b cukup tumpang tindih. Ini berarti bahwa interferensi saluran bersama adalah kemungkinan nyata kecuali saluran dengan jarak yang luas dipilih (1, 6, dan 11, misalnya). Juga, di Amerika, peraturan mengizinkan penggunaan saluran 1-11 saja, sementara di Eropa saluran 1-13 diizinkan, dan di Jepang semua 14 saluran diizinkan.



Channel overlap in the 2.4 GHz band.

Standar 802.11g menawarkan jalur peningkatan yang relatif mudah dari 802.11b. Seperti 802.11a, 802.11g menggunakan OFDM, tetapi pada pita 2,4 GHz digunakan oleh 802.11b dan dengan tata letak saluran yang sama. Ini memudahkan vendor untuk menawarkan perangkat 802.11g yang dapat menawarkan dukungan mundur untuk klien 802.11b lama. 802.11g memiliki kecepatan data nominal 54 Mbps. Saat dalam mode kompatibilitas 802.11b, ia kembali menggunakan DSSS.

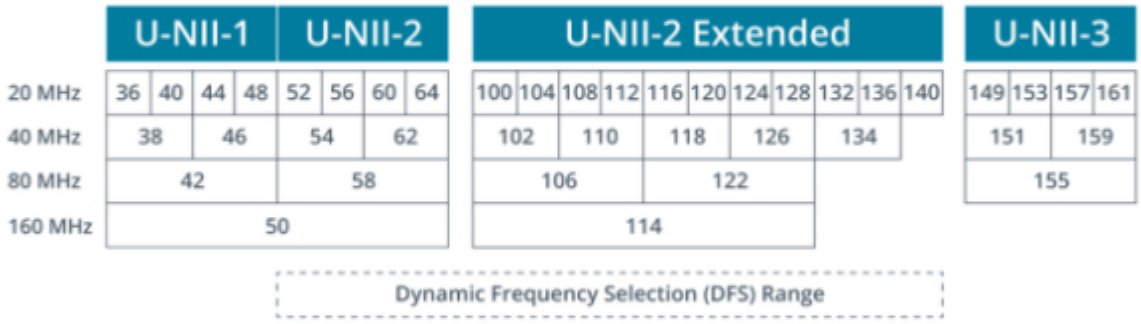
- IEEE 802.11n, MIMO, dan Pengikatan Saluran

  Standar 802.11n meningkatkan bandwidth dengan menggandakan sinyal dari 2 menjadi 4 antena terpisah (rantai radio) menggunakan kumpulan teknologi yang umumnya disebut sebagai *Multiple Input Multiple Output* (MIMO). Konfigurasi rantai radio 802.11n diidentifikasi dengan notasi AxB:C, di mana A adalah jumlah antena pemancar, B adalah jumlah antena penerima, dan C adalah jumlah aliran transmisi dan penerimaan simultan. Maksimum yang mungkin adalah 4x4:4, tetapi konfigurasi umum adalah 2x2:2 atau 3x3:2. Misalnya, titik akses 4x4:4 dapat mengalokasikan dua aliran yang membawa data

berbeda ke klien 2x2:2, sehingga meningkatkan bandwidth. Ini disebut sebagai multiplexing spasial.

Memiliki lebih banyak antena pengirim dan penerima juga dapat digunakan untuk meningkatkan keandalan sinyal, daripada meningkatkan bandwidth. Jika aliran data yang sama dikirim oleh dua atau tiga antena pemancar, penerima dapat menggabungkannya untuk memperoleh sinyal yang lebih kuat dan meningkatkan jangkauan pada kecepatan data yang diberikan. Demikian pula, beberapa antena penerima dapat memperoleh sinyal yang lebih kuat, bahkan jika hanya ada satu aliran transmisi. Ini disebut sebagai keragaman spasial. Misalnya, rantai radio 2x2:2 dan 2x3:2 memiliki throughput yang sama, tetapi rantai 2x3:2 dapat lebih memanfaatkan keragaman spasial untuk meningkatkan jangkauan.

Produk 802.11n juga dapat menggunakan saluran di pita 2,4 GHz atau pita 5 GHz. 802.11n juga memungkinkan dua saluran 20 MHz yang berdekatan untuk digabungkan menjadi satu saluran 40 MHz, yang disebut sebagai ikatan saluran. Karena bandwidth terbatas 2,4 GHz, pada jaringan dengan beberapa AP, ikatan saluran adalah pilihan praktis hanya di pita 5 GHz. Pita 5 GHz memiliki rentang frekuensi yang lebih besar (hingga 500 MHz di AS), sehingga dapat menyediakan hingga 23 saluran yang tidak tumpang tindih. Namun, saluran tersebut tidak selalu bersebelahan, yang sedikit mengurangi opsi untuk saluran berikat.



Opsi saluran berikat di sub-band 5 GHz Unlicensed National Information Infrastructure (U-NII). Saluran dalam jangkauan DFS dapat dinonaktifkan jika lokasi berada di dekat pemancar radar.

Tips: Adaptor klien yang lebih murah mungkin hanya mendukung pita 2,4 GHz. *access point* (AP) atau adaptor yang dapat mendukung keduanya disebut sebagai dual band. AP dual band dapat mendukung band 2,4 GHz dan 5 GHz secara bersamaan. Ini memungkinkan klien lawas dialokasikan ke pita 2,4 GHz.

Kecepatan data untuk 802.11n adalah 72 Mbps per aliran. Dengan asumsi jumlah maksimum empat aliran spasial dan kondisi optimal, kecepatan data nominal dapat mencapai 600 Mbps untuk saluran berikat 40 MHz. 802.11n dapat bekerja dalam mode High Throughput (HT)/greenfield untuk kinerja maksimum atau mode campuran HT untuk kompatibilitas dengan standar yang lebih lama (801.11a-ht, 802.11b-ht, dan

802.11g-ht). Mode campuran mengurangi kinerja WLAN secara keseluruhan, karena melibatkan transmisi identifikasi warisan dan bingkai penghindaran tabrakan (perlindungan HT) tetapi tidak sejauh perangkat 802.11n dikurangi menjadi (katakanlah) kecepatan data 802.11g. Beroperasi dalam mode greenfield kemungkinan besar akan menyebabkan gangguan yang berarti jika ada WLAN lama yang beroperasi di sekitar saluran yang sama. Ada juga mode lama (non-HT), di mana mekanisme HT 802.11n dinonaktifkan sepenuhnya. Anda dapat menggunakan mode ini jika Anda memiliki titik akses berkemampuan 802.11n tetapi tidak memiliki perangkat klien 802.11n.

Dalam beberapa tahun terakhir, standar Wi-Fi telah diganti namanya dengan angka digit yang lebih sederhana. 802.11n sekarang secara resmi ditetapkan sebagai Wi-Fi 4.

- Wi-Fi 5 dan Wi-Fi 6
  Standar Wi-Fi 5 (atau 802.11ac) dan Wi-Fi 6 (802.11ax) melanjutkan pengembangan teknologi Wi-Fi untuk meningkatkan bandwidth dan mendukung jaringan modern.

  - Wi-Fi 5 (802.11ac)
    Wi-Fi 5 dirancang untuk bekerja hanya di pita 5 GHz. Pita 2,4 GHz dapat digunakan untuk standar lama (802,11g/n) dalam mode campuran. Tujuan Wi-Fi 5 adalah untuk mendapatkan throughput seperti Gigabit Ethernet atau lebih baik. Ini mendukung lebih banyak ikatan saluran (hingga saluran 80 atau 160 MHz), hingga 8 aliran spasial, daripada 4, dan modulasi yang lebih padat (pada jarak dekat). Cara Wi-Fi 5 menggunakan spektrum radio ditetapkan sebagai throughput sangat tinggi (VHT).

    Seperti 802.11n, hanya peralatan kelas perusahaan yang dilengkapi dengan antena yang cukup untuk menggunakan tiga aliran atau lebih, dan tidak ada perangkat yang pernah diproduksi dengan aliran lebih dari 4x4:4. Titik akses Wi-Fi 5 dipasarkan menggunakan nilai AC, seperti AC5300. Nilai 5300 mewakili 1000 Mbps melalui saluran pita 40 MHz 2,4 GHz dan dua aliran 2.167 Mbps melalui saluran pita 80 MHz 5 GHz.

  - Wi-Fi 6 (802.11ax)
    Wi-Fi 6 menggunakan modulasi dan penyandian sinyal yang lebih kompleks untuk meningkatkan jumlah data yang dikirim per paket sekitar 40%. Seperti Wi-Fi 5, produk diberi merek menggunakan throughput gabungan. Misalnya, AX6000 memungkinkan 1.148 Mbps pada radio 2,4 GHz dan 4.804 di atas 5 GHz.

    Cara Wi-Fi 6 menggunakan spektrum radio ditetapkan sebagai *high efficiency* (HE) untuk mencerminkan peningkatan ini. Tujuan Wi-Fi 6 adalah untuk memperkirakan kecepatan koneksi 10G (AX11000). Kecepatan data ini hanya dapat dicapai melalui penggunaan pita frekuensi 6 GHz yang baru.

Wi-Fi 6 memulihkan pengoperasian di pita 2,4 GHz, sebagian besar untuk mendukung konektivitas perangkat *Internet of Things* (IoT). Dalam Wi-Fi 6, skema modulasi *OFDM with multiple access* (OFDMA) memungkinkan sub-carrier atau nada dialokasikan dalam kelompok dengan ukuran berbeda, yang disebut sebagai unit sumber daya (RU), yang masing-masing dapat berkomunikasi secara paralel. Di mana RU kecil digunakan, ini mengurangi throughput tetapi memberikan lebih banyak peluang untuk jumlah perangkat yang lebih besar untuk ditransmisikan. Efeknya adalah untuk mengurangi latensi di mana banyak paket data kecil sedang ditransmisikan. Teknologi ini memberikan dukungan yang lebih baik untuk perangkat IoT. Stasiun yang membutuhkan lebih banyak bandwidth dapat diberikan RU yang lebih besar. RU juga dapat ditetapkan berdasarkan kelas parameter layanan, seperti memprioritaskan lalu lintas *voice over IP* (VoIP). Ini juga memungkinkan titik akses untuk mendukung warisan (stasiun Wi-Fi 4/5) secara efisien.

- MIMO multi-pengguna
  Dalam mode operasi 802.11 dasar, bandwidth dibagi antara semua stasiun karena protokol pertentangan CSMA/CA. Sebuah AP dapat berkomunikasi hanya dengan satu stasiun pada satu waktu; beberapa permintaan stasiun masuk ke antrian. Produk Wi-Fi 5 dan Wi-Fi 6 mengatasi masalah ini menggunakan beamforming atau *Multiuser MIMO* (MU-MIMO).

  Downlink MU-MIMO (DL MU-MIMO) memungkinkan AP menggunakan beberapa antenanya untuk memproses aliran spasial sinyal dalam satu arah secara terpisah ke aliran lainnya. Ini berarti bahwa grup stasiun pada alinyemen yang berbeda dapat terhubung secara bersamaan dan juga mendapatkan bandwidth yang lebih besar. Misalnya, jika empat stasiun diposisikan di utara, selatan, timur, dan barat dari AP 4x4:4, AP tersebut harus dapat memungkinkan masing-masing stasiun untuk terhubung mendekati kecepatan maksimum. Jika stasiun lain ditambahkan ke utara, kedua stasiun utara itu akan berbagi bandwidth yang tersedia di sepanjang jalur pancaran itu. Baik stasiun maupun AP harus mendukung MU-MIMO. Jika Wi-Fi 5 mendukung hingga empat stasiun yang berkomunikasi secara paralel hanya di atas 5 GHz, Wi-Fi 6 dapat mendukung hingga delapan di pita 2,4 GHz, 5 GHz, dan 6 GHz, sehingga memberikan kinerja yang lebih baik di area yang padat.

  Dengan DL MU-MIMO, hanya AP yang dapat memulai beamforming, sehingga hanya tersedia pada downlink dari AP ke stasiun (bukan stasiun ke AP). Wi-Fi 6 mendukung *uplink MU-MIMO* (UL MU-MIMO), memungkinkan stasiun untuk memulai *beamforming* dengan titik akses.

  Tips: Untuk *Wi-Fi* 5 dan Wi-Fi 6, peningkatan dirilis ke pasar secara bertahap. Misalnya, UL MU-MIMO dirilis dalam produk Wi-Fi 6 gelombang 2, yang juga menambahkan dukungan untuk pita frekuensi 6 GHz.

Tips: MU-MIMO dan OFDMA adalah teknologi yang berbeda namun saling melengkapi. MU-MIMO memanfaatkan aliran spasial, di mana OFDMA menggunakan subcarrier secara fleksibel di dalam saluran. Keduanya dapat bekerja sama untuk meningkatkan paralelisme (mendukung komunikasi dengan lebih banyak perangkat secara bersamaan).

- Teknologi Seluler 2G dan 3G
  Di mana Wi-Fi biasanya dioperasikan sebagai infrastruktur pribadi, radio seluler dioperasikan oleh penyedia telekomunikasi. Radio seluler membuat koneksi menggunakan sel atau stasiun pangkalan terdekat yang tersedia. Setiap base station memiliki jangkauan efektif hingga 5 mil (8 km). Stasiun pangkalan menghubungkan perangkat ke jaringan telekomunikasi global. Radio seluler bekerja di pita frekuensi 850 dan 1900 MHz (kebanyakan di Amerika) dan pita 900 dan 1800 MHz (di seluruh dunia).

  Standar komunikasi digital seluler digambarkan sebagai milik satu generasi. Untuk 2G, ada dua format bersaing, didirikan di pasar yang berbeda:

  - Telepon berbasis *Global System for Mobile Communication* (GSM) menggunakan *Time Division Multiple Access* (TDMA). Dengan TDMA, setiap pelanggan mendapatkan akses ke saluran radio dengan dialokasikan slot waktu. GSM memungkinkan pelanggan untuk menggunakan kartu modul identitas pelanggan (SIM) untuk menggunakan handset yang tidak terkunci dengan penyedia jaringan yang mereka pilih. GSM diadopsi secara internasional dan oleh AT-and-T dan T-Mobile di Amerika Serikat.

  - Handset berbasis TIA/EIA IS-95 (cdmaOne), menggunakan *Code Division Multiple Access* (CDMA). CDMA berarti bahwa setiap pelanggan menggunakan kode untuk memasukkan modulasi sinyal mereka dan "kunci" ini digunakan oleh penerima untuk mengekstrak lalu lintas pelanggan dari saluran radio. Dengan CDMA, handset dikelola oleh provider, bukan SIM. Adopsi CDMA sebagian besar terbatas pada penyedia telekomunikasi Sprint dan Verizon. Dalam kedua kasus, jaringan seluler dibangun terutama untuk mendukung panggilan suara, sehingga akses data 2G disediakan di atas, menggunakan *Circuit Switched Data* (CSD). CSD agak mirip dengan modem dial-up, meskipun tidak ada transmisi analog yang terlibat. CSD memerlukan koneksi data yang akan dibuat ke stasiun pangkalan (dikenakan biaya panggilan) dan hanya mampu sekitar 14,4 Kbps.

    Transisi dari 2G ke 3G melihat berbagai teknologi packet-switched dikerahkan ke ponsel:

  - *General Packet Radio Services/Enhanced Data Rates for GSM Evolution* (GPRS/EDGE) adalah pendahulu dari 3G (2.5G), dengan GPRS menawarkan hingga sekitar 48 Kbps dan EDGE sekitar 3-4 kali lipat. Tidak seperti CSD, GPRS dan EDGE memungkinkan koneksi data "selalu aktif", dengan

penggunaan yang ditagih berdasarkan konsumsi bandwidth daripada waktu koneksi.

- *Evolved High Speed Packet Access* (HSPA+) adalah standar 3G yang dikembangkan melalui beberapa iterasi dari Universal Mobile Telecommunications System (UMTS) yang digunakan pada jaringan GSM. HSPA+ secara nominal mendukung kecepatan unduh hingga 168 Mbps dan kecepatan unggah hingga 34 Mbps. Layanan berbasis HSPA+ sering dipasarkan sebagai 4G jika kecepatan data nominalnya lebih baik dari sekitar 20 Mbps.

  Perhatikan bahwa dengan HSPA, teknologi akses saluran TDMA telah ditinggalkan dan jenis CDMA digunakan.

- *CDMA2000/Evolution Data Optimized* (EV-DO) adalah standar 3G utama yang digunakan oleh penyedia jaringan CDMA. EV-DO dapat mendukung downlink 3,1 Mbps dan uplink 1,8 Mbps.

- Teknologi Seluler 4G dan 5G
  Pengganti jaringan 3G telah melihat konvergensi pada satu set standar dunia.

  - 4G/Evolusi Jangka Panjang
    Long Term Evolution (LTE) adalah standar 4G terkonvergensi yang didukung oleh penyedia jaringan GSM dan CDMA. Perangkat LTE harus memiliki kartu SIM yang dikeluarkan oleh penyedia jaringan yang terpasang. LTE memiliki downlink maksimum 150 Mbps secara teori, tetapi tidak ada jaringan penyedia yang dapat memberikan kecepatan seperti itu pada saat penulisan, dengan sekitar 20 Mbps jauh lebih khas dari kinerja kata nyata.

  Tips: LTE tidak menggunakan TDMA atau CDMA tetapi *Orthogonal Frequency Division Multiple Access* (OFDMA), yang juga digunakan oleh Wi-Fi 6.

  LTE Advanced (LTE-A) dimaksudkan untuk menyediakan downlink 300 Mbps, tetapi sekali lagi aspirasi ini tidak diimbangi dengan kinerja dunia nyata. Performa tipikal saat ini untuk LTE-A adalah hingga 90 Mbps.

  - 5G
    Menurut spesifikasi aslinya, layanan 4G seharusnya memberikan 1 Gbps untuk pengguna yang tidak bergerak atau bergerak lambat (termasuk pejalan kaki) dan 100 Mbps untuk akses dari kendaraan yang bergerak cepat. Kecepatan data tersebut sekarang menjadi standar minimum yang diharapkan untuk 5G. Seperti halnya 4G, kecepatan dunia nyata sama sekali tidak mendekati batas minimum yang diharapkan, mulai dari sekitar 50 Mbps hingga 300 Mbps pada saat penulisan.

5G menggunakan pita spektrum yang berbeda dari rendah (sub-6 GHz) hingga menengah/tinggi (20-60 GHz). Pita rendah memiliki jangkauan dan daya tembus yang lebih besar; pita tinggi, juga disebut sebagai millimeter wave (mmWave) membutuhkan jarak dekat (beberapa ratus kaki) dan tidak dapat menembus dinding atau jendela. Akibatnya, desain dan peluncuran layanan 5G relatif kompleks. Daripada satu antena besar yang melayani sel nirkabel besar, 5G melibatkan pemasangan ratusan antena yang lebih kecil untuk membentuk array yang dapat memanfaatkan multipath dan beamforming untuk mengatasi keterbatasan propagasi spektrum. Ini juga disebut sebagai MIMO masif. Selain kecepatan seluler yang lebih cepat, 5G diharapkan memberikan solusi broadband nirkabel tetap untuk rumah dan bisnis, dan untuk mendukung jaringan IoT.

Install Wireless Networks

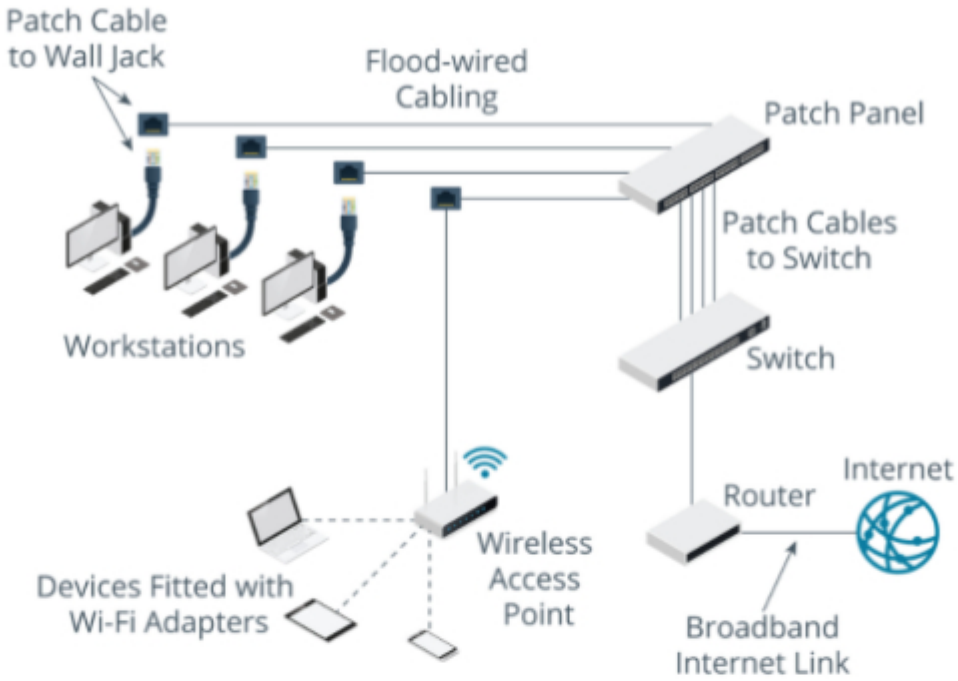
- Pendahuluan: Instal Jaringan Nirkabel
  Merancang jaringan nirkabel untuk memenuhi persyaratan untuk mendukung berbagai jenis perangkat dapat menjadi tugas yang kompleks. Merencanakan pemasangan menggunakan alat survey dapat memastikan bahwa masalah jangkauan dan interferensi diperhitungkan sejak awal, dan tidak menjadi masalah dukungan di kemudian hari.

- Topologi Infrastruktur dan Titik Akses Nirkabel
  Perangkat jaringan nirkabel disebut sebagai *stations* (STA), mirip dengan node pada jaringan kabel. Sebagian besar jaringan nirkabel digunakan dalam topologi infrastruktur. Dalam topologi infrastruktur, setiap stasiun dikonfigurasi untuk terhubung melalui stasiun pangkalan atau *access point* (AP), membentuk topologi bintang logis. AP menengahi komunikasi antara perangkat klien dan juga dapat menyediakan jembatan ke segmen jaringan kabel. Dalam dokumentasi 802.11, ini disebut sebagai *Basic Service Set* (BSS) infrastruktur. Alamat MAC dari AP digunakan sebagai *Basic Service Set Identifier* (BSSID). Lebih dari satu BSS dapat dikelompokkan bersama dalam *Extended Service Set* (ESS).



Access point. (Image © 123RF.com.)

Setiap stasiun klien memerlukan adaptor nirkabel yang kompatibel dengan standar yang didukung oleh *Access point*.



Konfigurasi WLAN dalam mode infrastruktur. (Images © 123RF.com.)

- Desain Situs Nirkabel
  Klien dikonfigurasi untuk bergabung dengan WLAN melalui nama jaringan atau *Service Set Identifier* (SSID). Panjang SSID dapat mencapai 32 byte dan untuk kompatibilitas maksimum hanya boleh menggunakan huruf dan angka ASCII ditambah karakter tanda hubung dan garis bawah. Dalam mode infrastruktur, ketika beberapa AP yang terhubung ke sistem distribusi yang sama dikelompokkan menjadi ESS, ini lebih tepat disebut *Extended SSID* (ESSID). Ini hanya berarti bahwa semua AP dikonfigurasi dengan SSID dan informasi keamanan yang sama. Area yang dilayani oleh satu AP disebut sebagai *basic service area* (BSA) atau sel nirkabel. Area dimana stasiun dapat menjelajah antara titik akses untuk tetap terhubung ke ESSID yang sama disebut sebagai *extended service area* (ESA).

    - Siaran SSID dan Bingkai Suar
      WLAN biasanya dikonfigurasi untuk mengiklankan keberadaannya dengan menyiarkan SSID. Hal ini memungkinkan pengguna untuk terhubung ke jaringan bernama. Jika siaran SSID ditekan, pengguna harus mengkonfigurasi koneksi ke jaringan secara manual. Beacon adalah bingkai manajemen khusus yang disiarkan oleh AP untuk mengiklankan WLAN. Bingkai suar berisi SSID (kecuali siaran dinonaktifkan), kecepatan data dan pensinyalan yang didukung, ditambah persyaratan enkripsi/otentikasi. Interval saat beacon disiarkan (diukur dalam milidetik) dapat dimodifikasi. Standarnya biasanya 100 ms. Meningkatkan interval mengurangi overhead penyiaran frame tetapi penundaan bergabung dengan jaringan dan dapat menghambat roaming antara AP.
-

Tips: Bahkan jika siaran SSID ditekan, cukup mudah bagi sniffer jaringan untuk mendeteksinya karena klien masih menggunakannya saat menghubungkan dengan AP.

- Persyaratan Kecepatan dan Jarak
  Perangkat yang mendukung standar Wi-Fi harus memiliki jangkauan dalam ruangan minimal 30 m (100 kaki). Radio 2,4 GHz mendukung rentang yang lebih baik daripada radio 5 GHz dan standar 802.11n dan yang lebih baru meningkatkan jangkauan dibandingkan dengan standar sebelumnya. Jangkauan luar ruangan dapat berupa jangkauan dalam ruangan ganda atau tiga kali lipat. Setiap stasiun menentukan kecepatan data yang sesuai berdasarkan kualitas sinyal menggunakan mekanisme yang disebut *Dynamic Rate Switching/Selection* (DRS). Jika sinyal kuat, stasiun akan memilih kecepatan data tertinggi yang tersedia (ditentukan oleh standar 802.11); jika sinyal lemah, stasiun akan mengurangi kecepatan data.

  Sinyal radio melewati benda padat, seperti dinding bata atau drywall biasa, tetapi dapat dilemahkan atau terhalang oleh dinding yang sangat tebal atau beton padat atau konstruksi logam. Perangkat berbasis radio lainnya juga dapat menyebabkan gangguan seperti halnya perangkat seperti lampu neon, oven microwave, telepon nirkabel, dan (dalam lingkungan industri), motor listrik dan mesin berat. Bluetooth menggunakan rentang frekuensi 2,4 GHz tetapi teknik modulasi yang berbeda, sehingga interferensi mungkin terjadi tetapi tidak umum.

  Akibatnya, serangkaian faktor yang kompleks perlu dipertimbangkan ketika Anda merencanakan jaringan nirkabel. Survei lokasi adalah alat perencanaan penting untuk memastikan bahwa WLAN memberikan kecepatan data yang dapat diterima ke jumlah perangkat yang didukung di semua lokasi fisik yang diharapkan.

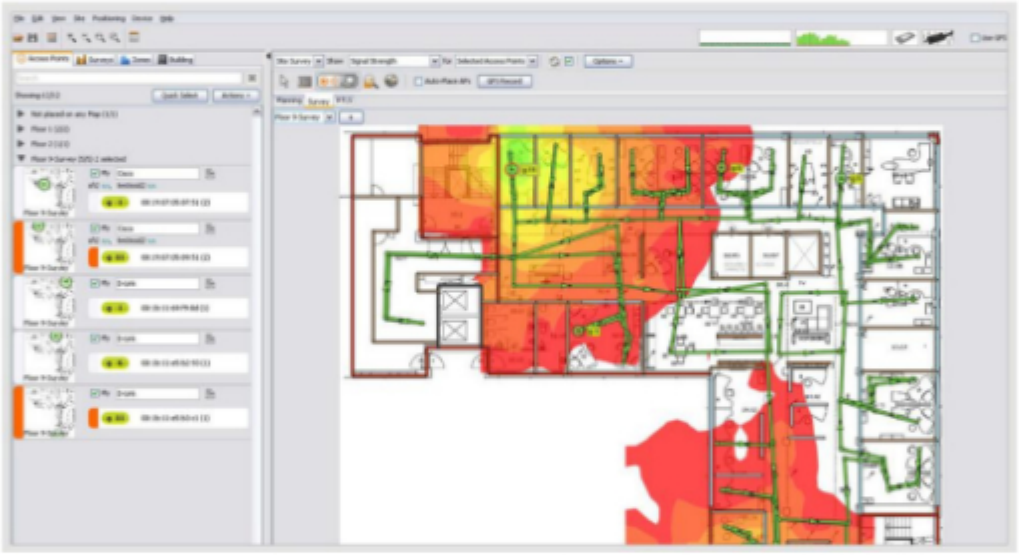
- Site Surveys and Heat Maps
  Survei lokasi dilakukan pertama dengan memeriksa cetak biru atau denah bangunan untuk memahami tata letak dan mengidentifikasi fitur yang mungkin menghasilkan *radio frequency interference* (RFI). Ini dapat didukung oleh inspeksi visual yang dapat mengungkapkan hal-hal yang tidak ditampilkan pada cetak biru, seperti rak logam tebal yang mengelilingi ruangan yang perlu memiliki akses WLAN. Setiap titik pemasangan AP membutuhkan port jaringan dan colokan listrik, sehingga akan membantu untuk mendapatkan rencana yang menunjukkan lokasi port yang tersedia.

  Tips: Sakelar yang mendukung *Power over Ethernet* (PoE) dapat digunakan untuk memberi daya pada AP yang kompatibel dengan PoE.

  Langkah selanjutnya adalah membuat rencana baru di mana Anda akan menandai sel WLAN dan AP terkait serta antenna booster. Idenya di sini adalah untuk menempatkan AP cukup dekat satu sama lain untuk menghindari "zona mati" - area di mana

konektivitas sulit atau kecepatan transfer data di bawah tingkat toleransi yang dapat diterima - tetapi cukup jauh sehingga satu AP tidak mengganggu yang lain atau yang satu AP dimanfaatkan secara berlebihan dan yang di dekatnya kurang dimanfaatkan.

Posisikan AP di lokasi yang direncanakan terlebih dahulu, kemudian gunakan laptop dengan adaptor nirkabel dan alat survey nirkabel, seperti Cisco Aironet, Metageek inSSIDer, atau Survei Situs Ekahau, untuk merekam kekuatan sinyal dan kecepatan data yang didukung di berbagai titik di tujuan *basic service area* (BSA). Banyak alat dapat menunjukkan kekuatan sinyal dalam saluran tertentu yang diperoleh di lokasi yang berbeda secara grafis menggunakan peta panas. Peta panas akan menunjukkan area dengan sinyal kuat dalam warna hijau dan kuning dengan peringatan oranye dan merah di mana kekuatan sinyal menurun. Langkah ini kemudian diulang untuk setiap lokasi yang direncanakan. AP tetangga harus dikonfigurasi dengan saluran yang tidak tumpang tindih untuk menghindari gangguan satu sama lain. Mungkin juga perlu untuk menyesuaikan daya pancar dari AP untuk mengukur BSA dengan tepat.



Heat map generated by Ekahau Site Survey. (Image © Ekahau Inc.)

- Roaming dan Menjembatani Nirkabel
  Klien dapat menjelajah dalam *extended service area* (ESA). ESA dibuat dengan menginstal AP dengan SSID yang sama dan konfigurasi keamanan yang dihubungkan oleh jaringan kabel, atau *Distribution System* (DS). Titik akses dikonfigurasi dengan saluran yang berbeda sehingga dimana BSA tumpang tindih, tidak ada gangguan. Ketika klien mendeteksi bahwa ia tidak lagi menerima sinyal yang baik, ia memeriksa sinyal lain dengan SSID yang sama di saluran lain atau pada pita frekuensi yang berbeda, dan jika ada sinyal yang lebih kuat, ia akan memutuskan sambungan dari AP saat ini. Stasiun kemudian dapat mengasosiasikan kembali dengan AP baru. Tergantung pada infrastruktur roaming dan jenis keamanan, stasiun mungkin harus mengautentikasi

ulang, atau jika roaming cepat 802.11r didukung, stasiun mungkin dapat menggunakan status autentikasi yang ada untuk menghasilkan properti keamanan untuk asosiasi baru.

Roaming seharusnya mulus, tetapi dalam praktiknya membangun kembali koneksi sering kali dapat menyebabkan masalah waktu habis untuk aplikasi. Untuk meningkatkan mobilitas, perlu ada keseimbangan antara menentukan apa yang merupakan sinyal "baik" dan frekuensi yang klien coba kaitkan dengan AP yang berbeda. Banyak adaptor mendukung pengaturan "agresivitas" roaming yang dapat dikonfigurasi untuk mencegah adaptor Wi-Fi "mengepak" antara dua AP atau (sebaliknya) untuk mencegah klien tetap terkait dengan AP yang lebih jauh ketika itu bisa mencapai bandwidth yang lebih baik melalui satu lebih dekat untuk itu.

Anda juga dapat mengkonfigurasi beberapa titik akses untuk mencakup area yang tidak memungkinkan untuk menjalankan kabel. Ini disebut sebagai sistem distribusi nirkabel (WDS). Anda harus mengatur AP untuk menggunakan saluran, SSID, dan parameter keamanan yang sama. AP dikonfigurasi dalam mode WDS/repeater. Satu AP dikonfigurasi sebagai stasiun pangkalan, sementara yang lain dikonfigurasi sebagai stasiun jarak jauh. Stasiun pangkalan dapat dihubungkan ke segmen kabel. Stasiun jarak jauh tidak boleh terhubung ke segmen kabel. Stasiun jarak jauh dapat menerima koneksi dari stasiun nirkabel dan meneruskan semua lalu lintas ke stasiun pangkalan.

Penggunaan lain untuk WDS adalah untuk menjembatani dua segmen kabel yang terpisah. Ketika WDS dikonfigurasi dalam mode bridge, AP tidak akan mendukung klien nirkabel; mereka hanya meneruskan lalu lintas antara segmen kabel.

Tips: Dukungan dan implementasi WDS dapat bervariasi antar produsen. Jika Anda menerapkan WDS, biasanya yang terbaik adalah menggunakan AP dari vendor yang sama.

- Pengontrol LAN Nirkabel
  Jaringan perusahaan mungkin memerlukan penggunaan puluhan atau ratusan titik akses. Jika AP dikelola secara individual, ini dapat menyebabkan kesalahan konfigurasi pada AP tertentu dan dapat mempersulit untuk mendapatkan tampilan keseluruhan dari penerapan nirkabel, termasuk klien mana yang terhubung ke AP dan klien atau AP mana yang menghasilkan lalu lintas paling banyak.



Pengontrol nirkabel, alat tingkat perusahaan yang mampu mendukung hingga 1500 AP dan 20.000 klien. (Image © 123RF.com.)

Daripada mengkonfigurasi setiap perangkat secara individual, solusi nirkabel perusahaan seperti yang diproduksi oleh Cisco, Ruckus, atau Ubiquiti memungkinkan manajemen terpusat dan pemantauan AP di jaringan. Ini dapat dicapai melalui penggunaan perangkat keras khusus yang disebut pengontrol LAN nirkabel. Atau, beberapa implementasi menggunakan aplikasi perangkat lunak untuk memusatkan fungsi manajemen, yang dapat dijalankan di server atau workstation.

AP yang firmwarenya berisi logika pemrosesan yang cukup untuk dapat berfungsi secara mandiri dan menangani klien tanpa menggunakan pengontrol nirkabel dikenal sebagai AP gemuk, sedangkan AP yang membutuhkan pengontrol nirkabel agar berfungsi dikenal sebagai AP tipis. Kontroler nirkabel Cisco biasanya berkomunikasi dengan AP dengan menggunakan *Lightweight Access Point Protocol* (LWAPP). LWAPP memungkinkan AP yang dikonfigurasi untuk bekerja dalam mode ringan untuk mengunduh SSID, mode standar, saluran, dan konfigurasi keamanan yang sesuai. Alternatif untuk LWAPP termasuk protokol turunan *Control And Provisioning of Wireless Access Points* (CAPWAP) atau protokol berpemilik.

Selain mengkonfigurasi peralatan secara otomatis, pengontrol nirkabel dapat menggabungkan lalu lintas klien dan menyediakan titik peralihan dan perutean pusat antara WLAN dan LAN kabel. Itu juga dapat menetapkan klien untuk memisahkan VLAN. Penggabungan VLAN otomatis memastikan bahwa jumlah total stasiun per VLAN disimpan dalam batas yang ditentukan, mengurangi lalu lintas siaran yang berlebihan. Fungsi lainnya adalah untuk memasok daya ke titik akses kabel, menggunakan *Power over Ethernet* (PoE).

- Topologi Ad Hoc dan Mesh
  Sementara sebagian besar jaringan korporat dan banyak SOHO dikonfigurasi dalam mode infrastruktur, ada juga topologi nirkabel yang memungkinkan stasiun membuat tautan peer-to-peer.

    - Topologi Ad Hoc
      Dalam topologi ad hoc, adaptor nirkabel memungkinkan koneksi ke dan dari perangkat lain. Dalam dokumentasi 802.11, ini disebut sebagai Independent Basic Service Set (IBSS). Topologi ini tidak memerlukan access point. Semua stasiun dalam jaringan ad hoc harus berada dalam jangkauan satu sama lain. Jaringan ad hoc mungkin sesuai dengan kelompok kerja kecil perangkat, atau konektivitas ke satu perangkat, seperti printer bersama, tetapi tidak dapat diskalakan untuk implementasi jaringan besar.

  Tips: IBSS tidak didukung oleh model driver WDI yang diperbarui di versi terbaru Windows (docs.microsoft.com/en-us/windows-hardware/drivers/network/wdi-features-not-carried-over-in-wdi).

    - Topologi Mesh
      Standar 802.11s mendefinisikan *Wireless Mesh Network* (WMN). Ada juga berbagai protokol dan produk mesh berpemilik. Tidak seperti jaringan ad hoc, node dalam WMN (disebut stasiun mesh) mampu menemukan satu sama lain dan mengintip, membentuk *Mesh Basic Service Set* (MBSS). Stasiun mesh dapat melakukan penemuan jalur dan penerusan antar peer menggunakan protokol perutean, seperti *Hybrid Wireless Mesh Protocol* (HWMP).

      Fitur-fitur ini membuat topologi mesh lebih terukur daripada topologi ad hoc karena stasiun tidak perlu berada dalam jangkauan radio langsung satu sama lain - transmisi dapat diteruskan oleh stasiun perantara. Topologi mesh menjadi semakin populer dan merupakan dasar dari sebagian besar jaringan *Internet of Things* (IoT).

Memecahkan Masalah Jaringan Nirkabel

- Pendahuluan: Memecahkan Masalah Jaringan Nirkabel
  Beberapa lingkungan dan tuntutan kinerja dapat mempersulit penyebaran jaringan nirkabel. Berbagai alat dan teknik tersedia untuk menilai kinerja Wi-Fi dan memastikan jaringan yang sangat tersedia untuk semua pengguna.

- Penilaian Kinerja Nirkabel
  Masalah nirkabel dapat secara luas dibagi menjadi masalah dengan kekuatan sinyal atau gangguan (seperti masalah pemasangan kabel di LAN kabel) dan masalah konfigurasi. Topik ini berfokus pada masalah yang memengaruhi kekuatan dan kinerja sinyal, tetapi selalu periksa apakah parameter keamanan dan otentikasi dikonfigurasi

dengan benar sebelum menganggap Anda memiliki masalah konektivitas lapisan fisik. Masalah konfigurasi dibahas dalam topik berikutnya.

Seperti halnya jaringan kabel, Anda harus membedakan antara kecepatan dan throughput saat mengukur dan menilai kinerja nirkabel terhadap spesifikasi dan batasan standar Wi-Fi tertentu:

- Kecepatan adalah kecepatan data yang ditetapkan pada lapisan fisik dan tautan data. Kecepatan tautan nominal ditentukan oleh dukungan standar (Wi-Fi 5 atau Wi-Fi 6, misalnya), penggunaan saluran berikat, dan pengoptimalan, seperti MU-MIMO. Jika pengirim dan penerima berjauhan atau mengalami gangguan, tarif yang lebih rendah akan dinegosiasikan untuk membuat tautan lebih andal.

- *Throughput* adalah jumlah data yang dapat ditransfer pada lapisan jaringan, membuang overhead dari lapisan 1 dan 2. Seringkali istilah goodput digunakan untuk menggambarkan transfer data yang dicapai pada lapisan aplikasi (memperhitungkan overhead dari bidang header dan packet loss/retransmisi).

Seperti halnya pemasangan kabel, atenuasi mengacu pada melemahnya sinyal karena jarak antar perangkat meningkat. Ini dapat digambarkan lebih tepat sebagai redaman frekuensi radio (RF) atau kehilangan jalur ruang bebas. Dengan bertambahnya jarak dari antena, kekuatan sinyal berkurang sesuai dengan aturan kuadrat terbalik. Misalnya, menggandakan jarak mengurangi kekuatan sinyal dengan faktor empat. Sementara itu, sumber interferensi secara kolektif melapisi sinyal latar belakang yang bersaing, yang disebut sebagai noise. Faktor-faktor ini memaksakan batasan jarak pada seberapa jauh klien dapat dari titik akses.

Atenuasi dan kekuatan sinyal diukur dalam desibel. Kekuatan sinyal direpresentasikan sebagai rasio pengukuran terhadap 1 miliwatt (mw), di mana 1 mW sama dengan 0 dBm. Unit dB dan dBm dapat digabungkan untuk menganalisis kerugian dan keuntungan dalam kekuatan sinyal di sepanjang jalur komunikasi. Misalnya, jika Anda mengirimkan sinyal radio pada 1 mW dan menggunakan antena untuk meningkatkan sinyal, daya efektifnya adalah:

0 dBm + 3 dB = 2 mW = ~3 dBm

Sebaliknya, kerugian dB karena redaman atau kebisingan berarti hilangnya daya/kekuatan sinyal:

3 dBm – 1 dB = 2 dBm = ~1,58 mW

Karena 0 dBm adalah 1 mW, nilai negatif untuk dBm mewakili sebagian kecil dari miliwatt. Misalnya, -30 dBm adalah 0,001 mW; -60 dBm adalah 0,000001 mW.

Perangkat Wi-Fi semuanya dibatasi oleh peraturan yang mengatur penggunaan spektrum dan hanya mengeluarkan daya dalam jumlah kecil.

- Kekuatan sinyal
  Received Signal Strength Indicator (RSSI) adalah kekuatan sinyal dari pemancar di ujung klien. Saat Anda mengukur RSSI, dBm akan menjadi nilai negatif (sebagian milliwatt) dengan nilai yang mendekati nol menunjukkan kinerja yang lebih baik. Nilai sekitar - 65 dBm menunjukkan sinyal yang baik, sedangkan nilai di atas -80 dBm kemungkinan besar akan mengalami kehilangan paket atau terputus. RSSI harus melebihi sensitivitas penerima minimum.

  Tergantung pada vendornya, RSSI dapat diukur secara langsung dalam dBm atau mungkin berupa nilai indeks yang terkait dengan skala pengukuran dBm. Indeks RSSI dapat diukur sebagai 0-60, 0-127, atau sebagai 0-255. Pada klien, indeks ini ditampilkan sebagai sejumlah bar kekuatan sinyal pada ikon adaptor.

  Perbandingan kekuatan sinyal data dengan kebisingan latar belakang disebut *Signal-To-Noise Ratio* (SNR). Kebisingan juga diukur dalam dBm, tetapi di sini nilai yang mendekati nol kurang diterima karena mewakili tingkat kebisingan yang lebih tinggi. Misalnya, jika sinyal 65 dBm dan noise 90 dBm, SNR adalah selisih antara dua nilai, yang dinyatakan dalam dB (25 dB). Jika kebisingan -80 dBm, SNR adalah 15 dB dan koneksi akan jauh lebih buruk.

  RSSI dan SNR dapat diukur dengan menggunakan penganalisis Wi-Fi. Software jenis ini bisa di install di laptop atau smartphone. Ini akan merekam statistik untuk AP yang saat ini dikaitkan dengan klien dan mendeteksi titik akses lain di sekitarnya.



Survei jaringan Wi-Fi menggunakan inSSIDer. Bagan menunjukkan saluran mana yang aktif dan kekuatan sinyal jaringan yang berbeda di setiap saluran. (Tangkapan layar digunakan dengan izin dari MetaGeek.)

- Jenis Antena
  Jenis antena menentukan pola propagasi atau bentuk gelombang radio yang ditransmisikan. Sebagian besar perangkat nirkabel memiliki antena tipe batang vertikal omnidirectional sederhana, yang menerima dan mengirim sinyal ke segala arah kurang lebih sama. Titik akses dengan antena omnidirectional idealnya dipasang di langit-langit untuk jangkauan terbaik, kecuali jika langit-langitnya sangat tinggi. Pola propagasi berbentuk seperti torus (donat), bukan bola, dan memancar lebih kuat di bidang horizontal daripada di bidang vertikal. Menempatkan antena di atas ketinggian kepala akan meminimalkan gangguan dari penghalang furniture dengan memungkinkan garis pandang ke sebagian besar perangkat penghubung, tetapi memposisikannya terlalu tinggi (di atas sekitar 25 kaki) akan mengurangi kekuatan sinyal, terutama untuk stasiun yang berada tepat di bawah antena. Anda dapat memperoleh AP dengan antena omnidirectional downtilt untuk digunakan di langit-langit tinggi.

  Untuk memperluas sinyal ke area tertentu, Anda dapat menggunakan antena yang terfokus pada satu arah (*unidirectional*). Pengirim dan penerima harus menggunakan antena arah, atau salah satu akan dapat menerima sinyal tetapi tidak mengirim tanggapan. Jenis antena searah termasuk faktor bentuk Yagi (batang dengan sirip) dan parabola (piringan atau kisi). Antena searah berguna untuk koneksi jembatan nirkabel *point-to-point*. Peningkatan kekuatan sinyal yang diperoleh dengan memfokuskan sinyal disebut sebagai gain dan diukur dalam dBi (*decibel isotropic*). Jumlah directionality, disebut sebagai beamwidth, diukur dalam derajat. Sepasang antena 10 derajat sangat

terarah dan akan membutuhkan keselarasan yang lebih tepat daripada sepasang antena 90 derajat.



Berbagai jenis antena generik: dari kiri ke kanan, antena batang vertikal, antena Yagi, antena parabola/parabola, dan antena grid parabola.

Polarisasi mengacu pada orientasi gelombang yang merambat dari antena. Jika Anda membayangkan antena tipe batang, ketika batang mengarah ke atas relatif terhadap lantai, gelombang terpolarisasi secara horizontal; jika Anda mengarahkan batang sejajar dengan lantai, gelombang terpolarisasi vertikal. Untuk memaksimalkan kekuatan sinyal, antena transmisi dan penerima biasanya menggunakan polarisasi yang sama. Hal ini sangat penting ketika menggunakan antena satu arah untuk link point-to-point. Beberapa antena terpolarisasi ganda, artinya antena dapat dipasang di salah satu orientasi. Antena terpolarisasi ganda juga merupakan cara terbaik untuk mendukung perangkat seluler, karena antena ini dapat dipegang oleh penggunanya dalam berbagai orientasi.

- Masalah Cakupan Nirkabel Tidak Memadai
  Cakupan nirkabel yang tidak memadai mengacu pada titik-titik di dalam gedung tanpa atau sinyal Wi-Fi yang lemah. Jika kekuatan sinyal yang cukup tidak dapat diperoleh dan sumber gangguan tidak dapat dikurangi, satu-satunya solusi adalah memasang perangkat tambahan untuk menutupi celah tersebut. Jika Anda tidak dapat memperluas sistem distribusi (jaringan kabel) untuk mendukung titik akses tambahan, Anda perlu mengkonfigurasi jembatan nirkabel atau menggunakan perluasan jangkauan.

    - Penempatan Antena
      Penempatan antena yang salah dapat menyebabkan atau memperburuk masalah redaman dan interferensi. Gunakan survei lokasi dan peta panas untuk menentukan posisi optimal untuk Titik Akses dan (jika tersedia) arah untuk mengarahkan antena yang dapat disesuaikan. Juga, menggunakan jenis antena yang salah dapat mempengaruhi kekuatan sinyal pada titik tertentu. Antena satu arah hanya cocok untuk koneksi point-to-point, bukan untuk akses klien umum. Antena internal yang dibangun ke dalam AP juga dapat dioptimalkan untuk mengirim dan menerima di beberapa arah lebih dari yang lain. Misalnya, Titik Akses yang dirancang untuk pemasangan di langit-langit dapat menghasilkan sinyal yang lebih kuat dalam kerucut yang diarahkan ke bawah dari sumbu pusatnya, sedangkan sinyal dari Titik Akses serupa yang dirancang untuk

pemasangan di dinding lebih cenderung miring ke luar. Lihat dokumentasi untuk model AP spesifik Anda atau gunakan perangkat lunak survei lokasi untuk menghasilkan peta panas.

Tips: Ingatlah bahwa beberapa perangkat klien mungkin mendukung standar seperti 802.11n, tetapi hanya memiliki radio 2,4 GHz pita tunggal. Mereka tidak akan dapat bergabung dengan jaringan 5 GHz.

- Atenuasi Kabel Antena
  Sumber redaman lainnya adalah di mana antena terhubung pada jarak tertentu dari titik akses melalui kabel coax. Kehilangan sinyal di sepanjang kabel ini disebut sebagai redaman kabel antena. Kabel LMR/HDF/CFD 200 memiliki redaman sekitar 0,6 dB/m (decibel per meter), sedangkan kabel 400 meningkatkannya menjadi sekitar 0,22 dB/m. Kehilangan konektor biasanya dihitung sebagai 0,15 dB.

  Tips: Jika perangkat memiliki antena yang dapat dilepas, periksa apakah antena tersebut terpasang dengan benar. Antena yang longgar atau terputus dapat mengurangi jangkauan perangkat atau mencegah konektivitas sama sekali.

- Pengaturan Daya/Daya Terpancar Isotropik yang Efektif
  Daya di mana titik akses mentransmisikan dapat dikonfigurasi. *Effective Isotropic Radiated Power* (EIRP) dihitung sebagai jumlah daya pancar, rugi kabel/konektor antena, dan penguatan antena. Misalnya, jika Anda mengonfigurasi tautan titik-ke-titik dengan antena terarah, Anda mungkin mendapatkan nilai berikut untuk EIRP:

  15 dBm (Transmit Power) – 1 dB (Cable Loss) + 6 dBi (Gain) = 20 dBm (100 mW)

  EIRP untuk setiap radio dilaporkan melalui titik akses atau perangkat lunak manajemen pengontrol. EIRP tidak boleh melebihi batas peraturan. Batas daya berbeda untuk pita 2,4 GHz dan 5 GHz dan untuk mode operasi point-to-multipoint versus point-to-point.

  Meningkatkan daya pancar biasanya bukan merupakan solusi efektif untuk meningkatkan jangkauan nirkabel. Sementara AP mungkin memiliki EIRP sekitar 23 dBm, perangkat smartphone lebih cenderung sekitar 10 hingga 14 dBm. Jika klien mendeteksi sinyal yang kuat, itu akan menetapkan kecepatan data yang tinggi. Namun, karena EIRP radio klien jauh lebih rendah, ia gagal mengirimkan sinyal yang kuat kembali ke AP. Karena mencoba menggunakan kecepatan data yang tinggi, ini menghasilkan kesalahan paket yang berlebihan.

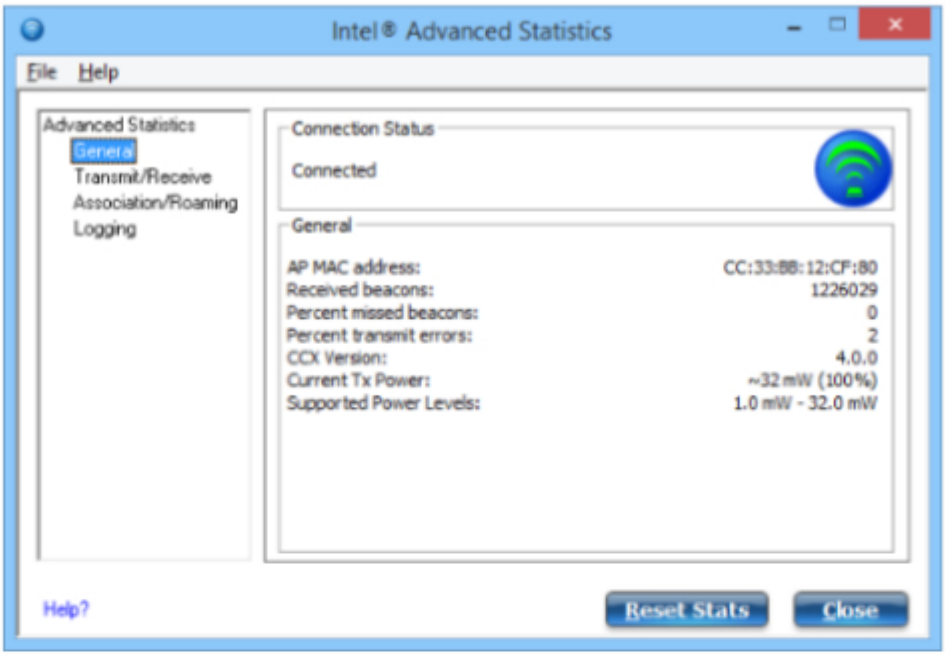
Sebagai aturan umum, daya AP harus 2/3 dari daya klien terlemah. Misalnya, jika klien terlemah dapat menghasilkan 14 dBm, AP harus mentransmisikan pada 9 hingga 10 dBm.

- Pemanfaatan Saluran dan Masalah Tumpang Tindih
  Tumpang tindih saluran mengacu pada masalah interferensi yang dihasilkan dari beberapa titik akses yang semuanya berada dalam jangkauan satu sama lain dan dikonfigurasi untuk menggunakan panjang gelombang yang sama. Ada dua jenis utama gangguan saluran:

  - ***Co-channel interference*** **(CCI)**-Ini dapat lebih akurat digambarkan sebagai pertentangan. Ketika beberapa titik akses menggunakan saluran yang sama, kesempatan untuk mengirimkan berkurang. Perangkat nirkabel harus menggunakan CSMA/CA untuk menemukan peluang transmisi. CCI dapat diukur sebagai persentase yang disebut sebagai pemanfaatan saluran. Utilisasi saluran dapat diukur dari titik akses atau menggunakan penganalisis Wi-Fi. Sebagai tujuan desain, saluran harus menunjukkan pemanfaatan tidak lebih dari 50%.

  - ***Adjacent channel interference*** **(ACI)**-Ini terjadi ketika titik akses dikonfigurasi untuk menggunakan saluran yang berbeda tetapi tumpang tindih, seperti 1 dan 3 di pita 2,4 GHz. ACI memperlambat proses CSMA/CA dan meningkatkan tingkat kebisingan. Salah satu tujuan desain untuk situs multi-AP adalah membuat sel bersih sehingga klien dapat memilih AP dengan sinyal terkuat dengan mudah dan WLAN beroperasi dengan gangguan saluran bersama yang minimum. Setidaknya jarak 25 MHz harus diizinkan untuk menghindari tumpang tindih saluran. Oleh karena itu, dalam praktiknya, tidak lebih dari tiga AP terdekat yang menggunakan pita 2,4 GHz dapat memiliki saluran yang tidak tumpang tindih. Ini dapat diimplementasikan, misalnya, dengan memilih saluran 1 untuk AP1, saluran 6 untuk AP2, dan saluran 11 untuk AP3. Saat Anda menggunakan pita 5 GHz untuk 802.11a atau Wi-Fi 4/5/6, tersedia lebih banyak saluran yang tidak tumpang tindih.

  Dalam lingkungan yang kompleks, mungkin perlu untuk menyesuaikan tingkat daya yang digunakan oleh Titik Akses pada saluran tertentu. Menggunakan daya maksimum yang tersedia pada AP dapat mengakibatkannya mengganggu "sel" lain dan situasi di mana klien dapat "mendengar" AP tetapi tidak dapat "berbicara" dengannya karena tidak memiliki daya yang cukup.



Memeriksa tingkat daya pada stasiun nirkabel menggunakan utilitas konfigurasi Intel PROSet Wi-Fi. (Tangkapan layar milik Intel Corp.)

Untuk mengaktifkan roaming tanpa batas untuk klien seluler, sel yang dilayani oleh setiap AP perlu tumpang tindih sampai batas tertentu untuk mendukung roaming. Ini adalah salah satu elemen desain situs yang paling sulit untuk diperbaiki, karena perilaku dan kemampuan klien untuk roaming dapat sangat bervariasi. Jika ada kebijakan bawa perangkat Anda sendiri (BYOD), masalah dukungan ini akan semakin membesar.

Masalah dengan roaming dapat diidentifikasi dengan menganalisis waktu asosiasi titik akses untuk perangkat klien. Pengontrol WLAN akan dapat melacak mobilitas klien, menunjukkan setiap titik akses dan waktu yang terkait dengan klien tersebut. Jika sejumlah besar klien menutup antara dua titik akses berulang kali, desain situs mungkin perlu diselidiki untuk memecahkan masalah roaming.

- Masalah Kelebihan Kapasitas
  Kapasitas berlebih (atau saturasi perangkat) terjadi ketika terlalu banyak perangkat klien terhubung ke AP yang sama. Jumlah maksimum klien yang dapat didukung oleh AP bervariasi, tergantung pada standar Wi-Fi yang digunakan dan jenis lalu lintas jaringan yang dihasilkan. Misalnya, penjelajahan web biasanya akan menempatkan beban yang lebih ringan di jaringan daripada lalu lintas server-klien lokal atau kemungkinan setidaknya memindahkan hambatan apapun lebih jauh ke hulu ke WAN, daripada ke jaringan nirkabel. Sementara keadaan individu harus dipertimbangkan, maksimal 30 client per AP secara umum diterima sebagai aturan praktis. Dalam merancang jaringan, AP yang cukup harus disediakan di lokasi yang sesuai untuk mendukung kepadatan

klien yang diharapkan pada rasio ini. AP biasanya dapat dikonfigurasi untuk menerapkan jumlah koneksi maksimum, sehingga klien tambahan akan terhubung ke AP terdekat berikutnya. Bahkan dengan jumlah klien yang relatif rendah, jaringan nirkabel dapat mengalami kejenuhan bandwidth. Karena nirkabel adalah media siaran, bandwidth yang tersedia dibagi antara semua klien. Jadi, jika satu klien adalah babi bandwidth, yang lain mungkin merasa sulit untuk mempertahankan koneksi yang andal.

Dalam solusi Wi-Fi perusahaan, pengontrol biasanya akan menyediakan alat pelaporan untuk mendiagnosis masalah bandwidth dan melaporkan klien mana yang menggunakan bandwidth paling banyak. Itu juga dapat melaporkan pemanfaatan saluran nirkabel dan mengonfigurasi AP dan klien untuk menetapkan kembali saluran secara dinamis untuk mengurangi penggunaan yang berlebihan. Jika pembentuk lalu lintas dikerahkan, itu dapat bekerja secara otomatis untuk membatasi bandwidth ke node yang terlalu aktif.

- Masalah Interferensi
  Jika perangkat berada dalam jangkauan yang didukung tetapi sinyalnya lemah atau Anda tidak dapat tersambung, kemungkinan ada gangguan. Selain gangguan saluran yang dijelaskan sebelumnya, ada beberapa sumber gangguan lain yang perlu dipertimbangkan:
  - ***Reflection/bounce (multipath interference)***-Cermin atau permukaan mengkilap menyebabkan sinyal memantul, yang berarti bahwa penundaan variabel diperkenalkan. Ini menyebabkan paket hilang dan akibatnya kecepatan data turun.

    Tips: Standar Wi-Fi 4/5/6 sebenarnya menggunakan bouncing (multipath) sebagai sarana untuk mengoptimalkan throughput dan jangkauan melalui MIMO.

  - ***Refraction*** -Kaca atau air dapat menyebabkan gelombang radio membelok dan mengambil jalur yang berbeda ke penerima. Ini juga dapat menyebabkan kecepatan data turun.

  - ***Absorption***-Ini mengacu pada sejauh mana dinding dan jendela akan mengurangi kekuatan sinyal (sebagian energi gelombang radio hilang sebagai panas ketika melewati bahan konstruksi). Dinding internal mungkin "berbiaya" 3 hingga 15 dB, tergantung pada bahan yang digunakan (beton menjadi penyerap paling efektif). Frekuensi 2,4 GHz memiliki penetrasi yang lebih baik daripada frekuensi 5 GHz, mengingat output daya yang sama. Untuk meminimalkan penyerapan dari perabot kantor (dan orang), gunakan Titik Akses yang dipasang di langit-langit.

  - ***Electromagnetic interference*** **(EMI)**-Interferensi dari radio kuat atau sumber elektromagnetik yang bekerja di pita frekuensi yang sama, seperti perangkat Bluetooth, telepon nirkabel, atau oven microwave. EMI dapat dideteksi dengan

menggunakan spectrum analyzer. Tidak seperti penganalisis Wi-Fi, penganalisis spektrum harus menggunakan penerima radio khusus-adaptor Wi-Fi menyaring apa pun yang bukan sinyal Wi-Fi. Mereka biasanya dipasok sebagai unit genggam dengan antena terarah, sehingga lokasi gangguan yang tepat dapat ditentukan. Perubahan 6 dB pada tingkat sumber tertentu menunjukkan pengurangan separuh atau penggandaan jarak antara penganalisis dan sumber sumber RF.

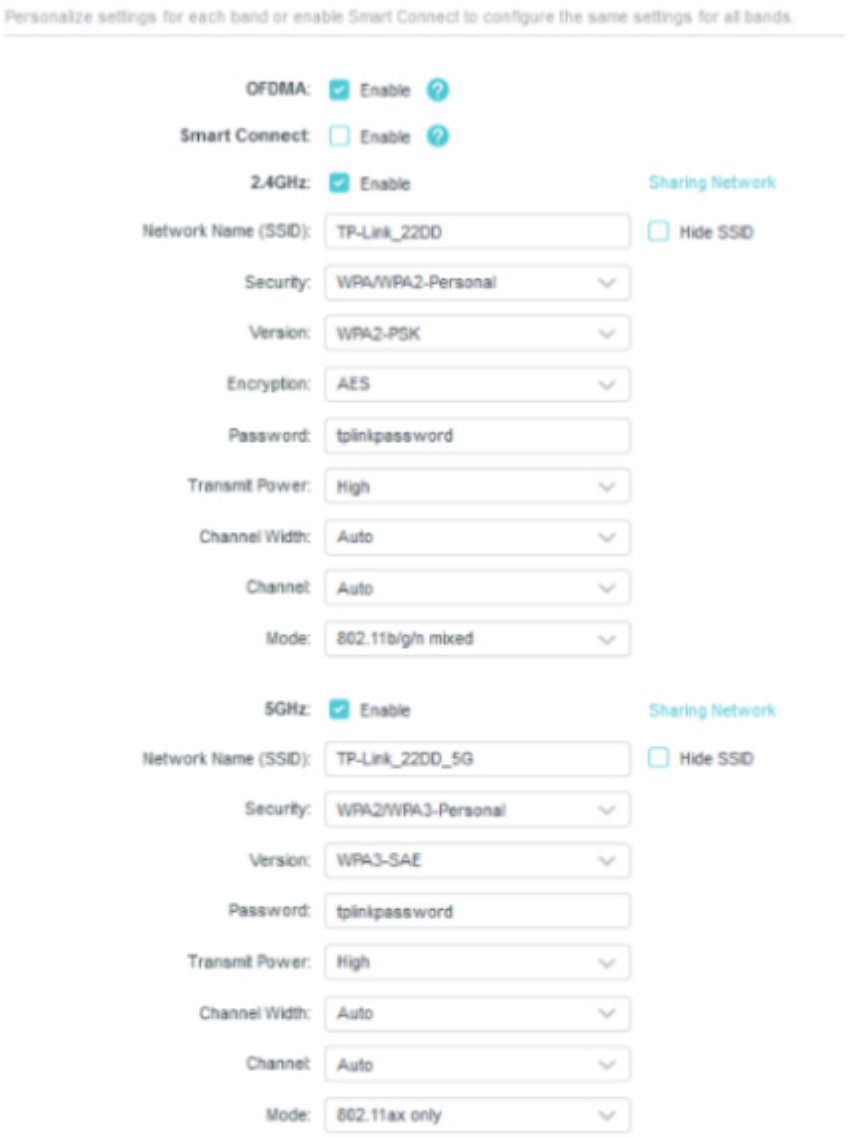
Tips: Pertimbangkan juga bahwa masalah sinyal dapat disebabkan oleh seseorang yang mencoba menyerang jaringan dengan mengganggu AP yang sah dan membuat klien terhubung ke AP yang tidak benar.

Konfigurasikan dan Pecahkan Masalah Keamanan Nirkabel

- Pendahuluan: Mengkonfigurasi dan Memecahkan Masalah Keamanan Nirkabel
  Koneksi nirkabel populer di kalangan pengguna tetapi juga menimbulkan risiko besar bagi seluruh jaringan kecuali jika diamankan dengan benar dengan kontrol akses. Dalam topik ini, Anda akan mengidentifikasi metode keamanan nirkabel yang berbeda dan persyaratan konfigurasinya serta memecahkan masalah umum dengan pengaturan nirkabel.

- Standar Enkripsi Wi-Fi
  Selain desain situs, jaringan nirkabel harus dikonfigurasi dengan pengaturan keamanan. Tanpa enkripsi, siapa pun dalam jangkauan dapat mencegat dan membaca paket yang melewati jaringan nirkabel. Pilihan pengaturan keamanan mana yang akan diterapkan ditentukan oleh dukungan perangkat untuk berbagai standar enkripsi Wi-Fi, menurut jenis infrastruktur otentikasi, dan oleh tujuan WLAN. Standar enkripsi menentukan protokol kriptografi yang didukung, cara menghasilkan kunci enkripsi, dan metode yang tersedia untuk mengotentikasi stasiun nirkabel ketika mereka mencoba untuk bergabung (atau mengasosiasikan dengan) jaringan.

  Versi pertama *Wi-Fi Protected Access* (WPA) dirancang untuk memperbaiki kerentanan kritis dalam standar *wired equivalent privacy* (WEP) sebelumnya. Seperti WEP, versi 1 dari WPA menggunakan RC4 stream cipher untuk mengenkripsi lalu lintas tetapi menambahkan mekanisme yang disebut *Temporal Key Integrity Protocol* (TKIP) untuk mencoba mengurangi berbagai serangan terhadap WEP yang telah dikembangkan.



Mengkonfigurasi titik akses TP-LINK SOHO dengan enkripsi nirkabel dan pengaturan otentikasi. Dalam contoh ini, pita 2,4 GHz memungkinkan koneksi lama dengan keamanan WPA2-Personal, sedangkan jaringan 5 GHz untuk perangkat berkemampuan 802.11ax (Wi-Fi 6) yang menggunakan autentikasi WPA3-SAE. (Tangkapan layar digunakan dengan izin dari TP-Link Technologies.)

Baik WEP maupun versi WPA asli tidak dianggap cukup aman untuk penggunaan berkelanjutan. Mereka dapat dimanfaatkan oleh berbagai jenis serangan replay yang bertujuan untuk memulihkan kunci enkripsi. WPA2 menggunakan cipher Advanced Encryption Standard (AES) yang digunakan dalam Counter Mode dengan Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES menggantikan RC4 dan CCMP menggantikan TKIP. CCMP menyediakan enkripsi yang diautentikasi, yang dirancang untuk membuat serangan replay menjadi lebih sulit.

Kelemahan juga ditemukan di WPA2, yang menyebabkan penggantian yang dimaksudkan oleh WPA3.

- Otentikasi Pribadi
  Untuk mengamankan jaringan, Anda harus dapat mengonfirmasi bahwa hanya pengguna yang valid yang terhubung ke jaringan tersebut. Autentikasi Wi-Fi hadir dalam tiga jenis: pribadi, terbuka, dan perusahaan. Dalam kategori autentikasi pribadi, ada dua metode: *pre-shared key authentication* (PSK) dan autentikasi simultan yang setara (SAE).

  - Otentikasi Kunci Pra-Berbagi WPA2
    Di WPA2, otentikasi kunci *pre-shared key* (PSK) menggunakan frasa sandi untuk menghasilkan kunci yang digunakan untuk mengenkripsi komunikasi. Ini juga disebut sebagai otentikasi grup karena sekelompok pengguna berbagi rahasia yang sama. Ketika titik akses diatur ke mode WPA2-PSK, administrator mengonfigurasi frasa sandi antara 8 dan 63 karakter. Ini dikonversi ke jenis nilai hash, yang disebut sebagai *the pairwise master key* (PMK). Rahasia yang sama harus dikonfigurasi pada titik akses dan pada setiap node yang bergabung dengan jaringan. PMK digunakan sebagai bagian dari jabat tangan 4 arah WPA2 untuk mendapatkan berbagai kunci sesi.

    Semua jenis otentikasi PSK Wi-Fi telah terbukti rentan terhadap serangan yang mencoba memulihkan frasa sandi. Minimal, frasa sandi harus memiliki panjang minimal 14 karakter untuk mencoba mengurangi risiko retak.

  - Otentikasi Pribadi WPA3
    Sementara WPA3 masih menggunakan frasa sandi untuk mengotentikasi stasiun dalam mode pribadi, WPA3 mengubah metode rahasia ini digunakan untuk menyetujui kunci sesi. Skema yang digunakan juga disebut sebagai *Password Authenticated Key Exchange* (PAKE). Di WPA3, protokol *Simultaneous Authentication of Equals* (SAE) menggantikan jabat tangan 4 arah, yang telah terbukti rentan terhadap berbagai serangan.

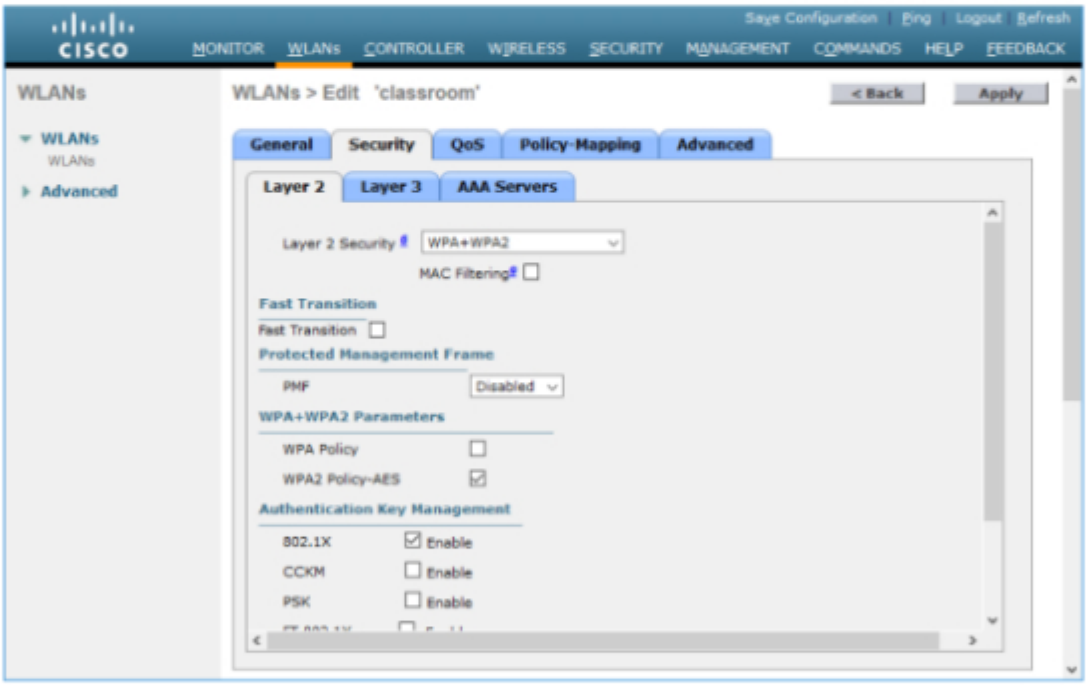
  Tips: Antarmuka konfigurasi untuk titik akses dapat menggunakan label yang berbeda untuk metode ini. Anda mungkin melihat WPA2-Personal dan WPA3-SAE daripada WPA2-PSK dan WPA3-Personal, misalnya. Selain itu, titik akses dapat dikonfigurasi hanya untuk WPA3 atau dengan dukungan untuk WPA2 lama (mode Transisi Pribadi WPA3)

  .
- Otentikasi Perusahaan/IEEE 802.1X
  Masalah utama dengan mode otentikasi pribadi adalah bahwa distribusi kunci atau frasa sandi tidak dapat diamankan dengan benar, dan bahwa pengguna dapat memilih frasa

yang tidak aman. Otentikasi pribadi juga gagal memberikan akuntansi, karena semua pengguna berbagi kredensial yang sama.

Sebagai alternatif autentikasi pribadi, metode autentikasi perusahaan WPA mengimplementasikan IEEE 802.1X untuk menggunakan mekanisme Extensible Authentication Protocol (EAP) untuk mengautentikasi terhadap direktori jaringan. 802.1X mendefinisikan penggunaan EAP over Wireless (EAPoW) untuk memungkinkan titik akses meneruskan data otentikasi tanpa mengizinkan jenis akses jaringan lainnya. Ini dikonfigurasi dengan memilih WPA2-Enterprise atau WPA3-Enterprise sebagai metode keamanan pada titik akses.

Dengan otentikasi perusahaan, ketika stasiun nirkabel meminta asosiasi, AP mengaktifkan saluran hanya untuk lalu lintas EAPoW. Ini meneruskan kredensial pemohon ke server AAA (RADIUS atau TACACS+) di jaringan kabel untuk validasi. Ketika pemohon telah diautentikasi, server AAA mengirimkan *master key* (MK) ke pemohon. Pemohon dan server otentikasi kemudian mendapatkan kunci master berpasangan (PMK) yang sama dari MK. Server AAA mengirimkan PMK ke titik akses. Stasiun nirkabel dan titik akses menggunakan PMK untuk memperoleh kunci sesi, baik menggunakan metode jabat tangan empat arah WPA2 atau WPA3 SAE.



Menggunakan Pengontrol LAN Nirkabel Virtual Cisco untuk menetapkan kebijakan keamanan untuk WLAN-Kebijakan ini memberlakukan penggunaan WPA2 dan penggunaan otentikasi 802.1X (Perusahaan). (Gambar © dan Courtesy of Cisco Systems, Inc. Penggunaan tidak sah tidak diizinkan.)

- Otentikasi Perusahaan/IEEE 802.1X
- Masalah utama dengan mode otentikasi pribadi adalah bahwa distribusi kunci atau frasa sandi tidak dapat diamankan dengan benar, dan bahwa pengguna dapat memilih frasa yang tidak aman. Otentikasi pribadi juga gagal memberikan akuntansi, karena semua pengguna berbagi kredensial yang sama.

  Sebagai alternatif autentikasi pribadi, metode autentikasi perusahaan WPA mengimplementasikan IEEE 802.1X untuk menggunakan mekanisme Extensible Authentication Protocol (EAP) untuk mengautentikasi terhadap direktori jaringan. 802.1X mendefinisikan penggunaan EAP over Wireless (EAPoW) untuk memungkinkan titik akses meneruskan data otentikasi tanpa mengizinkan jenis akses jaringan lainnya. Ini dikonfigurasi dengan memilih WPA2-Enterprise atau WPA3-Enterprise sebagai metode keamanan pada titik akses.

  Dengan otentikasi perusahaan, ketika stasiun nirkabel meminta asosiasi, AP mengaktifkan saluran hanya untuk lalu lintas EAPoW. Ini meneruskan kredensial pemohon ke server AAA (RADIUS atau TACACS+) di jaringan kabel untuk validasi. Ketika pemohon telah diautentikasi, server AAA mengirimkan kunci master (MK) ke pemohon. Pemohon dan server otentikasi kemudian mendapatkan kunci master berpasangan (PMK) yang sama dari MK. Server AAA mengirimkan PMK ke titik akses. Stasiun nirkabel dan titik akses menggunakan PMK untuk memperoleh kunci sesi, baik menggunakan metode jabat tangan empat arah WPA2 atau WPA3 SAE.

- Masalah Konfigurasi Keamanan Wi-Fi
  Meskipun kehilangan sinyal dan gangguan merupakan faktor yang selalu perlu dipertimbangkan, jika ada masalah konektivitas dasar, maka Anda mungkin ingin menyelidiki konfigurasi klien dan/atau AP terlebih dahulu.

  - SSID Salah dan Masalah Frasa Sandi Salah
    Jika siaran SSID ditekan, stasiun masih dapat terhubung ke WLAN dengan memasukkan nama jaringan secara manual. Jika demikian, periksa apakah klien dikonfigurasi dengan SSID/ESSID yang benar. Ingat bahwa nilai ini peka huruf besar/kecil. Secara teknis, SSID dapat berisi spasi dan karakter khusus, tetapi hal ini dapat menyebabkan masalah sehingga sebaiknya dihindari. Periksa apakah pengaturan otentikasi sama di semua perangkat. Jika frasa sandi digunakan, pastikan itu dimasukkan dengan benar. Pada AP, pastikan jenis autentikasi tidak disetel untuk dibuka, kecuali jika tujuannya adalah untuk memberikan akses publik yang tidak terbatas.

    Tips: Ada kemungkinan dua AP beroperasi dengan SSID yang sama. Jika otentikasi diperlukan, koneksi dengan SSID yang salah akan gagal. Jika tidak ada otentikasi (jaringan terbuka), maka host akan terhubung tetapi berhati-hatilah, karena ini mungkin merupakan upaya untuk mengintip lalu lintas host menggunakan AP jahat. Juga, jika pengguna bergabung dengan WLAN

untuk pertama kalinya, mungkin ada SSID dari WLAN yang tumpang tindih dengan nama default yang sangat mirip dan pengguna mungkin bingung tentang nama mana yang harus dipilih.

Masalah Ketidakcocokan Protokol Enkripsi Jika pengguna memberikan kunci atau kredensial yang benar, periksa apakah klien dapat mendukung standar enkripsi dan otentikasi yang dikonfigurasi pada AP. Pembaruan driver atau patch OS mungkin diperlukan. Ketidakcocokan protokol enkripsi akan menyebabkan koneksi gagal, meskipun kredensial yang benar diberikan.

- Masalah Pemisahan Klien
  Dalam operasi normal, titik akses dan klien menggunakan bingkai manajemen untuk mengontrol koneksi. Titik akses biasanya menyiarkan bingkai suar untuk mengiklankan kemampuan layanan. Klien dapat memilih untuk mengautentikasi terlebih dahulu dan kemudian mengaitkan ke titik akses saat mereka pindah ke jangkauan suar. Klien atau titik akses dapat menggunakan bingkai disasosiasi dan/atau deautentikasi untuk memberitahu pihak lain bahwa sambungan telah berakhir. Klien yang sah mungkin memutuskan hubungan tetapi tidak mengautentikasi karena jelajah di antara titik akses nirkabel di area layanan yang diperluas. Seorang klien mungkin "mengepak" antara dua titik akses, menyebabkan banyak disasosiasi dan reassociations. Selidiki titik akses atau log peristiwa pengontrol untuk mengidentifikasi penyebab disasosiasi.

  Jika klien terputus secara tiba-tiba dan tidak ada roaming, gangguan, atau masalah driver, Anda harus mempertimbangkan kemungkinan serangan berbahaya. Serangan disasosiasi mengeksploitasi kurangnya enkripsi dalam lalu lintas bingkai manajemen untuk mengirim bingkai palsu. Salah satu jenis serangan disasosiasi menyuntikkan bingkai manajemen yang menipu alamat MAC dari stasiun korban tunggal dalam pemberitahuan disasosiasi, menyebabkannya terputus dari jaringan. Varian lain dari serangan itu menyiarkan bingkai palsu untuk memutuskan semua stasiun. Bingkai dapat dipalsukan untuk mengirim pemberitahuan disasosiasi atau deautentikasi.

  Serangan disassociation/deauthentication dapat digunakan untuk melakukan serangan denial of service terhadap infrastruktur nirkabel atau untuk mengeksploitasi stasiun yang terputus untuk mencoba memaksa koneksi ulang ke WAP jahat. Serangan disasosiasi/deauthentication juga dapat digunakan bersama dengan serangan replay yang ditujukan untuk memulihkan kunci jaringan.

- Buka Otentikasi dan Masalah Portal Captive
  Mengkonfigurasi titik akses untuk otentikasi terbuka berarti bahwa klien tidak diharuskan untuk mengotentikasi. Mode ini akan digunakan pada AP publik atau "hotspot". Di WPA/WPA2, ini juga berarti bahwa data yang dikirim melalui tautan tidak dienkripsi. Otentikasi terbuka dapat digabungkan dengan mekanisme otentikasi sekunder yang dikelola melalui browser. Ketika klien mengasosiasikan dengan hotspot terbuka dan meluncurkan browser, klien diarahkan ke portal captive atau halaman splash. Ini akan memungkinkan klien untuk mengautentikasi ke jaringan penyedia hotspot (melalui

HTTPS, sehingga login aman). Portal juga dapat dirancang untuk menegakkan syarat dan ketentuan dan/atau menerima pembayaran untuk mengakses layanan Wi-Fi.

Sebagian besar masalah portal tawanan muncul karena pengalihan tidak berfungsi. Portal tawanan harus menggunakan HTTPS. Sebagian besar browser modern akan memblokir pengalihan ke situs yang tidak menggunakan TLS. Artinya portal captive juga perlu diinstal dengan sertifikat digital yang dikeluarkan oleh otoritas sertifikasi (CA) yang dipercaya oleh browser klien.

Saat menggunakan nirkabel terbuka, pengguna harus memastikan bahwa mereka mengirim data web rahasia hanya melalui koneksi HTTPS dan hanya menggunakan layanan email, VoIP, IM, dan transfer file dengan SSL/TLS diaktifkan. Pilihan lain adalah bagi pengguna untuk bergabung dengan jaringan pribadi virtual (VPN). Pengguna akan mengasosiasikan dengan hotspot terbuka kemudian memulai koneksi VPN. Ini menciptakan "terowongan" terenkripsi antara komputer pengguna dan server VPN. Hal ini memungkinkan pengguna untuk menelusuri web atau terhubung ke layanan email tanpa ada yang menguping di jaringan Wi-Fi terbuka yang dapat mencegat komunikasi tersebut. VPN dapat disediakan oleh perusahaan pengguna atau mereka dapat menggunakan penyedia layanan VPN pihak ketiga. Tentu saja, jika menggunakan pihak ketiga, pengguna harus dapat mempercayai mereka secara implisit. VPN harus menggunakan tunneling berbasis sertifikat untuk menyiapkan metode otentikasi "dalam".

MODUL 16

Membandingkan Tautan WAN dan Metode Akses Jarak Jauh

PENGANTAR PELAJARAN

Sebagian besar jaringan lokal memerlukan semacam koneksi eksternal, baik ke Internet global atau dalam WAN perusahaan. Komunikasi jarak jauh ini biasanya difasilitasi oleh tautan penyedia layanan. Mendukung WAN dan akses Internet secara efektif merupakan kompetensi penting untuk dipelajari.

Dalam pelajaran ini, Anda akan mengidentifikasi karakteristik penawaran penyedia layanan WAN dan komponen implementasi jaringan akses jarak jauh.

TUJUAN PELAJARAN

Dalam pelajaran ini, Anda akan:

- Jelaskan tautan penyedia WAN.
- Bandingkan dan kontraskan metode akses jarak jauh.

A. Jelaskan Tautan Penyedia WAN

Pendahuluan: Jelaskan Tautan Penyedia WAN

Memahami berbagai perangkat dan metode konektivitas WAN akan membantu Anda mendukung konektivitas Internet dan konfigurasi WAN perusahaan. Anda perlu memahami kemampuan dan keterbatasan tautan penyedia WAN untuk memilih yang paling cocok untuk jaringan Anda.

Jaringan Area Luas dan Model OSI

Teknologi jaringan area luas (WAN) mendukung komunikasi data melalui jarak yang lebih jauh daripada LAN. Istilah WAN perusahaan digunakan untuk menggambarkan WAN yang digunakan dan dikendalikan oleh satu organisasi. Namun, meskipun suatu perusahaan dapat mengontrol WAN-nya, jarang memiliki semua infrastruktur yang mendukungnya. Komunikasi jarak jauh biasanya melibatkan penggunaan jaringan publik. Jaringan publik dimiliki oleh perusahaan telekomunikasi (telco) dan menyediakan layanan WAN untuk bisnis dan rumah tangga. Organisasi sering memilih untuk menggunakan jaringan publik, karena biayanya jauh lebih murah daripada menerapkan solusi pribadi. Penyedia layanan sering memiliki hak akses ke lokasi yang tidak tersedia untuk organisasi lain, seperti di bawah jalan.

Seperti halnya LAN, lapisan Fisik WAN menjelaskan jenis media dan spesifikasi antarmuka. Di mana tautan penyedia adalah kabel tembaga, beberapa jenis modem biasanya digunakan, bukan sakelar. Modem melakukan modulasi sinyal keluar dan demodulasi data masuk, bekerja hanya pada lapisan fisik model OSI. Modulasi berarti mengubah gelombang elektromagnetik untuk mewakili informasi, seperti menggunakan amplitudo (tinggi) gelombang untuk mewakili bit. Modem lama melakukan modulasi digital ke analog untuk transmisi melalui saluran suara. Modem analog (atau dial-up) hanya mendukung bandwidth rendah (hingga 56 Kbps). Modem

digital melakukan jenis modulasi yang berbeda untuk mengubah sinyal digital yang diterima sebagai frame Ethernet untuk transmisi melalui media WAN. Jenis modem digital termasuk unit layanan data (DSU) untuk saluran sewa, modem saluran pelanggan digital (DSL), modem kabel, dan modem satelit.

Pada lapisan data link, WAN sering menggunakan protokol yang lebih sederhana untuk LAN Ethernet karena tautannya lebih cenderung point-to-point dan tidak memerlukan banyak kerumitan. Konon, Ethernet semakin banyak digunakan untuk konektivitas ujung ke ujung melalui WAN.

Pada lapisan jaringan, situs pelanggan dan penyedia dialamatkan menggunakan IP. Router tepi pelanggan (CE) terhubung ke tepi penyedia (PE) melalui antarmuka lapisan tautan yang mendasarinya. Penyedia mengalokasikan alamat IPv4/IPv6 publik atau rentang alamat kepada pelanggan.

WAN Provider Links

Membuat tautan penyedia WAN berarti pemasangan kabel penyedia akses di beberapa titik di tempat Anda, dan kemudian memasang modem dan peralatan perut ke saluran itu. Titik masuk terkait di mana jaringan penyedia akses berakhir disebut titik demarkasi (atau singkatnya demarc) atau titik masuk minimum (MPOE). Titik demark mewakili akhir dari tanggung jawab perusahaan telekomunikasi untuk memelihara bagian pemasangan kabel tersebut. Setiap masalah kabel yang timbul dari sisi lain demarc point adalah tanggung jawab pelanggan.

Modem dan router atau peralatan akses lain yang disediakan atau disewa oleh pelanggan dan dipasang di lokasi mereka disebut sebagai peralatan tempat pelanggan (CPE). Beberapa penyedia mungkin bertanggung jawab atas kesalahan yang muncul di CPE, tergantung pada kontrak dan keadaan pemasangan.

Demark dan CPE harus dipasang di lokasi yang aman di dalam lokasi, dengan kontrol akses untuk membatasi area tersebut hanya untuk staf yang terbatas. Lokasi ini disebut sebagai fasilitas pintu masuk dalam standar pemasangan kabel terstruktur TIA/EIA.

T-Carrier and Leased Line Provider Links

Sistem T-carrier dikembangkan oleh penyedia telekomunikasi Bell Labs untuk memungkinkan beberapa panggilan ditempatkan pada satu kabel. T-carrier memungkinkan lalu lintas suara didigitalkan untuk transportasi di sekitar inti jaringan telekomunikasi. Ini juga memungkinkan jenis data digital lainnya untuk diangkut dan dapat disediakan langsung ke pelanggan sebagai jalur sewa. T-carrier didasarkan pada Time Division Multiplexing (TDM). Protokol memberikan setiap sirkuit (atau saluran) slot waktu. Setiap saluran 64 Kbps menyediakan bandwidth yang cukup untuk panggilan suara digital.

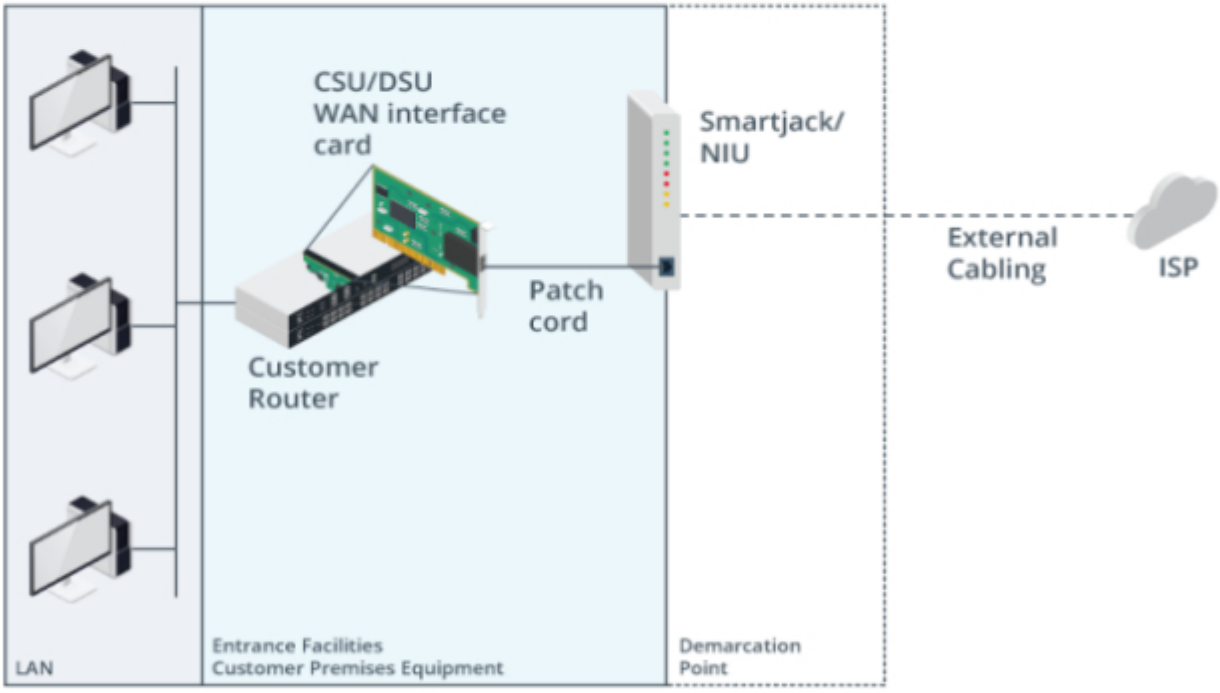
Satu saluran 64 Kbps dikenal sebagai DS0 atau tautan pita sempit. Namun, untuk layanan data jalur sewa, tingkat dasar pembawa-T adalah sirkuit sinyal digital DS1 atau T1. Layanan ini

terdiri dari 24 saluran yang dimultipleks menjadi satu koneksi digital full duplex 1,544 Mbps yang dapat digunakan untuk suara dan/atau data. Jalur T1 sendiri dapat dimultipleks untuk menyediakan bandwidth yang lebih besar.

Saluran T1 dari penyedia layanan diakhiri di demarc pada smartjack atau Network Interface Unit (NIU). Soket pintar memiliki antarmuka RJ-48C atau RJ-48X di sisi pelanggan yang digunakan untuk menghubungkan ke Unit Layanan Saluran/Unit Layanan Data (CSU/DSU) pelanggan. Pengkabelan dari soket pintar ke CSU/DSU dapat menggunakan kabel patch RJ-45 biasa (panjang hingga 3 meter/10 kaki), tetapi kabel 22 AWG dua pasang berpelindung dengan kabel konektor untuk RJ-48 diperlukan untuk jarak yang lebih jauh dari itu.

Tips: Soket RJ-48X memiliki batang korslet untuk menyediakan loopback pada sambungan jika peralatan di sisi pelanggan dicabut. Ini memungkinkan penyedia layanan untuk menguji saluran dari jarak jauh.

DSU mengkodekan sinyal dari Data Terminal Equipment (DTE) yaitu, sistem telekomunikasi internal private branch exchange (PBX) perusahaan dan/atau router IP-ke sinyal digital serial yang ditransmisikan melalui kabel tembaga. Bagian DSU berfungsi sebagai modem digital, sedangkan CSU digunakan untuk melakukan tes diagnostik di telepon. Perangkat dapat dipasok secara terpisah, tetapi lebih umum mereka digabungkan sebagai kartu antarmuka WAN tunggal yang dapat dicolokkan ke router atau PBX yang kompatibel.



WAN termination equipment. (Image © 123RF.com.)

Pada lapisan data link, leased line T1 biasanya menggunakan High-level Data Link Control (HDLC) atau Point-to-Point Protocol (PPP).

Digital Subscriber Line Provider Links

Digital subscriber line (DSL) adalah teknologi untuk mentransfer data melalui saluran telepon tingkat suara, sering disebut sebagai loop lokal. DSL menggunakan frekuensi di atas yang digunakan oleh suara manusia sebagai saluran komunikasi dupleks penuh.

Modem DSL
Modem DSL dipasang sebagai CPE, biasanya sebagai "router nirkabel" multifungsi, di mana port WAN RJ-11 terhubung ke jack telepon penyedia melalui kabel pita pendek. Modem DSL juga dapat disediakan sebagai peralatan terpisah atau kartu plug-in untuk router. Modem DSL mandiri terhubung ke saluran telepon melalui port RJ-11 dan ke router jaringan lokal (atau satu komputer di jaringan lokal) melalui port Ethernet RJ-45.



RJ-11 DSL (left) and RJ-45 LAN (right) ports on a DSL modem. (Image © 123RF.com.)

Filter (pemisah) harus dipasang pada setiap titik telepon untuk mencegah kebisingan mempengaruhi panggilan suara atau tautan DSL. Ini dapat dipasang di titik demarc oleh teknisi telekomunikasi atau dipasang sendiri di setiap titik telepon oleh pelanggan.

Kelemahan utama DSL adalah, sebagai teknologi kawat tembaga, ia mengalami atenuasi. Jangkauan maksimum modem DSL biasanya sekitar 3 mil (5 km), tetapi semakin lama koneksi, semakin besar penurunan kecepatan data. Pengkabelan domestik mungkin juga memiliki kualitas yang relatif buruk dan melewati lingkungan yang "berisik".

Jenis DSL

Ada berbagai jenis atau rasa DSL. Ini distandarisasi oleh ITU dalam serangkaian rekomendasi G..

- DSL simetris (SDSL) disebut demikian karena menyediakan bandwidth downlink dan uplink yang sama. Ada berbagai jenis layanan DSL simetris. Layanan SDSL cenderung disediakan sebagai paket bisnis, bukan untuk pelanggan perumahan.
- Asymmetrical DSL (ADSL) (G.992) adalah versi konsumen DSL yang menyediakan downlink cepat tetapi uplink lambat. Ada berbagai iterasi ADSL, dengan yang terbaru (ADSL2+) menawarkan kecepatan downlink hingga sekitar 24 Mbps dan kecepatan uplink hingga 3,3 Mbps. Penyedia layanan dapat memberlakukan batasan penggunaan untuk membatasi jumlah data yang diunduh per bulan. Kecepatan sebenarnya dapat dipengaruhi oleh kualitas pemasangan kabel di tempat konsumen dan antara tempat dan pertukaran, dan oleh jumlah pengguna yang terhubung ke DSLAM (pertentangan) yang sama.

Fiber to the Curb

Kendala utama untuk menyediakan akses WAN yang dapat mendekati kinerja LAN adalah bandwidth di last mile, di mana infrastruktur kabel tembaga umumnya tidak baik. Proyek untuk memperbarui kabel ini untuk menggunakan tautan serat optik disebut dengan istilah umum Fiber to the X (FTTx).

Solusi paling mahal adalah Fiber to the Premises (FTTP) atau varian huniannya Fiber to the Home (FTTH). Poin penting tentang kedua implementasi ini adalah bahwa tautan serat diakhiri di demarc. Solusi lain dapat digambarkan sebagai Fiber to the Node (FTTN) atau Fiber to the Curb (FTTC). Ini mempertahankan semacam kabel tembaga ke demarc sambil memperluas tautan serat ke kabinet komunikasi yang melayani banyak pelanggan. Penyedia layanan dengan akar mereka di jaringan telepon menggunakan DSL kecepatan sangat tinggi (VDSL) untuk mendukung FTTC. VDSL (G.993) mencapai kecepatan bit yang lebih tinggi daripada jenis DSL lainnya dengan mengorbankan jangkauan. Ini memungkinkan untuk mode simetris dan asimetris. Lebih dari 300 m (1000 kaki), link asimetris mendukung 52 Mbps downstream dan 6 Mbps upstream, sedangkan link simetris mendukung 26 Mbps di kedua arah. VDSL2 menetapkan tingkat jangkauan yang sangat pendek (100 m/300 kaki) sebesar 100 Mbps (dua arah).

Tips: Jenis modem harus sesuai dengan layanan. Modem khusus ADSL tidak dapat digunakan untuk mengakses layanan VDSL.

Cable Provider Links

Koneksi Internet kabel biasanya tersedia bersama dengan Cable Access TV (CATV). Jaringan ini kadang-kadang digambarkan sebagai hybrid fiber coax (HFC) karena mereka menggabungkan jaringan inti serat optik dengan link coax ke CPE, tetapi lebih sederhana hanya digambarkan sebagai broadband kabel.



A cable modem-The RJ-45 port connects to the local network, while the coax port connects to the service provider network. (Image © 123RF.com.)

Pemasangan modem kabel mengikuti prinsip umum yang sama seperti untuk modem DSL. Modem kabel dihubungkan ke komputer atau router melalui Ethernet atau adaptor USB dan dengan jaringan penyedia akses melalui segmen pendek coax. Lebih coax kemudian menghubungkan semua tempat di jalan dengan Cable Modem Termination System (CMTS), yang mengarahkan lalu lintas data melalui tulang punggung serat ke Point of Presence (PoP) ISP dan dari sana ke Internet. Kabel berdasarkan Data Over Cable Service Interface Specification (DOCSIS) mendukung kecepatan downlink hingga 38 Mbps (Amerika Utara) atau 50 Mbps (Eropa) dan uplink hingga 27 Mbps. DOCSIS versi 3 memungkinkan penggunaan saluran multipleks untuk mencapai bandwidth yang lebih tinggi.

Metro-optical Provider Links

Carrier Ethernet menyediakan jalur sewa Ethernet point-to-point atau point-to-multipoint melalui jaringan area luas. Carrier Ethernet juga dapat disebut sebagai tautan penyedia metro-optik. Istilah Metro Ethernet mengacu pada Carrier Ethernet di mana cakupan geografisnya terbatas pada satu kota. Standar untuk Carrier Ethernet dikembangkan oleh MEF (mef.net). Carrier Ethernet dapat menggunakan berbagai jenis konektivitas fisik. Beberapa contoh termasuk:

- Ethernet over Fiber Menggunakan spesifikasi IEEE 802.3 10GBASE-LR dan 10GBASE-ER.
- Ethernet over Copper Menggunakan varian DSL seperti single-pair high-speed DSL (SHDSL) dan VDSL untuk mengatasi batasan jarak biasa dari Ethernet tembaga. Ini tidak mendukung kecepatan yang sama dengan LAN Ethernet (biasanya 2-10 Mbps), tetapi beberapa pasangan dapat digabungkan untuk bandwidth yang lebih tinggi.

Di atas metode konektivitas fisik, ada beberapa kategori layanan untuk Carrier Ethernet. Dua di antaranya adalah E-line dan E-LAN:

- E-line-Membuat link point-to-point antara dua situs. Beberapa E-line dapat dikonfigurasi pada antarmuka Metro Ethernet tunggal, dengan masing-masing E-line mewakili VLAN terpisah.
- E-LAN-Membuat topologi mesh antara beberapa situs.

Layanan ini dapat digunakan oleh pelanggan untuk menggabungkan beberapa situs bersama-sama atau sebagai cara untuk menghubungkan jaringan perusahaan mereka ke Internet. Dari sudut pandang pelanggan, Carrier Ethernet memiliki banyak keunggulan. Fakta bahwa Carrier Ethernet mudah diskalakan memberi bisnis fleksibilitas untuk menyesuaikan layanan dengan tuntutan mereka yang terus berubah. Juga, fakta bahwa protokol dan pembingkaian Ethernet yang sama digunakan pada LAN dan konektivitas ke ruang jaringan publik dapat membuat konfigurasi router, Layer 3 *switches*, dan firewall menjadi lebih sederhana.

Sambungan serat penuh juga disediakan untuk pelanggan perumahan dan bisnis kecil, meskipun ketersediaan seringkali terbatas pada beberapa wilayah metropolitan. Daripada dedicated leased line, layanan ini digunakan sebagai jaringan optik pasif (PON). Paket ditawarkan dalam tingkatan mulai dari 100 Mbps hingga 1 Gbps.

Dalam PON, kabel serat tunggal dijalankan dari pertukaran terdekat ke terminal jalur optik (OLT) yang terletak di jalan. Tautan ini menggunakan multiplexing divisi panjang gelombang padat (DWDM) untuk mendukung rasio kabel backhaul ke pelanggan 1:64 atau 1:128. Dari OLT, splitter mengarahkan frekuensi panjang gelombang setiap pelanggan melalui serat yang lebih pendek ke unit jaringan optik (ONU) atau terminal jaringan optik (ONT) yang dipasang di demarc. ONU/ONT mengubah sinyal optik menjadi sinyal listrik. ONU/ONT terhubung ke router pelanggan menggunakan kabel patch kabel tembaga.

Microwave Satellite

Sistem satelit menyediakan area cakupan yang jauh lebih besar daripada yang dapat dicapai dengan menggunakan teknologi lain. Piring gelombang mikro disejajarkan dengan satelit orbital yang dapat menyampaikan sinyal antar lokasi secara langsung atau melalui satelit lain. Meluasnya penggunaan penerima televisi satelit memungkinkan layanan konektivitas Internet domestik melalui koneksi satelit. Layanan satelit untuk bisnis juga berkembang, terutama di daerah pedesaan di mana layanan DSL atau kabel tidak mungkin tersedia.

Koneksi satelit mengalami masalah latensi yang cukup parah karena sinyal harus menempuh jarak ribuan mil lebih banyak daripada koneksi terestrial, menyebabkan penundaan empat hingga lima kali lipat dari yang mungkin diharapkan melalui jalur darat. Misalnya, jika Anda mengetahui bahwa mengakses situs di AS dari Eropa membutuhkan waktu 200 mdtk melalui

tautan darat (bawah laut), mengakses situs yang sama melalui tautan satelit dapat memerlukan penundaan 900 mdtk. Ini adalah masalah untuk aplikasi waktu nyata, seperti konferensi video, VoIP, dan game multipemain.

Untuk membuat sambungan Internet satelit, ISP memasang antena parabola, yang disebut sebagai very small aperture terminal (VSAT), di tempat pelanggan dan menyelaraskannya dengan satelit orbit. Ukuran VSAT berkisar antara 1,2 hingga 2,4 meter dengan diameter. Satelit berada di orbit geostasioner di atas khatulistiwa, sehingga di belahan bumi utara piringan akan mengarah ke selatan. Antena terhubung melalui kabel koaksial ke modem Digital Video Broadcast Satellite (DVB-S).

B. Bandingkan dan Kontraskan Metode Akses Jarak Jauh
Pendahuluan: Bandingkan dan Kontraskan Metode Akses Jarak Jauh
Dengan tenaga kerja seluler saat ini, sebagian besar jaringan harus mendukung koneksi oleh karyawan jarak jauh, kontraktor, dan pelanggan ke sumber daya jaringan mereka. Koneksi jarak jauh ini sering menggunakan jaringan publik yang tidak tepercaya, seperti Internet. Untuk mengatasi risiko keamanan yang terkait dengan jaringan publik, organisasi menerapkan jaringan pribadi virtual (VPN) melalui jaringan publik untuk memastikan komunikasi yang aman. Akibatnya, memahami bagaimana menerapkan protokol VPN akses jarak jauh yang aman akan menjadi bagian utama dari pekerjaan Anda sebagai profesional jaringan.

Otentikasi dan Otorisasi Akses Jaringan Jarak Jauh

Akses jaringan jarak jauh berarti bahwa perangkat pengguna tidak membuat koneksi kabel atau nirkabel langsung ke jaringan. Koneksi terjadi melalui atau melalui jaringan perantara, biasanya WAN publik. Secara historis, akses jaringan jarak jauh mungkin menggunakan modem analog yang terhubung melalui sistem telepon. Saat ini, sebagian besar akses jarak jauh diimplementasikan sebagai jaringan pribadi virtual (VPN), yang berjalan melalui Internet.

Mengingat bahwa, mengelola akses jarak jauh pada dasarnya melibatkan tugas yang sama seperti mengelola jaringan lokal. Hanya pengguna resmi yang telah berhasil diautentikasi yang diizinkan mengakses sumber daya jaringan lokal dan saluran komunikasi. Kompleksitas tambahan muncul karena bisa lebih sulit untuk memastikan keamanan stasiun kerja dan server jarak jauh dan ada peluang lebih besar untuk login jarak jauh untuk dieksploitasi.

Pembuatan server akses jarak jauh (RAS) harus disertai dengan dokumentasi yang menjelaskan penggunaan layanan, risiko keamanan dan tindakan pencegahan, dan pengguna layanan yang berwenang. Juga harus ada otorisasi untuk menjalankan layanan dari manajer jaringan. Kebijakan akses jarak jauh kemudian harus menerapkan langkah-langkah yang diidentifikasi melalui kompilasi dokumentasi. Pembatasan kebijakan tipikal adalah:

- Membatasi akses ke pengguna atau grup yang ditentukan.
- Membatasi akses ke waktu yang ditentukan dalam sehari atau hari-hari tertentu dalam seminggu.

- Membatasi hak istimewa di jaringan lokal (idealnya, pengguna jarak jauh hanya akan diizinkan mengakses bagian jaringan yang ditentukan dengan jelas).
- Mencatat dan mengaudit akses masuk dan upaya masuk.

Selain itu, rencana pengelolaan harus memastikan bahwa RAS dan perangkat keras lainnya selalu diperbarui dengan pembaruan perangkat lunak atau firmware terbaru. Akses administratif ke perangkat juga harus diamankan, menggunakan otentikasi yang kuat.

Protokol Tunneling dan Enkapsulasi

Sebagian besar solusi akses jaringan jarak jauh modern menggunakan infrastruktur akses Internet dan menyiapkan terowongan aman untuk komunikasi pribadi melalui Internet. Ini disebut sebagai jaringan pribadi virtual (VPN). Sebagian besar situs bisnis dan perumahan memiliki konektivitas Internet, sehingga solusi ini sangat efisien dalam hal biaya. Perhatian utama adalah menyediakan keamanan untuk transmisi yang melewati jaringan publik dan mencegah pengguna yang tidak sah menggunakan koneksi VPN.

Protokol Point-to-Point
VPN bergantung pada protokol tunneling. Tunneling digunakan ketika host sumber dan tujuan berada di jaringan logis yang sama tetapi terhubung melalui jaringan fisik yang berbeda. Point-to-Point Protocol (PPP) adalah protokol enkapsulasi yang bekerja pada lapisan Data Link (Layer 2). PPP digunakan untuk mengenkapsulasi paket IP untuk transmisi melalui saluran digital serial. PPP tidak memiliki mekanisme keamanan, jadi harus digunakan dengan protokol lain untuk menyediakan terowongan yang aman.

Generic Routing Encapsulation
Di mana PPP bekerja di Layer 2, Generic Routing Encapsulation (GRE) bekerja di Layer 3. Sebuah paket GRE sendiri dapat merangkum paket IP (atau sebagian besar jenis protokol lapisan jaringan lainnya) sebagai muatannya. Paket GRE "luar" diberi nomor protokol 47 dan memiliki bidang sumber IP dan alamat headernya sendiri. Paket GRE kemudian dienkapsulasi dalam bingkai Layer 2 untuk transmisi ke router hop berikutnya. Setiap router perantara hanya memeriksa header GRE luar untuk menentukan tujuan penerusan. Di tujuan akhir, router penerima mende-enkapsulasi paket GRE untuk mengekstrak muatan IP bagian dalam dan meneruskan paket bagian dalam itu ke tujuannya. GRE tidak memiliki mekanisme untuk mengautentikasi pengguna atau perangkat dan sering digunakan dengan protokol lain dalam solusi VPN.

IP Security
Internet Protocol Security (IPSec) juga beroperasi pada lapisan jaringan (Layer 3) dari model OSI untuk mengenkripsi paket yang melewati jaringan apa pun. IPSec sering digunakan dengan protokol lain untuk menyediakan keamanan koneksi, tetapi semakin sering digunakan sebagai protokol VPN asli.

Transport Layer Security
Transport Layer Security (TLS) melalui TCP atau datagram TLS (DTLS) melalui UDP dapat digunakan untuk mengenkapsulasi frame atau paket IP. Kelemahan utama adalah karena TLS sudah beroperasi pada lapisan sesi, header dari paket dalam dan luar menambah overhead yang signifikan.

Client-to-Site Virtual Private Networks

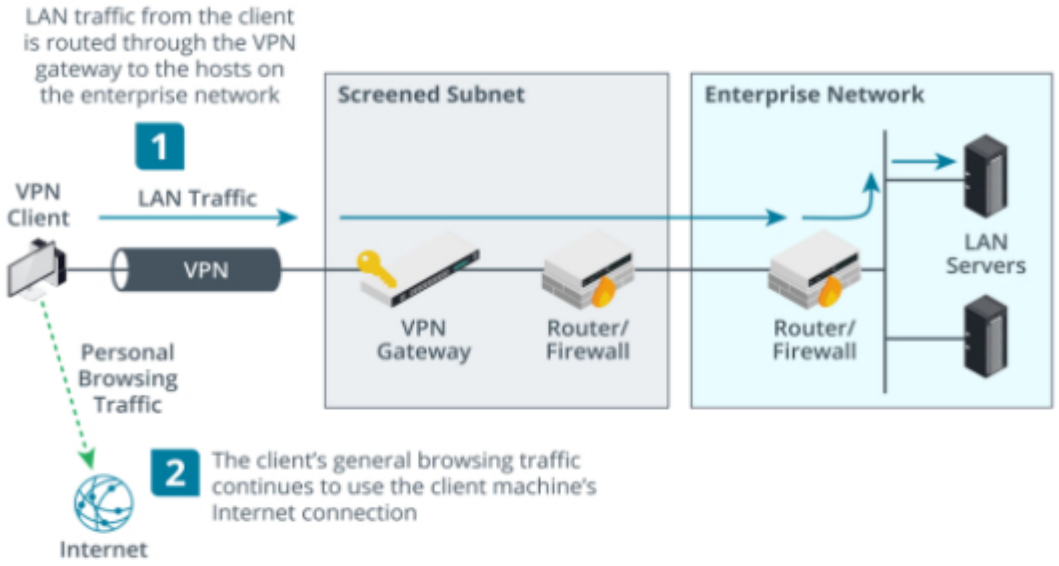
VPN dapat diimplementasikan dalam beberapa topologi. Dalam topologi akses klien-ke-situs atau jarak jauh, klien VPN terhubung melalui jaringan publik ke gateway VPN (router berkemampuan VPN) yang diposisikan di tepi jaringan lokal (biasanya server akses VPN akan berada di layar subjaringan). Client-to-site adalah model "telecommuter", yang memungkinkan pekerja rumahan dan karyawan yang bekerja di lapangan untuk terhubung ke jaringan perusahaan.

VPN klien-ke-situs dapat dikonfigurasi menggunakan sejumlah protokol. Solusi SSL/TLS VPN menggunakan sertifikat untuk membuat terowongan aman. Salah satu contohnya adalah Secure Socket Tunneling Protocol (SSTP) Microsoft. Cisco Layer 2 Tunneling Protocol (L2TP) juga banyak digunakan, bersama dengan IPSec. Semua solusi ini memerlukan perangkat lunak klien untuk beroperasi. Sebagian besar solusi VPN menggunakan arsitektur EAP dan AAA/RADIUS untuk mengotentikasi perangkat klien dan pengguna.

Tips: Point-to-Point Tunneling Protocol (PPTP) Microsoft pernah digunakan secara luas tetapi memiliki terlalu banyak kelemahan keamanan untuk digunakan dengan aman.

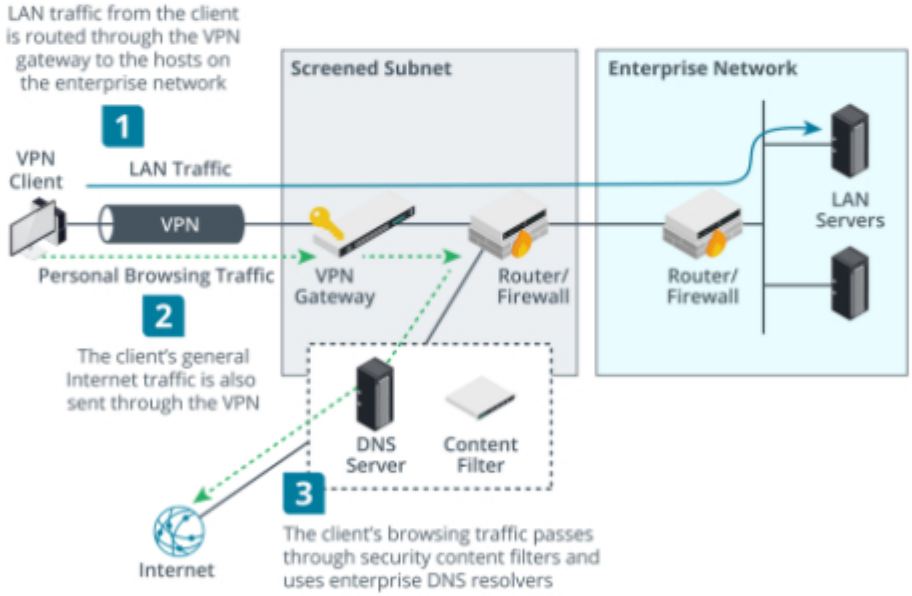
Saat klien yang terhubung ke VPN akses jarak jauh mencoba mengakses situs lain di Internet, ada dua cara untuk mengelola koneksi:

- Split tunnel : klien mengakses Internet secara langsung menggunakan konfigurasi IP "asli" dan server DNS-nya.



Split tunnel VPN traffic flow. (Images © 123RF.com.)

- Full tunnel : Akses internet dimediasi oleh jaringan perusahaan, yang akan mengubah alamat IP klien dan server DNS dan dapat menggunakan proxy.



Full tunnel VPN traffic flow. (Images © 123RF.com.)

Terowongan penuh menawarkan keamanan yang lebih baik, tetapi terjemahan alamat jaringan dan operasi DNS yang diperlukan dapat menyebabkan masalah dengan beberapa situs web, terutama layanan cloud. Ini juga berarti lebih banyak data yang disalurkan melalui tautan dan koneksi dapat menunjukkan latensi yang lebih tinggi.

Remote Host Access and Remote Desktop Gateways

VPN akses jarak jauh mengacu pada perluasan akses jaringan lokal melalui jaringan publik perantara, sehingga komputer jarak jauh secara efektif bergabung ke jaringan lokal. Akses jarak jauh juga dapat merujuk ke akses host jarak jauh, di mana pengguna mengoperasikan komputer atau mengkonfigurasi peralatan jaringan tanpa harus menggunakan terminal lokal. Jenis akses host jarak jauh ini dapat diimplementasikan dalam jaringan lokal atau melalui jaringan publik. Ini dapat digunakan untuk berbagai tujuan:

- Konfigurasi jarak jauh dari peralatan jaringan. Sebagian besar peralatan ini tanpa kepala (tidak memiliki monitor video atau perangkat input) dan koneksi jarak jauh adalah satu-satunya opsi konfigurasi yang praktis. Jenis koneksi ini biasanya diimplementasikan menggunakan Secure Shell (SSH).
- Koneksi desktop jarak jauh memungkinkan administrator untuk mengonfigurasi server atau pengguna untuk mengoperasikan komputer dari jarak jauh. Jika protokol desktop jarak jauh menyediakan akses GUI, protokol lain dapat digunakan untuk akses terminal saja.
- Gateway desktop jarak jauh memungkinkan akses pengguna ke aplikasi jaringan. Gateway juga dapat digunakan untuk menghubungkan pengguna ke desktop virtual, di mana OS klien dan perangkat lunak aplikasi disediakan sebagai alat virtual. Atau, gateway desktop jarak jauh adalah sarana untuk mengimplementasikan VPN tanpa klien.

Remote Desktop Protocol and Virtual Network Computing

Remote Desktop Protocol (RDP) Microsoft dapat digunakan untuk mengakses mesin fisik secara satu-ke-satu. Atau, situs dapat mengoperasikan gateway desktop jarak jauh yang memfasilitasi akses ke desktop virtual atau aplikasi individual yang berjalan di server jaringan (docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to -rds). Layanan serupa disediakan oleh produk Citrix (citrix.com/products).

Ada beberapa alternatif populer untuk Remote Desktop. Sebagian besar mendukung akses jarak jauh ke platform selain Windows (macOS dan iOS, Linux, Chrome OS, dan Android misalnya). Contohnya termasuk TeamViewer (teamviewer.com/en) dan Virtual Network Computing (VNC) , yang diimplementasikan oleh beberapa penyedia berbeda (terutama realvnc.com/en).

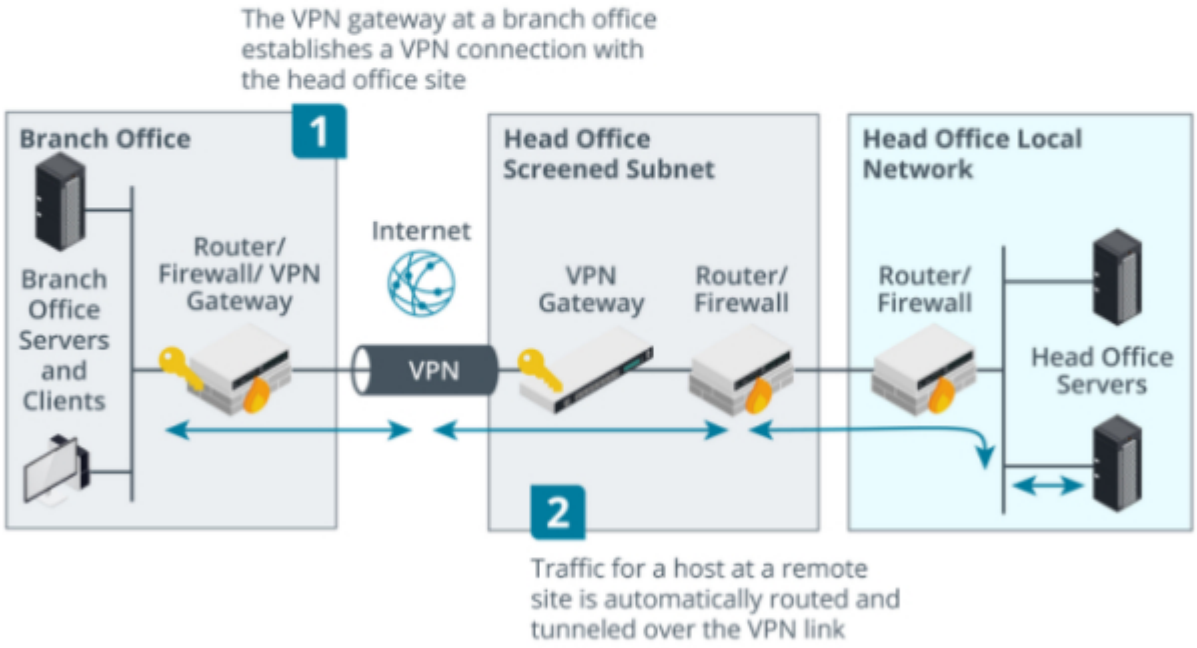
Clientless VPNs

Secara tradisional, produk desktop jarak jauh dan VPN klien-ke-situs memerlukan aplikasi klien yang mengimplementasikan protokol dan metode autentikasi yang didukung oleh desktop jarak jauh/gerbang VPN. Elemen kanvas yang diperkenalkan di HTML5 memungkinkan browser menggambar dan memperbarui desktop dengan jeda yang relatif sedikit. Itu juga dapat menangani audio. Ini memungkinkan perangkat lunak browser biasa terhubung ke desktop

jarak jauh atau VPN. Ini disebut sebagai VPN HTML5 atau VPN tanpa klien (guacamole.apache.org). Solusi ini juga menggunakan protokol yang disebut WebSockets, yang memungkinkan pesan dua arah dikirim antara server dan klien tanpa memerlukan overhead permintaan HTTP terpisah.

Site-to-Site Virtual Private Networks

VPN juga dapat digunakan dalam model situs-ke-situs untuk menghubungkan dua atau lebih jaringan pribadi. Di mana koneksi VPN akses jarak jauh biasanya dimulai oleh klien, VPN situs-ke-situs dikonfigurasi untuk beroperasi secara otomatis. Gateway bertukar informasi keamanan menggunakan protokol apa pun yang menjadi dasar VPN. Ini membangun hubungan kepercayaan antara gateway dan menyiapkan koneksi aman untuk menyalurkan data. Host di setiap situs tidak perlu dikonfigurasi dengan informasi apa pun tentang VPN. Infrastruktur perutean di setiap situs menentukan apakah akan mengirimkan lalu lintas secara lokal atau mengirimkannya melalui terowongan VPN. Ini juga disebut sebagai tunneling wajib. Tunnel wajib dapat ditempatkan secara permanen (statis), atau dapat ditempatkan berdasarkan jenis data atau klien (dinamis).



Site-to-site VPN. (Images © 123rf.com.)

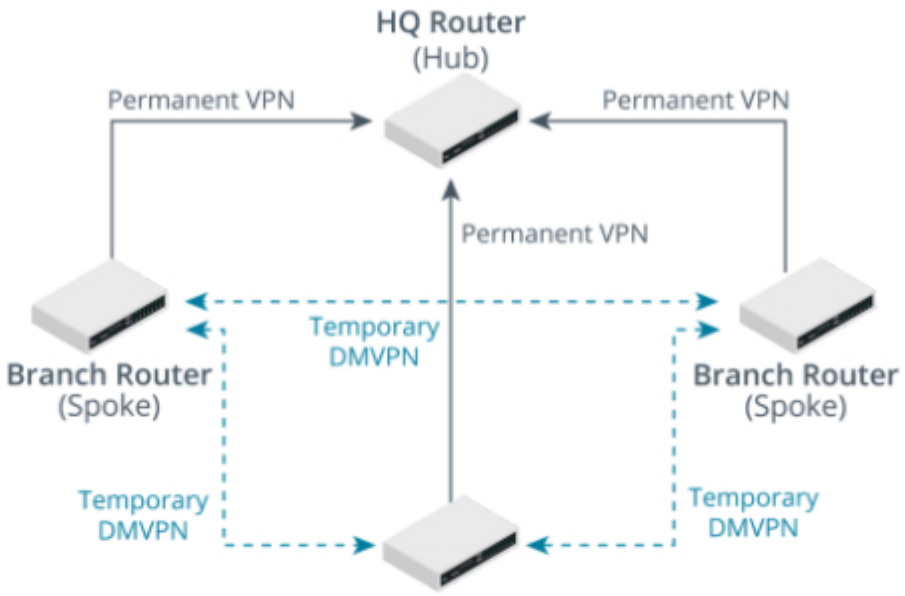
Tips: VPN tidak selalu dibuat melalui Internet publik. Penyedia layanan WAN dapat mengimplementasikan VPN melalui jaringannya. Penyedia dapat menggunakan teknologi mirip VLAN untuk mengisolasi data pelanggan dari lalu lintas lain. Ini adalah model umum untuk VPN situs-ke-situs.

Kiat: Meskipun VPN dicakup di sini sebagai bagian dari akses jarak jauh, VPN dapat digunakan dengan berguna di jaringan lokal sebagai jenis segmentasi jaringan. Misalnya, departemen pengembangan produk mungkin perlu menyediakan komunikasi yang aman dengan departemen pemasaran.

Hub and Spoke VPNs and VPN Headends

VPN site-to-site yang melibatkan lebih dari dua situs menghubungkan situs jarak jauh (or spokes) ke situs kantor pusat (hub) dengan menggunakan terowongan statis yang dikonfigurasi antara hub dan masing-masing jari-jari. Ini disebut sebagai topologi hub dan spoke. Router VPN yang dipasang di kantor pusat atau hub harus menjadi mesin yang kuat yang mampu menggabungkan volume lalu lintas yang tinggi. Router VPN ini juga disebut sebagai VPN headend. Headend VPN biasanya dipasang dalam grup untuk penyeimbangan beban dan toleransi kesalahan. Headend VPN harus dapat diskalakan untuk memenuhi tingkat permintaan yang berubah. Router VPN yang dipasang di jari-jari, disebut sebagai router kantor cabang.

VPN multipoint dinamis (DMVPN) memungkinkan VPN diatur secara dinamis sesuai dengan kebutuhan dan permintaan lalu lintas. Konsep aslinya dikembangkan oleh Cisco tetapi telah diadopsi oleh vendor lain dan sekarang berjalan di berbagai platform router. DMVPN memungkinkan penggunaan topologi mesh dinamis antara beberapa situs jarak jauh, secara efektif mengatur VPN langsung, daripada situs jarak jauh yang harus merutekan lalu lintas melalui hub. Setiap situs dapat berkomunikasi dengan semua jari-jari lainnya secara langsung di mana pun mereka berada.



DMVPN topology. Each branch office establishes a permanent VPN with the HQ (hub) but can also create spoke-to-spoke VPNs dynamically. (Images © 123RF.com.)

Untuk mengkonfigurasi DMVPN, setiap router situs jarak jauh masih terhubung ke router hub menggunakan terowongan IPSec. Karena sebagian besar lalu lintas situs jarak jauh kemungkinan besar berada di kantor pusat utama, ini memastikan lalu lintas normal ini ditangani secara efisien. Jika dua situs jarak jauh (jari-jari) ingin berkomunikasi satu sama lain, jari-jari yang memicu tautan menginformasikan hub. Hub akan memberikan detail koneksi untuk jari-jari lain yang memfasilitasi terowongan IPSec dinamis yang akan dibuat langsung di antara kedua jari-jari. Proses ini meminta penggunaan Next Hop Router Protocol (NHRP) untuk mengidentifikasi alamat tujuan dan tunneling GRE. GRE merangkum paket IPSec terenkripsi. Kedua situs jarak jauh menggunakan tautan komunikasi fisik antara dua lokasi tetapi semua lalu lintas mengalir melalui pengaturan terowongan VPN terenkripsi sementara di antara mereka. DMVPN kemudian akan memutuskan berapa lama VPN sementara ini tetap ada berdasarkan pengatur waktu dan arus lalu lintas.

Dengan cara ini, DMVPN memungkinkan situs jarak jauh untuk terhubung satu sama lain melalui WAN publik atau Internet, seperti saat menggunakan konferensi video, tetapi tidak memerlukan koneksi VPN statis antar situs. Penerapan IPSec VPN sesuai permintaan ini lebih efisien. Kebijakan perutean dapat digunakan untuk memilih jalur yang paling andal antara situs jarak jauh, yang berpotensi mengurangi kemungkinan latensi dan jitter yang memengaruhi layanan suara/video apa pun yang berjalan melalui VPN.

Internet Protocol Security

Internet Protocol Security (IPSec) dapat digunakan untuk mengamankan komunikasi IPv4 dan/atau IPv6 pada jaringan lokal dan sebagai protokol akses jarak jauh.

Setiap host yang menggunakan IPSec harus diberi kebijakan. Kebijakan IPSec menetapkan mekanisme otentikasi dan juga protokol dan mode untuk koneksi. Host harus dapat mencocokkan setidaknya satu metode keamanan yang cocok untuk koneksi yang akan dibuat. Ada dua protokol inti di IPSec, yang dapat diterapkan secara tunggal atau bersama-sama, tergantung pada kebijakannya.

Authentication Header

Protokol Authentication Header (AH) melakukan hash kriptografik di seluruh paket, termasuk header IP, ditambah kunci rahasia bersama (hanya diketahui oleh host yang berkomunikasi), dan menambahkan rahasia ini di headernya sebagai Nilai Pemeriksaan Integritas (ICV) . Penerima melakukan fungsi yang sama pada paket dan kunci dan harus memperoleh nilai yang sama untuk mengonfirmasi bahwa paket tersebut belum dimodifikasi. Payload tidak dienkripsi sehingga protokol ini tidak memberikan kerahasiaan. Juga, penyertaan bidang header IP di ICV berarti bahwa pemeriksaan akan gagal di seluruh gateway NAT, di mana alamat IP ditulis ulang. Akibatnya, AH tidak sering digunakan.



IPSec datagram using AH-The integrity of the payload and IP header is ensured by the Integrity Check Value (ICV), but the payload is not encrypted.

Encapsulating Security Payload (ESP) memberikan kerahasiaan dan/atau otentikasi dan integritas. Ini dapat digunakan untuk mengenkripsi paket daripada hanya menghitung hash. ESP melampirkan tiga bidang ke paket: header, trailer (menyediakan padding untuk fungsi kriptografi), dan Nilai Pemeriksaan Integritas. Tidak seperti AH, ESP mengecualikan header IP saat menghitung ICV.



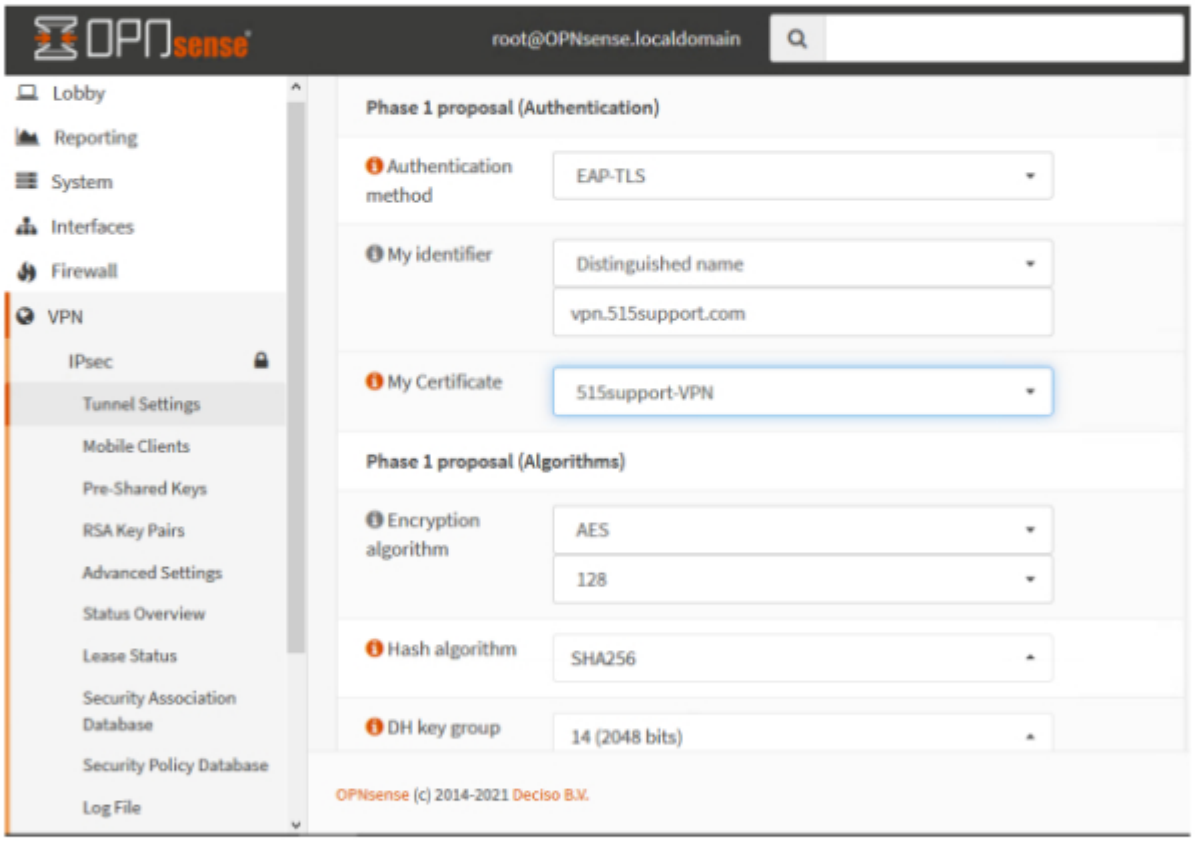
IPSec datagram using ESP-The TCP header and payload from the original packet is encapsulated within ESP and encrypted to provide confidentiality.

Tips: Dengan ESP, algoritma untuk kerahasiaan (cipher simetris) dan otentikasi/integritas (fungsi hash) biasanya diterapkan bersama-sama. Namun, dimungkinkan untuk menggunakan satu atau yang lain.

Tips: Prinsip-prinsip yang mendasari IPSec sama untuk IPv4 dan IPv6, tetapi format headernya berbeda. IPSec menggunakan header ekstensi di IPv6 sementara di IPv4, ESP dan AH dialokasikan nomor protokol IP baru (50 dan 51), dan memodifikasi header IP asli atau merangkum paket asli, tergantung pada mode transport atau tunnel yang digunakan.

Mode IKE dan IPSec

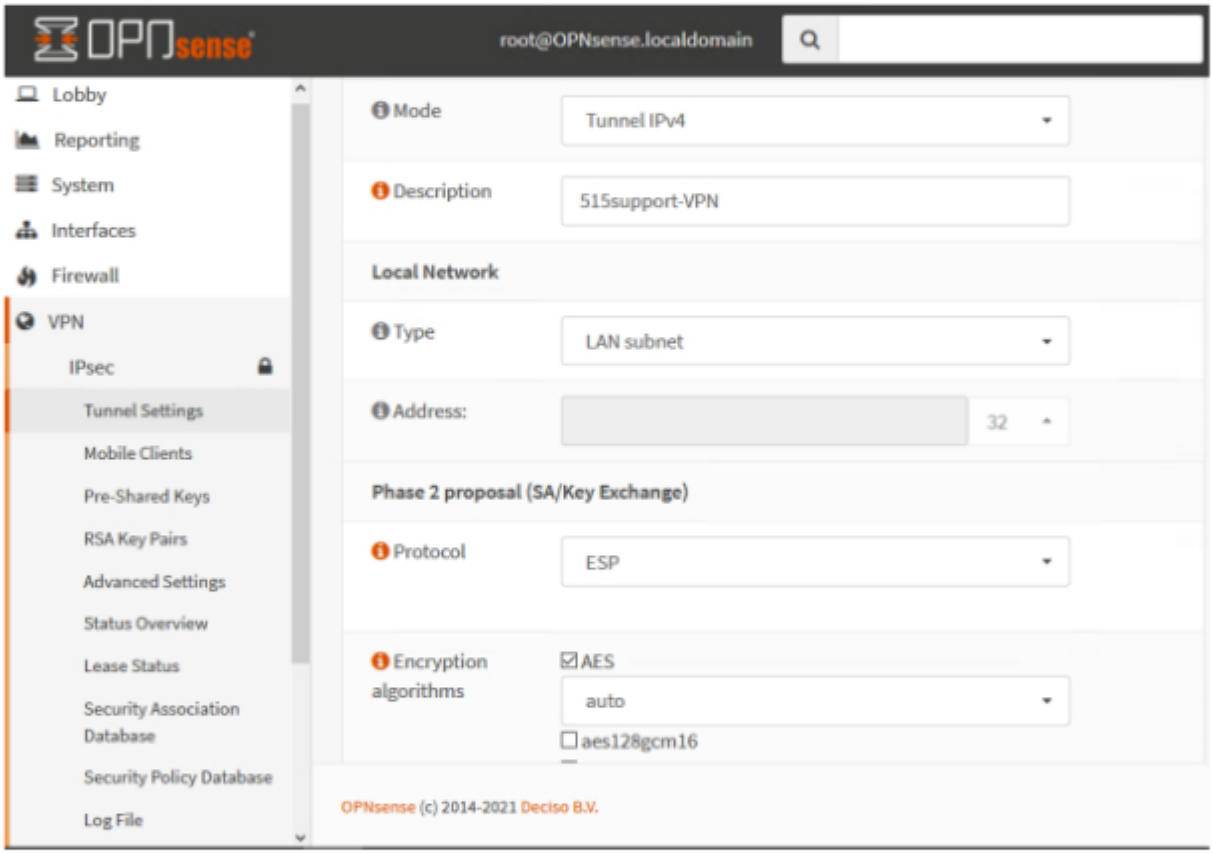
Enkripsi dan fungsi hashing IPSec bergantung pada rahasia bersama. Rahasia harus dikomunikasikan ke kedua host dan host harus mengkonfirmasi identitas satu sama lain (mutual authentication). Protokol Internet Key Exchange (IKE) menangani otentikasi dan pertukaran kunci, yang disebut sebagai Asosiasi Keamanan (SA).



Configuring IKE in the OPNsense security appliance. (Screenshot used with permission from OPNsense.)

IPSec can be used in two modes:

- Transport mode : mode ini digunakan untuk mengamankan komunikasi antara host di jaringan pribadi (implementasi ujung ke ujung). Ketika ESP diterapkan dalam mode transport, header IP untuk setiap paket tidak dienkripsi, hanya data payload. Jika AH digunakan dalam mode transport, AH dapat memberikan integritas untuk header IP.
- Tunnel mode : mode ini digunakan untuk komunikasi antara gateway VPN melalui jaringan yang tidak aman (membuat VPN). Ini juga disebut sebagai implementasi router. Dengan ESP, seluruh paket IP (header dan payload) dienkripsi dan dienkapsulasi sebagai datagram dengan header IP baru. AH tidak memiliki kasus penggunaan nyata dalam mode terowongan, karena kerahasiaan biasanya diperlukan.



Configuring an IPSec tunnel in the OPNsense security appliance. (Screenshot used with permission from OPNsense.)

Out-of-Band Management Methods

Beberapa peralatan jaringan, seperti sakelar yang tidak dikelola, tidak menawarkan opsi konfigurasi atau antarmuka apa pun. Anda hanya perlu mencolokkannya, dan mereka beroperasi secara otomatis. Sakelar dan peralatan yang dikelola, seperti router, firewall, sakelar, dan titik akses, mendukung fungsi yang lebih kompleks dan dapat dikonfigurasi serta

dipantau melalui beberapa antarmuka. Fungsi alat yang dikelola dapat diakses melalui salah satu antarmuka manajemen perangkat. Sebuah alat dapat mendukung antarmuka berikut:

- Console Port : Ini memerlukan menghubungkan perangkat yang menjalankan perangkat lunak emulator terminal (laptop, misalnya) ke perangkat melalui antarmuka fisik terpisah menggunakan kabel konsol (atau rollover) khusus. Emulator terminal kemudian dapat digunakan untuk memulai antarmuka baris perintah (CLI).
- AUX port : Port ini dirancang untuk terhubung ke modem analog dan menyediakan akses jarak jauh melalui tautan dial-up. Setelah port AUX diaktifkan dan dikonfigurasi, modem dapat dihubungkan dengannya menggunakan kabel serial RS-232, kabel rollover RJ-45 berkabel khusus dan adaptor terminal (RJ-45 hingga DB9), atau kabel manajemen (RJ -45 hingga DB9). Konfigurasikan modem dengan pengaturan tautan serial yang sesuai (lihat panduan vendor), sambungkan ke saluran telepon yang sesuai, dan alokasikan nomor ekstensi. Host jarak jauh dapat terhubung ke CLI alat dengan menggunakan program emulasi terminal seperti HyperTerminal atau Putty.
- Management port :Ini berarti mengonfigurasi antarmuka jaringan virtual dan alamat IP pada perangkat yang akan digunakan untuk fungsi manajemen dan menghubungkannya melalui salah satu port Ethernet normal. Port harus diaktifkan untuk fungsi ini (beberapa peralatan dilengkapi dengan port manajemen khusus). Menggunakan Telnet (tidak aman) atau Secure Shell (SSH) untuk terhubung ke CLI dari jarak jauh melalui antarmuka manajemen dengan cara ini disebut sebagai terminal virtual.



USB and RJ-45 type console ports plus AUX and other management interfaces on a router. (Image © 123RF.com.)

Metode manajemen dapat digambarkan sebagai in-band atau out-of-band (OOB). Tautan manajemen in-band adalah tautan yang berbagi lalu lintas dengan komunikasi lain di jaringan "produksi". Port konsol adalah metode manajemen out-of-band secara fisik; link terbatas pada perangkat yang terpasang. Saat Anda menggunakan antarmuka manajemen berbasis browser atau terminal virtual, tautan dapat dibuat out-of-band dengan menghubungkan port yang digunakan untuk akses manajemen ke infrastruktur jaringan yang terpisah secara fisik. Jelas, ini mahal untuk diterapkan, tetapi manajemen out-of-band lebih aman dan berarti bahwa akses ke perangkat dipertahankan ketika ada masalah yang mempengaruhi jaringan produksi.

Dengan koneksi in-band, keamanan yang lebih baik dapat diterapkan dengan menggunakan VLAN untuk mengisolasi lalu lintas manajemen. Ini mempersulit calon penyadap untuk melihat atau memodifikasi lalu lintas yang melewati antarmuka manajemen. OOB virtual semacam ini masih berarti bahwa akses dapat dikompromikan oleh kegagalan jaringan di seluruh sistem.

Tips: Gunakan protokol koneksi aman (HTTPS daripada HTTP, atau SSH daripada Telnet) untuk antarmuka manajemen. Ini juga berlaku untuk OOB, tetapi sangat penting untuk manajemen in-band.

Modul 17

Explaining Organizational and Physical Security Concepts

Explain Organizational Documentation and Policies

- Pendahuluan: Menjelaskan Dokumentasi dan Kebijakan Organisasi
  Dalam topik ini, Anda akan belajar menjelaskan bagaimana dokumentasi manajemen konfigurasi, diagram, kebijakan tertulis, dan praktik terbaik digunakan untuk mengelola dan memecahkan masalah jaringan.

- Rencana dan Prosedur Operasi
  Menjalankan jaringan yang efisien bukan hanya tentang memasang kabel dan perangkat jaringan. Administrasi jaringan dalam hal dokumentasi dan manajemen adalah tugas penting.

    - ***Configuration Management***
      Configuration Management berarti mengidentifikasi dan mendokumentasikan semua infrastruktur dan perangkat yang dipasang di situs. ITIL® adalah dokumentasi populer tentang aktivitas dan proses praktik yang baik dan terbaik untuk memberikan layanan TI. Di bawah ITIL, manajemen konfigurasi diimplementasikan menggunakan elemen-elemen berikut:

        - Aset layanan adalah hal, proses, atau orang yang berkontribusi pada penyampaian layanan TI. Setiap aset harus diidentifikasi dengan semacam label.

        - *A Configuration Item* (CI) adalah aset yang memerlukan prosedur manajemen khusus agar dapat digunakan untuk memberikan layanan. CI ditentukan oleh atributnya.

        - Sebuah baseline mendokumentasikan status CI yang disetujui atau disahkan. Hal ini memungkinkan proses audit untuk mendeteksi perubahan yang tidak terduga atau tidak sah. Garis dasar dapat berupa garis dasar konfigurasi (misalnya, ACL diterapkan ke firewall) atau garis dasar kinerja (seperti throughput yang dicapai oleh firewall).

        - *A Configuration Management System* (CMS) adalah alat dan database yang mengumpulkan, menyimpan, mengelola, memperbarui, dan menyajikan informasi tentang CI. Jaringan kecil mungkin menangkap informasi ini dalam spreadsheet dan diagram; ada aplikasi khusus untuk CMS perusahaan.

    - ***Change Management***

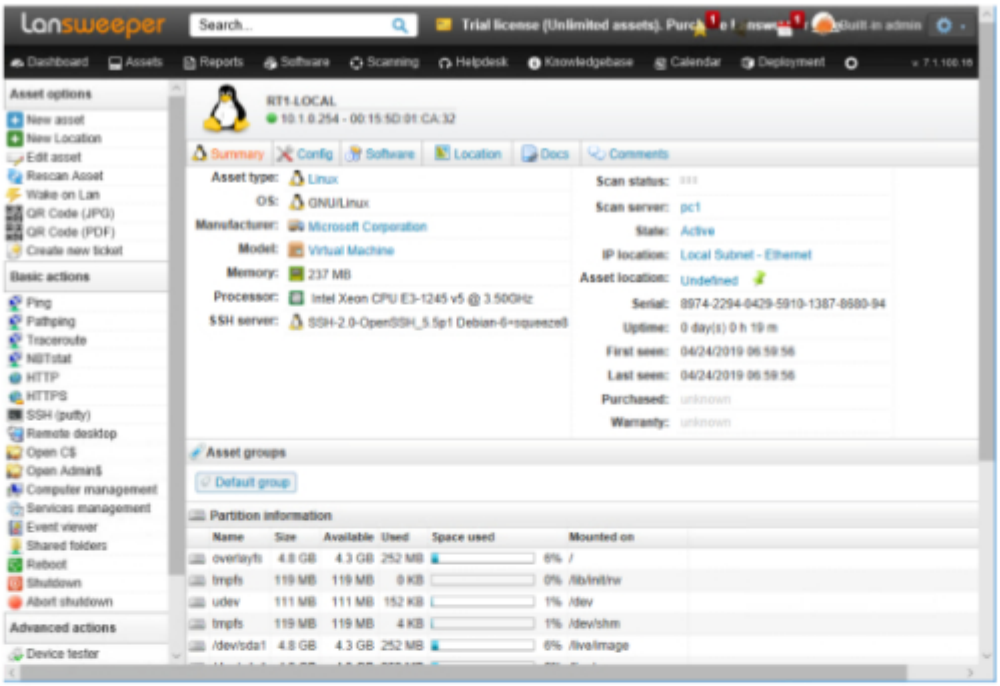
Proses manajemen perubahan yang terdokumentasi meminimalkan risiko waktu henti yang tidak terjadwal dengan menerapkan perubahan secara terencana dan terkendali. Kebutuhan untuk berubah sering digambarkan sebagai reaktif, di mana perubahan dipaksakan pada organisasi, atau sebagai proaktif, di mana kebutuhan akan perubahan dimulai secara internal. Perubahan juga dapat dikategorikan menurut potensi dampak dan tingkat risikonya (misalnya, besar, signifikan, kecil, atau normal).

Dalam proses manajemen perubahan formal, kebutuhan atau alasan untuk perubahan dan prosedur untuk menerapkan perubahan tersebut dicatat dalam dokumen *Request for Change* (RFC) dan diajukan untuk disetujui. RFC kemudian akan dipertimbangkan pada tingkat yang sesuai dan pemangku kepentingan yang terkena dampak akan diberitahu. Perubahan besar atau signifikan dapat dikelola sebagai proyek terpisah dan memerlukan persetujuan melalui *Change Advisory Board* (CAB).

- ***Standard Operating Procedures***
  Perubahan konfigurasi harus dilakukan hanya jika ada tiket pekerjaan yang valid yang mengizinkan perubahan. Ini berarti bahwa aktivitas semua personel jaringan, apakah itu menginstal perangkat baru atau pemecahan masalah, dicatat dalam log pekerjaan. Dalam lingkungan yang terdokumentasi sepenuhnya, setiap tugas akan diatur oleh *standard operating procedure* (SOP). SOP menetapkan tujuan dan pertimbangan utama, seperti anggaran, keamanan, atau standar kontak pelanggan, untuk melakukan tugas dan mengidentifikasi garis tanggung jawab dan otorisasi untuk melakukannya. SOP juga dapat berisi langkah-langkah terperinci untuk menyelesaikan tugas dengan cara yang disetujui, atau langkah-langkah ini dapat disajikan sebagai instruksi kerja.

- System Life Cycle Plans and Procedures
  Sangat penting bagi organisasi untuk memiliki inventarisasi aset berwujud dan tidak berwujud. Dalam hal manajemen jaringan, aset adalah peralatan jaringan (router, sakelar, perangkat manajemen ancaman, titik akses), server, stasiun kerja, dan infrastruktur jaringan pasif (pengkabelan dan koneksi silang).

  - Laporan Audit
    Laporan audit berfokus pada mengidentifikasi dan mencatat aset. Ada banyak rangkaian perangkat lunak dan solusi perangkat keras terkait yang tersedia untuk membantu pelacakan audit dan pengelolaan inventaris. Basis data manajemen aset dapat dikonfigurasi untuk menyimpan informasi sebanyak atau sesedikit yang dianggap perlu, meskipun data tipikal adalah jenis, model, nomor seri, ID aset, lokasi, pengguna, nilai, dan informasi layanan. Untuk setiap catatan aset, juga harus ada salinan atau tautan ke dokumentasi vendor yang sesuai. Ini termasuk faktur dan kontrak garansi/dukungan serta panduan dukungan dan pemecahan masalah.



Produk seperti Lansweeper membantu manajemen inventaris dengan memindai host jaringan dan menyusun database informasi aset secara otomatis. (Tangkapan layar digunakan dengan izin dari Lansweeper.)

- Laporan Penilaian
  Jika laporan audit berfokus pada mengidentifikasi dan mendokumentasikan aset, laporan penilaian mengevaluasi konfigurasi dan penerapan aset tersebut, seperti penyimpangan dari konfigurasi atau kinerja dasar. Laporan akan membuat rekomendasi di mana jaringan tidak memenuhi tujuan untuk kinerja atau keamanan. Laporan audit dan penilaian sering dikontrakkan kepada pihak ketiga dan mungkin didorong oleh tuntutan peraturan atau kepatuhan.

- Siklus Hidup Sistem
  Salah satu fungsi audit dan penilaian adalah mengelola siklus hidup sistem. Peta jalan siklus hidup sistem mengacu pada akuisisi, penyebaran, penggunaan, dan penonaktifan aset yang terkontrol. Laporan audit dan penilaian dapat mengidentifikasi aset yang tidak lagi didukung sepenuhnya oleh vendor atau yang tidak lagi memenuhi persyaratan kinerja atau keamanan.

- Diagram Jaringan Fisik
  Dokumentasi aset dan item konfigurasi (CI) menggunakan diagram secara signifikan. Diagram adalah cara terbaik untuk menangkap hubungan kompleks antara elemen jaringan. Penting untuk tidak mencoba memasukkan terlalu banyak informasi karena hal ini cenderung membuat diagram terlalu rumit untuk berguna. Akibatnya, sejumlah besar jenis diagram digunakan dalam manajemen jaringan. Satu perbedaan mendasar adalah

antara diagram jaringan fisik dan logis. Di dalam kelas diagram jaringan fisik, tipe berikut biasanya digunakan.

- Rencana denah
  Denah lantai adalah diagram rinci dari lokasi kabel dan port. Misalnya, Anda mungkin menggunakan denah lantai untuk mendokumentasikan lokasi port dinding dan kabel di kantor. Denah lantai yang akurat secara fisik sulit untuk dirancang dan cenderung membutuhkan bantuan seorang arsitek atau profesional grafis.

- Diagram pengkabelan
  Diagram pengkabelan (atau pin-out) menunjukkan informasi terperinci tentang pemutusan pasangan terpilin pada jack RJ-45 atau RJ-48C atau Insulation Displacement Connector (IDC). Anda juga dapat menggunakan diagram pengkabelan untuk mendokumentasikan bagaimana untaian serat optik diakhiri.

  Tips: Anda harus mendokumentasikan diagram pengkabelan yang digunakan untuk menghentikan pasangan bengkok. Ethernet disambungkan dengan T568A atau T568B, dan standar yang sama harus digunakan secara konsisten di seluruh jaringan.

- Bingkai Distribusi
  Diagram lokasi port mengidentifikasi bagaimana port dinding yang terletak di area kerja dihubungkan kembali ke port dalam bingkai distribusi atau panel patch dan kemudian dari port panel patch ke port switch. Dalam sistem pengkabelan terstruktur, ada dua jenis kerangka distribusi:

  - ***Main Distribution Frame*** **(MDF)**-Lokasi untuk switching internal tingkat distribusi/inti. MDF akan menghentikan tautan batang dari beberapa Bingkai Distribusi Menengah (IDF). MDF juga berfungsi sebagai lokasi pemutusan sirkuit eksternal (WAN). Anda harus memastikan bahwa tautan WAN ke Internet atau ke kantor jarak jauh dari MDF diberi label dengan jelas dan informasi penting seperti alamat IP dan bandwidth didokumentasikan. Penyedia WAN akan menetapkan ID sirkuit, dan Anda perlu mengutip ini jika mengajukan masalah dukungan apa pun.

  - ***Intermediate Distribution Frame*** **(IDF)**-Dalam jaringan besar, satu atau lebih IDF menyediakan pemutusan untuk sakelar lapisan akses yang melayani area tertentu, seperti satu lantai kantor. Setiap IDF memiliki link trunk ke MDF. Pastikan ini diberi label dengan jelas dan berbeda dari port akses.

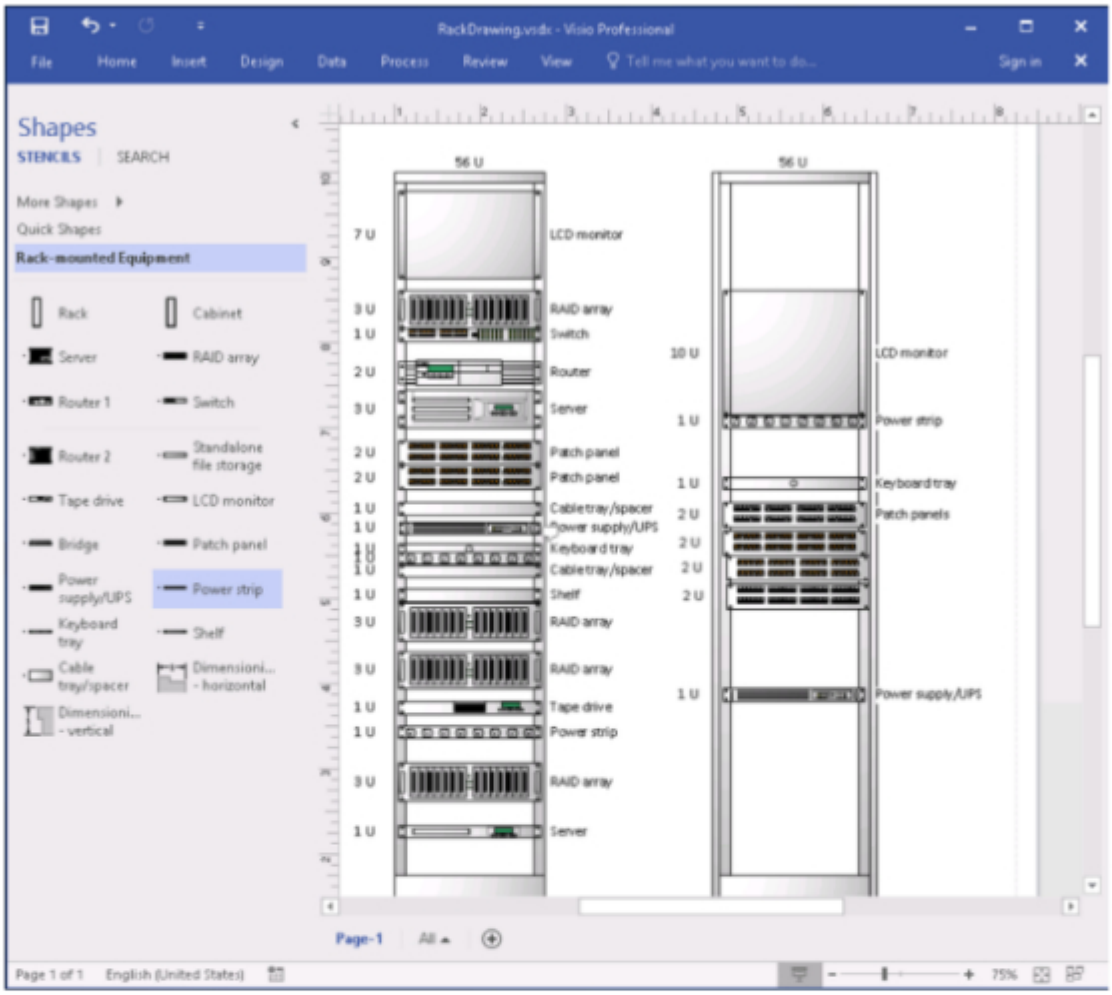
    Tips: Selain memiliki diagram, akan sangat berguna untuk mengambil foto konfigurasi saat ini dengan menggunakan kamera digital atau smartphone. Ini memberikan referensi visual tambahan untuk pemecahan masalah dan mengidentifikasi perubahan yang tidak sah.

Tips: Agar diagram fisik kabel dan aset masuk akal, harus ada sistem pelabelan untuk mengidentifikasi aset ini. Jenis konvensi penamaan port yang khas adalah untuk mengidentifikasi alfanumerik untuk kampus (untuk jaringan multikampus), gedung (untuk jaringan kampus), ruang telekomunikasi, dan pelabuhan. Misalnya, CB01-01A-D01 dapat merujuk ke terminasi kabel di Gedung Kampus Utama (CB01), ruang telekomunikasi A di lantai 1 (01A), port data 1 (D01). Kabel terstruktur dan kabel patch harus diberi label di kedua ujungnya untuk sepenuhnya mengidentifikasi sirkuit.

- Laporan Survei Situs
  Laporan survei situs nirkabel melapisi denah lantai dengan grafik yang menunjukkan kekuatan sinyal dan pemanfaatan saluran di berbagai titik di gedung.

- Diagram Rak
  Sistem rak adalah sistem rak baja yang dikonfigurasi secara khusus untuk panel patch, sakelar dan router, dan perangkat server. Rak adalah lebar standar dan dapat memuat peralatan yang menggunakan kelipatan tinggi standar 1,75" yang disebut unit (U). Misalnya, sakelar dasar mungkin berukuran 1U sementara tinggi server mungkin 4U (7").

  Diagram rak mencatat posisi setiap alat di rak. Anda dapat memperoleh stensil yang mewakili peralatan vendor dari situs web mereka atau koleksi seperti visiocafe.com. Anda dapat merekam informasi konfigurasi kunci untuk setiap item menggunakan label. Selain tag servis dan ID port serta tautan, Anda harus mengidentifikasi stopkontak mana pada catu daya tak terputus (UPS) yang terhubung ke unit catu daya (PSU) alat mana.



Merancang tata letak rak di Microsoft Visio. (Tangkapan layar digunakan dengan izin dari Microsoft.)

- Diagram Jaringan Logis versus Fisik
  Berbeda dengan diagram seperti denah lantai yang digambar dengan skala yang akurat, skema adalah representasi sistem yang disederhanakan atau diabstraksi. Dalam hal topologi jaringan fisik, diagram skematik dapat menunjukkan penempatan umum peralatan dan ruang telekomunikasi, ditambah ID perangkat dan port, tanpa mencoba untuk menangkap posisi yang tepat atau ukuran relatif dari salah satu elemen. Skema juga dapat digunakan untuk mewakili struktur logis jaringan dalam hal zona dan subnet.

  Saat Anda membuat skema jaringan, tahan keinginan untuk merepresentasikan terlalu banyak dalam satu diagram. Misalnya, buat diagram terpisah untuk lapisan PHY, Data Link, dan Logical (IP). Beberapa informasi yang sesuai untuk ditampilkan pada setiap lapisan meliputi:

- ***PHY (Physical layer)***-ID Aset dan tautan kabel. Anda dapat menggunakan kode warna atau gaya garis untuk mewakili jenis kabel (pastikan diagram memiliki legenda yang menyertainya untuk menjelaskan skema Anda).

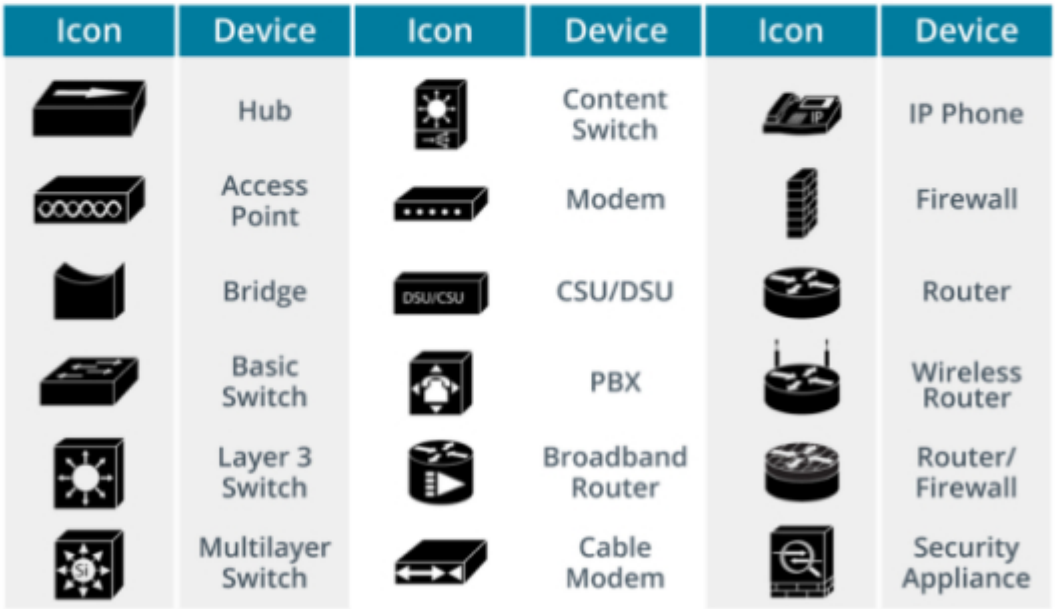
- ***Data Link (Layer 2)***-Menampilkan interkoneksi antara switch dan router, dengan ID aset (atau IP manajemen alat), ID antarmuka, serta protokol dan bandwidth link-layer. Anda dapat menggunakan ketebalan garis untuk mewakili bandwidth, tetapi untuk kejelasan, sebaiknya gunakan label juga.

- ***Logical (IP/Layer 3)***-Alamat IP antarmuka router (ditambah penetapan IP statis lainnya) dan firewall, ditambah tautan yang menunjukkan ID jaringan IP dan netmask, ID VLAN (jika digunakan), dan cakupan DHCP.

- ***Application-***Instant Server dan port TCP/UDP sedang digunakan. Anda juga dapat menyertakan informasi konfigurasi dan baseline kinerja (CPU, memori, penyimpanan, dan pemanfaatan jaringan) pada tingkat ini.

  Skema dapat digambar secara manual menggunakan alat seperti Microsoft® Visio® atau dikompilasi secara otomatis dari perangkat lunak pemetaan jaringan.

  Skema dapat menggunakan ikon perwakilan atau gambar atau gambar model produk yang sebenarnya. Sejauh ikon pergi, yang dibuat oleh Cisco diakui sebagai standar. Ini tersedia secara bebas (tanpa perubahan) dari situs web Cisco (cisco.com/c/en/us/about/brand-center/network-topology-icons.html). Beberapa perangkat yang lebih umum digunakan ditampilkan di sini:



Ikon jaringan Cisco yang umum. (Gambar © dan Courtesy of Cisco Systems, Inc. Penggunaan tidak sah tidak diizinkan.)

- Rencana dan Prosedur Tanggapan Keamanan
  Rencana dan prosedur respons keamanan menetapkan apa yang harus dilakukan ketika jenis peristiwa tertentu terjadi. Rencana-rencana tersebut berupaya untuk mengantisipasi kejadian-kejadian yang tidak diharapkan agar dampak yang ditimbulkan dapat diminimalisir.

- Rencana Tanggap Insiden
  Rencana respons insiden menetapkan prosedur, alat, metode komunikasi, dan pedoman untuk menangani insiden keamanan. Sebuah insiden adalah di mana keamanan dilanggar atau ada percobaan pelanggaran. Tanggapan insiden adalah salah satu bidang keamanan yang paling sulit untuk direncanakan dan diterapkan karena tujuannya mungkin tidak sesuai:

  1. Tujuan langsung biasanya untuk melindungi data rahasia atau meminimalkan dampak dari kehilangannya dan membangun kembali sistem kerja yang aman.

  2. Mungkin juga penting untuk menyimpan bukti insiden dengan tujuan menuntut para pelaku. Namun, pengumpulan bukti forensik dapat mengganggu ketersediaan kembali.

  3. Tindak lanjut atau analisis pelajaran yang didapat akan berusaha untuk mencegah terulangnya insiden serupa.

  Tindakan penanggap pertama segera setelah deteksi insiden dapat berdampak penting pada tujuan ini, sehingga kebijakan yang efektif dan profesional respons insiden yang terlatih sangat penting. Tanggapan insiden juga mungkin memerlukan tindakan terkoordinasi dan otorisasi dari beberapa departemen atau manajer yang berbeda, yang menambah tingkat kerumitan lebih lanjut.

- Rencana Pemulihan Bencana
  Jika respons insiden difokuskan pada pelanggaran kebijakan keamanan individu, *a disaster recovery plan* (DRP) menangani insiden skala besar. Ini biasanya akan menjadi insiden yang mengancam kinerja atau keamanan seluruh situs. Sebuah DRP harus mencapai hal berikut:

  - Identifikasi skenario untuk bencana alam dan non-alam dan pilihan untuk melindungi sistem.

  - Identifikasi tugas, sumber daya, dan tanggung jawab untuk menangani bencana. Pemulihan bencana berfokus pada tugas-tugas seperti mengalihkan layanan ke sistem atau situs failover dan memulihkan sistem dan data dari cadangan.

  - Latih staf dalam prosedur perencanaan bencana dan bagaimana bereaksi dengan baik terhadap kejadian yang merugikan.

- Rencana kelanjutan bisnis
  Dimana pemulihan bencana berfokus pada rencana untuk skenario tertentu, *business continuity plan* (BCP) atau *continuity of operations plan* (COOP) adalah kumpulan proses dan sumber daya yang memungkinkan organisasi untuk mempertahankan operasi bisnis normal dalam menghadapi beberapa peristiwa yang merugikan. Kegiatan perencanaan berkelanjutan berfokus pada fungsi yang dilakukan oleh bisnis atau organisasi lain:

  - *Business impact analysis* (BIA) mengidentifikasi misi penting dan fungsi bisnis utama dan risiko yang akan muncul jika organisasi tidak dapat memenuhinya.

  - *IT contingency planning* (ITCP) atau *IT service continuity planning* (ITSCP) memastikan bahwa fungsi-fungsi ini didukung oleh sistem TI yang tangguh, bekerja untuk mengidentifikasi dan mengurangi semua titik kegagalan dari suatu proses atau fungsi.

- Kebijakan Pengerasan dan Keamanan
  Kebijakan keamanan menetapkan kewajiban bagi setiap karyawan untuk memastikan kerahasiaan, integritas, dan ketersediaan aset data atau sistem pemrosesan yang mereka gunakan sebagai bagian dari pekerjaan mereka. Kebijakan keamanan keseluruhan ini akan dilengkapi dengan berbagai kebijakan operasional untuk mengatur area aktivitas atau konfigurasi tertentu.

- Sumber Daya Manusia (SDM) adalah departemen yang diberi tugas merekrut dan mengelola sumber daya organisasi yang paling berharga dan kritis: orang. Salah satu fungsi SDM adalah mengkomunikasikan kebijakan keamanan kepada karyawan, termasuk setiap pembaruan kebijakan. Fungsi lainnya adalah untuk menegakkan tindakan disipliner (mungkin dalam hubungannya dengan manajer departemen).

- *Onboarding*
  Onboarding adalah proses menyambut karyawan baru ke organisasi. Prinsip serupa berlaku untuk menerima pemasok atau kontraktor baru. Beberapa tugas yang paling mempengaruhi keamanan selama proses orientasi adalah sebagai berikut:

  - ***Background check***-Proses ini pada dasarnya menentukan bahwa seseorang adalah seperti yang mereka katakan dan tidak menyembunyikan aktivitas kriminal, kebangkrutan, atau hubungan yang akan membuat mereka tidak cocok atau berisiko. Karyawan yang bekerja di lingkungan dengan kerahasiaan tinggi atau dengan akses ke transaksi bernilai tinggi jelas perlu mendapat pengawasan yang lebih ketat.

  - ***Identity and access management*** (IAM)-Membuat akun bagi pengguna untuk mengakses sistem komputer, menetapkan hak istimewa yang sesuai, dan memastikan kredensial akun hanya diketahui oleh pengguna yang valid.

- ***Asset allocation***-Menyediakan komputer atau perangkat seluler untuk pengguna atau menyetujui penggunaan perangkat BYOD.

- ***Training/policies***-Jadwalkan kesadaran keamanan yang sesuai serta pelatihan dan sertifikasi yang relevan dengan peran.

- Offboarding
  Offboarding adalah proses memastikan bahwa seorang karyawan meninggalkan perusahaan dengan anggun. Dari segi keamanan, ada beberapa proses yang harus diselesaikan:

  - **IAM**-Nonaktifkan akun pengguna dan hak istimewa. Pastikan bahwa setiap aset informasi yang dibuat atau dikelola oleh karyawan tetapi dimiliki oleh perusahaan dapat diakses (dalam hal kunci enkripsi atau file yang dilindungi kata sandi).

  - ***Retrieving company assets***-Amankan perangkat seluler, kunci, kartu pintar, media USB, dan sebagainya. Karyawan perlu mengonfirmasi (dan dalam beberapa kasus membuktikan) bahwa mereka tidak menyimpan salinan aset informasi apa pun.

  - ***Returning personal assets***-Perangkat milik karyawan harus dihapus dari data dan aplikasi perusahaan. Karyawan juga dapat diizinkan untuk menyimpan beberapa aset informasi (seperti email pribadi atau informasi kontak), tergantung pada kebijakan yang berlaku.

  Kepergian beberapa jenis karyawan harus memicu proses tambahan untuk mengamankan kembali sistem jaringan. Contohnya termasuk karyawan dengan pengetahuan mendetail tentang sistem dan prosedur keamanan dan akses ke kredensial akun bersama atau umum. Kredensial ini harus segera diubah.

- Kebijakan Penggunaan
  Kebijakan penggunaan menetapkan aturan tentang bagaimana pengguna harus berinteraksi dengan sistem jaringan dan data.

- Kebijakan Kata Sandi
  Kebijakan kata sandi menginstruksikan pengguna tentang praktik terbaik dalam memilih dan memelihara kredensial akses jaringan. Kebijakan perlindungan kata sandi mengurangi risiko penyerang dapat menyusup ke akun dan menggunakannya untuk meluncurkan serangan lain di jaringan. Misalnya, pengguna harus diinstruksikan untuk tidak menuliskan kata sandi, menyimpannya dalam file yang tidak aman, atau membaginya dengan pengguna lain. Kebijakan pengelolaan kredensial juga perlu memperingatkan pengguna tentang berbagai jenis rekayasa sosial dan serangan phishing.

Kebijakan yang diberlakukan sistem dapat membantu menegakkan prinsip-prinsip manajemen kredensial dengan menetapkan persyaratan untuk kata sandi yang dipilih pengguna. Aturan berikut memberlakukan kerumitan kata sandi dan membuatnya sulit ditebak atau dikompromikan:

- ***Length***-Semakin panjang kata sandi, semakin kuat itu. Kata sandi jaringan yang kuat biasanya terdiri dari 12 hingga 16 karakter. Kata sandi atau frasa sandi yang lebih panjang mungkin digunakan untuk sistem atau perangkat penting misi yang jarang masuk.

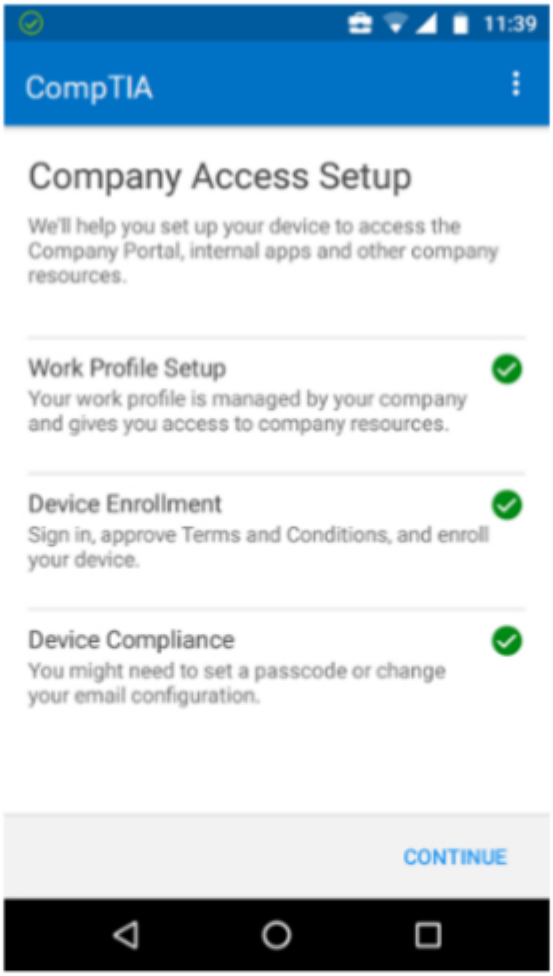
- ***Complexity***-Memvariasikan karakter dalam kata sandi membuatnya lebih tahan terhadap serangan berbasis kamus.

- ***Aging and history***-Mengharuskan kata sandi diubah secara berkala dan mencegah penggunaan kembali kata sandi yang dipilih sebelumnya.

Tips: Anda juga harus memperhatikan bahwa panduan terbaru yang dikeluarkan oleh NIST (nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf) tidak menggunakan beberapa elemen "tradisional" dari kebijakan kata sandi, seperti kerumitan dan penuaan .

- Kebijakan Penggunaan yang Dapat Diterima
  An acceptable use policy (AUP) menetapkan penggunaan produk atau layanan yang diizinkan. Ini mungkin juga menyatakan penggunaan yang dilarang secara eksplisit. Kebijakan semacam itu mungkin digunakan dalam konteks yang berbeda. Misalnya, AUP dapat diberlakukan oleh bisnis untuk mengatur bagaimana karyawan menggunakan peralatan dan layanan, seperti telepon atau akses Internet, yang disediakan untuk mereka di tempat kerja. Contoh lain mungkin ISP yang memberlakukan kebijakan penggunaan wajar yang mengatur penggunaan layanan akses Internetnya.

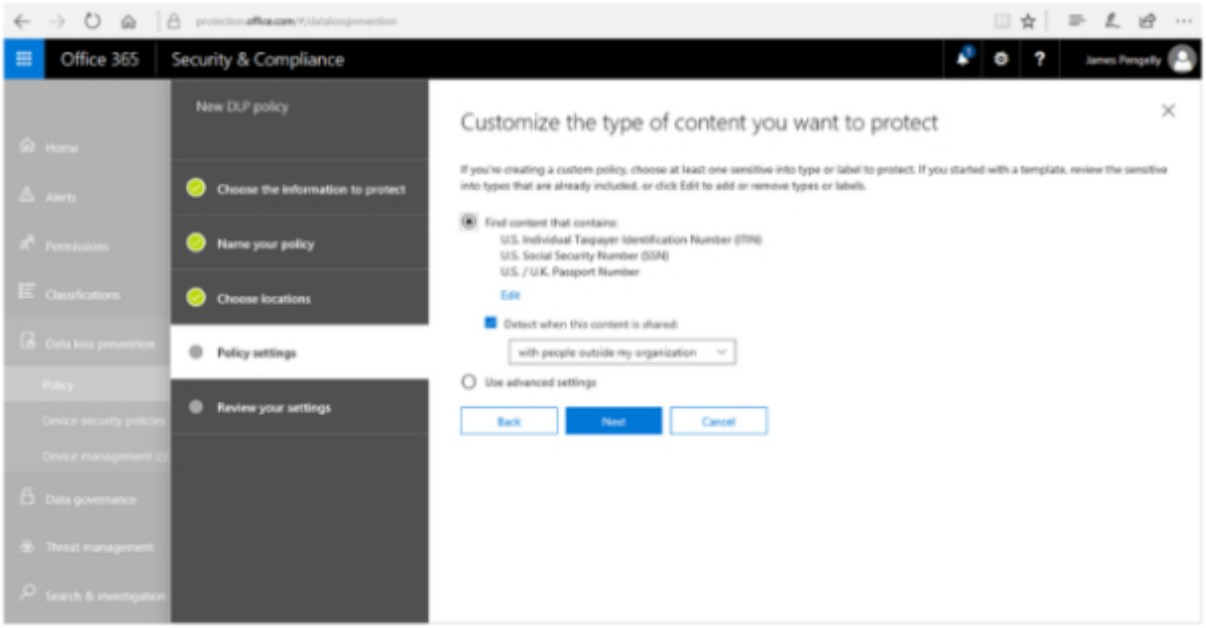
- Kebijakan BYOD
  Model penerapan seluler menjelaskan cara karyawan diberikan perangkat dan aplikasi ponsel cerdas atau tablet. Beberapa perusahaan mengeluarkan karyawan dengan perangkat yang dimiliki dan dikendalikan perusahaan dan bersikeras bahwa hanya ini yang digunakan untuk memproses data perusahaan. Perusahaan lain mungkin menerapkan kebijakan bawa perangkat Anda sendiri (BYOD). BYOD berarti bahwa ponsel dimiliki oleh karyawan dan dapat digunakan di jaringan perusahaan selama memenuhi spesifikasi minimum yang dipersyaratkan oleh perusahaan (dalam hal versi dan fungsionalitas OS). Karyawan harus menyetujui pemasangan aplikasi perusahaan dan hingga tingkat pengawasan dan audit tertentu. Sangat sering, perangkat BYOD terdaftar dengan perangkat lunak manajemen perusahaan dan dikonfigurasi dengan ruang kerja dan aplikasi perusahaan yang di kotak pasir.



Perangkat lunak manajemen perusahaan dapat digunakan untuk mengelompokkan data perusahaan dari data pribadi pada perangkat BYOD. (Tangkapan layar digunakan dengan izin dari Google.)

- Pencegahan kehilangan data
  Pencurian atau kehilangan informasi rahasia dan/atau pribadi disebut sebagai pelanggaran data. Pelanggaran data dapat membuat organisasi terkena biaya reputasi dan keuangan yang besar. Akibatnya, penanganan data adalah area aktivitas yang harus dikelola dengan ketat oleh kebijakan dan kontrol teknis.

  Produk pencegahan kehilangan data (DLP) memindai konten dalam format terstruktur (seperti database dengan model kontrol akses formal) atau format tidak terstruktur, seperti email atau dokumen pengolah kata. Produk DLP menggunakan semacam database atau algoritme kamus (pencocokan ekspresi reguler) untuk mengidentifikasi data rahasia atau pribadi/sensitif. Transfer konten ke media yang dapat dipindahkan atau melalui email atau ke jejaring sosial atau layanan penyimpanan cloud kemudian dapat diblokir jika tidak sesuai dengan kebijakan yang telah ditentukan sebelumnya.



Membuat kebijakan pencegahan kehilangan data di Office 365. (Tampilan layar digunakan dengan izin dari Microsoft.)

- Kebijakan Akses Jarak Jauh
  Jika karyawan diberi hak untuk terhubung ke jaringan perusahaan dari lokasi yang jauh menggunakan VPN, penggunaan hak akses jarak jauh mereka harus diatur oleh kontrol teknis dan kebijakan. Beberapa masalah yang harus dikurangi antara lain sebagai berikut:

    - ***Malware protection***-Komputer mungkin tidak dapat diakses oleh sistem jaringan yang digunakan untuk memperbarui dan menerapkan perlindungan malware. Ini mungkin harus diserahkan kepada pengguna akhir. Jika worm atau Trojan diinstal, keamanan jaringan dapat dikompromikan.

    - ***Security information***-Informasi otentikasi dapat disimpan di klien (menyimpan kata sandi, misalnya), membuat jaringan rentan jika komputer dicuri.

    - ***Data transfer***-File yang disalin ke klien mungkin tidak lagi diamankan dengan benar, meningkatkan potensi bahwa informasi rahasia dapat dicuri bersama dengan perangkat.

    - ***Local privileges***-Pengguna komputer jarak jauh mungkin dikonfigurasi dengan hak administratif tetapi tidak memiliki pemahaman tentang bagaimana hak istimewa tersebut dapat dieksploitasi atau disalahgunakan. Mereka mungkin menginstal perangkat lunak yang tidak sah pada mesin atau membuatnya lebih rentan terhadap malware dengan menjelajahi web menggunakan akun administratif mereka.

- ***Weak authentication***-Mengandalkan kombinasi nama pengguna dan kata sandi tidak cukup aman dalam skenario akses jarak jauh. Otentikasi dua faktor menggunakan kartu pintar atau pengenalan biometrik selain PIN atau kata sandi harus diterapkan. Jika ini bukan pilihan, kebijakan kata sandi yang kuat harus ditegakkan, dan pengguna disadarkan akan risiko nyata dari menuliskan atau membagikan kata sandi mereka.

- ***Untrusted networks***-Pengguna mungkin mengonfigurasi otentikasi yang lemah pada jaringan nirkabel rumah atau menggunakan titik akses publik, meningkatkan risiko serangan pengintaian.

Solusi utama untuk masalah keamanan akses jarak jauh adalah mendidik pengguna jarak jauh tentang risiko keamanan dan tanggung jawab mereka. Penegakan dapat diberikan dengan mengaudit perangkat jarak jauh secara berkala untuk memastikan bahwa antivirus, firewall, dan patch OS/browser/aplikasi terus diperbarui dan untuk memeriksa apakah perangkat lunak yang tidak berlisensi belum diinstal. Juga bijaksana untuk membatasi apa yang dapat diakses oleh pengguna jarak jauh di jaringan lokal dan sangat membatasi hak-hak akun komputer jarak jauh. Prinsip hak istimewa terkecil harus diterapkan.

- Kesepakatan Bersama
  Perjanjian digunakan antara perusahaan dan karyawannya dan antara perusahaan untuk menegakkan kinerja dan tujuan keamanan.

- Persyaratan Perjanjian Tingkat Layanan
  Sebuah perjanjian tingkat layanan (SLA) adalah perjanjian kontrak yang menetapkan persyaratan rinci di mana layanan yang sedang berlangsung disediakan. Ini dapat berupa kontrak formal yang mengikat secara hukum antara bisnis pemasok dan pelanggan atau perjanjian yang kurang formal, seperti SLA yang disepakati antara departemen internal. Persyaratan SLA mendefinisikan aspek layanan, seperti ruang lingkup, karakteristik kinerja, dan tanggung jawab yang disepakati antara penyedia layanan dan pelanggan.

  Bergantung pada sifat bisnis organisasi Anda, Anda mungkin bertanggung jawab untuk mempertahankan persyaratan SLA yang disepakati dengan pelanggan Anda, menggunakan SLA untuk menjamin standar layanan dari pemasok Anda, atau keduanya.

- Perjanjian Larangan pengungkapan informasi rahasia
  Perjanjian non-disclosure (NDA) adalah dasar hukum untuk melindungi aset informasi. Ini mendefinisikan penggunaan data sensitif apa yang diizinkan, pembatasan penyimpanan dan distribusi apa yang harus ditegakkan, dan hukuman apa yang akan dikenakan atas pelanggaran perjanjian. Kontrak kerja kemungkinan besar mengandung

klausul NDA. NDA juga digunakan antara perusahaan dan kontraktor dan antara dua perusahaan.

- Nota kesepahaman
  Memorandum of Understanding (MOU) adalah perjanjian awal atau eksplorasi untuk mengungkapkan niat untuk bekerja sama. MOU biasanya dimaksudkan untuk menjadi relatif informal dan tidak bertindak sebagai kontrak yang mengikat. MOU hampir selalu memiliki klausul yang menyatakan bahwa para pihak harus menghormati kerahasiaan.

Compare and Contrast Internet of Things Devices

- Pendahuluan: Bandingkan dan Kontraskan Perangkat Internet of Things
  Banyak orang dan bisnis menerapkan perangkat Internet of Things (IoT) di rumah dan kantor mereka, dan beberapa bisnis bergantung pada teknologi sistem tertanam yang mendasari untuk manufaktur dan kontrol inventaris. Dalam topik ini, Anda akan mempelajari bagaimana teknologi ini dapat diintegrasikan secara aman dengan atau di samping jaringan data perusahaan.

- *Internet of Things*
  Istilah *Internet of Things* (IoT) digunakan untuk menggambarkan jaringan global perangkat pribadi, peralatan rumah tangga, sistem kontrol rumah, kendaraan, dan barang-barang lainnya yang telah dilengkapi dengan sensor, perangkat lunak, dan konektivitas jaringan. Fitur-fitur ini memungkinkan jenis objek untuk berkomunikasi dan melewatkan data antara mereka sendiri dan sistem tradisional lainnya seperti server komputer. Ini sering disebut sebagai komunikasi *Machine to Machine* (M2M).

- Perangkat Cerdas tingkat konsumen
  Perangkat pintar digunakan untuk menerapkan sistem otomatisasi rumah. Jaringan perangkat pintar IoT umumnya akan menggunakan jenis komponen berikut:

    - ***Hub/control system***-perangkat IoT biasanya memerlukan hub komunikasi untuk memfasilitasi jaringan nirkabel. Juga harus ada sistem kontrol, karena sebagian besar perangkat IoT tidak memiliki kepala, artinya mereka tidak memiliki antarmuka kontrol pengguna. Hub tanpa kepala dapat diimplementasikan sebagai speaker pintar yang dioperasikan oleh kontrol suara atau menggunakan aplikasi smartphone/PC untuk konfigurasi.

    - ***Smart devices***-IoT menerapkan fungsi tersebut, seperti bohlam lampu pintar, lemari es, termostat/kontrol pemanas, atau bel pintu/telepon entri video yang dapat Anda operasikan dari jarak jauh. Perangkat ini mampu menghitung, menyimpan, dan fungsi jaringan yang semuanya berpotensi rentan terhadap eksploitasi. Sebagian besar perangkat pintar menggunakan kernel Linux atau Android. Karena mereka menjalankan komputer mini secara efektif, perangkat pintar rentan terhadap beberapa serangan standar yang terkait dengan aplikasi

web dan fungsi jaringan. Periferal terintegrasi seperti kamera atau mikrofon dapat dikompromikan untuk memfasilitasi pengawasan.

- Sistem Kontrol Akses Fisik dan Bangunan Pintar
  A physical access control system (PACS) adalah jaringan kunci yang dipantau, alarm penyusup, dan kamera pengintai video. *A building automation system* (BAS) atau gedung pintar untuk kantor dan pusat data dapat mencakup PACS, tetapi juga konfigurasi dan *heating, ventilation, and air conditioning* (HVAC) berbasis jaringan, pengendalian kebakaran, daya dan penerangan, serta elevator dan eskalator. Subsistem ini diimplementasikan oleh *programmable logic controller* (PLC) dan berbagai jenis sensor yang mengukur suhu, tekanan udara, kelembaban, hunian ruangan, dan sebagainya.

- Sistem Kontrol Industri/Kontrol Pengawasan dan Akuisisi Data
  Internet of Things dan sistem tertanam lainnya digunakan dalam banyak sektor industri, termasuk pembangkit dan distribusi energi, penambangan dan pemurnian bahan mentah, fabrikasi dan manufaktur, dan logistik (memindahkan dan mengirimkan komponen dan barang).

  Sistem industri memiliki prioritas yang berbeda dengan sistem TI. Seringkali, komponen elektromekanis berbahaya terlibat, jadi keselamatan adalah prioritas utama. Proses industri juga memprioritaskan ketersediaan dan integritas daripada membalikkan kerahasiaan triad CIA sebagai triad AIC.

- Alur Kerja dan Sistem Otomasi Proses
  An industrial control system (ICS) menyediakan mekanisme untuk alur kerja dan otomatisasi proses. ICS mengontrol mesin yang digunakan dalam infrastruktur penting, seperti pemasok listrik, pemasok air, layanan kesehatan, telekomunikasi, dan layanan keamanan nasional. Sebuah ICS yang mengelola otomatisasi proses dalam satu situs biasanya disebut sebagai *distributed control system* (DCS).

  ICS terdiri dari perangkat dan peralatan pabrik dengan PLC tertanam. PLC dihubungkan oleh jaringan kabel ke aktuator yang mengoperasikan katup, motor, pemutus sirkuit, dan komponen mekanis lainnya, ditambah sensor yang memantau beberapa keadaan lokal, seperti suhu. Output dan konfigurasi PLC dilakukan oleh satu atau lebih *human-machine interfaces* (HMI). HMI mungkin berupa panel kontrol lokal atau perangkat lunak yang berjalan pada host komputasi. PLC terhubung dalam loop kontrol, dan seluruh sistem otomasi proses dapat diatur oleh server kontrol. Konsep penting lainnya adalah sejarawan data, yang merupakan basis data dari semua informasi yang dihasilkan oleh loop kontrol.

- Kontrol Pengawasan dan Akuisisi Data
  A supervisory control and data acquisition (SCADA) menggantikan server kontrol dalam ICS multi-situs skala besar. SCADA biasanya dijalankan sebagai perangkat lunak pada

komputer biasa, mengumpulkan data dari dan mengelola perangkat dan peralatan pabrik dengan PLC tertanam, yang disebut sebagai perangkat lapangan. SCADA biasanya menggunakan komunikasi WAN, seperti seluler atau satelit, untuk menghubungkan server SCADA ke perangkat lapangan.

- Jaringan IoT
  Setiap perangkat dalam jaringan IoT diidentifikasi dengan beberapa bentuk nomor seri atau kode unik yang tertanam dalam sistem operasi atau kontrolnya sendiri dan dapat beroperasi di dalam infrastruktur Internet yang ada, baik secara langsung maupun melalui perantara. Karena perangkat ini cenderung kecil dan sering tidak berdaya atau bergantung pada daya baterai, produk jaringan Ethernet, seluler, dan Wi-Fi standar yang menghubungkan komputer tidak selalu cocok untuk digunakan. Standar dan produk jaringan lainnya telah dikembangkan untuk memfasilitasi jaringan IoT.

- Jaringan Teknologi Operasional
  Jaringan kabel untuk aplikasi industri disebut sebagai jaringan *operational technology* (OT). Ini biasanya menggunakan protokol data serial atau Ethernet industri. Industrial Ethernet dioptimalkan untuk transfer deterministik real-time. Jaringan semacam itu mungkin menggunakan tautan data dan protokol jaringan yang dikembangkan vendor, serta protokol aplikasi khusus.

- Jaringan Seluler
  Jaringan seluler untuk IoT memungkinkan komunikasi jarak jauh melalui sistem yang sama yang mendukung ponsel dan ponsel cerdas. Ini juga disebut radio baseband, setelah prosesor baseband yang menjalankan fungsi modem seluler. Ada beberapa teknologi radio baseband:

  - ***Narrowband-IoT*** **(NB-IoT**)-ini mengacu pada versi daya rendah dari Long Term Evolution (LTE) atau standar seluler 4G. Sinyal menempati bandwidth lebih sedikit daripada seluler biasa. Ini berarti kecepatan data terbatas (20-100 kbps), tetapi sebagian besar sensor perlu mengirim paket kecil dengan latensi rendah, daripada melakukan transfer data besar. Narrowband juga memiliki daya tembus yang lebih besar, membuatnya lebih cocok untuk digunakan di lokasi yang tidak dapat diakses, seperti terowongan atau jauh di dalam gedung, di mana konektivitas seluler biasa tidak mungkin dilakukan.

  - ***LTE Machine Type Communication*** **(LTE-M)**-ini adalah sistem berdaya rendah lainnya tetapi mendukung bandwidth yang lebih tinggi (hingga sekitar 1 Mbps).

- Z-Wave dan Zigbee
  Z-Wave adalah protokol komunikasi nirkabel yang digunakan terutama untuk otomatisasi rumah. Z-Wave Alliance mengoperasikan program sertifikasi untuk perangkat dan perangkat lunak. Z-Wave menciptakan topologi jaringan mesh. Perangkat dapat dikonfigurasi untuk bekerja sebagai repeater untuk memperluas jaringan tetapi ada

batas empat "hop" antara perangkat pengontrol dan titik akhir. Z-Wave telah terdaftar di sebagian besar negara di seluruh dunia dan menggunakan frekuensi radio dalam rentang tinggi 800 hingga 900 MHz yang rendah. Ini dirancang untuk berjalan dalam waktu lama (bertahun-tahun) dengan daya baterai.

Zigbee memiliki kegunaan yang mirip dengan Z-Wave dan merupakan teknologi pesaing sumber terbuka untuk itu. Zigbee Alliance mengoperasikan program sertifikasi untuk berbagai teknologi dan standarnya. Zigbee menggunakan pita frekuensi 2,4 GHz. Frekuensi yang lebih tinggi ini memungkinkan lebih banyak bandwidth data dengan mengorbankan jangkauan dibandingkan dengan Z-Wave dan risiko interferensi yang lebih besar dari komunikasi radio 2,4 GHz lainnya. Zigbee mendukung lebih banyak perangkat secara keseluruhan dalam satu jaringan mesh (65.000 dibandingkan dengan 232 untuk Z-Wave), dan tidak ada batasan hop untuk komunikasi antar perangkat.

- Penempatan dan Keamanan
  Masalah penempatan untuk sistem tertanam dan IoT paling baik dipertimbangkan dengan membaginya menjadi tiga kelompok utama: perangkat tingkat konsumen, teknologi bangunan pintar, dan sistem industri.

  Sementara jaringan perangkat individu mungkin menggunakan Z-Wave atau Zigbee, hub untuk otomatisasi rumah ditambah peralatan yang lebih besar biasanya terhubung langsung ke jaringan Wi-Fi lokal. Perangkat pintar tingkat konsumen dan produk otomatisasi rumah dapat didokumentasikan dengan buruk dan manajemen patch/proses respons keamanan vendor mungkin tidak memadai. Ketika dirancang untuk penggunaan di rumah, perangkat IoT dapat mengalami default yang lemah. Mereka dapat dikonfigurasi untuk "bekerja" dengan upaya konfigurasi minimum. Mungkin ada langkah-langkah yang disarankan untuk mengamankan perangkat yang tidak pernah digunakan pelanggan.

  Di ruang kerja perusahaan, risiko utama dari penempatan perangkat pintar adalah bayangan TI, di mana karyawan menggunakan perangkat yang mendukung jaringan tanpa melalui proses manajemen perubahan dan konfigurasi. Kerentanan pada perangkat akan menempatkannya pada risiko dieksploitasi sebagai titik akses ke jaringan. Perangkat ini juga menimbulkan risiko untuk kerja jarak jauh, di mana karyawan bergabung dengan VPN perusahaan menggunakan jaringan nirkabel rumah yang kemungkinan mengandung banyak kerentanan dan kelemahan konfigurasi yang tidak terdokumentasi.

  Risiko-risiko ini dapat dikurangi dengan audit rutin dan melalui pelatihan kesadaran keamanan karyawan.

- Bangunan Pintar
  Berbeda dengan komponen kelas konsumen, harus ada lebih sedikit ruang untuk kompromi dalam mekanisme masuk dan komponen kontrol iklim/pencahayaan dari

sistem bangunan pintar yang dirancang dengan benar. Manajemen dan pemantauan sistem harus dilakukan melalui segmen jaringan yang terisolasi. Manajemen konfigurasi dan proses kontrol perubahan harus memastikan bahwa tidak ada konfigurasi yang lemah yang diperkenalkan dan bahwa saran vendor dilacak untuk setiap kerentanan atau eksploitasi yang diketahui sehingga ini dapat ditambal atau dikurangi.

- ICS/SCADA
  Sementara ICS atau SCADA biasanya diimplementasikan sebagai OT khusus atau jaringan WAN nirkabel, mungkin ada titik di mana jaringan ini terhubung ke jaringan data perusahaan. Secara historis, tautan rentan dan host penghubung ini telah dieksploitasi oleh aktor ancaman. Ada risiko baik untuk sistem tertanam dari jaringan data dan aset data perusahaan dan sistem dari jaringan tertanam. Hubungan antara PL dan jaringan TI harus dipantau dan tunduk pada kontrol akses.

Modul 18

Explaining Disaster Recovery and High Availability Concepts

Explain Disaster Recovery Concepts

- Pendahuluan: Jelaskan Konsep Pemulihan Bencana
  Meskipun Anda telah mempertimbangkan skenario pemecahan masalah di mana satu host kehilangan konektivitas jaringan atau ketika kesalahan pada switch, router, atau layanan DHCP/DNS menimbulkan masalah untuk segmen jaringan, Anda juga perlu mempertimbangkan masalah dengan ketersediaan jaringan di seluruh situs. Rencana yang digunakan untuk meminimalkan risiko masalah di seluruh lokasi disebut sebagai kelangsungan bisnis, sedangkan rencana yang digunakan untuk mengurangi masalah ini jika terjadi disebut pemulihan bencana. Pada tahap ini dalam karier Anda, penting bagi Anda untuk memahami konsep yang mendasari rencana ini, sehingga Anda dapat membantu kelangsungan bisnis dan operasi pemulihan bencana.

- Ketersediaan Tinggi
  Salah satu sifat utama dari sistem yang tangguh adalah ketersediaan. Ketersediaan adalah persentase waktu sistem online, diukur selama periode tertentu, biasanya satu tahun. Akibat wajar dari ketersediaan adalah waktu henti; yaitu, persentase atau jumlah waktu selama sistem tidak tersedia.

  Ketersediaan yang tinggi merupakan karakteristik dari suatu sistem yang dapat menjamin tingkat ketersediaan tertentu. Metrik *Maximum Tolerable Downtime* (MTD) menyatakan persyaratan untuk fungsi bisnis. Waktu Henti dihitung dari jumlah interval layanan terjadwal (Waktu Layanan yang Disetujui) ditambah pemadaman yang tidak direncanakan selama periode tersebut. Ketersediaan tinggi dapat diterapkan sebagai 24x7 (24 jam per hari, 7 hari per minggu) atau 24x365 (24 jam per hari, 365 hari per tahun). Untuk sistem kritis, ketersediaan akan digambarkan sebagai dua-sembilan (99%) hingga lima- atau enam-sembilan (99,9999%).

Availability	Annual MTD (hh:mm:ss)
99.9999%	00:00:32
99.999%	00:05:15
99.99%	00:52:34
99.9%	08:45:36
99%	87:36:00

  Sebuah sistem di mana hampir tidak ada waktu henti yang dijadwalkan dan pemadaman yang sangat jarang juga disebut sebagai ketersediaan berkelanjutan. Ketersediaan

semacam ini diperlukan ketika tidak hanya keharusan komersial, tetapi juga bahaya cedera atau hilangnya nyawa yang terkait dengan kegagalan sistem. Contohnya termasuk jaringan yang mendukung perangkat medis, sistem kontrol lalu lintas udara dan satelit komunikasi, serta teknologi yang muncul seperti kendaraan otonom berjaringan dan aplikasi kota pintar baru, dari sistem penegakan hukum pintar hingga sistem sinyal lalu lintas pintar.

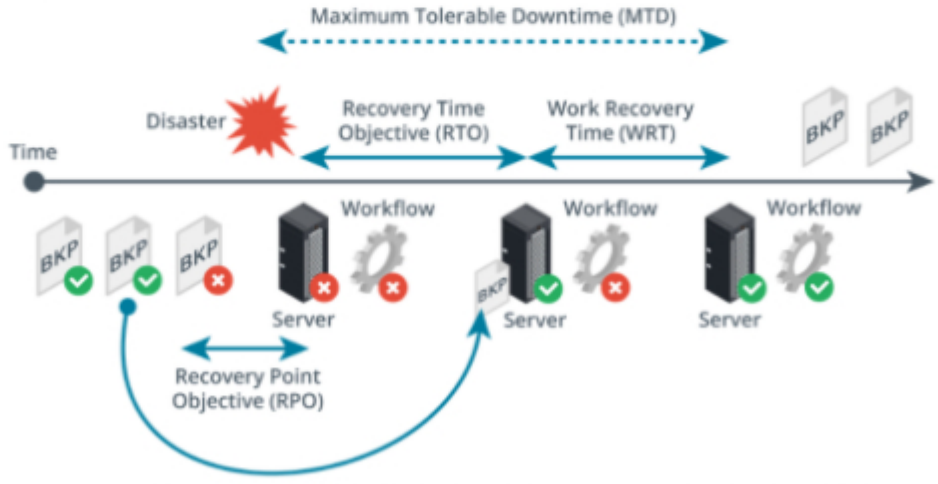
Metrik MTD menetapkan batas atas jumlah waktu pemulihan yang dimiliki sistem dan pemilik aset untuk melanjutkan operasi. Metrik tambahan dapat digunakan untuk mengatur operasi pemulihan:

- *Recovery time objective* (RTO) adalah periode setelah bencana di mana sistem TI individu dapat tetap offline. Ini menunjukkan jumlah waktu maksimum yang diizinkan untuk mengidentifikasi bahwa ada masalah dan kemudian melakukan pemulihan (misalnya, memulihkan dari cadangan atau beralih di sistem alternatif).

- *Work Recovery Time* (WRT). Setelah pemulihan sistem, mungkin ada pekerjaan tambahan untuk mengintegrasikan kembali sistem yang berbeda, memulihkan data dari cadangan, menguji fungsionalitas secara keseluruhan, dan memberi tahu pengguna sistem tentang setiap perubahan atau praktik kerja yang berbeda sehingga fungsi bisnis kembali didukung sepenuhnya.

  RTO+WRT tidak boleh melebihi MTD!

- *Recovery Point Objective* (RPO) adalah jumlah kehilangan data yang dapat dipertahankan sistem, diukur dalam satuan waktu. Artinya, jika database dihancurkan oleh virus, RPO 24 jam berarti data dapat dipulihkan dari salinan cadangan ke titik tidak lebih dari 24 jam sebelum database terinfeksi.



Metrik yang mengatur fungsi penting misi. (Gambar © 123RF.com.)

- Toleransi Kesalahan dan Redundansi
  Kesalahan biasanya didefinisikan sebagai peristiwa yang menyebabkan layanan menjadi tidak tersedia. Setiap sistem TI akan didukung oleh aset, seperti server, array disk, sakelar, router, dan sebagainya. Setiap aset rentan terhadap kesalahan. Indikator Kinerja Utama (KPI) dapat digunakan untuk menentukan keandalan setiap aset dan menilai apakah tujuan untuk MTD, RTO, dan RPO dapat dipenuhi. Beberapa KPI utama yang berkaitan dengan keandalan komponen adalah sebagai berikut:

  - ***Mean Time Between Failures*** **(MTBF)** mewakili masa pakai produk yang diharapkan. Perhitungan untuk MTBF adalah total waktu operasional dibagi dengan jumlah kegagalan. Misalnya, jika Anda memiliki 10 peralatan yang bekerja selama 50 jam dan dua di antaranya gagal, MTBF adalah 250 jam/kegagalan (10*50)/2.

  - ***Mean Time to Failure*** **(MTTF)** menyatakan metrik serupa untuk komponen yang tidak dapat diperbaiki. Misalnya, hard drive dapat dijelaskan dengan MTTF, sedangkan server, yang dapat diperbaiki dengan mengganti hard drive, akan dijelaskan dengan MTBF. Perhitungan MTTF adalah total waktu operasional dibagi jumlah perangkat. Misalnya, katakanlah dua drive dipasang di server dalam larik RAID. Satu gagal setelah 10 tahun, tetapi tidak pernah diganti, dan yang kedua gagal setelah 14 tahun, menjatuhkan array dan server. MTTF drive adalah (10+14)/2 = 12 tahun.

    MTTF/MTBF dapat digunakan untuk menentukan jumlah redundansi aset yang harus dimiliki sistem. Sistem redundan dapat melakukan failover ke aset lain jika ada kesalahan dan terus beroperasi secara normal. Ini juga dapat digunakan untuk mengetahui seberapa besar kemungkinan kegagalan akan terjadi.

  - ***Mean Time to Repair*** **(MTTR)** adalah ukuran waktu yang dibutuhkan untuk memperbaiki suatu kesalahan sehingga sistem dikembalikan ke operasi penuh. Ini juga dapat digambarkan sebagai waktu yang berarti untuk mengganti atau memulihkan. MTTR dihitung sebagai jumlah total jam pemeliharaan tidak terencana dibagi dengan jumlah insiden kegagalan. Nilai rata-rata ini dapat digunakan untuk memperkirakan apakah tujuan waktu pemulihan (recovery time objective/RTO) dapat dicapai.

  Sebuah sistem yang dapat mengalami kegagalan pada masing-masing komponen dan sub-sistem dan terus memberikan tingkat layanan yang sama (atau hampir sama) dikatakan toleran terhadap kesalahan. Toleransi kesalahan sering dicapai dengan menyediakan redundansi untuk komponen kritis untuk menghilangkan titik kegagalan tunggal. Sebuah komponen redundan atau failover adalah salah satu yang tidak penting untuk fungsi normal dari suatu sistem tetapi yang memungkinkan sistem untuk pulih dari kegagalan komponen lain. Contoh perangkat dan solusi yang memberikan toleransi kesalahan adalah sebagai berikut:

- ***Redundant spares***-Komponen seperti catu daya, kartu jaringan, drive (RAID), dan kipas pendingin memberikan perlindungan terhadap kegagalan perangkat keras. Konfigurasi server yang sepenuhnya redundan dikonfigurasi dengan beberapa komponen untuk setiap fungsi (daya, jaringan, dan penyimpanan). Komponen yang rusak kemudian akan secara otomatis beralih ke komponen yang berfungsi. Tautan jaringan-Jika ada beberapa jalur antara sakelar dan router, perangkat ini dapat secara otomatis beralih ke jalur yang berfungsi jika kabel atau port jaringan rusak.

- ***Uninterruptible power supplies* (UPSs) *and standby power supplies***-Menyediakan perlindungan daya jika terjadi kegagalan daya total (padam) dan jenis masalah daya gedung lainnya.

- ***Backup strategies***-Menyediakan perlindungan untuk data.

- ***Cluster services***- sarana untuk memastikan bahwa kegagalan total server tidak mengganggu layanan secara umum.

- Situs Pemulihan
  Dalam lingkup perencanaan kesinambungan bisnis, rencana pemulihan bencana (DRPs) menjelaskan prosedur khusus yang harus diikuti untuk memulihkan sistem atau situs ke status kerja. Bencana dapat berupa apa saja mulai dari hilangnya daya atau kegagalan komponen kecil hingga bencana buatan manusia atau alam, seperti kebakaran, gempa bumi, atau aksi terorisme.
-
- Menyediakan perangkat dan suku cadang yang berlebihan atau tautan jaringan memungkinkan perangkat cadangan untuk ditukar jika sistem yang ada gagal. Jaringan tingkat perusahaan sering kali juga menyediakan situs cadangan. Situs cadangan adalah lokasi lain yang dapat memberikan tingkat layanan yang sama (atau serupa). Bencana atau kegagalan sistem di satu situs akan menyebabkan layanan gagal ke situs pemrosesan alternatif. Perencanaan pemulihan bencana harus menunjukkan bagaimana hal ini akan terjadi, pemeriksaan apa yang perlu dilakukan untuk memastikan bahwa failover telah terjadi dengan sukses (tanpa kehilangan data transaksional atau ketersediaan layanan), dan cara kembali ke situs utama setelah fungsionalitas dipulihkan di sana.

  Ketahanan situs digambarkan sebagai panas, hangat, atau dingin:

  - Situs yang panas dapat segera di-failover. Ini biasanya berarti bahwa situs tersebut sudah berada dalam kepemilikan organisasi dan siap untuk digunakan. Misalnya, situs panas dapat terdiri dari bangunan dengan peralatan komputer operasional yang terus diperbarui dengan kumpulan data langsung.

    - Situs hangat bisa serupa, tetapi dengan persyaratan bahwa kumpulan data terbaru perlu dimuat.

    - Situs yang dingin membutuhkan waktu lebih lama untuk disiapkan. Sebuah situs dingin mungkin sebuah bangunan kosong dengan perjanjian sewa di tempat untuk memasang peralatan apa pun yang diperlukan bila diperlukan.

  Jelas, menyediakan redundansi pada skala ini bisa sangat mahal. Situs sering disewa dari penyedia layanan. Namun, dalam keadaan darurat nasional, permintaan akan layanan tersebut kemungkinan akan melebihi pasokan! Pilihan lain adalah bagi bisnis untuk masuk ke dalam pengaturan timbal balik untuk memberikan dukungan timbal balik. Ini hemat biaya tetapi rumit untuk direncanakan dan disiapkan.

  Bagi banyak perusahaan, solusi yang paling hemat biaya adalah memindahkan pemrosesan dan penyimpanan data ke situs cloud. Seorang operator cloud harus mampu menjaga hot site redundancy agar bencana di satu wilayah geografis tidak mengganggu layanan, karena cloud akan didukung oleh pusat data di wilayah yang berbeda.

- Sarana dan Prasarana Pendukung
  Keandalan situs individu tidak hanya bergantung pada sistem TI. Situs harus dilengkapi dengan daya dan kondisi iklim yang andal.

- Pemanas ruangan, Ventilasi, AC
  Kontrol lingkungan mengurangi hilangnya ketersediaan melalui masalah mekanis dengan peralatan, seperti panas berlebih. Sistem kontrol bangunan mempertahankan lingkungan kerja yang optimal untuk berbagai bagian bangunan. Akronim HVAC (*Heating, Ventilation, Air Conditioning*) sering digunakan untuk menggambarkan layanan ini. HVAC menggunakan sensor suhu dan sensor pendeteksi kelembaban (untuk mengukur kelembapan).

- Pemadaman Kebakaran
  Undang-undang kesehatan dan keselamatan menentukan mekanisme apa yang harus diterapkan oleh organisasi untuk mendeteksi dan menekan kebakaran. Beberapa elemen dasar keselamatan kebakaran meliputi:

    - Pintu keluar kebakaran yang ditandai dengan baik dan prosedur evakuasi darurat yang diuji dan dipraktekkan secara teratur.

    - Desain bangunan yang tidak memungkinkan api menyebar dengan cepat, dengan memisahkan area yang berbeda dengan dinding dan pintu tahan api.

    - Sistem pendeteksi asap atau kebakaran otomatis, serta alarm yang dapat dioperasikan secara manual.

Sistem pencegah kebakaran bekerja berdasarkan segitiga api. Segitiga api bekerja berdasarkan prinsip bahwa api membutuhkan panas, oksigen, dan bahan bakar untuk menyala dan terbakar. Menghapus salah satu dari elemen tersebut memberikan pemadaman kebakaran (dan pencegahan). Di Amerika Serikat (dan sebagian besar negara lain), kebakaran dibagi berdasarkan kelas di bawah sistem NFPA (*National Fire Protection Association*), menurut bahan mudah terbakar yang memicu api. Alat pemadam api portable datang dalam beberapa jenis yang berbeda, dengan masing-masing jenis dirancang untuk melawan kelas api tertentu. Khususnya, alat pemadam Kelas C menggunakan pemadam berbasis gas dan dapat digunakan dimana resiko sengatan listrik membuat jenis lain tidak cocok.

Tempat juga dapat dilengkapi dengan sistem penyiram di atas kepala. Alat penyiram pipa basah bekerja secara otomatis, dipicu oleh panas, dan mengeluarkan air. Sistem pipa basah terus-menerus menahan air pada tekanan tinggi, sehingga ada beberapa risiko pipa pecah dan pemicu yang tidak disengaja, serta kerusakan yang akan ditimbulkan jika terjadi kebakaran yang sebenarnya. Ada beberapa alternatif sistem pipa basah yang dapat meminimalkan kerusakan yang mungkin disebabkan oleh air yang membanjiri ruangan.

- Manajemen daya
  Semua jenis node jaringan memerlukan catu daya yang stabil untuk beroperasi. Peristiwa listrik, seperti lonjakan atau lonjakan tegangan, dapat merusak komputer dan peralatan jaringan, sementara hilangnya daya karena pemadaman atau pemadaman listrik akan menyebabkan peralatan gagal. Brownout adalah saat tegangan turun sebentar, sedangkan pemadaman adalah hilangnya daya total yang berlangsung beberapa detik atau lebih. Manajemen daya berarti menerapkan sistem untuk memastikan bahwa peralatan dilindungi dari kejadian ini dan bahwa operasi jaringan dapat berlanjut tanpa gangguan atau dipulihkan dengan cepat.

- Unit Distribusi Daya
  Sirkuit yang memasok daya jaringan ke rak, lemari jaringan, atau ruang server harus memenuhi kapasitas beban semua peralatan yang terpasang (ditambah ruang untuk pertumbuhan). Akibatnya, sirkuit ke ruang server biasanya memiliki kapasitas lebih tinggi daripada sirkuit domestik atau kantor (30 atau 60 amp sebagai lawan 13 amp, misalnya). Sirkuit ini dapat dijalankan melalui unit distribusi daya (PDU). PDU memiliki sirkuit untuk "membersihkan" sinyal daya, memberikan perlindungan terhadap lonjakan, lonjakan, dan pemadaman listrik, dan dapat diintegrasikan dengan catu daya tak terputus (UPS).

  Pada skala yang lebih kecil, PDU juga tersedia sebagai soket "strip" yang dapat menerima beban lebih tinggi daripada strip pengenal 13 amp biasa. Soket tersebut dipasang di rak dan dapat diorientasikan secara horizontal atau vertikal untuk memungkinkan opsi pemasangan kabel dan tata letak yang berbeda. PDU juga sering

mendukung fungsi pemantauan daya jarak jauh, seperti melaporkan beban dan status, mengalihkan daya ke soket hidup dan mati, atau menyalakan soket dalam urutan tertentu.

- Cadangan Baterai dan Catu Daya Tak Terputus
  Jika terjadi kehilangan daya, pengoperasian sistem dapat dipertahankan selama beberapa menit atau jam (tergantung beban) menggunakan cadangan baterai. Cadangan baterai dapat disediakan di tingkat komponen untuk drive disk dan cache array RAID. Baterai melindungi setiap operasi baca atau tulis yang di-cache pada saat listrik padam.

  Pada tingkat sistem, *an uninterruptible power supply* (UPS) akan menyediakan sumber daya sementara jika terjadi pemadaman. Waktu kerja UPS dapat berkisar dari beberapa menit untuk model dengan peringkat desktop hingga berjam-jam untuk sistem perusahaan. Dalam bentuknya yang paling sederhana, UPS terdiri dari kumpulan baterai dan sirkuit pengisiannya ditambah inverter untuk menghasilkan tegangan AC dari tegangan DC yang dipasok oleh baterai. Model UPS yang berbeda mendukung keluaran daya dan faktor bentuk yang berbeda-dari desktop hingga rak yang dipasang tergantung pada kebutuhan Anda.

- generator
  Waktu proses yang diizinkan oleh UPS harus cukup untuk melakukan failover ke sumber daya alternatif, seperti generator siaga. Jika tidak ada sumber daya sekunder, UPS setidaknya akan memungkinkan administrator untuk mematikan server atau alat dengan benar-pengguna dapat menyimpan file, dan OS dapat menyelesaikan rutinitas mematikan yang tepat.

  Sebuah generator listrik cadangan dapat memberikan daya ke seluruh bangunan, seringkali selama beberapa hari. Kebanyakan generator menggunakan solar, propana, atau gas alam sebagai sumber bahan bakar. UPS selalu diperlukan untuk melindungi dari gangguan apapun pada layanan komputer. Sebuah generator cadangan tidak dapat dibawa online cukup cepat untuk menanggapi kegagalan daya.

  Pusat data juga berinvestasi dalam sumber daya terbarukan, seperti matahari, angin, panas bumi, sel bahan bakar hidrogen, dan hidro. Kemampuan untuk menggunakan energi terbarukan merupakan faktor kuat dalam menentukan lokasi terbaik untuk pusat data baru. Solusi baterai skala besar, seperti Tesla's Powerpack (tesla.com/powerpack), mungkin dapat memberikan alternatif untuk pembangkit listrik cadangan. Ada juga teknologi yang muncul untuk menggunakan semua sumber daya baterai dari pusat data sebagai microgrid untuk penyimpanan daya (scientificamerican.com/article/how-big-batteries-at-data-centers-could-replace-power-plants).

- Manajemen Pencadangan Perangkat Jaringan
  Semua kelangsungan bisnis dan prosedur perencanaan pemulihan bencana menggunakan cadangan. Pelaksanaan dan frekuensi pencadangan harus direncanakan dengan hati-hati dan dipandu oleh kebijakan. Dalam manajemen jaringan, kebijakan pencadangan kurang terfokus pada data yang disimpan di server dan lebih pada pemulihan switch, router, firewall, dan penyeimbang beban yang rusak dengan cepat.

  Setiap perangkat harus memiliki konfigurasi dasar yang terdokumentasi. Proses penerapan harus mampu menerapkan konfigurasi ini ke perangkat pengganti atau saat memulihkan perangkat yang rusak.

  Salah satu komplikasi di sini adalah bahwa sebagian besar peralatan jaringan memiliki konfigurasi startup atau persisten dan konfigurasi yang berjalan. Dalam kebanyakan kasus, ini harus sama. Ada kemungkinan bahwa pengawasan konfigurasi meninggalkan konfigurasi berjalan yang valid yang tidak pernah disimpan sebagai konfigurasi startup. Audit reguler dan prosedur manajemen konfigurasi lainnya harus digunakan untuk mendeteksi dan memulihkan konfigurasi yang berjalan yang berbeda dari konfigurasi yang disimpan.

  Sebagian besar perangkat juga akan mendukung riwayat versi konfigurasi sebelumnya yang memungkinkan perubahan dibatalkan jika menyebabkan masalah.

  Alat juga dapat mendukung dua mode pencadangan:

  - State/bare metal-Jenis gambar snapshot dari keseluruhan sistem. Ini dapat diterapkan kembali ke perangkat apa pun dengan merek dan model yang sama sebagai pemulihan sistem.

  - File konfigurasi-Salinan data konfigurasi dalam format terstruktur, seperti bahasa markup yang dapat diperluas (XML). File ini dapat digunakan dalam pemulihan dua tahap di mana citra OS atau firmware diterapkan terlebih dahulu (atau peralatan baru disediakan) dan kemudian konfigurasi dipulihkan dengan mengimpor file cadangan.

  Perangkat jaringan juga dapat menyimpan informasi status yang belum ditulis ke log dan yang tidak akan ditangkap oleh cadangan file konfigurasi saja. Informasi status mencakup data seperti tabel MAC di sakelar atau tabel NAT di firewall. Firewall tingkat lanjut mungkin berisi data tambahan seperti malware/tanda tangan pendeteksi penyusupan. Beberapa perangkat mungkin mencatat data status ke database internal yang dapat dicadangkan secara berkala. Dalam kasus lain, jika informasi ini perlu dipertahankan, peralatan harus dikonfigurasi untuk mencatat data status ke server jauh, menggunakan protokol seperti syslog.

Explain High Availability Concepts

- Pendahuluan: Jelaskan Konsep Ketersediaan Tinggi
  Tautan jaringan sering kali merupakan titik kegagalan tunggal yang kritis. Router dan switch dapat menyediakan banyak jalur melalui jaringan untuk mencegah ketergantungan yang berlebihan pada node kritis tunggal. Penyeimbang beban dapat mengalihkan lalu lintas klien ke node pemrosesan alternatif, mengurangi kemacetan dan memungkinkan layanan failover jika host atau rute jaringan turun. Dalam topik ini, Anda akan belajar menjelaskan teknologi yang digunakan untuk menyediakan jaringan yang sangat tersedia.

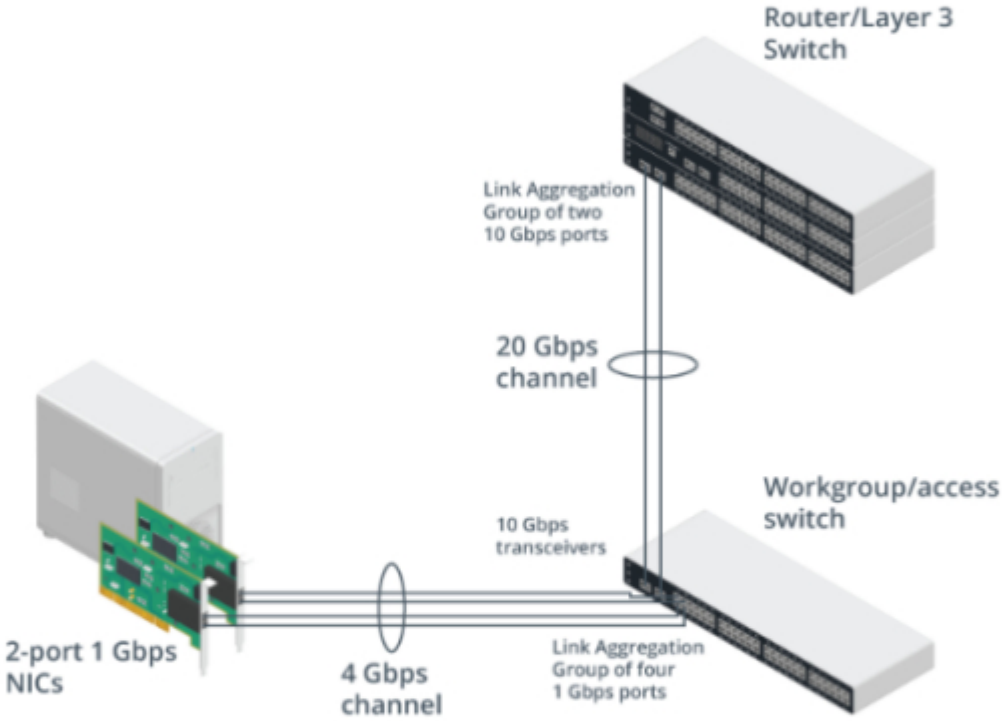
- Multipath
  Multipathing berarti bahwa node jaringan memiliki lebih dari satu link fisik ke node lain. Multipathing adalah fitur default dari internetwork mesh penuh dan parsial, di mana router dapat memilih jalur alternatif melalui jaringan jika tautan tidak tersedia. Multipathing dapat digunakan di mana saja yang membutuhkan redundansi tautan. Dua skenario tambahan yang umum adalah koneksi ke *storage area networks* (SAN) dan akses Internet melalui *Internet Service Provider* (ISP):

  - ***SAN multipathing***-Dalam SAN, server menggunakan penyimpanan bersama yang diakses melalui tautan jaringan. Multipathing berarti bahwa server memiliki setidaknya dua pengontrol SAN masing-masing dengan tautan khusus ke jaringan penyimpanan.

  - ***Multiple ISPs***-Jika suatu organisasi bergantung pada satu ISP untuk akses Internet, sirkuit itu mewakili satu titik kegagalan yang kritis. Bahkan jika ada beberapa sirkuit ke ISP yang sama, masalah dalam perutean ISP atau infrastruktur DNS tersebut dapat mengakibatkan hilangnya konektivitas sepenuhnya. Mengontrak dengan beberapa ISP dan menggunakan kebijakan perutean untuk meneruskan lalu lintas melalui beberapa sirkuit eksternal memberikan toleransi kesalahan dan penyeimbangan beban. Anda perlu memastikan bahwa ISP mengoperasikan infrastruktur terpisah dan tidak menggunakan pengaturan peering.

  Toleransi kesalahan ini berkurang jika link kedua ISP menggunakan fasilitas pintu masuk yang sama. Peristiwa bencana fisik seperti gempa bumi atau kerusakan konstruksi kemungkinan akan mempengaruhi kedua rangkaian kabel. Jalur yang beragam mengacu pada tautan penyediaan melalui saluran kabel terpisah yang secara fisik jauh satu sama lain. Pilihan lain adalah menyediakan tautan seluler sebagai cadangan, meskipun meskipun teknologi 5G tersedia, ini kemungkinan akan mengurangi bandwidth tautan secara substansial, dan bahkan kemudian, backhaul 5G mungkin menggunakan beberapa infrastruktur serat yang sama dengan sirkuit kabel.

- Agregasi Tautan/Tim NIC
  Agregasi tautan berarti menggabungkan dua atau lebih tautan kabel yang terpisah antara host dan switch ke dalam satu saluran logis. Dari ujung host, ini juga bisa disebut kerja sama NIC; di ujung switch , itu bisa disebut agregasi port dan disebut oleh Cisco sebagai EtherChannel. Istilah ikatan juga secara luas menggantikan agregasi. Misalnya, adaptor jaringan tunggal dan segmen kabel mungkin mendukung 1 Gbps; ikatan ini dengan adaptor lain dan segmen kabel memberikan link 2 Gbps. Agregasi link juga dapat digunakan dalam uplink antara dua switch atau antara switch dan router atau antara dua router.



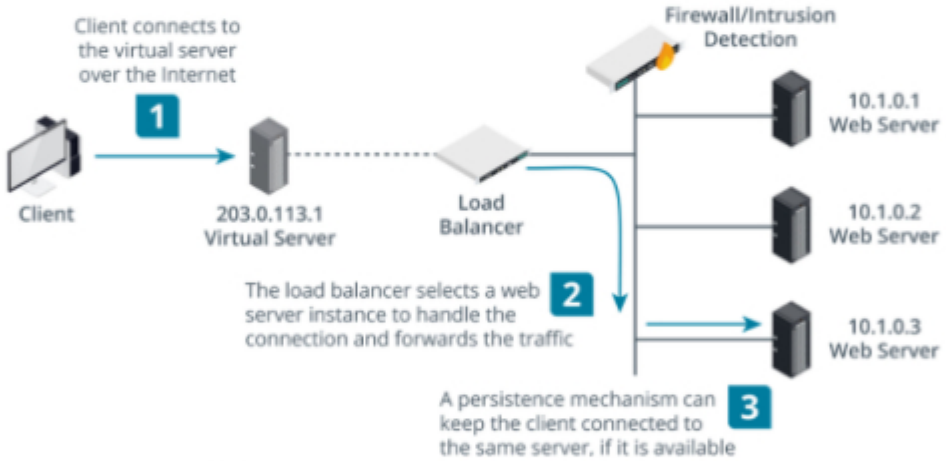
Node server menggunakan tim NIC untuk membuat tautan saluran 4 Gbps dari empat port 1 Gbps ke sakelar grup kerja, sementara sakelar grup kerja mengikat transceiver uplink untuk membuat saluran 20 Gbps ke router.

Agregasi tautan juga dapat memberikan redundansi; jika salah satu link rusak, koneksi masih dipertahankan oleh link lainnya. Hal ini juga sering hemat biaya; kartu Gigabit Ethernet empat port mungkin tidak cocok dengan bandwidth port 10 GbE tetapi akan lebih murah.

Tips: Konfigurasi ini sepenuhnya berlebihan hanya jika fungsi bisnis tidak bergantung pada kecepatan penuh tautan terikat. Jika satu port gagal, dan tautan turun menjadi 1 Gbps, tetapi bandwidth itu tidak mencukupi, tidak ada redundansi penuh.

Agregasi tautan biasanya diimplementasikan menggunakan standar IEEE 802.3ad/802.1ax. Antarmuka terikat 802.3ad digambarkan sebagai Grup Agregasi Tautan (LAG). 802.3ad juga mendefinisikan *Link Aggregation Control Protocol* (LACP), yang dapat digunakan untuk mendeteksi kesalahan konfigurasi dan memulihkan dari kegagalan salah satu tautan fisik.

- Load Balancer
  Di mana tim NIC memungkinkan penyeimbangan beban di tingkat komponen, penyeimbang beban dapat digunakan sebagai perangkat keras atau instans perangkat lunak untuk mendistribusikan permintaan klien di seluruh node server di peternakan atau kumpulan. Anda dapat menggunakan penyeimbang beban dalam situasi apa pun di mana Anda memiliki beberapa server yang menyediakan fungsi yang sama. Contohnya termasuk server web, server email front-end, dan konferensi web, konferensi A/V, atau server media streaming. Penyeimbang beban ditempatkan di depan jaringan server dan mendistribusikan permintaan dari jaringan klien atau Internet ke server aplikasi. Alamat layanan diiklankan ke klien sebagai server virtual. Ini digunakan untuk menyediakan layanan yang dapat diskalakan dari beban ringan hingga berat, menyediakan layanan yang toleran terhadap kesalahan, dan untuk memberikan mitigasi terhadap serangan penolakan layanan (DDoS) terdistribusi.



Topologi arsitektur load balancing dasar. (Gambar © 123RF.com.)

Ada dua jenis utama penyeimbang beban:

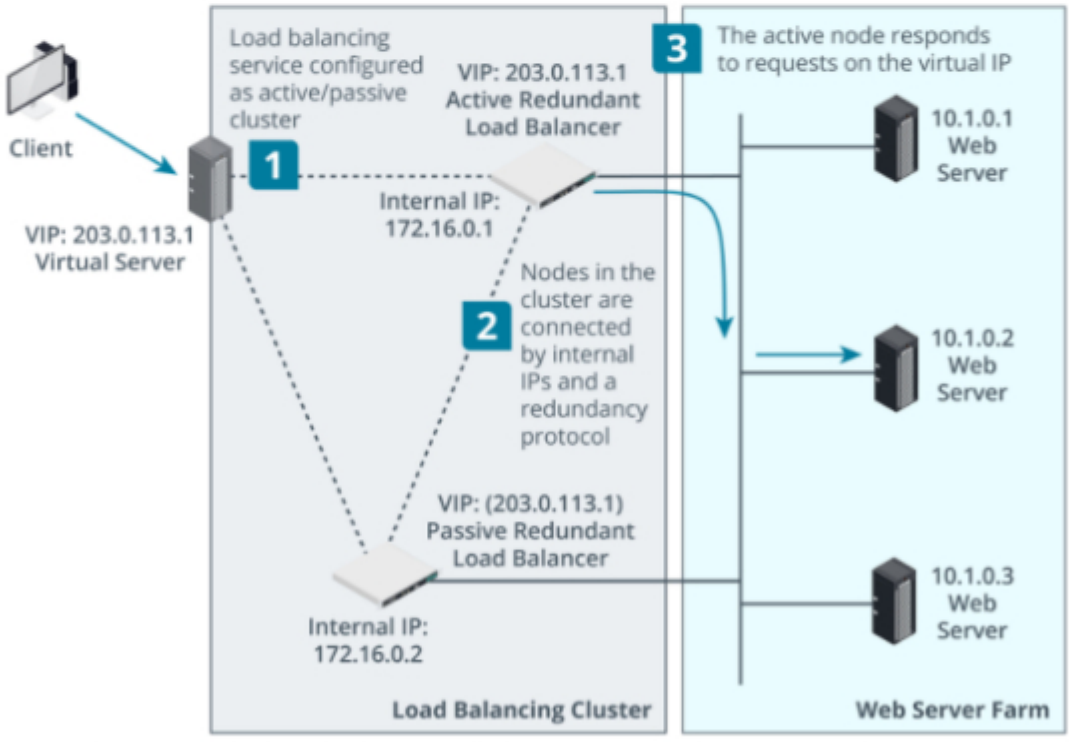
- ***Layer 4 switch***-Basic load balancer membuat keputusan penerusan pada alamat IP dan nilai header TCP/UDP, bekerja pada layer transport model OSI.

- ***Layer 7 switch (content switch)***-Karena aplikasi web menjadi lebih kompleks, penyeimbang beban modern harus dapat membuat keputusan penerusan berdasarkan data tingkat aplikasi, seperti permintaan untuk URL atau tipe data tertentu seperti streaming video atau audio . Ini membutuhkan logika yang lebih kompleks, tetapi kekuatan pemrosesan peralatan modern sudah cukup untuk menangani ini.

Tips: Kami terbiasa mengasosiasikan switch dengan Layer 2 (Ethernet), tetapi peralatan dapat melakukan penerusan seperti switch pada Layer 3, Layer 4, dan Layer 7. Ini secara kolektif disebut sebagai switch multilayer.

- Perangkat Keras/Cluster yang Berlebihan
  Di mana penyeimbang beban mendistribusikan lalu lintas antara node pemrosesan independen, pengelompokan memungkinkan beberapa node pemrosesan redundan yang berbagi data satu sama lain untuk menerima koneksi. Jika salah satu node di cluster berhenti bekerja, koneksi dapat failover ke node yang berfungsi. Untuk klien, cluster tampaknya menjadi server tunggal.

- IP virtual
  Misalnya, Anda mungkin ingin menyediakan dua peralatan penyeimbang beban sehingga jika salah satu gagal, yang lain masih dapat menangani koneksi klien. Tidak seperti load balancing dengan satu alat, IP publik yang digunakan untuk mengakses layanan dibagi antara dua instance dalam cluster. Ini disebut sebagai IP virtual atau alamat bersama atau mengambang. Instans dikonfigurasi dengan koneksi pribadi, yang masing-masing diidentifikasi dengan alamat IP "aslinya". Koneksi ini menjalankan beberapa jenis protokol redundansi, seperti *Common Address Redundancy Protocol* (CARP), yang memungkinkan node aktif untuk "memiliki" IP virtual dan merespons koneksi. Protokol redundansi juga mengimplementasikan mekanisme detak jantung untuk memungkinkan failover ke node pasif jika node aktif mengalami kesalahan.



Topologi arsitektur load balancing berkerumun. (Gambar © 123RF.com.)

Jenis topologi yang sama dapat digunakan untuk menyebarkan router dan firewall untuk ketersediaan tinggi dan berbagi beban.

Pada contoh sebelumnya, jika satu node aktif, yang lain pasif. Ini disebut sebagai pengelompokan aktif-pasif. Keuntungan utama dari konfigurasi aktif/pasif adalah kinerja tidak berpengaruh selama failover. Namun, biaya perangkat keras dan sistem operasi lebih tinggi karena kapasitas yang tidak terpakai.

Cluster aktif-aktif berarti bahwa kedua node memproses koneksi secara bersamaan. Hal ini memungkinkan administrator untuk menggunakan kapasitas maksimum dari perangkat keras yang tersedia sementara semua node berfungsi. Jika terjadi failover, beban kerja node yang gagal segera dan secara transparan dialihkan ke node yang tersisa. Pada saat ini, beban kerja pada node yang tersisa lebih tinggi dan kinerja menurun.

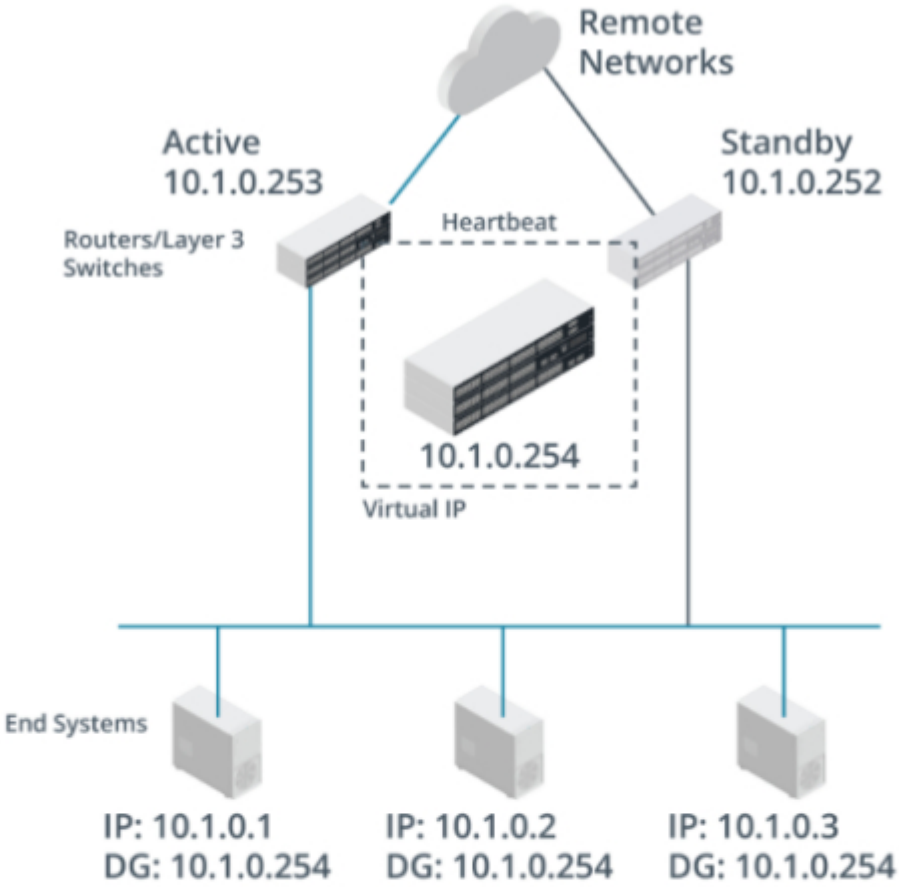
Tips: Dalam konfigurasi aktif-pasif standar, setiap node aktif harus dicocokkan dengan node pasif. Ada konfigurasi N+1 dan N+M yang menyediakan lebih sedikit node pasif daripada node aktif, untuk mengurangi biaya.

- Redundansi Hop Pertama
  Dalam topologi jaringan mesh penuh atau sebagian, rute alternatif dapat ditemukan untuk mem-bypass router yang gagal atau koneksi yang salah. Namun, sistem akhir biasanya dilayani oleh satu router yang dikonfigurasi sebagai gateway default. Meskipun dimungkinkan untuk mengonfigurasi host dengan beberapa gateway default untuk toleransi kesalahan, ini tidak bekerja dengan baik dalam praktiknya, karena memerlukan tingkat kerumitan yang lebih besar dalam algoritme perutean host daripada yang biasanya diterapkan pada host sistem akhir.

  Untuk mengatasi masalah ini, berbagai jenis protokol redundansi hop pertama (FHRP) telah dikembangkan.

- Protokol Router Siaga Panas
  Hot Standby Router Protocol (HSRP) berpemilik yang dikembangkan oleh Cisco memungkinkan beberapa router fisik berfungsi sebagai gateway default tunggal untuk subnet. Untuk melakukan ini, setiap router harus memiliki antarmuka yang terhubung ke subnet, dengan alamat MAC dan alamat IP uniknya sendiri. Selain itu, mereka juga perlu dikonfigurasi untuk berbagi alamat IP virtual umum dan alamat MAC umum. Grup router yang dikonfigurasi dengan cara ini dikenal sebagai grup siaga. Mereka berkomunikasi di antara mereka sendiri menggunakan multicast IP dan memilih router aktif berdasarkan prioritas yang dikonfigurasi oleh administrator. Router aktif merespons setiap lalu lintas yang dikirim ke alamat IP virtual. Dari router yang tersisa di grup standby, router dengan prioritas tertinggi berikutnya dipilih sebagai router siaga. Router siaga memantau status router aktif dan mengambil alih peran jika router aktif menjadi

tidak tersedia, juga memicu pemilihan router siaga baru dari router yang tersisa dalam grup.



Topologi Hot Standby Router Protocol (HSRP). (Gambar © 123RF.com.)

Tips: Cisco juga memiliki Gateway Load Balancing Protocol (GLBP) yang memungkinkan konfigurasi keseimbangan beban aktif/aktif.

- Protokol Redundansi Router Virtual
  Protokol standar terbuka *Virtual Router Redundancy Protocol* (VRRP) mirip dengan HSRP, perbedaannya terutama dalam terminologi dan format paket. Di VRRP, router aktif dikenal sebagai master, dan semua router lain dalam grup dikenal sebagai router cadangan. Tidak ada router siaga khusus; sebagai gantinya, semua router cadangan memantau status master, dan jika terjadi kegagalan, router master baru dipilih dari router cadangan yang tersedia berdasarkan prioritas.

  Salah satu keuntungan VRRP dibandingkan HSRP adalah tidak memerlukan setiap antarmuka router untuk diberi alamat IP yang unik. Dimungkinkan untuk mengkonfigurasi router VRRP untuk hanya menggunakan alamat IP virtual. Ini dapat berguna pada subnet di mana pemanfaatan ruang alamat tinggi.

Modul 19

Applying Network Hardening Techniques

Compare and Contrast Types of Attacks

- Pendahuluan: Bandingkan dan Kontraskan Jenis Serangan
  Desain keamanan jaringan yang efektif memerlukan pemahaman tentang bagaimana aktor ancaman dapat membahayakan pertahanan. Penelitian ancaman menghasilkan analisis jenis serangan umum, atau taktik, teknik, dan prosedur aktor ancaman (TTP). Anda harus dapat membandingkan dan membedakan jenis serangan yang umum untuk berpartisipasi secara efektif dalam respons insiden dan untuk memperkuat sistem terhadap intrusi.

- Jenis Serangan Umum
  Jaringan dapat diserang oleh berbagai jenis penyusup atau musuh karena berbagai alasan. Tujuan dari sebagian besar jenis musuh adalah untuk mencuri (mengeksfiltrasi) informasi dari jaringan, menyalahgunakan layanan jaringan (untuk penipuan, misalnya), atau untuk mengkompromikan ketersediaan jaringan. Serangan jenis ancaman orang dalam dapat diluncurkan dengan akses istimewa ke jaringan, sementara ancaman eksternal harus menemukan beberapa cara untuk mengakses jaringan, mungkin dengan menginstal malware pada sistem host.

- Serangan Jejak Kaki dan Sidik Jari
  Jejak kaki dan sidik jari adalah serangan enumerasi atau pengumpulan informasi. Footprinting memungkinkan aktor ancaman untuk menemukan topologi dan konfigurasi umum jaringan dan sistem keamanan. Jejak dapat dilakukan dengan serangan rekayasa sosial-membujuk pengguna untuk memberikan informasi atau mencari informasi yang telah dibuang sebagai sampah, misalnya. Pemindaian port secara khusus bertujuan untuk menghitung port aplikasi TCP atau UDP di mana host akan menerima koneksi.

  Sidik jari memungkinkan aktor ancaman untuk mengidentifikasi perangkat dan jenis serta versi OS. Ketika host yang menjalankan sistem operasi tertentu merespons pemindaian port, sintaks dari respons tersebut mungkin mengidentifikasi sistem operasi tertentu. Fakta ini juga berlaku untuk server aplikasi, seperti server web, server FTP, dan server surat. Tanggapan yang dibuat oleh server ini sering kali menyertakan header atau spanduk yang dapat mengungkapkan banyak informasi tentang server. Aktor ancaman dapat menggunakan informasi ini untuk menyelidiki kerentanan yang diketahui.

- Serangan *Spoofing*
  Istilah spoofing mencakup berbagai serangan yang berbeda. Spoofing dapat mencakup semua jenis serangan di mana penyerang menyamarkan identitasnya, atau di mana sumber informasi jaringan dipalsukan agar tampak sah. Rekayasa dan teknik sosial seperti phishing dan pharming, di mana penyerang membuat situs web palsu yang meniru situs asli, adalah jenis serangan spoofing. Dimungkinkan juga untuk menyalahgunakan cara kerja protokol atau bagaimana paket jaringan dibangun untuk

menyuntikkan data palsu atau diubah ke jaringan. Protokol ARP dan DNS sering digunakan sebagai vektor untuk jenis serangan ini.

- Penolakan serangan layanan
  A denial of service (DoS) menyebabkan layanan di host tertentu gagal atau menjadi tidak tersedia untuk pengguna yang sah. Kehabisan sumber daya Serangan DoS fokus pada kelebihan layanan dengan menggunakan CPU, RAM sistem, ruang disk, atau bandwidth jaringan. Serangan DoS juga dimungkinkan untuk mengeksploitasi kegagalan desain atau kerentanan lain dalam perangkat lunak aplikasi. Serangan DoS fisik mungkin melibatkan pemotongan saluran telepon atau kabel jaringan atau mematikan daya ke server. Serangan DoS mungkin dimotivasi oleh keinginan jahat untuk menimbulkan masalah. Mereka mungkin juga menjadi bagian dari serangan yang lebih luas, seperti pendahulu dari serangan spoofing atau eksfiltrasi data. DoS dapat membantu serangan ini dengan mengalihkan perhatian dan sumber daya dari target sebenarnya. Misalnya, serangan yang membutakan mencoba membebani sistem pencatatan atau peringatan dengan peristiwa.

- Serangan di jalan
  Serangan on-path adalah jenis serangan spoofing tertentu di mana aktor ancaman mengkompromikan koneksi antara dua host dan secara transparan mencegat dan menyampaikan semua komunikasi di antara mereka. Pelaku ancaman mungkin juga memiliki kesempatan untuk mengubah lalu lintas sebelum menyampaikannya.

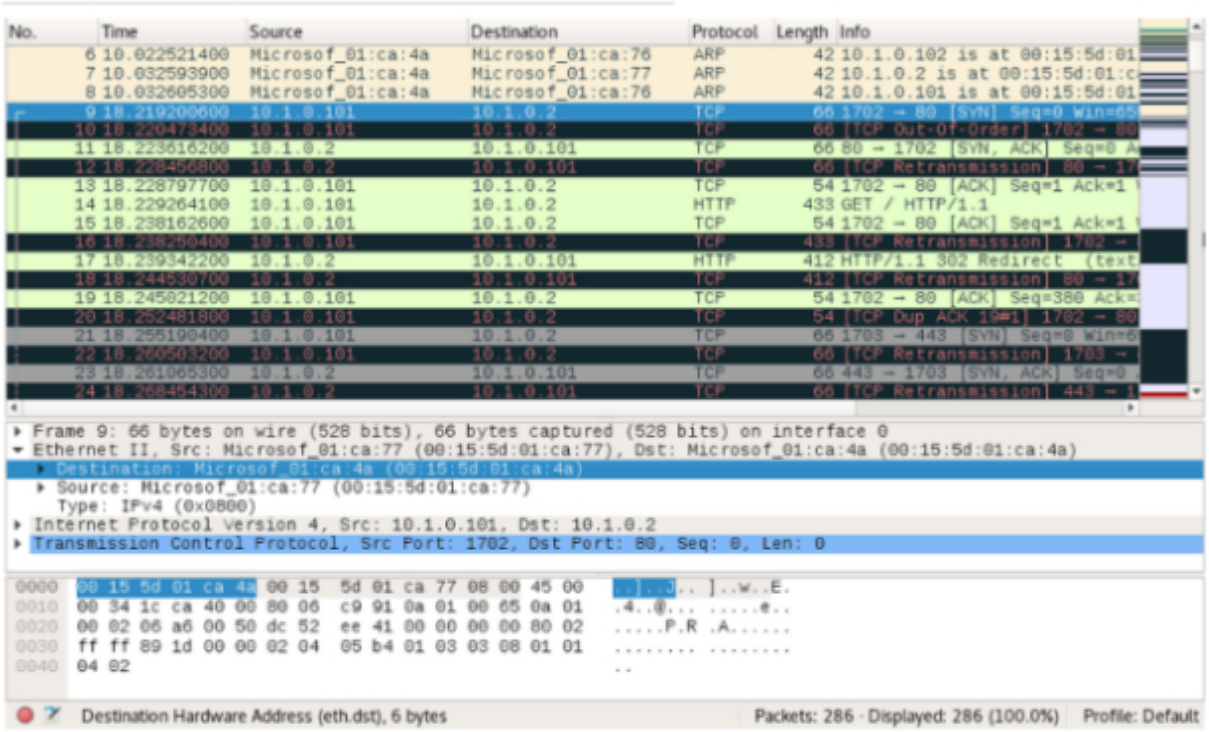
  Tips: Serangan di jalur juga dikenal dengan istilah *"Man-in-the-Middle (MitM)."* Istilah tersebut tidak inklusif dan/atau menggunakan metafora yang tidak tepat atau tidak jelas dan tidak digunakan lagi dalam dokumen tujuan ujian CompTIA terbaru.

- Spoofing MAC dan Spoofing IP
  Host dapat secara sewenang-wenang memilih alamat MAC dan/atau IP apa pun dan mencoba menggunakannya di jaringan. Pelaku ancaman mungkin mengeksploitasi ini untuk menipu nilai MAC atau alamat IP yang valid untuk mencoba menghindari daftar kontrol akses atau menyamar sebagai server yang sah. Agar jenis serangan ini berhasil, pelaku ancaman biasanya harus menonaktifkan host yang sah atau akan ada alamat duplikat di jaringan, yang akan memberikan hasil yang tidak terduga.

  IP spoofing juga digunakan di sebagian besar serangan *a denial of service* (DoS) untuk menutupi asal serangan dan mempersulit sistem target untuk memblokir paket dari sistem penyerang. Dalam jenis spoofing ini, aktor ancaman tidak peduli untuk tidak menerima lalu lintas kembali.

- Pemalsuan ARP
  Spoofing ARP, atau keracunan cache ARP, adalah cara umum untuk melakukan serangan di jalur. Ia bekerja dengan menyiarkan paket balasan ARP yang tidak diminta, juga dikenal sebagai balasan ARP serampangan, dengan alamat sumber yang menipu

antarmuka host atau router yang sah. Karena ARP tidak memiliki keamanan, semua perangkat dalam domain siaran yang sama dengan host jahat mempercayai komunikasi ini dan memperbarui tabel cache alamat MAC: IP mereka dengan alamat palsu. Karena aktor ancaman menyiarkan balasan ARP tanpa akhir, itu membanjiri antarmuka yang sah.



Mengamati keracunan ARP dalam penangkapan paket Wireshark. (Tangkapan layar milik Wireshark.)

Target yang biasa akan menjadi gateway default subnet. Jika serangan berhasil, semua lalu lintas yang ditujukan untuk jaringan jarak jauh akan dikirim ke penyerang. Aktor ancaman kemudian dapat melakukan serangan on-path untuk memantau komunikasi dan terus meneruskannya ke router untuk menghindari deteksi. Penyerang juga dapat memodifikasi paket sebelum meneruskannya. Keracunan ARP juga dapat melakukan serangan DoS dengan tidak meneruskan paket.

Keracunan ARP bisa sulit dideteksi tanpa memantau lalu lintas jaringan dengan cermat. Namun, upaya keracunan ARP cenderung menyebabkan kesulitan komunikasi sporadis, seperti gateway default yang tidak dapat dijangkau. Dalam kasus seperti itu, melakukan penangkapan jaringan dan memeriksa paket ARP dapat mengungkapkan paket racun, seperti halnya memeriksa cache ARP lokal untuk pemetaan beberapa alamat IP ke alamat MAC yang sama.

Tips: Meskipun IPv6 tidak menggunakan ARP, IPv6 juga rentan terhadap spoofing lapisan 2 jika protokol *Neighbor Discovery* (ND) yang tidak terenkripsi digunakan.

- *Rogue DHCP*
  Serangan di jalur juga dapat diluncurkan dengan menjalankan server DHCP jahat. Komunikasi DHCP tidak dapat di autentikasi, jadi host umumnya akan mempercayai paket penawaran pertama yang diterimanya. Aktor ancaman dapat mengeksploitasi ini untuk mengatur mesinnya sebagai gateway default subnet atau resolver DNS.

- Serangan Keracunan DNS
  Keracunan DNS adalah serangan yang membahayakan proses resolusi nama. Biasanya, penyerang akan mengganti alamat IP yang valid untuk situs web terpercaya, seperti mybank.example, dengan alamat IP penyerang. Penyerang kemudian dapat mencegah semua paket yang diarahkan ke mybank.example dan memantulkannya ke situs sebenarnya, membuat korban tidak menyadari apa yang terjadi (disebut sebagai pharming). Atau, spoofing DNS dapat digunakan untuk serangan DoS dengan mengarahkan semua lalu lintas untuk FQDN tertentu ke alamat IP yang tidak valid (lubang hitam).

  Salah satu cara untuk menyerang DNS adalah dengan merusak proses resolusi nama klien. Ini dapat dicapai dengan mengubah server yang digunakan untuk menyelesaikan *query*, mencegat dan memodifikasi lalu lintas DNS, atau mencemari cache nama klien (dengan memodifikasi file HOSTS, misalnya). Keracunan cache server DNS (atau polusi) adalah serangan pengalihan lain, tetapi alih-alih mencoba menumbangkan layanan nama yang digunakan oleh klien, ini bertujuan untuk merusak catatan yang disimpan oleh server DNS itu sendiri.

```
   HOSTNAME   www.web.local    yes       Hostname to hijack
   INTERFACE                   no        The name of the interface
   NEWADDR    192.168.2.192    yes       New address for hostname
   RECONS     192.168.2.254    yes       The nameserver used for reconnaissance
   RHOST      192.168.1.1      yes       The target address
   SNAPLEN    65535            yes       The number of bytes to capture
   SRCADDR    Real             yes       The source address to use for sending t
he queries (Accepted: Real, Random)
   SRCPORT    0                yes       The target server's source query port (
0 for automatic)
   TIMEOUT    500              yes       The number of seconds to wait for new d
ata
   TTL        46348            yes       The TTL for the malicious host entry
   XIDS       0                yes       The number of XIDs to try for each quer
y (0 for automatic)

msf auxiliary(bailiwicked_host) > run

[-] Failure: This hostname is already in the target cache: www.web.local
[-]          Cache entry expires on 2017-09-17 09:08:17 -0700... sleeping.
^C[-] Auxiliary interrupted by the console user
[*] Auxiliary module execution completed
msf auxiliary(bailiwicked_host) > set hostname updates.web.local
hostname => updates.web.local
msf auxiliary(bailiwicked_host) > run

[*] Targeting nameserver 192.168.1.1 for injection of updates.web.local. as 192.
168.2.192
[*] Querying recon nameserver for web.local.'s nameservers...
[*]  Got an NS record: web.local.              604800  IN      NS      ns.web.lo
cal.
[*]   Querying recon nameserver for address of ns.web.local....
[*]    Got an A record: ns.web.local.           604800  IN      A       192.168.
1.1
[*]     Checking Authoritativeness: Querying 192.168.1.1 for web.local....
[*]     ns.web.local. is authoritative for web.local., adding to list of nameser
vers to spoof as
[*] Calculating the number of spoofed replies to send per query...
[*]   race calc: 100 queries | min/max/avg time: 0.0/0.0/0.0 | min/max/avg repli
es: 0/1/0
[*] The server did not reply, giving up.
[*] Auxiliary module execution completed
msf auxiliary(bailiwicked_host) >
```

Mencoba meracuni cache server DNS-Serangan ini gagal.

- Serangan Melompat VLAN

  VLAN hopping adalah serangan yang dirancang untuk mengirim lalu lintas ke VLAN selain dari sistem host. Ini mengeksploitasi fitur VLAN asli 802.1Q. VLAN asli dirancang untuk menyediakan kompatibilitas dengan sakelar yang tidak mendukung VLAN. Penyerang, menggunakan perangkat yang ditempatkan di VLAN asli, membuat bingkai dengan dua header tag VLAN. Saklar trunk pertama untuk memeriksa frame menghapus header pertama, dan frame akan diteruskan ke VLAN target. Serangan semacam itu hanya dapat mengirim paket satu arah tetapi dapat digunakan untuk melakukan serangan DoS terhadap host pada VLAN yang berbeda. Penandaan ganda

dapat dikurangi dengan memastikan bahwa VLAN asli menggunakan ID yang berbeda untuk VLAN yang dapat diakses pengguna mana pun.

Serangan hopping VLAN juga dapat diluncurkan dengan memasang perangkat yang menipu pengoperasian sakelar ke jaringan dan menegosiasikan pembuatan port trunk. Sebagai port trunk, perangkat penyerang akan menerima semua lalu lintas antar-VLAN. Serangan ini dapat dikurangi dengan memastikan bahwa port yang diizinkan untuk digunakan sebagai trunk telah ditentukan sebelumnya dalam konfigurasi switch dan port akses tidak diizinkan untuk dikonfigurasi secara otomatis sebagai port trunk.

- Serangan Jaringan Nirkabel
  Jaringan nirkabel dapat membuka beberapa jalan bagi aktor ancaman untuk mendapatkan akses jaringan yang tidak sah.

- *Rogue Access Points*
  Rogue Access Points adalah salah satu yang telah diinstal pada jaringan tanpa otorisasi, baik dengan niat jahat atau tidak. Pengguna jahat dapat mengatur AP semacam itu dengan sesuatu yang mendasar seperti ponsel cerdas dengan kemampuan tethering, dan pengguna yang tidak jahat dapat mengaktifkan AP semacam itu secara tidak sengaja. Jika terhubung ke LAN tanpa keamanan, AP yang tidak sah membuat pintu belakang untuk menyerang jaringan.

- *Evil Twins*
  A rogue AP yang menyamar sebagai yang sah disebut kembaran jahat. Kembar jahat mungkin mengiklankan nama jaringan yang mirip (SSID) dengan yang sah. Misalnya, kembaran jahat mungkin dikonfigurasi dengan nama jaringan "perusahaan" di mana nama jaringan yang sah adalah "perusahaan." Atau, kembaran jahat mungkin menipu SSID dan BSSID (alamat MAC) dari titik akses resmi dan kemudian penyerang mungkin menggunakan beberapa teknik DoS untuk mengatasi AP yang sah. Setelah serangan DoS berhasil, pengguna akan dipaksa untuk memutuskan sambungan dari jaringan dan kemudian secara manual mencoba untuk menyambung kembali. Pada saat itu, dengan banyak pengguna yang sibuk dan mencoba untuk kembali bekerja, beberapa atau semua mungkin terkait dengan AP kembaran jahat dan mengirimkan frasa sandi jaringan atau kredensial mereka untuk otentikasi.

- Bagaimanapun dikonfigurasi, ketika pengguna terhubung ke kembaran jahat, mungkin dapat memanen informasi otentikasi dan, jika mampu menyediakan jaringan yang lebih luas atau akses Internet, jalankan serangan on-path untuk mengintip koneksi yang dibuat dengan server atau situs web.

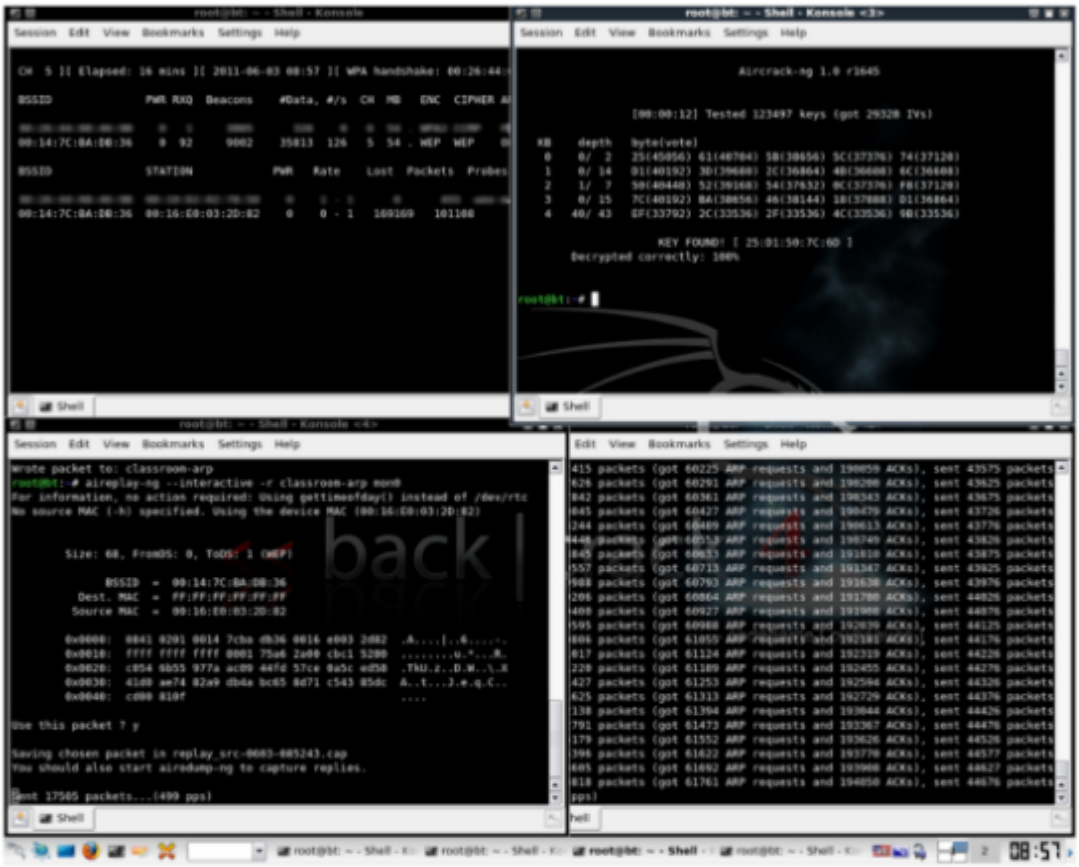


Mensurvei jaringan Wi-Fi menggunakan Xirrus Wi-Fi Inspector (xirrus.com) -Perhatikan keberadaan perangkat cetak yang dikonfigurasi dengan otentikasi terbuka (tanpa keamanan) dan alat TV pintar (memerlukan otentikasi). (Tangkapan layar digunakan dengan izin dari Xirrus.)

- Salah satu solusi untuk risiko rogue access point adalah dengan menggunakan keamanan EAP-TLS sehingga server otentikasi dan klien melakukan otentikasi bersama. Ada juga berbagai pemindai dan sistem pemantauan yang dapat mendeteksi AP nakal, yang disebut sebagai *wireless intrusion detection system*l (WIDS) atau *wireless intrusion prevention system* (WIPS).

- Serangan *Deauthentication*
  Penggunaan kembaran jahat dapat digabungkan dengan serangan deauthentication. Ini mengirimkan aliran bingkai manajemen palsu yang menyebabkan klien melakukan deautentikasi dari AP. Ini memungkinkan penyerang untuk memasukkan kembaran

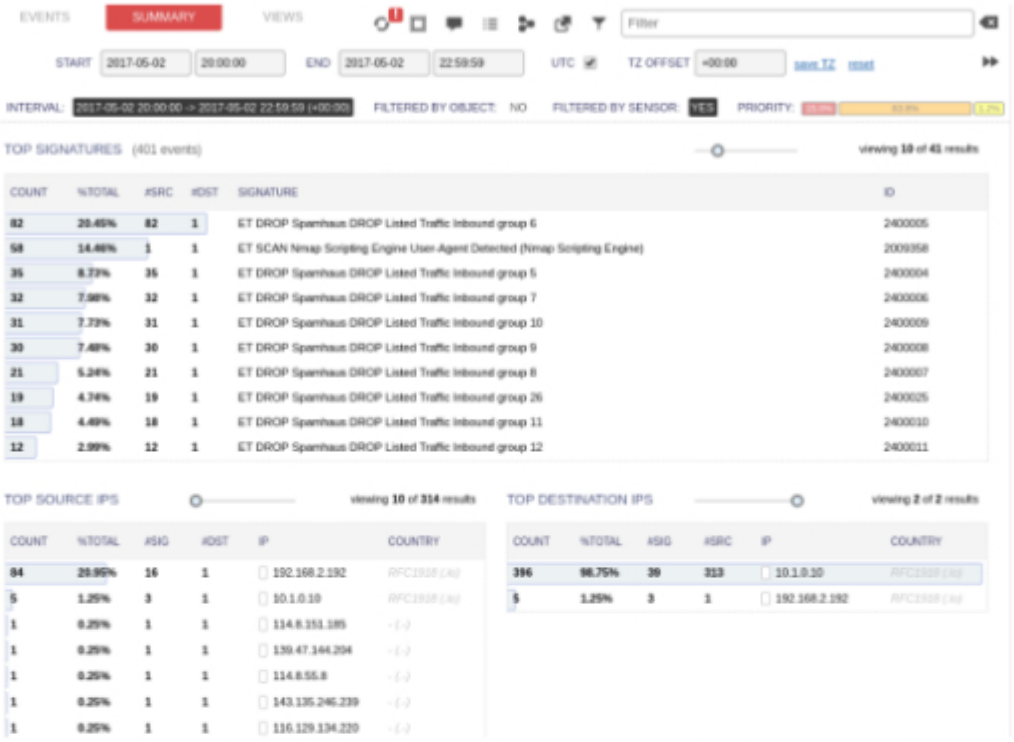
jahat, mengendus informasi tentang proses otentikasi, atau melakukan serangan penolakan layanan (DoS) terhadap infrastruktur nirkabel. Serangan ini bekerja melawan WEP dan WPA. Serangan dapat dikurangi jika infrastruktur nirkabel mendukung Management Frame Protection (MFP/802.11w). Baik AP maupun klien harus dikonfigurasi untuk mendukung MFP.



Aireplay mengendus paket ARP untuk memanen infus sementara Airodump menyimpannya ke tangkapan, yang dapat dianalisis Aircrack untuk mengidentifikasi kunci enkripsi yang benar.

- Serangan DoS dan Botnet Terdistribusi
  Serangan DoS (DDoS) terdistribusi diluncurkan secara bersamaan oleh banyak host. Beberapa jenis serangan DDoS hanya bertujuan untuk menghabiskan bandwidth jaringan, menyangkalnya ke host yang sah. Lainnya menyebabkan kelelahan sumber daya pada permintaan pemrosesan host, menghabiskan siklus CPU dan memori. Ini menunda pemrosesan lalu lintas yang sah dan berpotensi merusak sistem host sepenuhnya. Misalnya, serangan banjir SYN bekerja dengan menahan paket ACK klien selama jabat tangan tiga arah TCP. Alamat IP klien dipalsukan, artinya IP yang tidak valid atau acak dimasukkan sehingga paket SYN/ACK server salah arah. Server dapat mempertahankan antrian koneksi yang tertunda. Ketika tidak menerima paket ACK dari klien, itu mengirim ulang paket SYN/ACK beberapa kali sebelum "waktu habis" dan menyerah pada koneksi. Masalahnya adalah server mungkin hanya dapat mengelola

koneksi tertunda dalam jumlah terbatas, yang diisi oleh serangan DoS dengan cepat. Ini berarti bahwa server tidak dapat menanggapi lalu lintas asli.



Menjatuhkan lalu lintas dari rentang IP yang masuk daftar hitam dengan menggunakan alat Security Onion Network Security Monitoring (NSM). (Tangkapan layar milik Security Onion.)

- Serangan DoS/Amplifikasi Refleksi Terdistribusi
  Serangan banjir TCP SYN yang lebih kuat adalah jenis serangan refleksi terdistribusi (DRDoS) atau amplifikasi. Dalam serangan ini, musuh memalsukan alamat IP korban dan mencoba membuka koneksi dengan beberapa server. Server tersebut mengarahkan respons SYN/ACK mereka ke server korban. Ini dengan cepat menghabiskan bandwidth yang tersedia dari korban.

  Jenis teknik yang sama dapat digunakan untuk membombardir jaringan korban dengan tanggapan terhadap permintaan DNS palsu. Salah satu keuntungan dari teknik ini adalah meskipun permintaannya kecil, respons terhadap permintaan DNS dapat dibuat untuk memasukkan banyak informasi, jadi ini adalah cara yang sangat efektif untuk membanjiri bandwidth jaringan korban dengan jauh lebih terbatas. sumber daya di jaringan penyerang. *Network Time Protocol* (NTP) dapat disalahgunakan dengan cara yang sama.

- Botnet
  Botnet adalah sekelompok host yang disusupi yang dapat digunakan untuk meluncurkan serangan DDoS dan DRDoS. Seorang aktor ancaman pertama-tama akan

mengkompromikan satu atau dua mesin untuk digunakan sebagai penangan atau penggembala. Penangan digunakan untuk mengkompromikan ratusan atau ribuan atau jutaan host zombie dengan alat DoS (bot). Untuk mengkompromikan host, penyerang harus menginstal malware yang membuka koneksi jarak jauh pintu belakang. Penyerang kemudian dapat menggunakan malware untuk menginstal bot dan memicu zombie untuk meluncurkan serangan pada saat yang sama. Jaringan yang dibangun antara penangan dan bot disebut jaringan perintah dan kontrol (C-dan-C atau C2).

Tips: Semua jenis perangkat yang mendukung Internet rentan terhadap kompromi. Ini termasuk kamera yang mendukung web, router SOHO, dan TV pintar serta peralatan lainnya. Ini disebut sebagai botnet *Internet of Things* (IoT).

- Serangan Malware dan Ransomware
  Banyak upaya penyusupan yang dilakukan terhadap jaringan komputer bergantung pada penggunaan perangkat lunak berbahaya, atau malware. Malware dapat didefinisikan secara sederhana sebagai perangkat lunak yang melakukan sesuatu yang buruk, dari sudut pandang pemilik sistem. Ada banyak jenis malware, tetapi tidak diklasifikasikan secara ketat, sehingga beberapa definisi tumpang tindih atau kabur. Beberapa klasifikasi malware, seperti Trojan, virus, dan worm, fokus pada vektor yang digunakan oleh malware. Vektor adalah metode yang dijalankan malware di komputer dan berpotensi menyebar ke host jaringan lain. Faktor rumit lainnya dengan klasifikasi malware adalah sejauh mana penginstalannya diharapkan atau ditoleransi oleh pengguna. Kategori berikut menjelaskan beberapa jenis malware menurut vektor:

  - ***Viruses and worms***-Ini mewakili beberapa jenis malware pertama dan menyebar tanpa izin apa pun dari pengguna dengan disembunyikan di dalam kode yang dapat dieksekusi dari proses lain.

  - ***Trojan***-Malware tersembunyi di dalam paket penginstal untuk perangkat lunak yang tampaknya sah. Jenis malware ini tidak meminta persetujuan apa pun untuk pemasangan dan secara aktif dirancang untuk beroperasi secara diam-diam.

  - ***Potentially unwanted programs (PUPs)/Potentially unwanted applications (PUAs)***-Perangkat lunak yang diinstal bersama dengan paket yang dipilih oleh pengguna atau mungkin dibundel dengan sistem komputer baru. Tidak seperti Trojan, keberadaan PUP tidak secara otomatis dianggap berbahaya. Itu mungkin telah diinstal tanpa persetujuan aktif atau persetujuan dari perjanjian lisensi yang sengaja membingungkan. Jenis perangkat lunak ini kadang-kadang digambarkan sebagai grayware daripada malware.

    Klasifikasi lain didasarkan pada muatan yang dikirimkan oleh malware. Payload adalah tindakan yang dilakukan oleh malware selain hanya mereplikasi atau

bertahan pada host. Contoh klasifikasi payload termasuk spyware, rootkit, *remote access Trojan* (RAT) atau *backdoor*, dan *ransomware*.

Ransomware adalah jenis malware yang mencoba memeras uang dari korban. Satu kelas ransomware akan menampilkan pesan yang mengancam, seperti meminta Windows untuk diaktifkan kembali atau menyarankan bahwa komputer telah dikunci oleh polisi karena digunakan untuk melihat pornografi anak atau untuk terorisme. Ini dapat memblokir akses ke komputer dengan menginstal program shell lain atau jendela browser yang sulit ditutup, tetapi serangan semacam ini biasanya relatif mudah untuk diperbaiki.

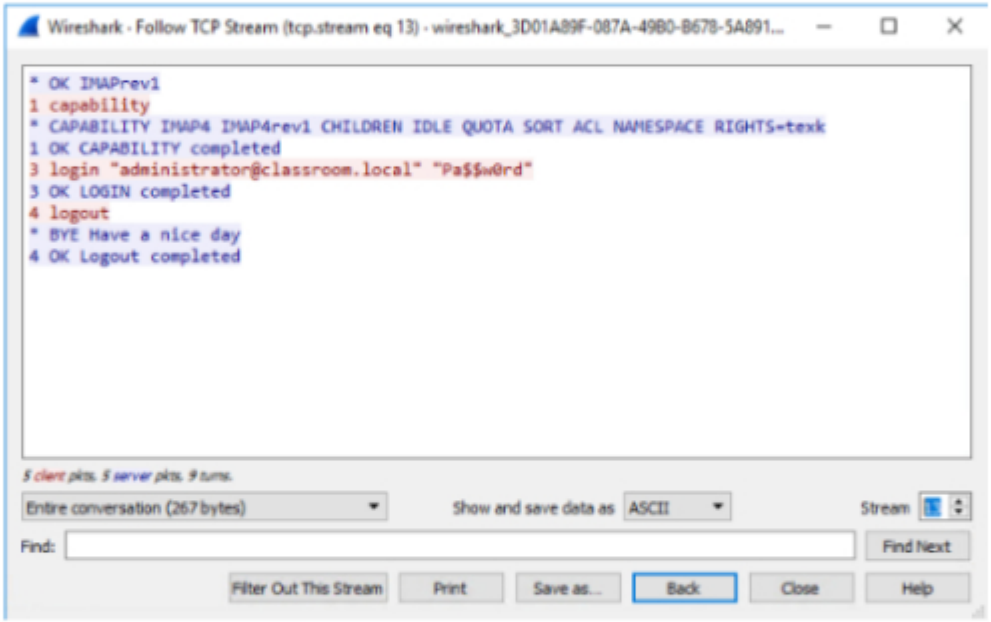
Kelas crypto-malware ransomware mencoba untuk mengenkripsi file data pada drive tetap, yang dapat dilepas, dan jaringan. Jika serangan berhasil, pengguna tidak akan dapat mengakses file tanpa mendapatkan kunci enkripsi pribadi, yang dipegang oleh penyerang. Jika berhasil, serangan semacam ini sangat sulit untuk dimitigasi, kecuali jika pengguna memiliki cadangan terbaru dari file yang dienkripsi. Salah satu contohnya adalah Cryptolocker, Trojan yang mencari file untuk dienkripsi dan kemudian meminta korban untuk membayar sejumlah uang sebelum waktu hitung mundur tertentu, setelah itu malware menghancurkan kunci yang memungkinkan dekripsi.



Ransomware WannaCry. Gambar Domain Publik Wikimedia. (Gambar oleh Wikimedia Commons.)

- Serangan Kata Sandi
  Serangan di jalur dan malware bisa sulit dilakukan. Banyak intrusi jaringan terjadi karena aktor ancaman dapat memperoleh kredensial untuk mengakses jaringan. Juga, ketika aktor ancaman memperoleh semacam akses melalui serangan on-path atau malware, mereka cenderung mencoba untuk meningkatkan hak istimewa untuk mendapatkan akses ke target lain di jaringan dengan mengumpulkan kredensial untuk akun administratif.

  Kata sandi atau hash kata sandi dapat ditangkap dengan mendapatkan file kata sandi atau dengan mengendus jaringan. Jika protokol menggunakan kredensial cleartext, maka aktor ancaman dapat dengan mudah membaca kata sandi cleartext dari frame yang diambil.



Jika kredensial otentikasi ditransmisikan dalam teks yang jelas, seperti versi protokol akses kotak surat IMAP yang tidak terenkripsi, kredensial dapat dicegat melalui packet sniffing dengan mudah. (Tangkapan layar milik Wireshark.)

Tips: Kata sandi mungkin dikirim dalam bentuk yang disandikan, seperti Base64, yang hanya merupakan representasi ASCII dari data biner. Ini tidak sama dengan enkripsi. Nilai kata sandi dapat dengan mudah diturunkan dari string Base64.

Dalam kebanyakan kasus, kata sandi disimpan dan ditransmisikan dengan aman dengan membuat hash kriptografis dari string yang dimasukkan oleh pengguna. Sebuah algoritma hash kriptografi, seperti Secure Hash Algorithm (SHA) atau Message Digest v5 (MD5), menghasilkan string panjang tetap dari string panjang variabel. Ini berarti, secara teori, tidak ada seorang pun kecuali pengguna (bahkan administrator sistem) yang mengetahui kata sandinya, karena teks biasa tidak dapat dipulihkan dari hash.

Perangkat lunak peretas kata sandi menggunakan berbagai metode untuk menyusun string kata sandi plaintext dari hash kriptografis:

- ***Dictionary***-Perangkat lunak mencocokkan hash dengan hash yang dihasilkan oleh kata-kata biasa yang ditemukan dalam kamus. Ini juga dapat mencakup informasi seperti nama pengguna dan perusahaan, nama hewan peliharaan, atau data lain apa pun yang mungkin digunakan orang secara naif sebagai kata sandi.

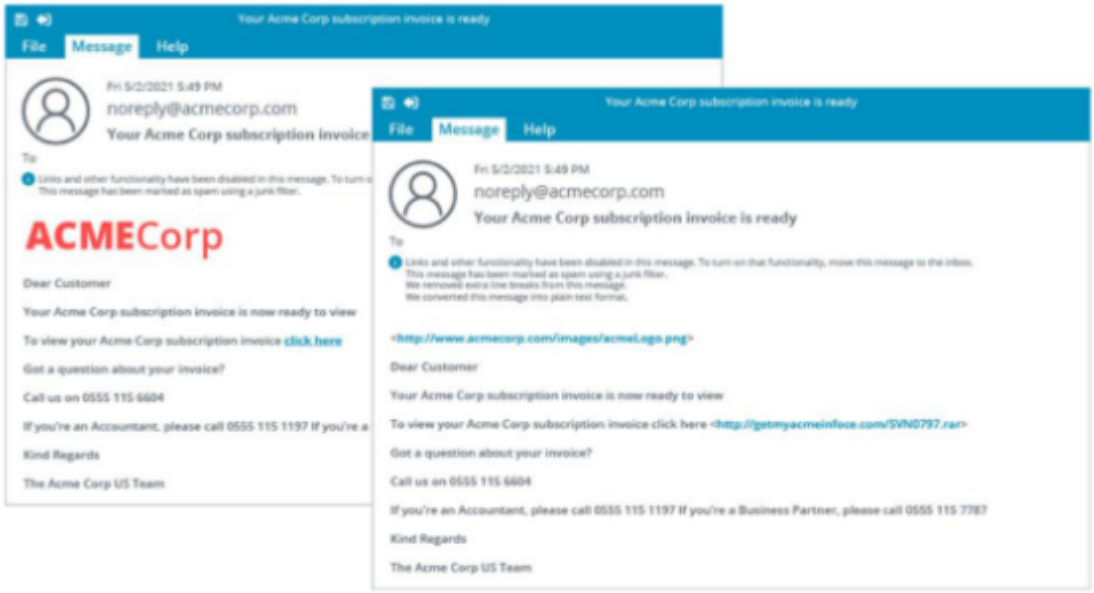
- ***Brute force***-Perangkat lunak mencoba mencocokkan hash dengan salah satu dari setiap kombinasi yang mungkin. Jika kata sandi pendek (di bawah delapan karakter) dan tidak rumit (hanya menggunakan huruf, misalnya), kata sandi mungkin dapat dibobol dalam hitungan menit. Kata sandi yang lebih panjang dan lebih kompleks meningkatkan jumlah waktu yang dibutuhkan untuk menjalankan serangan.

Aktor ancaman mungkin mendapatkan hash kata sandi dari protokol seperti SMB tanpa enkripsi yang dikonfigurasi. Risiko yang ditimbulkan oleh perengkahan perangkat lunak berarti lebih aman menggunakan enkripsi ujung ke ujung, seperti IPSec atau *Transport Layer Security* (TLS). Ini berarti bahwa semua data payload dienkripsi, dan network sniffer bahkan tidak dapat memulihkan hash kata sandi.

- Serangan Manusia dan Lingkungan
  Pelaku ancaman dapat menggunakan beragam teknik untuk mengkompromikan sistem keamanan. Prasyarat dari banyak jenis serangan adalah memperoleh informasi tentang jaringan dan sistem keamanan. Rekayasa sosial (atau meretas manusia) mengacu pada kumpulan teknik dan trik yang dirancang untuk membuat korban mengungkapkan informasi rahasia. Peniruan (berpura-pura menjadi orang lain) adalah salah satu teknik rekayasa sosial dasar. Serangan peniruan identitas klasik adalah pelaku ancaman menelepon ke departemen yang berpura-pura menelepon dari dukungan TI, mengklaim bahwa mereka harus menyesuaikan sesuatu pada sistem pengguna dari jarak jauh, dan membuat pengguna mengungkapkan kata sandi mereka. Agar serangan ini berhasil, pendekatannya harus persuasif dan membangun kepercayaan. Rekayasa sosial mungkin juga menggunakan intimidasi atau tipuan sebagai sarana untuk memperoleh informasi.

- Serangan *Phishing*
  Phishing adalah kombinasi dari rekayasa sosial dan spoofing. Ini membujuk atau menipu target untuk berinteraksi dengan sumber daya berbahaya yang disamarkan sebagai sumber terpercaya, secara tradisional menggunakan email sebagai vektor. Pesan phishing mungkin mencoba meyakinkan pengguna untuk melakukan beberapa tindakan, seperti menginstal malware yang disamarkan atau mengizinkan koneksi akses jarak jauh oleh penyerang. Jenis kampanye phishing lainnya menggunakan situs web palsu yang dibuat untuk meniru bank atau situs e-niaga atau sumber daya web lain yang

harus dipercaya oleh target. Penyerang kemudian mengirim email kepada pengguna situs web asli yang memberi tahu mereka bahwa akun mereka harus diperbarui atau dengan semacam peringatan atau alarm tipuan, menyediakan tautan tersamar yang sebenarnya mengarah ke situs palsu. Saat pengguna mengautentikasi dengan situs palsu, kredensial masuk mereka ditangkap.



Contoh email phishing-Di sebelah kanan, Anda dapat melihat pesan dalam bentuk aslinya karena klien email telah menghapus pemformatan (ditunjukkan di sebelah kiri) yang dirancang untuk menyamarkan sifat tautan.

- *Shoulder Surfing*
  Pelaku ancaman dapat mempelajari kata sandi atau PIN (atau informasi aman lainnya) dengan melihat pengguna mengetiknya. Ini disebut sebagai serangan selancar bahu. Terlepas dari namanya, penyerang mungkin tidak harus berada dalam jarak dekat dengan target—mereka dapat menggunakan teropong bertenaga tinggi atau CCTV untuk mengamati target secara langsung dari jarak jauh.

- *Tailgating and Piggybacking*
  Tailgating adalah cara memasuki area aman tanpa izin dengan mengikuti di belakang orang yang diizinkan membuka pintu atau pos pemeriksaan. Membonceng adalah situasi yang serupa tetapi berarti penyerang memasuki area aman dengan izin karyawan. Misalnya, penyerang mungkin menyamar sebagai anggota kru pembersih dan meminta karyawan menahan pintu agar tetap terbuka saat mereka membawa gerobak pembersih atau ember pel. Teknik lain adalah membujuk seseorang untuk menahan pintu agar tetap terbuka, menggunakan alasan, seperti "Saya lupa lencana/kunci saya." Sebagai alternatif, membonceng mungkin merupakan sarana dari pelaku ancaman orang dalam untuk mengizinkan akses ke seseorang tanpa mencatatnya di catatan masuk gedung.

Apply Network Hardening Techniques

- Pendahuluan: Menerapkan Teknik Pengerasan Jaringan
  Keamanan endpoint dan port switch adalah kontrol keamanan jaringan yang penting, memberikan pertahanan yang mendalam dengan mencegah pemasangan perangkat yang tidak sah. Jika Anda mengonfigurasi kebijakan untuk memastikan hanya perangkat yang diotorisasi yang terhubung ke jaringan, Anda juga memerlukan kebijakan untuk memastikan bahwa perangkat tersebut berada dalam konfigurasi yang aman dan sepenuhnya ditambal terhadap kerentanan. Sebagai teknisi jaringan, salah satu peran Anda akan memastikan bahwa host jaringan ditempatkan dalam konfigurasi yang aman sebelum diberikan akses.

- Pengerasan Perangkat dan Layanan
  Sebagai bagian dari strategi pertahanan mendalam, Anda perlu memikirkan untuk membuat setiap perangkat host dan infrastruktur jaringan aman dari gangguan atau penyalahgunaan. Mungkin tergoda untuk menganggap perangkat jaringan seperti switch dan router sebagai perangkat mandiri. Faktanya, perangkat ini sering menjalankan firmware yang cukup kompleks dan menampung banyak layanan untuk mengaktifkan manajemen dan konfigurasi jarak jauh. Menyebarkan sistem dalam konfigurasi yang aman dikenal sebagai pengerasan perangkat. Beberapa kebijakan yang akan membentuk konfigurasi aman meliputi hal-hal berikut:

    - **Ubah kata sandi/kredensial default**-Perangkat seperti titik akses nirkabel, sakelar, dan router terkadang dikirimkan dengan kata sandi manajemen default seperti kata sandi, admin, atau nama vendor perangkat. Ini harus diubah pada instalasi.

    - **Terapkan kompleksitas kata sandi/persyaratan panjangnya**-Kata sandi untuk infrastruktur jaringan harus sangat tahan terhadap serangan menebak dan memecahkan:

        - **Panjang**-Tidak ada kata sandi harus kurang dari delapan karakter. Namun, sebagai infrastruktur penting, kata sandi untuk peralatan jaringan harus 14+ karakter.

        - **Kompleksitas**-Memerlukan banyak kelas karakter (mencampur huruf, huruf besar, angka, dan simbol) tidak digunakan lagi oleh panduan terbaru NIST, tetapi masih merupakan persyaratan dalam banyak kebijakan kata sandi lokal.

    - **Menghindari kata sandi umum**-Jumlah serangan yang berhasil terhadap server web dan jaringan perusahaan telah menyebabkan basis data kredensial yang sangat besar diposting secara online. Analisis basis data ini menunjukkan berapa banyak pengguna-bahkan pengguna administratif-mengandalkan kata

sandi yang sederhana, seperti 123456 atau kata sandi. Dump basis data kata sandi ini memberi penyerang kamus yang berguna untuk digunakan saat mencoba memecahkan kredensial. Kata sandi apa pun yang dapat dicocokkan dengan istilah kamus sama sekali tidak aman dan tidak boleh digunakan.

- **Konfigurasikan akses berbasis peran**-Administrator default, pengguna super, atau akun root memiliki akses tak terbatas ke perangkat. Jika kredensial untuk akun ini dibagikan, risiko penyusupan menjadi sangat besar. Akses berbasis peran berarti bahwa sekumpulan izin terbatas dikonfigurasi untuk grup administratif yang berbeda, seperti memisahkan izin untuk mengkonfigurasi sistem dengan izin untuk mengkonfigurasi logging dan audit. Pemisahan tugas ini mengurangi dampak dari kompromi satu akun.

- **Nonaktifkan layanan jaringan yang tidak dibutuhkan**-Layanan atau protokol apa pun yang tidak digunakan harus dinonaktifkan. Ini mengurangi permukaan serangan alat jaringan atau OS. Permukaan serangan berarti berbagai hal yang mungkin dapat dieksploitasi oleh penyerang untuk membahayakan perangkat. Sangat penting untuk menonaktifkan antarmuka administrasi yang tidak digunakan.

- **Nonaktifkan protokol tidak aman**-Serangan pengendus dapat dikurangi dengan mengenkripsi saluran tempat komunikasi berlangsung. Ini berarti bahwa bahkan jika penyadap dapat mendengarkan pesan, dia tidak dapat memahaminya tanpa mendapatkan kunci enkripsi. Penting untuk memahami protokol mana yang tidak aman dalam hal penggunaan saluran yang tidak terenkripsi. Ini sangat penting saat menggunakan saluran untuk mengautentikasi. Protokol yang tidak aman harus ditinggalkan, dan protokol yang aman digunakan sebagai gantinya. Misalnya, versi asli SNMP tidak dienkripsi. Untuk menerapkan SNMP aman, konfigurasikan SNMPv3, yang mendukung enkripsi, atau gunakan protokol enkapsulasi seperti IPSec untuk mengenkripsi lalu lintas SNMP.

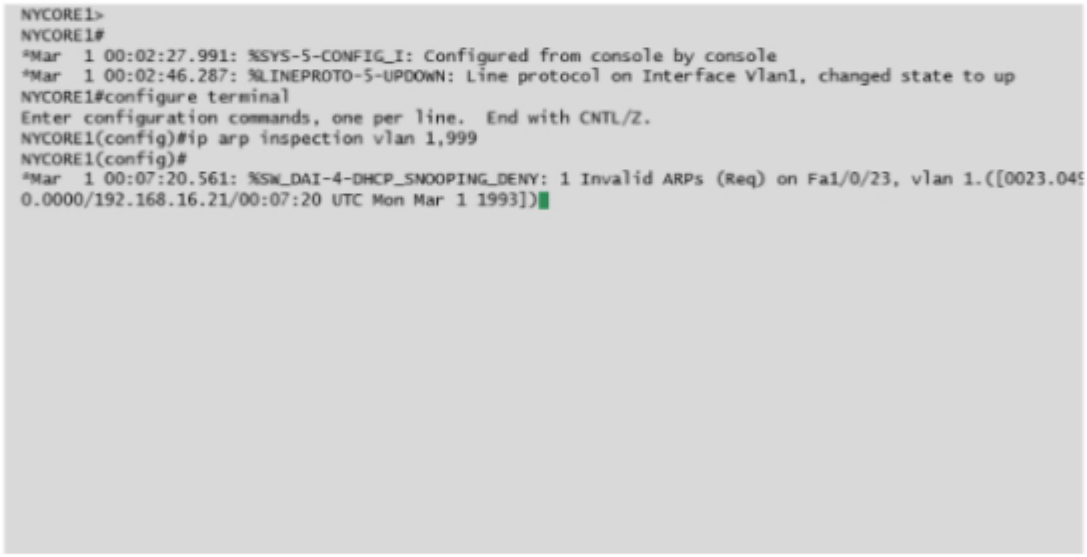
- Keamanan Titik Akhir dan Perlindungan Switchport
  Keamanan titik akhir adalah seperangkat prosedur dan teknologi keamanan yang dirancang untuk membatasi akses jaringan pada tingkat perangkat. Keamanan titik akhir kontras dengan fokus pada keamanan perimeter yang ditetapkan oleh topologi seperti subnet yang disaring dan teknologi seperti firewall. Keamanan titik akhir dirancang bukan untuk menggantikan keamanan perimeter tetapi untuk melengkapinya, menciptakan pertahanan yang mendalam.

  Akses ke port switch fisik dan perangkat keras switch harus dibatasi untuk staf yang berwenang, menggunakan ruang server/peralatan yang aman dan/atau lemari perangkat keras yang dapat dikunci. Untuk mencegah pemasangan perangkat klien yang tidak sah, port sakelar dapat dinonaktifkan menggunakan perangkat lunak manajemen atau diisolasi ke VLAN tanpa rute ke jaringan (VLAN lubang hitam). Pada

switch Cisco, pengaturan konfigurasi ini umumnya akan diterapkan menggunakan beberapa versi perintah atau sub-perintah switchport. Sebagai opsi lain, kabel patch dapat dilepas secara fisik dari port. Menonaktifkan port sepenuhnya dengan cara ini dapat menimbulkan banyak overhead administratif dan ruang lingkup kesalahan. Juga, itu tidak memberikan perlindungan lengkap, karena penyerang dapat mencabut perangkat dari port yang diaktifkan dan menghubungkan laptop mereka sendiri. Akibatnya, metode yang lebih canggih untuk memastikan keamanan pelabuhan telah dikembangkan.

- Penyaringan MAC dan Inspeksi ARP Dinamis
Mengonfigurasi pemfilteran MAC pada switch berarti menentukan alamat MAC mana yang diizinkan untuk terhubung ke port tertentu. Ini dapat dilakukan dengan membuat daftar alamat MAC yang valid atau dengan menentukan batas jumlah alamat yang diizinkan. Misalnya, jika keamanan port diaktifkan dengan maksimum dua alamat MAC, switch akan merekam dua MAC pertama yang terhubung ke port itu tetapi kemudian menghapus lalu lintas apa pun dari mesin dengan ID adaptor jaringan berbeda yang mencoba terhubung

Host jahat dapat menggunakan alamat MAC palsu untuk mencoba melakukan keracunan cache ARP terhadap host lain di jaringan dan melakukan serangan di jalur. Sebuah fitur keamanan port switch seperti *dynamic ARP inspection* (DAI) mencegah host yang terpasang ke port yang tidak dipercaya membanjiri segmen dengan balasan ARP serampangan. Inspeksi ARP memelihara database pemetaan IP:ARP yang terpercaya. Ini juga memastikan bahwa paket ARP dibuat secara valid dan menggunakan alamat IP yang valid.



Mengonfigurasi pemeriksaan ARP dan pengintaian DHCP pada sakelar Cisco. (Gambar © dan Courtesy of Cisco Systems, Inc. Penggunaan tidak sah tidak diizinkan.)

- *DHCP Snooping*
  Mengkonfigurasi pengintaian DHCP menyebabkan switch memeriksa lalu lintas DHCP yang tiba di port akses untuk memastikan bahwa host tidak mencoba menipu alamat MAC-nya. Ini juga dapat digunakan untuk mencegah server DHCP jahat beroperasi di jaringan. Dengan pengintaian DHCP, hanya penawaran DHCP dari port yang dikonfigurasi sebagai terpercaya yang diizinkan.

- Inspeksi Penemuan Tetangga dan Penjaga Iklan Router
  Inspeksi *Neighbor Discovery* (ND) dan *Router Advertisement* (RA) Guard melakukan fungsi yang mirip dengan pengintaian DAI dan DHCP untuk jaringan IPv6. Sebagian besar host memiliki IPv6 yang diaktifkan secara default dan menonaktifkannya sering kali dapat menyebabkan masalah yang tidak terduga. Akibatnya, perlindungan sakelar ini harus diaktifkan untuk mengurangi serangan spoofing dan on-path melalui IPv6.

- Keamanan Port/IEEE 802.1X Kontrol Akses Jaringan Berbasis Port
  Pembatasan dan pemfilteran MAC dan inspeksi ARP memberikan perlindungan terhadap serangan, tetapi itu bukan cara untuk memastikan hanya host yang valid yang terhubung ke jaringan. Keamanan port mengacu pada mekanisme Port-Based Network Access Control (PNAC) standar IEEE 802.1X. PNAC berarti bahwa sakelar melakukan semacam otentikasi perangkat yang terpasang sebelum mengaktifkan port.

  Di bawah 802.1X, perangkat yang meminta akses adalah pemohon. Sakelar, yang disebut sebagai autentikator, hanya mengaktifkan protokol *Extensible Authentication Protocol over LAN* (EAPoL) dan menunggu perangkat menyediakan data otentikasi. Authenticator meneruskan data ini ke server otentikasi, biasanya server RADIUS, yang memeriksa kredensial dan memberikan atau menolak akses. Jika akses diberikan, switch akan mengkonfigurasi port untuk menggunakan VLAN yang sesuai dan mengaktifkannya untuk lalu lintas jaringan biasa. Host yang tidak diautentikasi dapat ditolak semua jenis aksesnya atau ditempatkan di VLAN tamu dengan hanya akses terbatas ke seluruh jaringan.

- Praktik Terbaik VLAN dan PVLAN
  Fitur LAN virtual (VLAN) dari sakelar Ethernet terkelola biasanya digunakan untuk menerapkan kebijakan segmentasi. VLAN mengisolasi lalu lintas siaran Layer 2 untuk beralih port yang dikonfigurasi dengan ID VLAN yang sama. Setiap ID VLAN biasanya dipetakan ke subnet dan setiap penerusan lalu lintas antara VLAN harus dilakukan oleh router (atau switch Layer 3).

- VLAN pribadi
- Private VLAN (PVLAN) menerapkan lapisan segmentasi tambahan dengan membatasi kemampuan host dalam VLAN untuk berkomunikasi secara langsung satu sama lain. Ini mungkin digunakan oleh perusahaan hosting untuk mencegah server web yang dioperasikan oleh pelanggan yang berbeda dapat berkomunikasi. Mengisolasi instance server ini menggunakan PVLAN lebih sederhana daripada membuat beberapa VLAN

dan subnet. Demikian pula, ISP menggunakan PVLAN untuk mengisolasi lalu lintas pelanggan.

Saat mengkonfigurasi PVLAN, VLAN "host" disebut sebagai VLAN primer. Jenis port PVLAN berikut dapat dikonfigurasi dalam VLAN utama:

- ***Port promiscuous***-Dapat berkomunikasi dengan semua port di semua domain dalam PVLAN. Ini biasanya merupakan port yang melaluinya lalu lintas yang dirutekan dan/atau DHCP dikirim.

- ***Isolated port***-Dapat berkomunikasi dengan port promiscuous saja. Ini membuat subdomain dari satu host saja. PVLAN dapat berisi beberapa port yang terisolasi, tetapi masing-masing berada dalam subdomainnya sendiri.

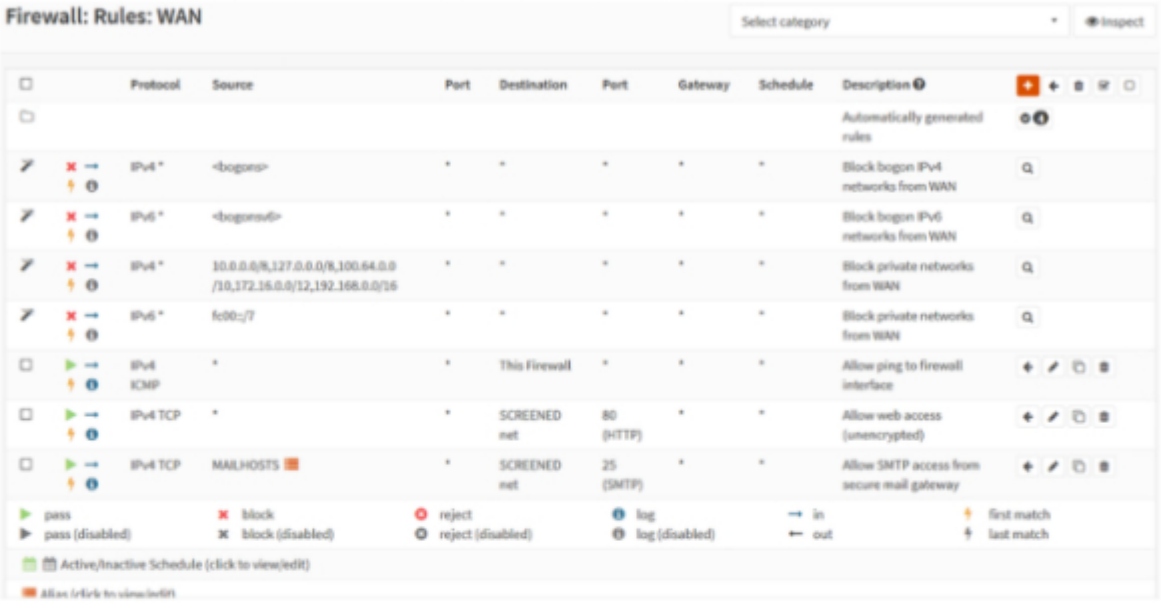
- ***Community port***-Dapat berkomunikasi dengan pelabuhan promiscuous dan dengan pelabuhan lain di komunitas yang sama. Ini membuat subdomain yang dapat berisi banyak host.

- VLAN Default dan VLAN Asli
  VLAN dengan ID 1 disebut sebagai VLAN default. Ini tidak dapat diubah. Namun, kecuali jika dikonfigurasi secara berbeda, semua port pada switch default berada di VLAN 1. Saat Anda menerapkan VLAN, Anda harus menghindari pengiriman lalu lintas data pengguna melalui VLAN default. Itu harus tetap tidak digunakan atau hanya digunakan untuk lalu lintas protokol antar-switch, jika perlu. Misalnya, lalu lintas spanning tree akan diizinkan untuk dijalankan di atas VLAN default. Pastikan port yang tidak digunakan tidak ditetapkan ke VLAN 1.

  VLAN asli adalah salah satu tempat lalu lintas yang tidak ditandai ditempatkan saat menerima bingkai melalui port trunk. Ketika sebuah switch menerima frame yang tidak ditandai melalui sebuah trunk, ia memberikan frame tersebut ke VLAN asli. Lalu lintas yang tidak ditandai mungkin berasal dari perangkat lama seperti hub atau sakelar lama yang tidak mendukung bingkai yang di enkapsulasi 802.1Q. VLAN asli awalnya diatur dengan VID yang sama dengan VLAN default (VID 1). Namun, Anda dapat dan harus mengubah ini untuk membuat VID asli menjadi ID yang sesuai. Ini tidak boleh sama dengan VLAN yang digunakan untuk lalu lintas data lainnya. VLAN ID (VID) asli yang sama harus dikonfigurasi untuk port trunk pada kedua switch.

- Aturan Firewall dan Konfigurasi ACL
  Firewall access control lists (ACL) dikonfigurasi berdasarkan prinsip akses paling sedikit. Ini sama dengan prinsip hak istimewa terkecil; hanya mengizinkan jumlah lalu lintas minimum yang diperlukan untuk pengoperasian layanan jaringan yang valid dan tidak lebih. Aturan di ACL firewall diproses dari atas ke bawah. Jika lalu lintas cocok dengan aturan yang mengizinkan paket, maka paket tersebut diizinkan untuk lewat. Akibatnya, aturan yang paling spesifik ditempatkan di atas. Aturan default terakhir biasanya

memblokir lalu lintas apa pun yang tidak cocok dengan aturan. Ini disebut penolakan implisit. Jika firewall tidak memiliki aturan penolakan implisit default, aturan penolakan semua eksplisit dapat ditambahkan secara manual ke akhir ACL.



Contoh aturan firewall yang dikonfigurasi di OPNsense. Aturan ini memblokir semua lalu lintas dari jaringan bogon dan rentang alamat IP pribadi, tetapi mengizinkan lalu lintas ICMP diarahkan ke antarmuka firewall, lalu lintas HTTP dari sumber mana pun, dan lalu lintas SMTP dari jaringan yang dikenal, yang didefinisikan sebagai alias MAILHOSTS. (Tangkapan layar digunakan dengan izin dari OPNsense.)

Setiap aturan dapat menentukan apakah akan memblokir atau mengizinkan lalu lintas berdasarkan parameter, sering disebut sebagai tupel. Jika Anda menganggap setiap aturan seperti baris dalam database, tupel adalah kolom. Misalnya, pada tangkapan layar, tupel termasuk Protokol, Sumber (alamat), (Sumber) Port, Tujuan (alamat), (Tujuan) Port, dan sebagainya.

Sebagai contoh konfigurasi ACL, iptables adalah utilitas baris perintah yang disediakan oleh banyak distribusi Linux yang memungkinkan administrator untuk mengedit aturan yang diterapkan oleh firewall kernel Linux. Iptables bekerja dengan rantai firewall, yang berlaku untuk berbagai jenis lalu lintas yang melewati sistem. Tiga rantai utama adalah:

- ***INPUT***-Mempengaruhi koneksi masuk. Misalnya, jika pengguna mencoba SSH ke server Linux, iptables akan mencoba mencocokkan alamat IP sumber dan port tujuan dengan aturan di rantai input.

- ***OUTPUT***-Untuk koneksi keluar. Misalnya, jika Anda mencoba melakukan ping ke FQDN seperti comptia.org, iptables akan memeriksa rantai keluarannya untuk melihat aturan terkait ping dan comptia.org (atau alamat IP yang ditentukan oleh

comptia.org) sebelum memutuskan untuk mengizinkan atau menolak upaya koneksi.

- ***FORWARD***-Digunakan untuk koneksi yang melewati host, daripada dikirim secara lokal. Rantai ini akan digunakan saat mengkonfigurasi host sebagai firewall jaringan.

Aturan dapat ditetapkan ke rantai ini, atau rantai baru dapat dibuat dan kemudian dihubungkan ke rantai sistem standar untuk memengaruhi arus lalu lintas. Untuk melihat status iptables saat ini dan volume lalu lintas menggunakan rantai, gunakan perintah:

iptables -L -v

Untuk mengubah aturan firewall, perintah seperti berikut akan digunakan.

Contoh-contoh ini memungkinkan satu alamat IP dari subnet tertentu untuk terhubung dan memblokir semua yang lain dari subnet yang sama.

iptables -A INPUT -s 10.1.0.1 -j ACCEPT

iptables -A INPUT -s 10.1.0.0/24 -j DROP

Saat Anda menetapkan aturan akses paling sedikit (jika kebijakan default INPUT dan OUTPUT diatur untuk menolak semua), Anda harus menetapkan aturan INPUT dan OUTPUT untuk mengizinkan sebagian besar jenis lalu lintas klien/server. Misalnya, untuk mengizinkan host beroperasi sebagai server SSH, konfigurasikan aturan berikut:

iptables -A INPUT -p tcp --dport 22 -s 10.1.0.0/24 -m state --

state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p tcp --sport 22 -d 10.1.0.0/24 -m state --

state ESTABLISHED -j ACCEPT

Perintah-perintah ini menggunakan sifat stateful dari firewall untuk membedakan antara koneksi baru dan yang sudah ada. Aturan pertama memungkinkan host di 10.1.0.0/24 net untuk memulai koneksi dengan server SSH pada host lokal melalui port 22. Aturan kedua memungkinkan server untuk menanggapi koneksi yang ada yang dibuat oleh host di subnet yang sama.

- Kontrol Pemolisian Pesawat
  The quality of service (QoS) stack membedakan tiga lapisan operasional: kontrol, data, dan manajemen. Sebuah alat jaringan menggunakan sumber daya minimal untuk

memproses lalu lintas data biasa, yang sering diproses oleh perangkat keras khusus (satu atau lebih chip ASIC) dan tidak memerlukan CPU tujuan umum. Sebaliknya, lalu lintas kontrol dan manajemen memerlukan pemrosesan berbasis perangkat lunak dan "dipasang" ke saluran CPU, membutuhkan sumber daya memori dan waktu prosesor. Bidang kontrol terdiri dari lalu lintas yang membuat jaringan itu sendiri tetap beroperasi, termasuk pembaruan perutean, lalu lintas ARP, pemberitahuan STP, pembaruan NTP, klasifikasi QoS dan permintaan reservasi tautan, dan seterusnya. Bidang manajemen terdiri dari lalu lintas yang memungkinkan administrasi jarak jauh dan pemantauan peralatan jaringan, seperti SSH, SNMP, NetFlow, dan syslog. Lalu lintas manajemen biasanya diarahkan ke alamat loopback alat.

Jaringan harus selalu mengizinkan bandwidth yang cukup dan sumber daya CPU/memori untuk kontrol dan manajemen lalu lintas. Jika lalu lintas ini diblokir, kemampuan jaringan untuk berfungsi terganggu. Malware worm atau alat pengintai berbahaya dapat mencoba menyamar sebagai lalu lintas berprioritas tinggi dari berbagai jenis. Ini menempatkan tuntutan tinggi yang tidak biasa pada router dan sakelar yang memproses lalu lintas pesawat, memengaruhi serangan DoS pada fungsi lain yang harus mereka lakukan. Ini juga digambarkan sebagai serangan *route processor* (RP) (meskipun perhatikan bahwa itu dapat dilakukan terhadap kedua router dan switch). Pemrosesan rute juga dapat terancam oleh kesalahan konfigurasi yang tidak disengaja.

Kebijakan kepolisian bidang kontrol dirancang untuk mengurangi risiko dari kerentanan pemroses rute. Kebijakan tersebut dapat menggunakan ACL untuk mengizinkan atau menolak lalu lintas kontrol dari sumber tertentu dan menerapkan pembatasan kecepatan jika sumber mengancam untuk membanjiri prosesor rute.

- Keamanan Nirkabel
  Fitur berikut dapat diaktifkan untuk menyediakan akses jaringan nirkabel yang aman.

  - ***Preshared keys* (PSK)** -Otentikasi grup memungkinkan stasiun terhubung ke jaringan menggunakan frasa sandi bersama, yang digunakan untuk menghasilkan kunci yang dibagikan sebelumnya (PSK). Frasa sandi harus cukup panjang (14+ karakter) untuk memastikan kunci yang kuat.

  - ***Extensible Authentication Protocol***-Sebuah access point dapat mengimplementasikan mekanisme keamanan port yang mirip dengan switch. Ini dikonfigurasi pada titik akses dengan memilih otentikasi perusahaan. Ini memungkinkan pengguna untuk mengautentikasi ke jaringan nirkabel terhadap server RADIUS menggunakan kredensial jaringan reguler mereka. EAP juga memungkinkan otentikasi perangkat menggunakan sertifikat digital.

  - ***Captive portal***-Jaringan tamu mungkin dikonfigurasi untuk melakukan otentikasi dengan mengarahkan stasiun ke halaman web yang aman. Pengguna harus mengautentikasi ke halaman dan memenuhi persyaratan yang ditetapkan

administrator lainnya, seperti menerima kebijakan penggunaan, sebelum stasiun diizinkan untuk menggunakan jaringan.

- ***MAC filtering***-Seperti halnya sakelar, titik akses dapat dikonfigurasi dengan daftar terima atau tolak alamat MAC yang diketahui.

- ***Geofencing***-Dapat digunakan untuk memastikan bahwa stasiun berada dalam area geografis yang valid untuk mengakses jaringan, seperti memastikan perangkat berada di dalam gedung daripada mencoba mengakses WLAN dari tempat parkir mobil atau lokasi eksternal lainnya.

- ***Antenna placement and power levels***-Desain dan survei lokasi memfasilitasi jangkauan nirkabel yang kuat ketika semua area yang diharapkan menerima sinyal yang kuat. Tingkat daya dan pemilihan saluran harus disetel sehingga titik akses tidak saling mengganggu atau menyiarkan sinyal yang dapat "didengar" oleh stasiun tetapi tidak dapat dibalas. Kehadiran pemancar yang sangat kuat (30 dBm+) mungkin menunjukkan adanya titik akses jahat kembar jahat.

- ***Wireless client isolation***-Klien yang terhubung ke WLAN biasanya berada dalam domain siaran yang sama dan dapat berkomunikasi satu sama lain. Titik akses dapat dikonfigurasi untuk mencegah hal ini sehingga stasiun hanya dapat berkomunikasi melalui gatewaynya. Lalu lintas peer-to-peer dijatuhkan oleh AP.

- ***Guest network isolation***-Jaringan tamu dapat menerapkan kebijakan keamanan dan penerusan terpisah daripada jaringan yang mengizinkan akses ke LAN perusahaan. Biasanya, jaringan tamu diizinkan mengakses Internet tetapi tidak ke server lokal. Sebagian besar router SOHO dilengkapi dengan jaringan tamu yang telah dikonfigurasi sebelumnya. Dalam suatu perusahaan, jaringan tamu akan diimplementasikan menggunakan VLAN terpisah.

- Pertimbangan Akses IoT
  Internet of Things (IoT) mungkin ada dalam sistem tertanam khusus dan jaringan bangunan pintar dan/atau sebagai perangkat pintar individual yang dipasang di tempat kerja karyawan. Akses tidak terkelola ke perangkat ini dapat menimbulkan risiko keamanan sehingga prosedur manajemen dan audit harus mendeteksi dan mengamankannya:

  Lakukan audit rutin untuk mencegah penyebaran perangkat dan peralatan pintar "IT bayangan" yang tidak terkendali. Ini dapat dibantu melalui perangkat lunak pemindaian yang berspesialisasi dalam identifikasi perangkat IoT, memberikan visibilitas ke dalam penerapannya. Juga, mendidik pengguna tentang risiko dari perangkat IoT dan perlunya mematuhi kebijakan keamanan dan TI.

Pastikan antarmuka administratif diamankan, dan konfigurasi serta manajemen perangkat ditetapkan ke peran organisasi yang sesuai.

- Sertakan semua perangkat IoT dalam patch dan audit manajemen kerentanan. Isolasi manajemen dan pemantauan lalu lintas untuk sistem tertanam untuk meminimalkan akses ke dan dari jaringan data perusahaan.

  Audit kebijakan dan prosedur keamanan pemasok secara teratur, terutama jika ada saluran pemantauan atau manajemen eksternal.

- Manajemen Patch dan Firmware
  Setiap jenis OS dan perangkat lunak aplikasi memiliki kerentanan yang menghadirkan peluang bagi calon penyerang. Segera setelah kerentanan diidentifikasi dalam produk yang didukung, vendor akan (atau harus) mencoba memperbaikinya. Pada saat yang sama, penyerang akan mencoba mengeksploitasinya. Tidak akan pernah ada satu daftar lengkap kerentanan untuk setiap OS dan aplikasi, jadi Anda harus selalu mengikuti saran keamanan sistem yang diposting di situs web vendor dan di sumber referensi keamanan lainnya. Manajemen tambalan mengacu pada prosedur yang diterapkan untuk mengelola penginstalan pembaruan untuk perangkat keras (firmware) dan perangkat lunak.

  Firmware pada perangkat seperti router/firewall mungkin merupakan perangkat lunak yang sangat canggih. Sangat umum bagi perangkat lunak semacam itu untuk mengetahui kerentanannya, jadi sangat penting untuk menggunakan versi yang aman. Memperbarui firmware dikenal sebagai mem-flash chip. Ini biasanya dilakukan melalui program pengaturan yang disediakan vendor. Penting untuk membuat cadangan konfigurasi sistem (terutama untuk firewall) sebelum melakukan pembaruan atau peningkatan firmware.

  OS host, seperti Windows, dapat menerapkan patch satu per satu. OS alat, seperti Cisco IOS, harus ditambal ke nomor versi tertentu dengan menerapkan gambar perangkat lunak baru. Untuk mengatasi kerentanan tertentu, Anda dapat menggunakan alat seperti Pemeriksa Perangkat Lunak IOS (tools.cisco.com/security/center/softwarechecker.x) untuk mengidentifikasi versi "perbaikan pertama" IOS untuk penasihat keamanan tersebut. Ini berarti bahwa perubahan lain dapat diperkenalkan, jadi diperlukan pengujian dan penilaian dampak yang cermat.

  Setelah Anda menyelesaikan pemeriksaan lingkungan dan kompatibilitas serta mencadangkan konfigurasi yang ada, proses pemutakhiran dasar adalah menyalin citra sistem baru ke memori flash peralatan. Ini dapat dilakukan melalui jaringan menggunakan *Trivial File Transfer Protocol* (TFTP) atau salinan file jarak jauh atau dengan menggunakan kartu memori flash yang dapat dilepas. Setelah pembaruan

gambar dilakukan, Anda menjalankan urutan perintah untuk mengganti gambar lama dan memuat yang baru saat startup.

Sebagian besar perubahan dan pembaruan versi perangkat lunak dan firmware ke atas, menuju versi yang lebih baru. Downgrade (atau rollback) mengacu pada kembali ke versi sebelumnya dari perangkat lunak atau firmware. Ini mungkin diperlukan untuk memperbaiki masalah yang disebabkan oleh perangkat atau perangkat lunak yang baru saja ditingkatkan atau diperbarui. Dalam beberapa keadaan, penurunan versi mungkin tidak dapat dilakukan. Perangkat jaringan mungkin tidak mendukung penurunan versi ke versi firmware sebelumnya, misalnya, atau OS mungkin harus diinstal ulang sepenuhnya. Saat menerapkan tambalan atau peningkatan, merupakan praktik umum untuk membuat cadangan konfigurasi, jika pengaturan harus diterapkan kembali setelah pembaruan. Saat menurunkan versi, cadangan konfigurasi mungkin tidak berfungsi karena mungkin melibatkan pengaturan yang tidak disertakan dalam versi sebelumnya.

Modul 20

Summarizing Cloud and Datacenter Architecture

Summarize Cloud Concepts

- Pendahuluan: Meringkas Konsep Cloud
  Layanan cloud memungkinkan perusahaan untuk mengalihdayakan daya komputasi dan infrastruktur jaringan/aplikasi. Komputasi awan mencakup berbagai implementasi dan layanan. Jika Anda berencana menggunakan layanan cloud, Anda perlu mengetahui apa saja pilihannya serta kelebihan dan kekurangannya. Memiliki pemahaman yang kuat tentang pilihan ini akan memungkinkan Anda untuk mengelola dan menerapkan teknologi ini dengan lebih baik di lingkungan Anda.

- Skalabilitas dan Elastisitas Cloud
  Dari sudut pandang konsumen, komputasi awan adalah layanan yang menyediakan contoh server sumber daya sesuai permintaan, penyimpanan file, basis data, atau aplikasi melalui jaringan, biasanya Internet. Layanan ini adalah cloud karena pengguna akhir tidak mengetahui atau bertanggung jawab atas detail pengadaan, implementasi, atau pengelolaan infrastruktur yang menopang sumber daya tersebut. Pengguna akhir tertarik dan hanya membayar layanan yang disediakan oleh cloud.

  Dari sudut pandang penyedia, menyediakan cloud sama seperti menyediakan jenis pusat data skala besar lainnya. Komputasi awan hampir selalu menggunakan satu atau lebih metode virtualisasi untuk memastikan bahwa sumber daya dengan cepat dan mudah disediakan untuk klien yang membutuhkannya.

    - Di antara manfaat lainnya, cloud memberikan skalabilitas dan elastisitas: Skalabilitas berarti bahwa biaya yang terlibat dalam penyediaan layanan ke lebih banyak pengguna adalah linier. Misalnya, jika jumlah pengguna berlipat ganda dalam sistem yang dapat diskalakan, biaya untuk mempertahankan tingkat layanan yang sama juga akan berlipat ganda (atau kurang dari dua kali lipat). Jika biaya lebih dari dua kali lipat, sistem kurang terukur. Skalabilitas dapat dicapai dengan menambahkan node (horizontal/scaling out) atau dengan menambahkan sumber daya ke setiap node (vertikal/scaling up).

    - Elastisitas mengacu pada kemampuan sistem untuk menangani perubahan sesuai permintaan secara real time. Suatu sistem dengan elastisitas tinggi tidak akan mengalami kehilangan layanan atau kinerja jika permintaan tiba-tiba berlipat ganda (atau tiga kali lipat, atau empat kali lipat). Sebaliknya, mungkin penting bagi sistem untuk dapat mengurangi biaya ketika permintaan rendah.

  Untuk memenuhi persyaratan skalabilitas dan elastisitas, penyedia cloud harus dapat menyediakan dan mencabut sumber daya secara otomatis. Ini dicapai melalui pengumpulan sumber daya dan virtualisasi. Pengumpulan sumber daya berarti bahwa perangkat keras yang membentuk pusat data penyedia cloud tidak didedikasikan atau

dicadangkan untuk satu akun pelanggan. Lapisan virtualisasi yang digunakan dalam arsitektur cloud memungkinkan penyedia menyediakan lebih banyak CPU, memori, disk, atau sumber daya jaringan menggunakan perangkat lunak manajemen, daripada (misalnya) harus pergi ke lantai pusat data, mencabut server, menambahkan modul memori , dan reboot.

- Model Penerapan Cloud
  Dalam kebanyakan kasus, cloud-yaitu, perangkat keras dan/atau perangkat lunak yang menghosting layanan-akan berada di luar lokasi relatif terhadap pengguna organisasi. Pengguna cloud biasanya memerlukan tautan Internet untuk mengakses layanan cloud. Namun, mungkin ada pengaturan kepemilikan dan akses yang berbeda untuk cloud. Model penyebaran cloud ini dapat dikategorikan secara luas sebagai berikut:

  Publik (atau *multi tenant)*-layanan yang ditawarkan melalui Internet oleh *cloud service providers* (CSP) kepada konsumen cloud, sering disebut sebagai penyewa. Dengan model ini, bisnis dapat menawarkan langganan atau pembiayaan bayar sesuai pemakaian, sementara pada saat yang sama menyediakan layanan tingkat rendah secara gratis. Sebagai sumber daya bersama, ada risiko terkait kinerja dan keamanan. Arsitektur *multi cloud* adalah tempat organisasi konsumen menggunakan layanan dari lebih dari satu CSP.

  - ***Hosted Private***-Diselenggarakan oleh pihak ketiga untuk penggunaan eksklusif organisasi. Ini lebih aman dan dapat menjamin tingkat kinerja yang lebih baik, tetapi juga lebih mahal.

  - ***Private***-Cloud Infrastruktur yang sepenuhnya pribadi dan dimiliki oleh organisasi. Dalam hal ini, kemungkinan ada satu unit bisnis yang didedikasikan untuk mengelola cloud sementara unit bisnis lain memanfaatkannya. Dengan komputasi awan pribadi, organisasi dapat melakukan kontrol yang lebih besar atas privasi dan keamanan layanan mereka. Jenis metode pengiriman ini lebih diarahkan ke perbankan dan layanan pemerintah yang membutuhkan kontrol akses yang ketat dalam operasinya.

    Jenis cloud ini dapat berada di dalam atau di luar lokasi relatif terhadap unit bisnis lainnya. Tautan di tempat jelas dapat memberikan kinerja yang lebih baik dan kecil kemungkinannya untuk mengalami pemadaman (kehilangan tautan Internet, misalnya). Di sisi lain, fasilitas offsite khusus dapat memberikan akses bersama yang lebih baik untuk banyak pengguna di lokasi yang berbeda.

  - ***Community***-Disinilah beberapa organisasi berbagi biaya cloud pribadi yang dihosting atau sepenuhnya pribadi. Ini biasanya dilakukan untuk mengumpulkan sumber daya untuk masalah bersama, seperti standarisasi dan kebijakan keamanan.

- ***Hybrid***-Sebuah solusi komputasi awan yang mengimplementasikan semacam solusi hybrid publik/swasta/komunitas/host/onsite/offsite. Misalnya, organisasi perjalanan mungkin menjalankan situs web penjualan hampir sepanjang tahun menggunakan cloud pribadi, tetapi "membuka" solusi ke cloud publik pada saat pemanfaatan yang jauh lebih tinggi diperkirakan. Sebagai contoh lain, penerapan hybrid dapat digunakan untuk menyediakan beberapa fungsi melalui cloud publik, tetapi tetap menjaga infrastruktur, aplikasi, dan data yang sensitif atau teregulasi di lokasi.

Fleksibilitas adalah keunggulan utama komputasi awan, tetapi implikasinya terhadap risiko data harus dipahami dengan baik saat Anda memindahkan data antara lingkungan penyimpanan pribadi dan publik.

- Model Layanan Cloud
  Serta model penyebaran layanan-layanan publik, swasta, hybrid, atau komunitas-cloud sering dibedakan pada tingkat kompleksitas dan pra konfigurasi yang disediakan. Model-model ini disebut sebagai *Something/Anything/Everything as a Service* (XaaS). Beberapa model XaaS yang paling umum adalah infrastruktur, perangkat lunak, platform, dan desktop.

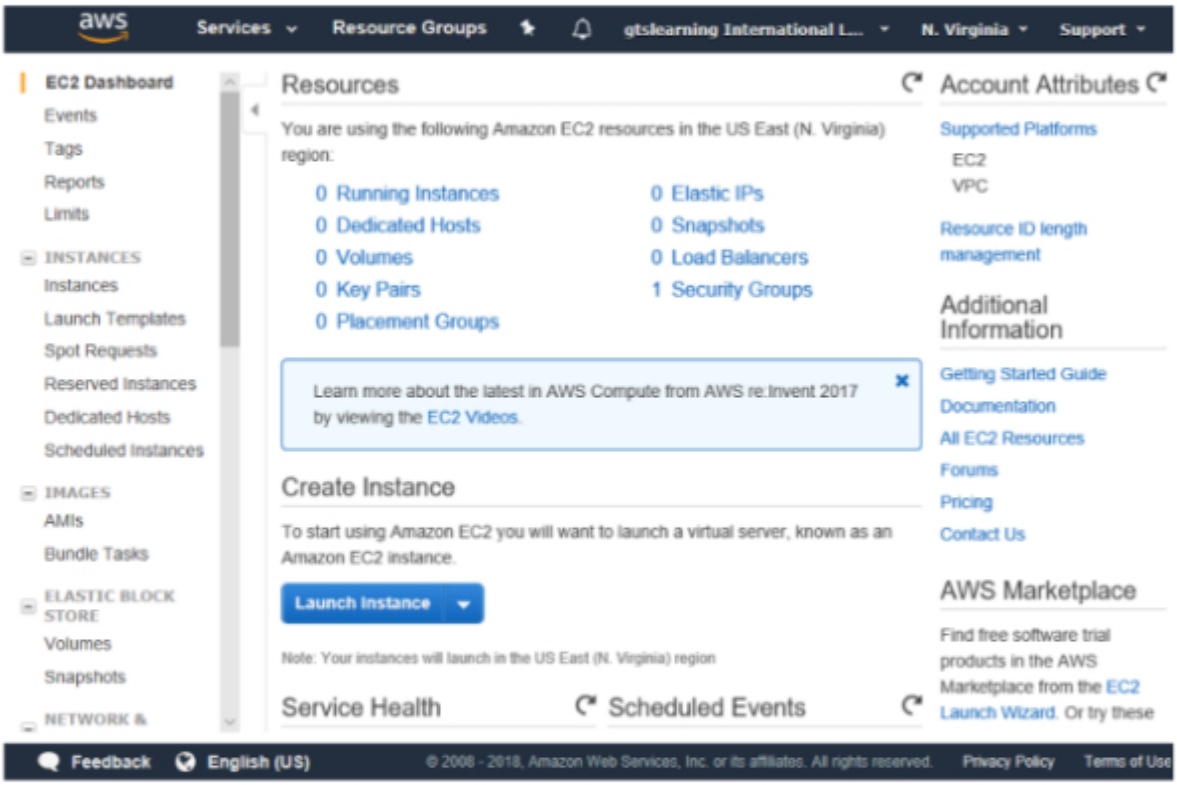
- Infrastruktur sebagai Layanan
  Infrastructure as a Service (IaaS) adalah sarana penyediaan sumber daya TI seperti server, load balancer, dan komponen storage area network (SAN) dengan cepat. Daripada membeli komponen ini dan tautan Internet yang mereka butuhkan, Anda menyewanya berdasarkan kebutuhan dari pusat data penyedia layanan. Contohnya termasuk Amazon Elastic Compute Cloud (aws.amazon.com/ec2), Microsoft® Azure® Virtual Machines (azure.microsoft.com/services/virtual-machines), dan OpenStack® (openstack.org).

- Perangkat Lunak sebagai Layanan
  Software as a Service (SaaS) adalah model yang berbeda dari penyediaan aplikasi perangkat lunak. Daripada membeli lisensi perangkat lunak untuk sejumlah kursi tertentu, bisnis akan mengakses perangkat lunak yang dihosting di server pemasok dengan pengaturan bayar sesuai penggunaan atau sewa (sesuai permintaan). Infrastruktur virtual memungkinkan pengembang untuk menyediakan aplikasi sesuai permintaan jauh lebih cepat daripada sebelumnya. Aplikasi dapat dikembangkan dan diuji di cloud tanpa perlu menguji dan menyebarkan di komputer klien. Contohnya termasuk Microsoft Office 365® (support.office.com), Salesforce® (salesforce.com), dan Google Workspace™ (workspace.google.com).

- Platform sebagai Layanan
  Platform as a Service (PaaS) menyediakan sumber daya di suatu tempat antara SaaS dan IaaS. Solusi PaaS tipikal akan menyebarkan server dan infrastruktur jaringan penyimpanan (sesuai IaaS) tetapi juga menyediakan platform aplikasi web/database

multi-tingkat di atas. Platform ini dapat didasarkan pada Oracle® atau MS SQL atau PHP dan MySQL™. Contohnya termasuk Oracle Database (cloud.Oracle.com/paas), Microsoft Azure SQL Database (azure.microsoft.com/services/sql-database), dan Google App Engine™ (cloud.google.com/appengine).

Berbeda dari SaaS, platform ini tidak akan dikonfigurasi untuk benar-benar melakukan apa pun. Pengembang Anda sendiri harus membuat perangkat lunak (aplikasi CRM atau e-niaga) yang berjalan menggunakan platform. Penyedia layanan akan bertanggung jawab atas integritas dan ketersediaan komponen platform, tetapi Anda akan bertanggung jawab atas keamanan aplikasi yang Anda buat di platform.



Dasbor untuk Amazon Web Services Elastic Compute Cloud (EC2) IaaS/PaaS. (Tangkapan layar milik Amazon.)

- Desktop sebagai Layanan
  Desktop as a Service (DaaS) adalah sarana penyediaan infrastruktur desktop virtual (VDI) sebagai layanan cloud. VDI memungkinkan browser klien untuk mengoperasikan desktop OS plus aplikasi perangkat lunak. Ini menghilangkan kebutuhan organisasi untuk menyebarkan dan memelihara PC klien dan penginstalan perangkat lunak.

- Opsi Konektivitas Cloud
  Konektivitas cloud adalah mekanisme di mana klien terhubung ke layanan cloud. Konektivitas dengan layanan berbasis cloud selalu melibatkan beberapa pengorbanan tetapi harus mempertimbangkan harga, bandwidth, latensi (penundaan), dan

ketersediaan. Secara praktis, ada beberapa opsi untuk menghubungkan staf organisasi dengan layanan berbasis cloud.

- Internet/Jaringan Pribadi Virtual
  Cara paling sederhana untuk berinteraksi dengan layanan cloud adalah dengan menggunakan situs web penyedia atau antarmuka pemrograman aplikasi (API) melalui Internet. Jenis koneksi ini juga dapat diimplementasikan sebagai jaringan pribadi virtual (VPN), jika ini didukung oleh penyedia layanan cloud. Metode VPN memiliki kelebihan karena hemat biaya dan mudah diatur di mana pun ada konektivitas Internet, yang ideal untuk organisasi yang memiliki struktur jaringan terfragmentasi atau terdistribusi. Namun, koneksi apa pun yang berjalan melalui Internet publik dapat mengalami kinerja yang buruk karena latensi dan pembatasan bandwidth, jadi ini biasanya bukan solusi untuk aplikasi misi kritis atau volume tinggi.

  Colocation dalam data center menawarkan solusi bandwidth yang lebih tinggi dengan menyediakan link langsung atau pribadi. Pelanggan membangun infrastruktur dalam pusat data yang didukung oleh penyedia cloud atau menyediakan tautan langsung dari jaringan perusahaannya ke pusat data, mungkin menggunakan koneksi pribadi yang dikonfigurasi dalam jaringan penyedia layanan. Pusat data memasang kabel sambungan silang atau VLAN antara pelanggan dan penyedia cloud, membuat tautan aman dengan latensi rendah dan bandwidth tinggi. Solusi ini lebih disukai untuk organisasi yang memiliki operasi yang lebih terpusat di mana koneksi ke cloud dapat berasal dari kantor pusat utama dan jaringan perusahaan milik perusahaan digunakan untuk memungkinkan akses lokasi cabang.

- Infrastruktur sebagai Kode
  Penggunaan teknologi cloud mendorong penggunaan pendekatan skrip untuk penyediaan, daripada menginstal sistem operasi dan aplikasi dan membuat perubahan konfigurasi atau menginstal patch secara manual. Pendekatan manajemen infrastruktur di mana otomatisasi dan orkestrasi sepenuhnya menggantikan konfigurasi manual disebut sebagai infrastruktur sebagai kode (IaC).
-
  Salah satu tujuan IaC adalah untuk menghilangkan sistem kepingan salju. Kepingan salju adalah konfigurasi atau bangunan yang berbeda dari yang lain. Kurangnya konsistensi atau penyimpangan dalam lingkungan platform menyebabkan masalah keamanan, seperti patch yang belum diinstal, dan masalah stabilitas, seperti skrip yang gagal dijalankan karena beberapa perbedaan konfigurasi kecil.

- Otomatisasi
  Otomatisasi menggunakan skrip berarti bahwa setiap konfigurasi atau tugas pembangunan dilakukan oleh blok kode. Script akan mengambil argumen standar sebagai data, sehingga ada sedikit ruang untuk ketidakpastian atas pilihan konfigurasi yang menyebabkan kesalahan. Ada dua jenis utama alat otomatisasi:

    - Alat imperatif memerlukan langkah-langkah yang tepat untuk diikuti untuk mencapai konfigurasi yang diinginkan sebagai input. Pendekatan ini paling mirip dengan otomatisasi melalui bahasa skrip tradisional seperti Bash dan PowerShell.

    - Alat deklaratif mengambil konfigurasi yang diinginkan sebagai input dan meninggalkan detail tentang bagaimana konfigurasi itu harus dicapai ke platform implementasi.

- Orkestrasi
  Di mana otomatisasi berfokus pada membuat satu tugas terpisah dengan mudah diulang, orkestrasi melakukan urutan tugas otomatis. Misalnya, Anda dapat mengatur penambahan VM baru ke kluster dengan beban seimbang. Proses end-to-end ini dapat mencakup penyediaan VM, mengkonfigurasinya dengan aplikasi dan pengaturan jaringan, menambahkan VM baru ke kluster dengan beban seimbang, dan mengkonfigurasi ulang distribusi bobot penyeimbang beban dengan konfigurasi cluster baru. Dalam melakukan ini, langkah-langkah yang diatur harus menjalankan banyak script otomatis atau panggilan layanan API.
-
- Agar orkestrasi berfungsi dengan baik, langkah otomatis harus terjadi dalam urutan yang benar, dengan mempertimbangkan ketergantungan; itu harus memberikan kredensial keamanan yang tepat di setiap langkah di sepanjang jalan; dan harus memiliki hak dan izin untuk melakukan tugas yang ditentukan. Orkestrasi dapat mengotomatisasi proses yang kompleks, membutuhkan lusinan atau ratusan langkah manual.

  Platform otomasi dan orkestrasi terhubung ke dan menyediakan administrasi, manajemen, dan orkestrasi untuk banyak platform dan layanan cloud populer. Salah satu keuntungan menggunakan platform orkestrasi pihak ketiga adalah perlindungan dari penguncian vendor. Jika Anda ingin bermigrasi dari satu penyedia cloud ke penyedia cloud lainnya, atau ingin pindah ke lingkungan multicloud, alur kerja otomatis sering kali dapat disesuaikan untuk digunakan pada yang baru. platform. Pemimpin industri di ruang ini termasuk Chef (chef.io), Wayang (puppet.com), Ansible (ansible.com), dan Kubernetes (kubernetes.io).

- Implikasi Keamanan Cloud
  Salah satu risiko menggunakan solusi berbasis cloud adalah bahwa data yang berpotensi rahasia atau rahasia komersial dapat ditransfer melalui tautan yang melampaui infrastruktur perusahaan dan kendali langsung. Karena itu, sangat penting untuk mengidentifikasi secara tepat risiko mana yang Anda transfer; untuk mengidentifikasi tanggung jawab mana yang dilakukan oleh penyedia layanan, dan mana yang tetap bersama Anda. Ini harus ditetapkan dalam perjanjian tingkat layanan (SLA) sebagai matriks tanggung jawab cloud. Pembagian tanggung jawab ini disebut

oleh Amazon sebagai keamanan cloud versus keamanan di cloud (aws.amazon.com/compliance/shared-responsibility-model).

Misalnya, dalam solusi SaaS, penyedia mungkin bertanggung jawab atas kerahasiaan, integritas, dan ketersediaan perangkat lunak. Mereka akan bertanggung jawab untuk mengkonfigurasi layanan server berkerumun yang toleran terhadap kesalahan; untuk firewall server dan membuat prosedur otentikasi, otorisasi, dan akuntansi yang tepat; untuk memindai intrusi dan memantau log jaringan; menerapkan OS dan patch perangkat lunak; dan seterusnya. Anda mungkin atau mungkin tidak bertanggung jawab atas beberapa atau semua fungsi manajemen perangkat lunak, seperti memastikan bahwa administrator dan pengguna mempraktikkan manajemen kata sandi yang baik, mengonfigurasi hak sistem, membuat cadangan data, dan sebagainya. Jika tugas-tugas penting adalah tanggung jawab penyedia layanan, Anda harus mencoba memastikan bahwa ada mekanisme pelaporan untuk menunjukkan bahwa tugas-tugas ini sedang diselesaikan, bahwa rencana pemulihan bencana mereka efektif, dan seterusnya.

Ketentuan lainnya adalah bahwa perusahaan Anda kemungkinan besar akan tetap bertanggung jawab secara langsung atas pelanggaran keamanan yang serius. Jika data pelanggan dicuri, misalnya, atau jika situs web yang dihosting diretas dan digunakan untuk mendistribusikan malware, "uang" hukum dan peraturan tetap berhenti di tangan Anda. Anda mungkin dapat menuntut penyedia layanan untuk ganti rugi, tetapi perusahaan Anda akan tetap menjadi titik penyelidikan. Anda mungkin juga perlu mempertimbangkan implikasi hukum dari penggunaan penyedia cloud jika servernya berada di negara lain.

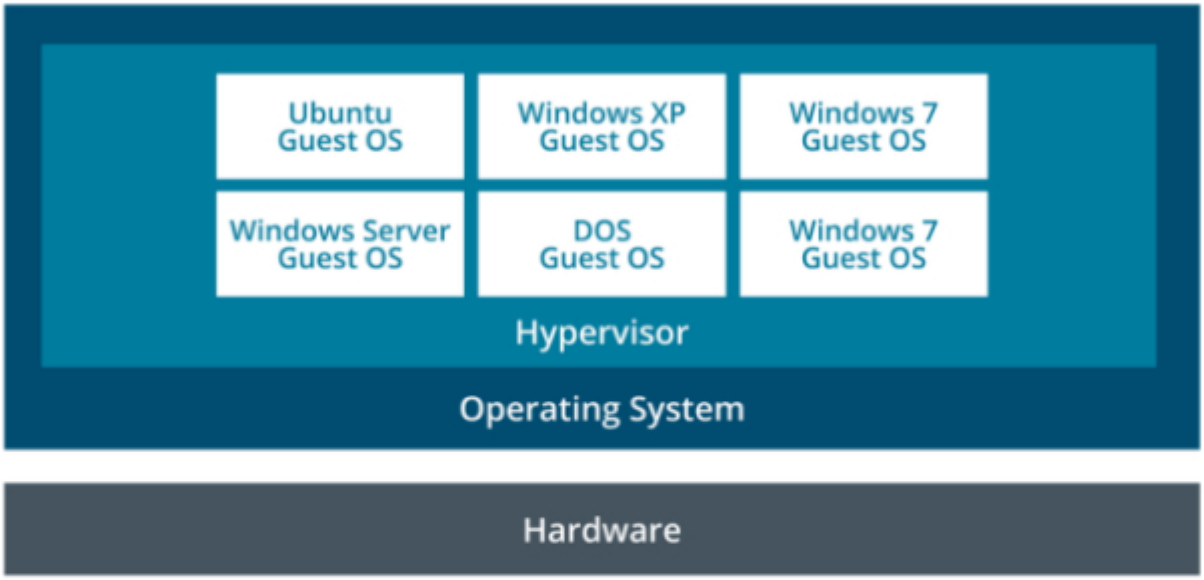
Anda juga harus mempertimbangkan risiko ancaman orang dalam, di mana orang dalam adalah administrator yang bekerja untuk penyedia layanan. Tanpa mekanisme keamanan yang efektif, seperti pemisahan tugas, ada kemungkinan mereka dapat memperoleh akses istimewa ke data Anda. Akibatnya, penyedia layanan harus dapat menunjukkan kepuasan Anda bahwa mereka dicegah untuk melakukannya. Ada juga risiko bahwa data Anda berada di dekat server virtual lain yang tidak dikenal dan bahwa beberapa jenis serangan dapat diluncurkan pada data Anda dari server virtual lain.

Explain Virtualization and Storage Area Network Technologies

- Pendahuluan: Menjelaskan Teknologi Jaringan Area Virtualisasi dan Penyimpanan Teknologi virtualisasi sekarang menjadi fitur utama jaringan dan sangat penting untuk pengoperasian layanan cloud. Ada berbagai jenis virtualisasi dan beberapa metode jaringan dengan komponen virtual. Penting untuk memahaminya jika Anda ingin menerapkan virtualisasi di lingkungan Anda.

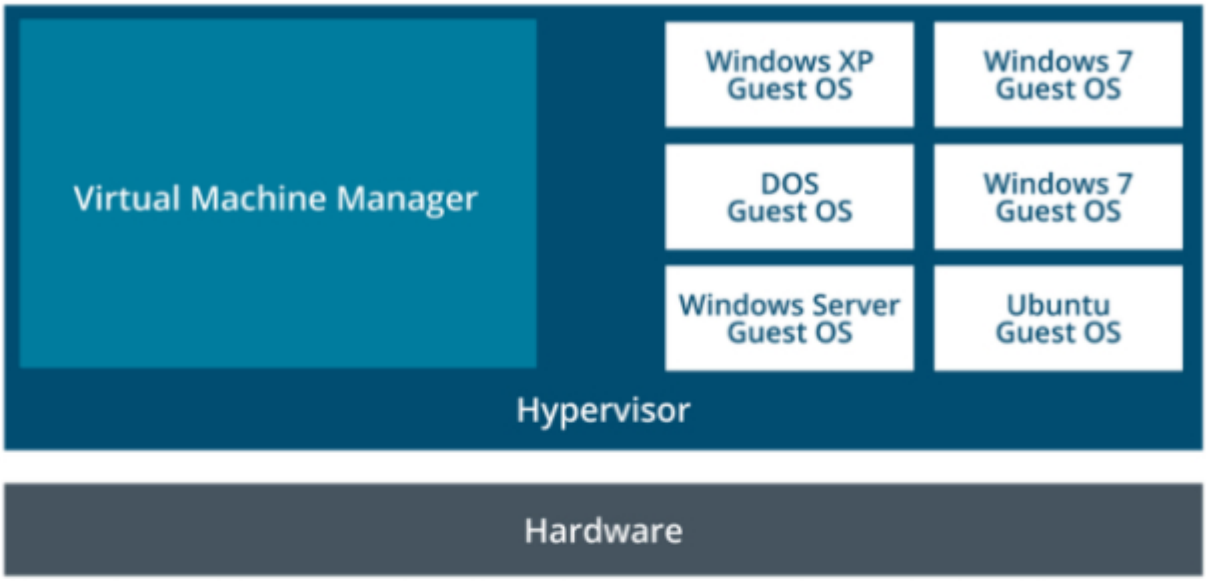
  Dalam topik ini, Anda juga akan belajar menjelaskan teknologi yang mendukung jaringan area penyimpanan (SAN). Saat merencanakan solusi penyimpanan jaringan, Anda perlu memahami kekuatan setiap jenis untuk memastikan Anda memilih solusi yang paling sesuai dengan kebutuhan Anda.

- Jenis Hypervisor
  Dalam host virtualisasi, hypervisor-atau monitor mesin virtual (VMM)-mengelola lingkungan virtual dan memfasilitasi interaksi dengan perangkat keras komputer dan jaringan. Satu perbedaan mendasar yang dapat dibuat antara platform virtual adalah antara metode host dan metode bare metal dalam berinteraksi dengan perangkat keras host. Dalam sistem OS tamu (atau berbasis host), aplikasi hypervisor (dikenal sebagai hypervisor Type II) itu sendiri diinstal ke sistem operasi host. Contoh hypervisor berbasis host termasuk VMware Workstation™, Oracle® Virtual Box, dan Parallels® Workstation. Perangkat lunak hypervisor harus mendukung OS host.



Virtualisasi OS tamu (hypervisor Tipe II). Hypervisor adalah aplikasi yang berjalan dalam OS asli, dan OS tamu diinstal di dalam hypervisor.

Platform virtual bare metal berarti bahwa hypervisor Type I diinstal langsung ke komputer dan mengelola akses ke perangkat keras host tanpa melalui OS host. Contohnya termasuk VMware ESXi® Server, Microsoft's Hyper-V®, dan Citrix's XENServer. Perangkat keras hanya perlu mendukung persyaratan sistem dasar untuk hypervisor ditambah sumber daya untuk jenis dan jumlah OS tamu yang akan diinstal.



Tipe I bare metal hypervisor. Hypervisor diinstal langsung pada perangkat keras host bersama dengan aplikasi manajemen, kemudian VM diinstal di dalam hypervisor.

- NIC dan Sakelar Virtual

  Di mana beberapa VM berjalan pada satu platform, virtualisasi menyediakan sarana bagi VM ini untuk berkomunikasi satu sama lain dan dengan komputer lain di jaringan (baik fisik maupun virtual) dengan menggunakan protokol jaringan standar. OS tamu yang berjalan di setiap mesin virtual disajikan dengan emulasi platform perangkat keras standar. Di antara perangkat keras yang ditiru akan menjadi satu atau lebih adapter jaringan. Jumlah adaptor dan konektivitasnya dapat dikonfigurasi melalui hypervisor.

  Di dalam VM, NIC virtual (vNIC) akan terlihat persis seperti adaptor jaringan biasa dan dapat dikonfigurasi dengan cara yang sama. Misalnya, protokol dan layanan dapat terikat padanya, memiliki alamat MAC, dan dapat diberikan alamat IPv4 dan/atau IPv6. Dengan kata lain, NIC virtual berfungsi identik dengan NIC fisik untuk transmisi data; itu hanya sepenuhnya berbasis perangkat lunak alih-alih menjadi kombinasi perangkat keras fisik, firmware, dan perangkat lunak driver.

  Biasanya, hypervisor akan mengimplementasikan konektifitas jaringan melalui satu atau lebih switch virtual (atau vSwitch dalam terminologi VMware). Ini melakukan fungsi yang sama dengan switch fisik Layer 2, kecuali bahwa mereka diimplementasikan dalam perangkat lunak, bukan perangkat keras. Konektivitas antara adaptor jaringan virtual di VM tamu dan switch virtual dikonfigurasikan melalui hypervisor. Ini analog dengan menghubungkan kabel patch antara komputer nyata dan switch nyata.

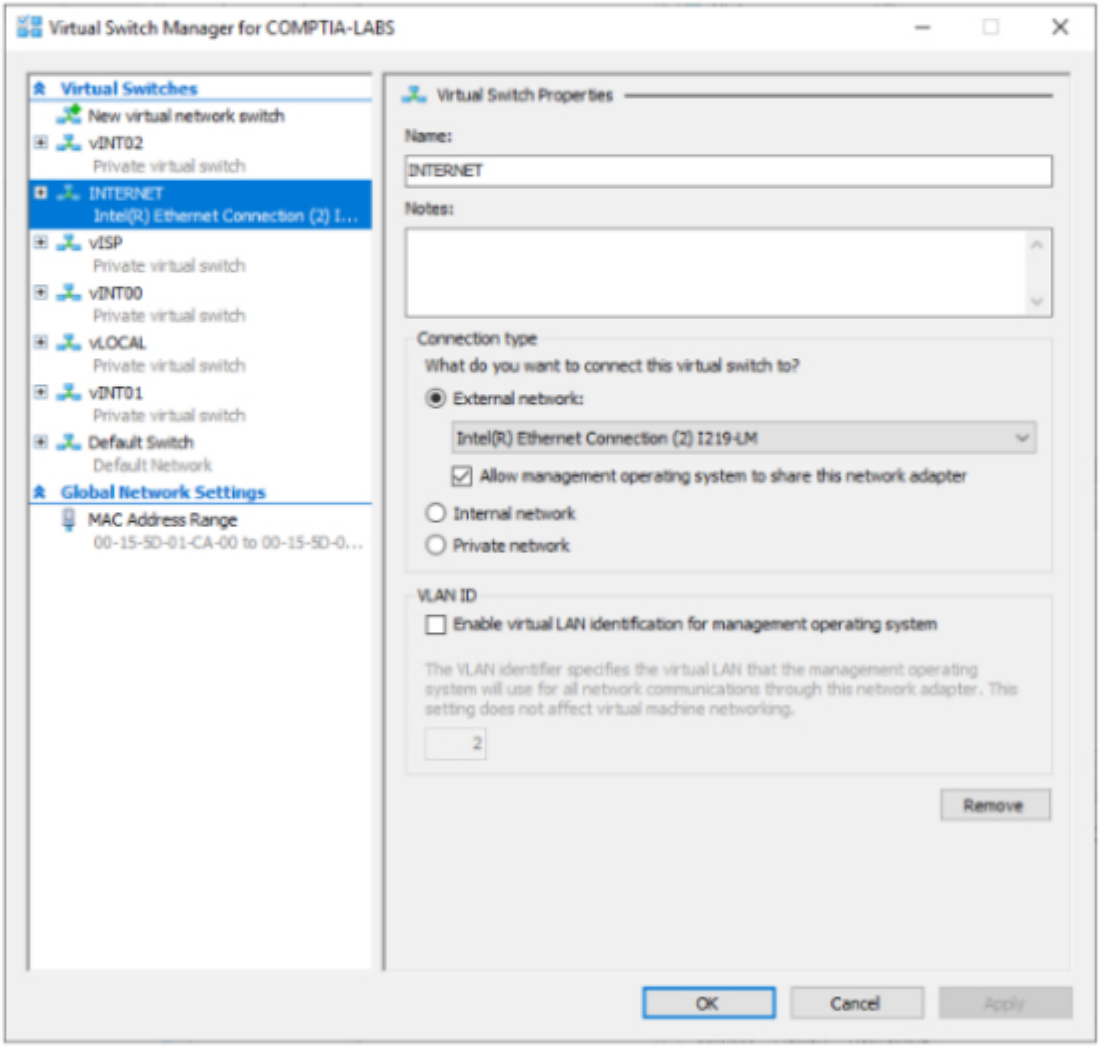
  Dalam model jaringan ini, VM dan switch virtual semuanya dapat ditampung dalam satu platform perangkat keras, jadi tidak ada lalu lintas jaringan aktual yang dihasilkan; sebagai gantinya, data dipindahkan dari buffer di satu VM ke VM lainnya. Dimungkinkan

juga untuk mengkonfigurasi konektivitas dengan switch virtual yang menjembatani jaringan virtual dan fisik melalui NIC fisik komputer host. Misalnya, dalam platform virtualisasi Hyper-V Microsoft, tiga jenis switch virtual dapat dibuat:

- ***External***-Mengikat ke NIC host untuk memungkinkan VM berkomunikasi di jaringan fisik.

- ***Internal***-Membuat jembatan yang hanya dapat digunakan oleh VM di host dan host itu sendiri. Jenis sakelar ini tidak mengizinkan akses ke jaringan fisik yang lebih luas.

- ***Private***-Membuat switch yang hanya dapat digunakan oleh VM. Mereka tidak dapat menggunakan switch untuk berkomunikasi dengan tuan rumah.



Mengonfigurasi sakelar virtual di hypervisor Hyper-V Microsoft. Saklar eksternal memungkinkan VM untuk menggunakan jaringan fisik melalui NIC host. Sakelar

pribadi tidak memiliki akses eksternal. (Tangkapan layar digunakan dengan izin dari Microsoft.)

Tips: Ketika VM diizinkan untuk berinteraksi dengan jaringan "nyata", host harus mendukung bandwidth tinggi, tautan jaringan ketersediaan tinggi. Kegagalan tautan fisik apa pun akan memengaruhi banyak VM.

Switch virtual dapat sederhana atau serumit yang dibuat oleh perangkat lunak hypervisor. Misalnya, mereka dapat digunakan untuk mengimplementasikan VLAN atau dikonfigurasi untuk melakukan pencerminan port. Dalam jaringan yang lebih maju, seperti vSphere VMware, Anda juga dapat memiliki switch virtual yang dapat menghubungkan tamu yang berjalan di beberapa host dan mengkonfigurasi peralihan lanjutan, seperti QoS dan pembentukan lalu lintas.

- Virtualisasi Fungsi Jaringan
  Ketika VM bergabung ke switch virtual, alamat MAC untuk NIC virtualnya dikonfigurasi melalui hypervisor. VM harus dikonfigurasi dengan alamat IP yang sesuai untuk subnetnya. Jika VM memerlukan tautan ke jaringan lain, VM harus ditetapkan sebagai gateway default. Anda mungkin juga ingin mengkonfigurasi keamanan untuk tautan jaringan, seperti menerapkan firewall. Tidak ada persyaratan jaringan virtual yang berbeda dari jaringan fisik.

  Anda dapat mengkonfigurasi parameter IP VM secara statis, atau Anda dapat menggunakan DHCP. Anda dapat menyediakan server DHCP sebagai VM di jaringan virtual, atau VM dapat menggunakan server DHCP jaringan fisik. Dengan beberapa jenis switch virtual yang menjembatani VM ke jaringan fisik, hypervisor dapat mengimplementasikan layanan DHCP dan/atau terjemahan alamat jaringan (NAT) ke VM.

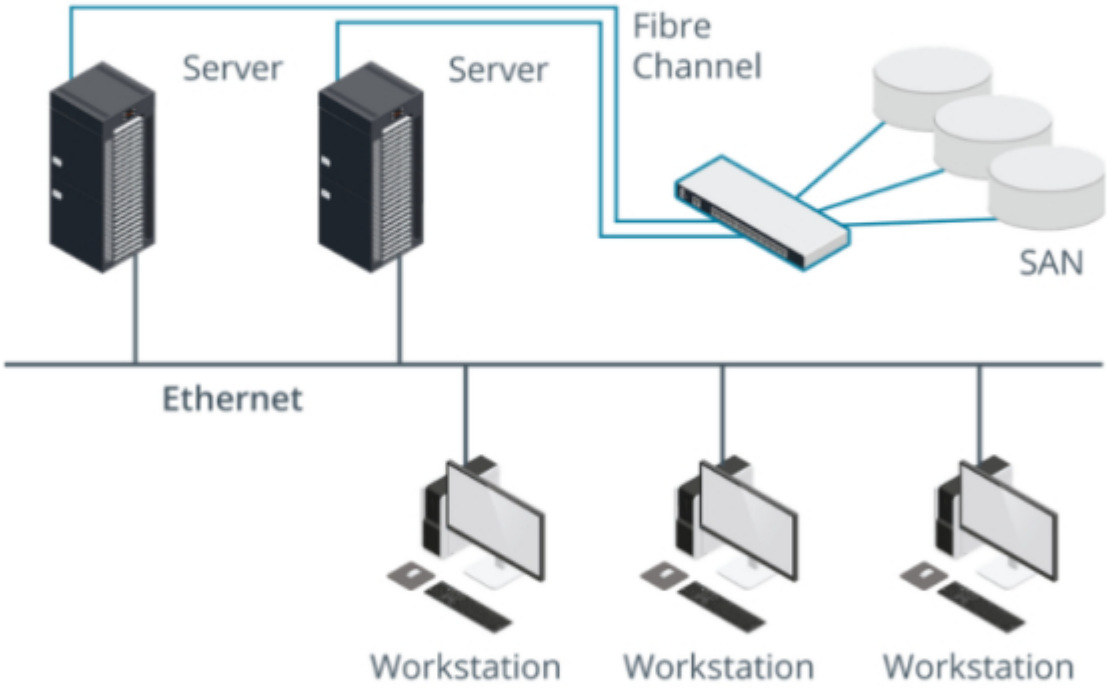
  Tips: Anda juga harus menyediakan DNS dan layanan sinkronisasi waktu untuk jaringan virtual.

  Setiap tamu Linux atau Windows Server VM dapat dikonfigurasi sebagai router untuk jaringan VM. Demikian pula, baik OS (atau perangkat lunak pihak ketiga yang diinstal di bawah VM tamu) dapat digunakan untuk mengimplementasikan firewall. VM memiliki fungsi yang sama dengan perangkat lunak yang diinstal pada komputer nyata.

  Dimungkinkan juga untuk menyediakan peralatan virtual. Dengan perangkat virtual, vendor mengembangkan produk perangkat lunak yang mengemulasi fungsi perangkat keras khusus yang ada (router, firewall, penyeimbang beban, atau deteksi malware/intrusi, misalnya) atau membuat perangkat lunak yang mengimplementasikan fungsi semacam itu dalam produk baru. Peralatan virtual ini mungkin dikembangkan terhadap arsitektur standar, seperti *Network Function Virtualization* (NFV) ETSI. NFV membagi penyediaan peralatan ini menjadi tiga domain:

- ***Virtual Network Function*** (VNF)-Menentukan dan menyebarkan contoh setiap alat virtual. VNF dirancang untuk dijalankan sebagai VM pada platform CPU standar.
- ***NFV infrastructure***-Mengontrol alokasi komputasi (CPU dan memori) ditambah penyimpanan dan sumber daya jaringan ke setiap VNF.
- ***Management and orchestration*** (MANO)-Memosisikan VNF dalam alur kerja untuk melakukan tugas penerusan dan pemfilteran yang dirancang untuknya.

- Jaringan Area Penyimpanan
  A storage area network (SAN) menyediakan akses ke perangkat penyimpanan di tingkat blok. Setiap operasi baca atau tulis alamat lokasi sebenarnya dari data pada media (Blok I/O). SAN diisolasi dari jaringan utama. Itu hanya diakses oleh server, bukan oleh PC klien dan laptop. Klien SAN adalah server yang menjalankan database atau aplikasi yang memerlukan akses ke penyimpanan bersama.



Jaringan area penyimpanan. (Gambar © 123RF.com.)

Sebuah SAN dapat mengintegrasikan berbagai jenis teknologi penyimpanan-RAID array dan tape library, misalnya. Ini dapat berisi campuran perangkat berkecepatan tinggi dan berbiaya rendah, memungkinkan penyimpanan berjenjang untuk mendukung berbagai jenis persyaratan akses file tanpa harus menyediakan drive cepat dan berbiaya tinggi secara berlebihan.

- Jenis Koneksi SAN
  SAN dapat diimplementasikan menggunakan berbagai teknologi, tetapi yang paling populer adalah Fibre Channel dengan bandwidth tinggi dan Fibre Channel melalui jaringan serat optik Ethernet.

- Saluran Serat
  Fibre Channel didefinisikan dalam standar T11 ANSI. Ejaan Inggris "fiber" sengaja dipilih untuk membedakan standar dari kabel serat optik, yang sering digunakan tetapi tidak diandalkan. SAN berdasarkan *Fibre Channel* (FC) *Switched Fabric* (FC-SW) melibatkan tiga jenis komponen utama:

  Initiator-Ini adalah perangkat klien SAN, seperti file atau server database yang diinstal dengan adaptor bus host saluran serat (HBA).

  - *Target*-Port jaringan untuk perangkat penyimpanan. Perangkat umum termasuk drive tunggal, array drive RAID, drive tape, dan perpustakaan tape. Ruang pada perangkat penyimpanan dibagi menjadi volume logis, masing-masing diidentifikasi dengan nomor unit logis 64-bit (LUN). Inisiator akan menggunakan perintah SCSI, *Serial Attached SCSI* (SAS), SATA, atau NVMe untuk mengoperasikan perangkat penyimpanan di jaringan, tergantung pada antarmuka mana yang mereka dukung. Sebagian besar perangkat memiliki beberapa port untuk penyeimbangan beban dan toleransi kesalahan.

  - Inisiator dan target diidentifikasi dengan 64-bit WorldWide Names (WWN), mirip dengan alamat MAC adaptor jaringan. Secara kolektif, inisiator dan target disebut sebagai node. Node dapat dialokasikan WWN mereka sendiri, disebut sebagai WWNN (WorldWide Node Name). Juga, setiap port pada node dapat memiliki WorldWide Port Name (WWPN) sendiri.

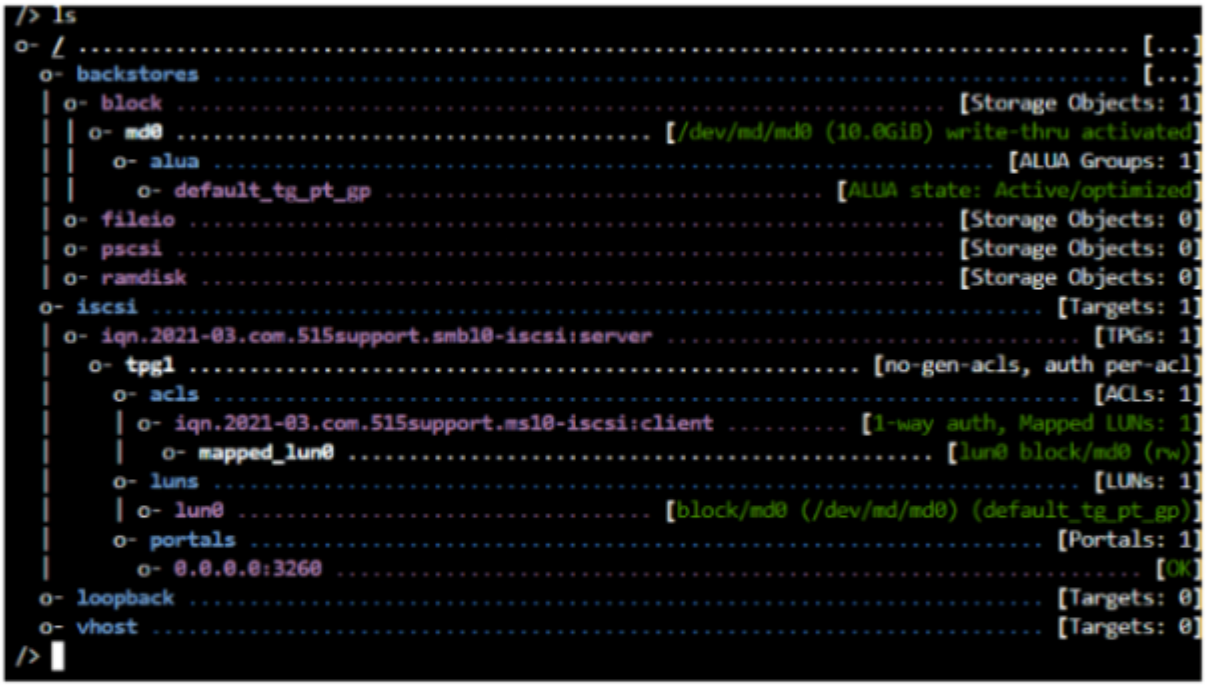
  - *FC switch*-Ini menyediakan interkoneksi antara inisiator dan target (fabrikasi). Topologi sakelar dan interkoneksi akan dirancang untuk menyediakan banyak jalur antara inisiator dan target, memungkinkan toleransi kesalahan dan penyeimbangan beban. Sakelar FC berkinerja tinggi sering disebut sebagai direktur. Fibre Channel dapat menggunakan tarif dari 1GFC (1 Gbps) hingga 128GFC. Dengan menggunakan kabel serat optik, kain FC dapat memiliki panjang hingga 10 km (6 mil) menggunakan kabel mode tunggal atau 500 m (1640 kaki) menggunakan kabel multimode.

- Saluran Fiber melalui Ethernet
  Penyediaan adaptor dan kabel Fibre Channel terpisah mahal. Seperti namanya, Fibre Channel over Ethernet (FCoE) adalah sarana untuk mengirimkan paket Fibre Channel melalui kabel dan sakelar Ethernet. FCoE memerlukan adaptor 10/40/100G khusus yang menggabungkan fungsi NIC dan HBA, yang disebut sebagai adapter jaringan

terkonvergensi (CNA). FCoE menggunakan tipe bingkai khusus, yang diidentifikasi dengan nilai EtherType 0x8096. Protokol memetakan WWN ke alamat MAC.

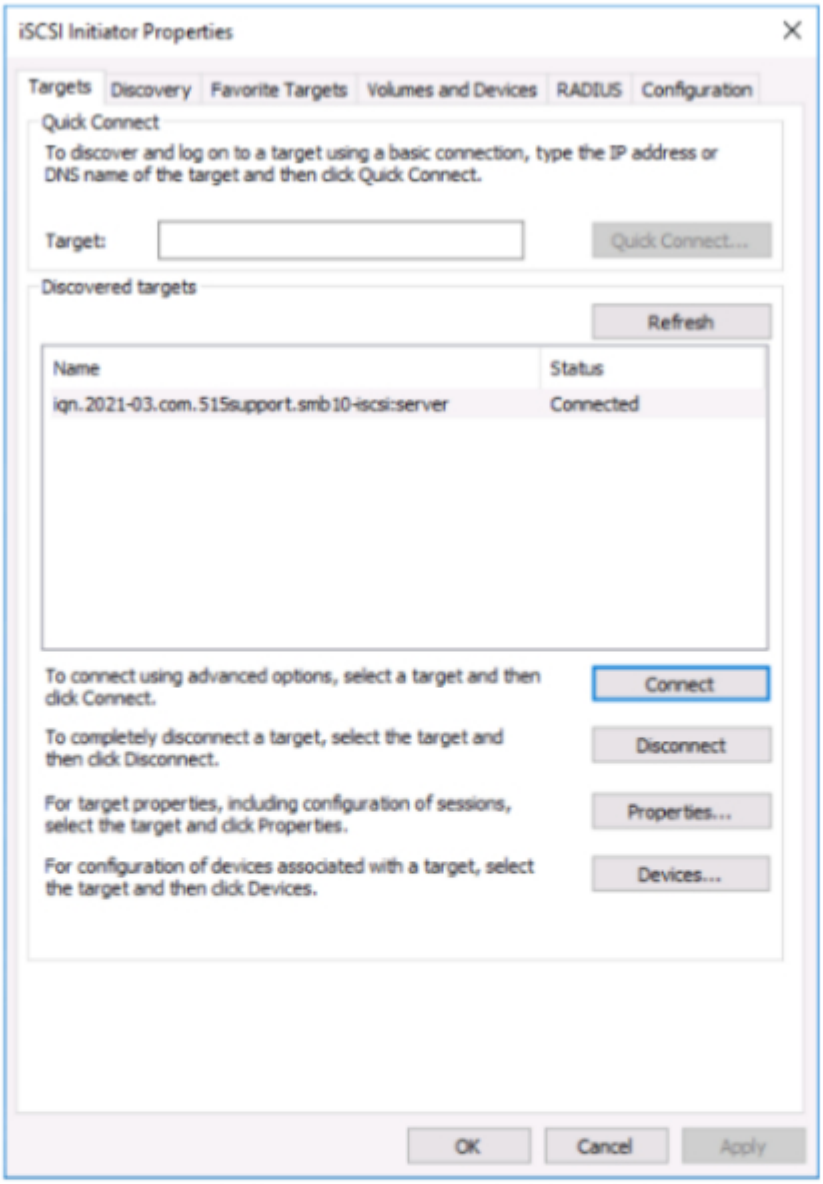
Tips: FCoE tidak berjalan di atas Ethernet standar. Ini membutuhkan mekanisme QoS untuk memastikan kontrol aliran dan pengiriman yang terjamin. Produk yang sesuai dengan FCoE disebut sebagai Ethernet lossless, Ethernet Pusat Data, atau Ethernet yang Ditingkatkan Terkonvergensi.

- iSCSI
  Internet Small Computer System Interface (iSCSI) adalah protokol tunneling IP yang memungkinkan transfer data SCSI melalui jaringan berbasis IP. iSCSI bekerja dengan adaptor dan switch jaringan Ethernet biasa.



Mengonfigurasi host Linux sebagai target iSCSI.

iSCSI dapat digunakan untuk menghubungkan SAN tetapi juga dilihat sebagai alternatif untuk Fibre Channel itu sendiri, karena tidak memerlukan sakelar atau adaptor khusus FC. Inisiator iSCSI dan fungsi target didukung oleh sistem operasi Windows Server dan Linux.



Menghubungkan ke target iSCSI menggunakan inisiator iSCSI di Windows Server.
(Tangkapan layar digunakan dengan izin dari Microsoft.)

Explain Datacenter Network Architecture

- Pendahuluan: Jelaskan Arsitektur Jaringan Pusat Data
  Pusat data memainkan peran penting di jaringan lokal dan cloud. Memahami topologi dan persyaratan otomatisasi yang berbeda dari jaringan ini akan sangat penting untuk mengejar karir yang sukses dalam jaringan.

- Desain Jaringan Pusat Data
  Pusat data adalah situs yang didedikasikan untuk menyediakan sumber daya server. Pusat data menghosting layanan jaringan (seperti otentikasi, pengalamatan, dan

resolusi nama), server aplikasi, dan jaringan area penyimpanan (SAN). Sebagian besar pusat data ditempatkan di fasilitas yang dibuat khusus, tetapi beberapa konsep juga berlaku untuk ruang server.

Pusat data memiliki fitur jaringan, daya, kontrol iklim, dan kontrol akses fisik khusus yang semuanya dirancang untuk menyediakan lingkungan yang sangat tersedia untuk menjalankan aplikasi penting. Tidak seperti jaringan perusahaan, pusat data tidak berisi PC klien, selain workstation administratif aman (SAW) yang diperkeras yang digunakan hanya untuk mengelola server.

Secara historis, pusat data dirancang untuk menggunakan arsitektur tiga tingkat yang sama dengan jaringan kampus perusahaan, dengan switch lapisan inti, distribusi, dan akses. Perubahan cara aplikasi dirancang sebagai layanan yang memanfaatkan virtualisasi dan instans sesuai permintaan telah mengubah sifat arus lalu lintas jaringan. Perubahan ini tercermin dalam desain topologi yang berbeda di pusat data.

- Arus Lalu Lintas
  Lalu lintas yang menuju dan dari pusat data disebut sebagai utara-selatan. Lalu lintas ini mewakili klien di luar pusat data yang membuat permintaan dan menerima tanggapan. Arus lalu lintas jaringan perusahaan juga biasanya utara-selatan. Perangkat klien terletak di switch grup kerja yang terhubung ke router, sedangkan server terhubung ke sakelar atau VLAN yang terpisah. Lalu lintas dari klien ke server melewati "utara" dari sakelar klien ke router dan kemudian kembali ke "selatan" ke switch server.

  Di pusat data yang mendukung cloud dan layanan Internet lainnya, sebagian besar lalu lintas sebenarnya antara server di dalam pusat data. Ini disebut sebagai lalu lintas timur-barat. Pertimbangkan klien mengunggah foto sebagai bagian dari posting media sosial. File gambar mungkin diperiksa oleh server analisis untuk pelanggaran kebijakan (misalnya, gambar tidak senonoh atau hak cipta), layanan pencarian/pengindeksan akan diperbarui dengan metadata gambar, gambar akan direplikasi ke server yang menyediakan jaringan pengiriman konten (CDN)), gambar akan disalin ke server cadangan, dan seterusnya. Satu permintaan ke cloud cenderung mengalir ke beberapa permintaan dan transfer di dalam cloud.

- Jaringan Hamparan
  Banyaknya lalu lintas timur-barat memperumit desain keamanan. Jika masing-masing transaksi berjenjang ini melewati firewall atau alat keamanan lainnya, itu akan membuat kemacetan parah. Persyaratan ini mendorong pembuatan peralatan keamanan virtual yang dapat memantau lalu lintas saat melewati antar server (blogs.cisco.com/security/trends-in-data-center-security-part-1-traffic-trends). Pada saat yang sama, implementasi keamanan bergerak menuju arsitektur tanpa kepercayaan. Zero trust menyiratkan jaringan yang sangat tersegmentasi di mana setiap tautan antara dua server harus diautentikasi dan disahkan.

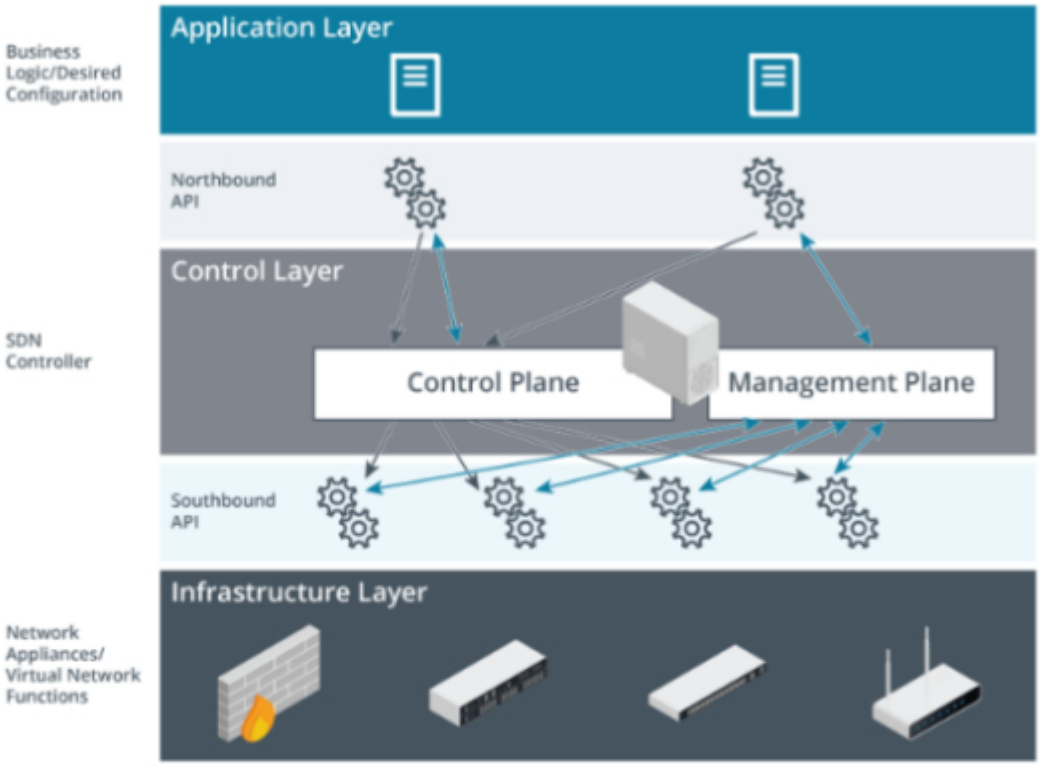
Jaringan overlay digunakan untuk mengimplementasikan jenis tautan logis titik-ke-titik ini antara dua node atau dua jaringan. Jaringan overlay mengabstraksikan kompleksitas topologi fisik yang mendasarinya. Jaringan overlay menggunakan protokol enkapsulasi dan jaringan yang ditentukan perangkat lunak untuk membuat terowongan logis antara dua node atau jaringan. Ketika digunakan di dalam pusat data, jaringan overlay biasanya diimplementasikan menggunakan virtual extensible LAN (VXLAN).

- Jaringan yang Ditentukan Perangkat Lunak
  Layanan cloud memerlukan penyediaan dan deprovisioning instans server dan jaringan yang cepat menggunakan otomatisasi dan orkestrasi, ditambah penggunaan jaringan overlay untuk membuat tautan titik-ke-titik dengan cepat dan andal. Ini berarti bahwa komponen-komponen ini harus dapat diakses sepenuhnya oleh skrip yang mewakili infrastruktur ideal sebagai kode. Jaringan yang ditentukan perangkat lunak (SDN) adalah model bagaimana proses ini dapat digunakan untuk menyediakan dan mencabut jaringan.

- Arsitektur SDN
  Dalam model SDN yang didefinisikan oleh IETF (https://datatracker.ietf.org/doc/html/rfc7426), fungsi jaringan dibagi menjadi tiga lapisan. Lapisan atas dan bawah adalah aplikasi dan infrastruktur:

  - Lapisan aplikasi-Menerapkan logika bisnis untuk membuat keputusan tentang bagaimana lalu lintas harus diprioritaskan dan diamankan dan di mana harus dialihkan. Lapisan ini mendefinisikan kebijakan seperti segmentasi, ACL, dan prioritas lalu lintas dan pemolisian/pembentukan.

  - Lapisan infrastruktur-Perangkat (fisik atau virtual) yang menangani penerusan aktual (pengalihan dan perutean) lalu lintas dan pengenaan ACL dan konfigurasi kebijakan lainnya untuk keamanan. Inovasi utama SDN adalah menyisipkan lapisan kontrol antara lapisan aplikasi dan lapisan infrastruktur. Fungsi bidang kontrol diimplementasikan oleh perangkat virtual yang disebut sebagai pengontrol SDN. Setiap lapisan memperlihatkan antarmuka pemrograman aplikasi (API) yang dapat diotomatisasi oleh skrip yang memanggil fungsi di lapisan atas atau bawah. Antarmuka antara aplikasi SDN dan pengontrol SDN digambarkan sebagai antarmuka layanan atau sebagai API "batas utara", sedangkan antarmuka antara pengontrol SDN dan perangkat infrastruktur adalah API "batas selatan".



Lapisan dan komponen dalam arsitektur jaringan yang ditentukan perangkat lunak khas. (Gambar © 123RF.com.)

Bidang Manajemen Dalam model SDN IETF, ada bidang penerusan (data) dan operasional yang terpisah di tingkat infrastruktur. Bidang operasional mengimplementasikan status perangkat, seperti penggunaan CPU dan memori. Sebuah bidang manajemen berada pada tingkat yang sama dengan bidang kontrol untuk berinteraksi dengan bidang operasional. Ini digunakan untuk mengimplementasikan pemantauan kondisi lalu lintas dan status jaringan.

- Topologi Tulang Belakang dan Daun
  Topologi tulang belakang dan daun memberikan dukungan yang lebih baik untuk lalu lintas timur-barat dan penggunaan jaringan SDN dan overlay dalam pusat data. Topologi tulang belakang dan daun memiliki dua lapisan:

  Lapisan tulang belakang terdiri dari tulang punggung switch tingkat atas. Perhatikan bahwa sementara ini digambarkan sebagai tulang punggung, switch tulang belakang tidak terhubung satu sama lain.

  Lapisan daun berisi switch akses. Setiap switch akses terhubung ke setiap switch tulang belakang dalam topologi mesh penuh. Saklar akses tidak pernah memiliki koneksi langsung satu sama lain.

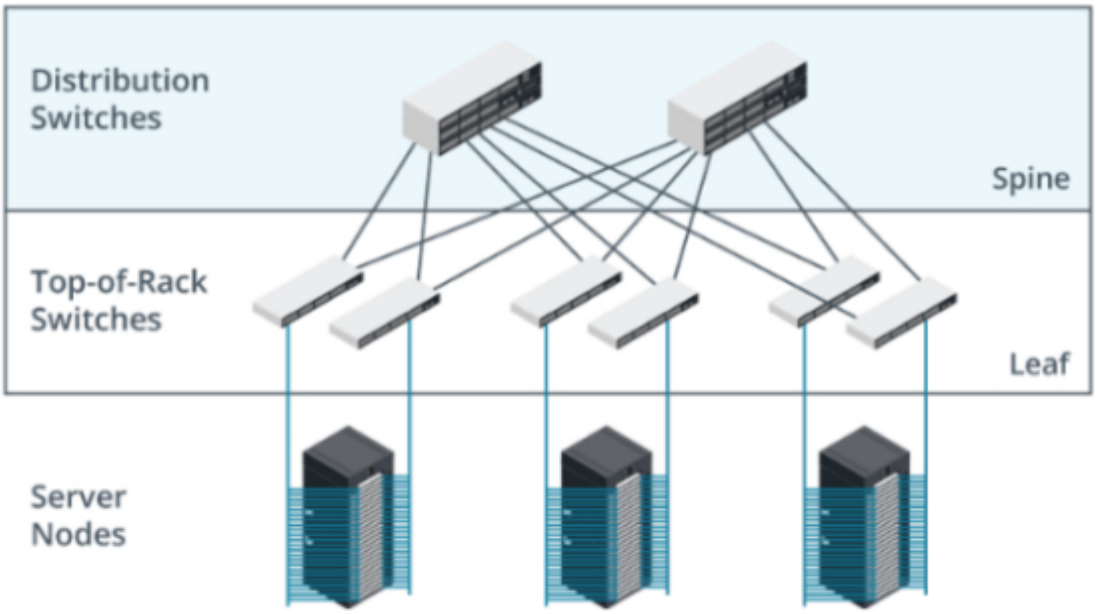


Diagram topologi tulang belakang dan daun. (Gambar © 123RF.com.)

Topologi tulang belakang dan daun memiliki sejumlah keunggulan:

- Setiap server hanya satu hop dari tulang punggung, membuat latensi jaringan lebih dapat diprediksi.

- Ada beberapa jalur redundan antara sakelar daun dan tulang punggung, memungkinkan penyeimbangan beban dan failover.

- Karena tidak ada koneksi langsung antara sakelar tulang belakang di tulang punggung atau antara sakelar daun, jaringan bebas loop dan tidak perlu menjalankan pohon rentang. Sebagai gantinya, setiap switch daun menjalankan protokol yang disebut *Equal Cost Multipathing* (ECMP) untuk mendistribusikan lalu lintas antara tautan ke switch tulang belakang.

- Server terhubung ke beberapa switch daun untuk redundansi multipath, menggunakan protokol gateway hop pertama untuk menentukan jalur aktif.

Switch akses lapisan daun diimplementasikan sebagai model switch top-of-rack (ToR). Ini adalah model sakelar yang dirancang untuk menyediakan konektivitas berkecepatan tinggi ke rak peralatan server dan mendukung bandwidth yang lebih tinggi daripada sakelar kelompok kerja biasa. Misalnya, di mana sakelar grup kerja mungkin memiliki port akses 1 Gbps dan port uplink 10 Gbps, switch top-of-rack memiliki port akses 10 Gbps dan port uplink 40/100 Gbps.

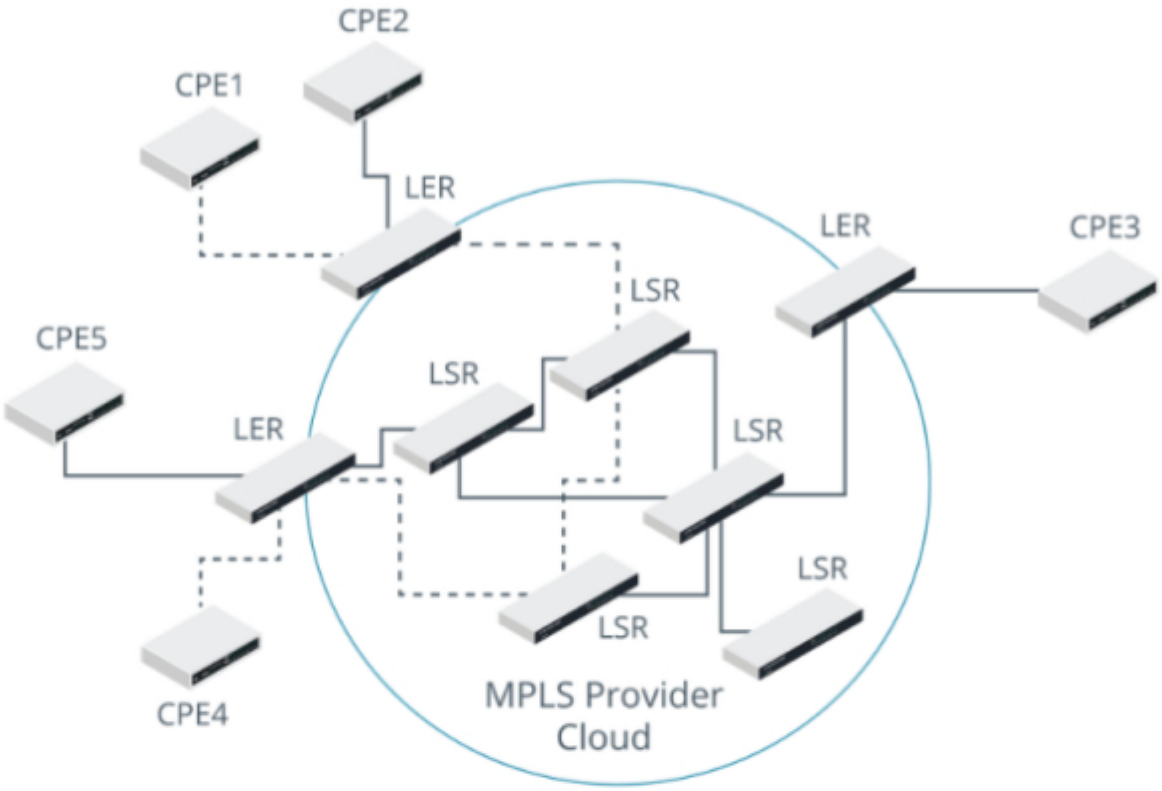
- Jenis Akses Pusat Data
  Selain desain internal dan konfigurasi pusat data, Anda juga perlu mempertimbangkan perubahan cara mengakses layanan pusat data. Pusat data lokal adalah pusat data yang terletak di situs yang sama dengan jaringan klien korporat yang dilayaninya. Jenis pusat data ini akan diakses melalui tautan Ethernet, tetapi akan ditempatkan di zona jaringan terpisah dengan ACL untuk menyaring akses oleh sistem klien.

- Akses Pusat Data Kantor Cabang
  Banyak jaringan perusahaan secara tradisional didasarkan pada desain hub and spoke, di mana layanan terkonsentrasi di kantor utama, atau hub, tetapi akses didistribusikan di sekitar beberapa kantor cabang di lokasi yang terpisah secara geografis. Kantor cabang mungkin terbatas dalam hal bandwidth rendah, link latency tinggi. Ini bisa berarti harus menginstal server ke lokasi cabang dan mereplikasi data antara mereka dan kantor pusat atau jaringan perusahaan.

  Protokol *Generic Routing Encapsulation* (GRE) merangkum data dari lapisan 2 (Ethernet) atau lapisan 3 (IP) untuk tunneling melalui jaringan transportasi yang sesuai. *Multipoint GRE* (mGRE) adalah versi protokol yang mendukung tautan point-to-multipoint, seperti hub and spoke dynamic multipoint VPN. Protokol ini banyak digunakan untuk menghubungkan kantor cabang ke pusat data lokal yang terletak di kantor pusat.

- Colocation
  Pusat data lokal tidak memiliki redundansi situs dan juga cenderung mengalami kinerja yang buruk saat diakses oleh kantor jarak jauh di negara yang berbeda. Membangun layanan pusat data lokal untuk beberapa lokasi geografis mahal. Salah satu opsinya adalah menggunakan layanan cloud publik tempat aplikasi dan data Anda diinstal ke server pihak ketiga. Ini hemat biaya, tetapi juga terkait dengan sejumlah risiko.
  Colocation berarti bahwa server pribadi perusahaan dan peralatan jaringan dipasang ke pusat data yang digunakan bersama oleh beberapa penyewa. Penyedia colocation mengelola lingkungan pusat data; server perusahaan dipasang ke ruang rak khusus di lantai pusat data. Rak atau ruang di dalam rak dikunci sehingga hanya pemegang kunci yang berwenang yang dapat memperoleh akses fisik ke peralatan server.

- Pengalihan Label Multiprotocol
  Solusi VPN berdasarkan mGRE/DMVPN yang menggunakan Internet publik sebagai jaringan transportasi dapat mengalami tingkat kinerja yang tidak dapat diprediksi. Sebagian besar penyedia WAN menawarkan Multiprotocol Label Switching (MPLS) sebagai sarana untuk membangun tautan pribadi dengan tingkat layanan yang terjamin. MPLS dapat beroperasi sebagai jaringan overlay untuk mengkonfigurasi link point-to-point atau point-to-multipoint antar node terlepas dari topologi fisik dan data link yang mendasarinya.



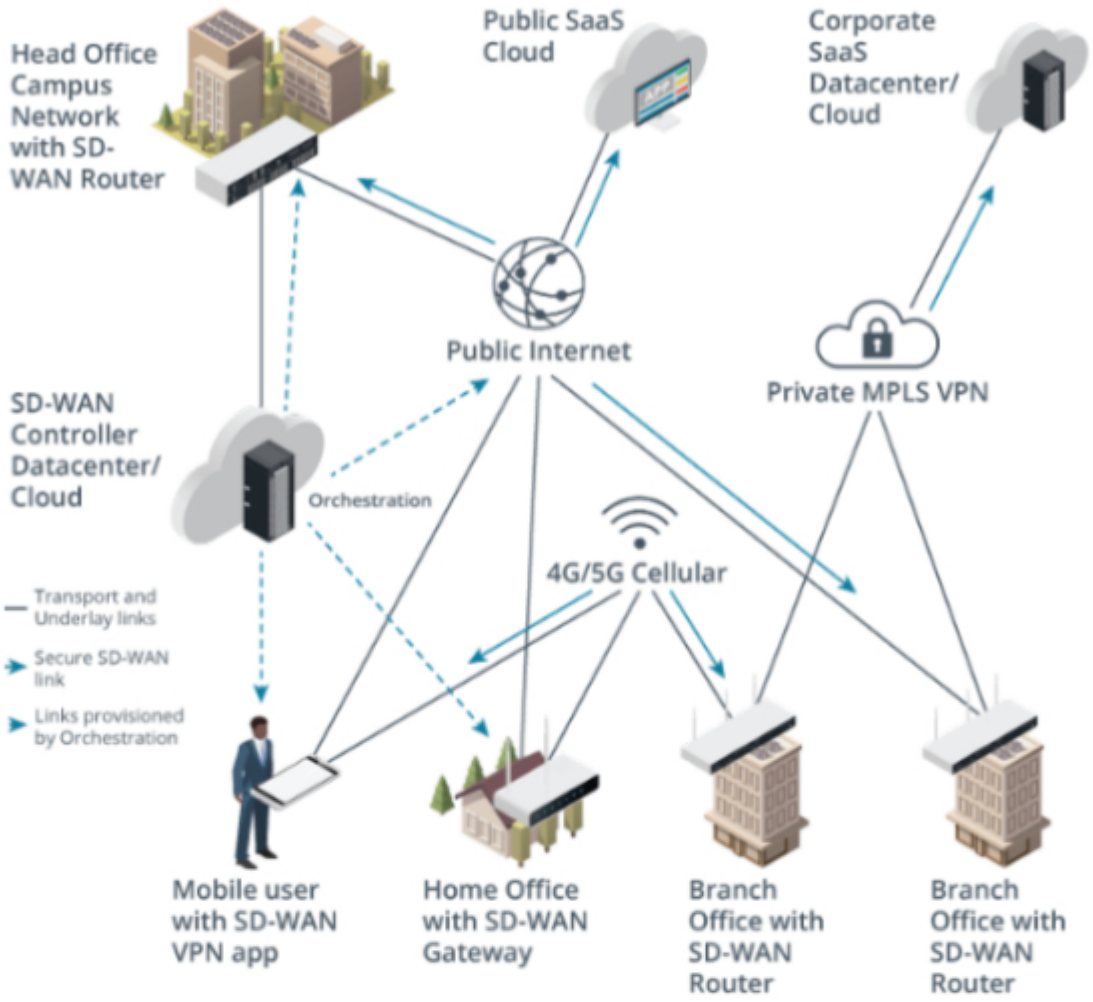
topologi MPLS. (Gambar © 123RF.com.)

Misalnya, dalam diagram ini, router CPE di situs 1 ingin berkomunikasi dengan situs 4. Router terhubung ke cloud MPLS penyedia layanan melalui Label Edge Router (LER). Router ini menyisipkan atau "mendorong" label atau header "shim" ke dalam setiap paket yang dikirim dari CPE1, dan kemudian meneruskannya ke LSR. Setiap LSR memeriksa shim dan menentukan Label Switched Path (LSP) untuk paket, berdasarkan jenis data, kemacetan jaringan, dan parameter rekayasa lalu lintas lainnya yang ditentukan oleh penyedia layanan. Ia menggunakan label, bukan header Layer 3, untuk meneruskan paket ke tetangganya. Dengan cara ini, pencarian tabel perutean yang mahal dapat dihindari. Shim dihapus (atau "muncul") oleh LER jalan keluar dan dikirim ke CPE4.

MPLS memungkinkan penyedia WAN untuk menawarkan berbagai solusi untuk kebutuhan jaringan perusahaan. Penggunaan dasar MPLS adalah untuk membuat VPN situs-ke-situs untuk menghubungkan LAN atau menghubungkan kantor cabang ke pusat data. Lalu lintas yang melewati VPN MPLS diisolasi dari pelanggan lain atau lalu lintas publik. Situs yang berbeda dapat menggunakan metode akses apa pun yang tersedia (DSL, seluler, leased line, atau Ethernet), dan situs dapat menggunakan topologi point-to-point atau multipoint sesuai kebutuhan. Penyedia MPLS dapat menerapkan kebijakan pembentukan lalu lintas untuk komunikasi antara LAN perusahaan dan pusat

data untuk menjamin tingkat layanan dan menyediakan redundansi tautan, membuat koneksi jauh lebih andal daripada koneksi melalui Internet terbuka.

- WAN yang ditentukan perangkat lunak
  Desain hub dan kantor cabang dengan pusat data lokal memiliki sejumlah kelemahan kinerja dan keandalan. Menggeser layanan ke satu atau lebih pusat data khusus di cloud atau menggunakan colocation mengurangi beberapa masalah ini. Ketersediaan dan integritas layanan dipisahkan dari pertimbangan aksesibilitas situs. Dalam model ini akses ke pusat data dari jaringan perusahaan, kantor cabang, dan lokasi remote/teleworker dapat difasilitasi melalui software-defined WAN (SD-WAN). SD-WAN menggantikan desain tipe hub dan spoke dengan konektivitas yang lebih efisien, namun tetap aman, ke cloud perusahaan dengan lebih sedikit biaya yang terkait dengan penyediaan layanan MPLS ke setiap lokasi terpencil.
-
  Dalam topologi kantor cabang, akses ke pusat data atau cloud akan dirutekan dan disahkan melalui kantor hub. SD-WAN adalah jenis jaringan overlay yang menyediakan WAN perusahaan di beberapa lokasi dan dapat memfasilitasi akses aman ke cloud langsung dari kantor cabang atau lokasi terpencil lainnya. Ini menggunakan otomatisasi dan orkestrasi untuk menyediakan tautan secara dinamis berdasarkan persyaratan aplikasi dan kemacetan jaringan, menggunakan IPSec untuk memastikan bahwa lalu lintas disalurkan melalui jaringan transportasi yang mendasarinya dengan aman. Solusi SD-WAN juga harus menerapkan mikro segmentasi dan kebijakan keamanan tanpa kepercayaan untuk memastikan bahwa semua permintaan dan tanggapan diautentikasi dan disahkan.



Komponen dalam solusi SD-WAN. (Gambar © 123RF.com.)

SD-WAN dikelola oleh pengontrol dan perangkat lunak manajemen yang terletak di pusat data perusahaan atau cloud publik. Setiap situs memiliki router, gateway, atau aplikasi VPN yang mendukung SD-WAN. Pengontrol SDN mengatur koneksi ke jaringan dan cloud yang terdaftar di SD-WAN. Ini menggunakan jaringan bawahan IP yang tersedia, seperti Internet broadband, seluler 4G/5G, atau VPN MPLS pribadi untuk menyediakan transportasi tercepat atau paling andal yang tersedia ke jaringan dan awan yang terdaftar di SD-WAN. Pengontrol juga memastikan bahwa setiap permintaan akses di autentikasi dan diotorisasi.