MODUL PEMBELAJARAN

Semester 3/3 SKS

Jaringan Enterprise

Teknologi Informasi

Jl. Gajah Mada, Baloi Sei Ladi
Batam, Kepulauan Riau 29442
Tel + 62 778 743 7111
Fax + 62 778 743 7112
www.uib.ac.id

Kata Pengantar

Puji syukur kehadirat Tuhan Yang Maha Esa sehingga Modul Pembelajaran Mata Kuliah Jaringan Enterprise ini dapat diselesaikan. Modul pembelajaran ini disusun untuk mencapai kompetensi mahasiswa yakni (1) Menganalisis masalah komputasi yang kompleks dan menerapkan prinsip-prinsip komputasi dan disiplin lain yang relevan untuk mengidentifikasi solusi, (2) Merancang, mengimplementasikan, dan mengevaluasi solusi berbasis komputasi untuk memenuhi serangkaian persyaratan komputasi tertentu dalam konteks disiplin program, (3) Berkomunikasi secara efektif dalam berbagai konteks profesional, (4) Berfungsi secara efektif sebagai anggota atau pemimpin tim yang terlibat dalam kegiatan yang sesuai dengan disiplin program, (5) Kemampuan menggunakan peralatan modern dalam menerapkan konsep-konsep dasar komputer yang dibutuhkan untuk mengkonfigurasi, mengelola dan mengintegrasikan sumber daya teknologi informasi, (6) Gunakan pendekatan sistemik untuk memilih, mengembangkan, menerapkan, mengintegrasikan, dan mengelola teknologi komputasi yang aman untuk mencapai tujuan pengguna. Penyusun telah berusaha untuk membuat modul pembelajaran sesuai dengan kompetensi yang diharapkan namun tetap menyadari bahwa masih terdapat kekurangan dalam modul pembelajaran ini. Modul pembelajaran akan terus ditinjau dan dikaji terkait dengan kebermanfaatan dan pengembangan ilmu pengetahuan terkait dengan bidang Jaringan Komputer. Akhir kata, semoga modul pembelajaran ini dapat bermanfaat bagi berbagai pihak.

Batam, 5, September 2022

Pendahuluan

A. Penjelasan Umum Modul

1. Kriteria Pengguna Modul

   Modul pembelajaran ini ditujukan untuk mahasiswa program sarjana Teknologi Informasi yang telah memiliki kompetensi yaitu (a) Jaringan dan Komunikasi Data, (b) Jaringan Terapan

2. Prasyarat Penggunaan Modul

   Modul pembelajaran ini berisikan teori/penjelasan lanjutan dari mata kuliah Jaringan dan Komunikasi Data pada semester 1 (satu) dan Jaringan Terapan pada semester 2 (dua) Untuk dapat memahami isi modul pembelajaran ini, pengguna diharapkan telah memahami Konsep dasar jaringan yan meliputi OSI *Layer* dan TCP/IP, Dasar Keamanan Jaringan, Konsep *Switch*, VLAN, STP, WLAN, FHRP, dan Konsep *Routing*.

3. Petunjuk Penggunaan Modul Pembelajaran

   Modul pembelajaran ini disusun sistematis berdasarkan Capaian Pembelajaran Lulusan yang telah dirumuskan serta kegiatan pembelajaran yang telah direncanakan di awal semester. Modul pembelajaran ini merupakan sarana belajar mandiri, dimana setiap kegiatan belajar pada modul digunakan untuk sesi sinkronus dan asinkronus yang setara dengan waktu n (besaran SKS) x 50 menit. Setiap kegiatan belajar dilengkapi dengan latihan dan penugasan beserta dengan kunci jawaban yang tersedia di akhir halaman. Pengguna modul diharapkan untuk dapat menyelesaikan modul pembelajaran secara runtut dari setiap kegiatan pembelajaran yang tersedia untuk dapat memenuhi kompetensi yang telah dirujuk di dalam.

B. Deskripsi Mata Kuliah

1. Identitas Mata Kuliah
   a. Nama Mata Kuliah : Jaringan Enterprise
   b. Kode Mata Kuliah/SKS : TI32019
   c. Semester : 3
2. Capaian Pembelajaran
   a. Capaian Pembelajaran Lulusan **(CPL)** :

   CPL-1 Menganalisis masalah komputasi yang kompleks dan menerapkan prinsip-prinsip komputasi dan disiplin lain yang relevan untuk mengidentifikasi solusi.

   CPL-2 Merancang, mengimplementasikan, dan mengevaluasi solusi berbasis komputasi untuk memenuhi serangkaian persyaratan komputasi tertentu dalam konteks disiplin program.

   CPL-3 Berkomunikasi secara efektif dalam berbagai konteks profesional.

   CPL-4 Berfungsi secara efektif sebagai anggota atau pemimpin tim yang terlibat dalam kegiatan yang sesuai dengan disiplin program.

		CPL-5 Kemampuan menggunakan peralatan modern dalam menerapkan konsep-konsep dasar komputer yang dibutuhkan untuk mengkonfigurasi, mengelola dan mengintegrasikan sumber daya teknologi informasi **CPL-6** Gunakan pendekatan sistemik untuk memilih, mengembangkan, menerapkan, mengintegrasikan, dan mengelola teknologi komputasi yang aman untuk mencapai tujuan pengguna.
b.	Capaian Pembelajaran Mata Kuliah **(CPMK)** :	**CPMK 1** Menentukan topik terkait dengan Jaringan Enterprise. **CPMK 2** Menganalisis masalah Jaringan Enterprise yang kompleks dan menerapkan prinsip-prinsip komputasi dan disiplin lain yang relevan untuk mengidentifikasi solusi. **CPMK 3** Merancang solusi Jaringan Enterprise untuk memenuhi kebutuhan pengguna. **CPMK 4** Mampuan menggunakan peralatan modern dalam menerapkan konsep-konsep dasar komputer yang dibutuhkan untuk mengkonfigurasi, mengelola dan mengintegrasikan sumber daya dalam mengimplementasikan Jaringan Enterprise **CPMK 5** Mampu mengembangkan keterampilan berpikir kritis dan pemecahan masalah, dan peningkatan pada Jaringan Enterprise **CPMK 6** Publikasi dan Pengakuan Proyek Jaringan Enterprise
c.	Sub Capaian Pembelajaran Mata Kuliah (**Sub-CPMK**)	**Sub-CPMK 1** Mampu menjelaskan jaringan Kampus, menentukan objek dan judul proyek jaringan kampus **Sub-CPMK 2** Mampu menjelaskan perkembangan jaringan kampus, mengidetifikasi sistem jaringan kampus yang suda ada, dan mampu mengidentifikasi permasalahan, serta merumuskan solusi jaringan kampus pada proyek **Sub-CPMK 3** Mampu menjelaskan trend ancaman jaringan kampus, dan mampu merancang jaringan dengan pendekatan praktik keamanan terbaik **Sub-CPMK 4** Mampu menjelaskan desain jaringan kampus, merancang topologi secara fisik dan logika, serta manajemen pengalamatan IP, serta mampu nenetukan kebuthan jaringan kampus pada proyek

Sub-CPMK 5 Mampu menjelaskan konsep routing dimamis dan mengimplementasikan protokol routing OSPF

Sub-CPMK 6 Mampu menjelaskan dan mengimplementasikan ACL

Sub-CPMK 7 Mampu menjelaskan dan mengimplementasikan NAT

Sub-CPMK 8 Mampu menjelaskan dan mengimplementasikan WAN

Sub-CPMK 9 Mampu menjelaskan dan mengimplementasikan VPN

Sub-CPMK 10 Mampu menjelaskan dan mengimplementasikan QoS

Sub-CPMK 11 Mampu menjelaskan konsep manajement jaringan, ngimplementasikan manajement jaringan pada jaringan kampus, dan mampu menganalisa data hasil monitoring manajemen jaringan dalam meningkatkan jaringan kampus

Sub-CPMK 12 Mampu mengimplementasikan tahapan-tahapan dalam melakukan pemeliharaan, dan pemecahan masalah jaringan kampus

Sub-CPMK 13 Mampu menyeusn laporan proyek dalam bentuk Artikel Ilmiah / Laporan PkM

Sub-CPMK 14 Mampu memaparkan hasil Proyek ke Peserta

Daftar Isi

Daftar Gambar

Daftar Tabel

Kegiatan Belajar 1
Jaringan Kampus

1. Sub-Capaian Pembelajaran Mata Kuliah

a. Mampu menjelaskan jaringan Kampus, menentukan objek dan judul proyek jaringan kampus
b. Mampu memahami perkembangan jaringan kampus, mengidetifikasi sistem jaringan kampus yang suda ada, dan mampu mengidentifikasi permasalahan, serta merumuskan solusi jaringan kampus pada proyek

2. Pokok Bahasan

a. Tentang Jaringan Kampus

Kita semua mengakses berbagai jaringan sepanjang kehidupan kita sehari-hari, yang tidak kita sadari secara aktif. Misalnya, ketika kita pulang ke rumah di penghujung hari, sebagian besar ponsel kita secara otomatis terhubung ke jaringan Wi-Fi. Jaringan rumah ini bisa sederhana atau kompleks. Jaringan rumah yang sederhana mungkin hanya memiliki satu *Router* nirkabel yang menyediakan akses Internet. Namun, jaringan rumah yang kompleks, bisa melayani lebih banyak perangkat dan dirancang untuk kehidupan *smart* yang kita alami sekarang. Secara khusus, jaringan rumah yang kompleks dapat menyediakan layanan jaringan berkecepatan tinggi untuk banyak terminal *smart* di rumah, termasuk televisi, *sound system*, ponsel, dan komputer pribadi. Jaringan ini juga dapat terhubung ke sistem *Network Attached Storage* (NAS) untuk menawarkan layanan seperti penyimpanan data yang aman, akuisisi konten otomatis, dan berbagi informasi. Demikian pula, jaringan rumah dapat bekerja sama dengan sistem perlindungan keamanan cerdas untuk memantau lingkungan rumah dari jarak jauh, mendeteksi ancaman secara smart, dan alarm yang berbunyi menyesuaikan. Dengan interkoneksi dengan sistem Internet of Tings (IoT), jaringan rumah dapat memberikan kontrol otomatis atau jarak jauh dari berbagai peralatan rumah dan perangkat cerdas. Contohnya, AC bisa dinyalakan terlebih dulu saat dalam perjalanan pulang, sehingga kita bisa merasa nyaman saat membuka pintu.

Dalam kebanyakan kasus, jaringan rumah terhubung secara eksternal ke Penyedia Jasa Layanan Internet (ISP). ISP menyediakan layanan Internet telekomunikasi yang luas bagi perusahaan dan pengguna individu, biasanya termasuk koneksi Internet, jalur pribadi, dan *Virtual Private Networks* (VPN), serta berbagai layanan bernilai tambah berdasarkan layanan Internet, seperti layanan TV Internet. ISP mencakup kota besar dan kecil dan umumnya memiliki tiga lapisan: lapisan inti, agregasi, dan akses. Lapisan inti terdiri dari *Router* yang menggunakan teknologi Wide Area Network (WAN); lapisan agregasi dibentuk dari *switch* Ethernet yang mengadopsi teknologi *Local Area Network* (LAN); dan lapisan akses terdiri dari *switch* Ethernet atau sebagai alternatifnya *Optical Line Terminals* (OLTs) dan *Optical Network Units* (ONUs) yang menggunakan teknologi *Passive Optical Network* (PON). ISP di seluruh dunia saling terhubung melalui WAN untuk membentuk Internet global.

Dengan demikian, di mana pun atau kapan pun kita mengeluarkan ponsel untuk mengakses Internet, kita menggunakan jaringan komunikasi seluler. Secara umum, jaringan komunikasi seluler dibangun dan dioperasikan oleh operator. Jaringan ini terdiri dari serangkaian

stasiun pangkalan, *Base Station Controllers* (BSCs), jaringan backhaul, dan jaringan inti. Dengan jaringan komunikasi seluler, pengguna di area geografis yang luas dapat menikmati akses Internet nirkabel berkecepatan tinggi dan layanan panggilan suara dengan mudah.

Selain dari jaringan sebelumnya, ada jenis jaringan lain yang sering kita temui.

Ketika kita berjalan ke Universitas untuk belajar, masuk ke kantor untuk bekerja, pergi berbelanja, pergi jalan-jalan, atau *check-in* ke hotel, kita mungkin melihat bahwa tempat-tempat ini juga tercakup oleh jaringan. Di Universitas, kita memiliki jaringan tertutup untuk para Dosen dan juga jaringan semi terbuka bagi para mahasiswa untuk mengakses sumber daya pembelajaran dan menjelajah Internet. Di dalam perusahaan, kita memiliki jaringan internal tertutup untuk karyawan, memfasilitasi pekerjaan mereka sambil memastikan keamanan. Di pusat perbelanjaan atau hotel, kita tidak hanya memiliki jaringan tertutup untuk karyawan, tetapi juga jaringan terbuka untuk pelanggan yang menyediakan layanan berkualitas tinggi untuk meningkatkan daya saing perusahaan. Semua jaringan ini termasuk dalam jaringan kampus.

Jaringan kampus adalah LAN yang terhubung sepenuhnya di area geografis yang kontinu dan terbatas. Jika sebuah kampus memiliki banyak area yang terputus-putus, jaringan di area yang terputus-putus ini dianggap sebagai beberapa jaringan kampus. Banyak perusahaan dan sekolah memiliki beberapa jaringan kampus yang terhubung melalui teknologi WAN.

Jaringan kampus bisa besar atau kecil. *Small Office Home Office* (SOHO) adalah contoh khas dari jaringan kampus dengan skala kecil, sementara sekolah, perusahaan, taman, dan pusat perbelanjaan adalah contoh jaringan kampus besar. Terlepas dari itu, skala jaringan kampus terbatas. Biasanya, jaringan kampus yang besar, seperti universitas/perguruan tinggi atau industri, dibatasi hingga beberapa kilometer persegi. Dalam lingkup ini, kita dapat menggunakan teknologi LAN untuk membangun jaringan tersebut. Jaringan kampus di luar lingkup ini biasanya dianggap sebagai area metropolitan, dan jaringan dianggap sebagai WAN, yang melibatkan teknologi WAN. Teknologi LAN yang umum digunakan di jaringan kampus adalah *Institute of Electrical and Electronics Engineers* (IEEE) 802.3 Ethernet (untuk akses kabel) dan teknologi IEEE 802.11 Wi-Fi (untuk akses nirkabel). Biasanya, jaringan kampus dikelola oleh satu entitas saja. Jika beberapa jaringan dalam suatu area dikelola oleh beberapa entitas, kita umumnya menganggap jaringan ini sebagai beberapa jaringan kampus. Jika jaringan ini dikelola oleh entitas yang sama, jaringan ini dianggap sebagai beberapa subnet dari jaringan kampus yang sama.

b. Sejarah jaringan Kampus

Asal mula jaringan kampus tidak ditandai dengan peristiwa zaman yang dikenal luas, tetapi mereka telah berkembang pesat dengan lahirnya Ethernet dan munculnya *switch* Ethernet. Selama beberapa dekade terakhir perkembangannya, jaringan kampus sebagian besar telah dibangun menggunakan Ethernet, dengan *switch* Ethernet digunakan sebagai komponen inti jaringan tersebut.

1. Generasi pertama

Pada tahun 1980, IEEE merilis standar IEEE 802.3 untuk mendefinisikan koneksi lapisan fisik, sinyal listrik, dan protokol *Media Access Control* (MAC). Dengan menggunakan

koneksi *twisted pair*, Ethernet lebih hemat biaya dan lebih mudah diimplementasikan daripada teknologi jaringan sebelumnya. Awalnya, jaringan kampus harus dibagi menjadi beberapa LAN, saling berhubungan melalui *Router* yang harganya mahal dan berkecepatan rendah.

Switch Ethernet awal bekerja pada lapisan data link dan oleh karena itu disebut *Layer* 2 *switch*. *Layer* 2 *switch* mendukung hingga 64 pengguna bersamaan, secara signifikan lebih banyak daripada saat hub digunakan. Jaringan pada periode ini mahal dan tidak efisien karena biasanya menggunakan *Router* sebagai node *backbone*.

2. Generasi kedua

Pada tahun 1990-an, dua penemuan inovatif muncul di bidang jaringan: *World Wide Web* (WWW) dan perangkat lunak pesan instan. WWW membutuhkan *bandwidth* yang cukup, yang tidak dapat disediakan pada jaringan *backbone* kampus berbasis *Router*. Dengan latar belakang ini, *Layer* 3 *switch* dikembangkan pada tahun 1996. *Backbone* jaringan kampus terdiri dari *switch Layer* 3 dengan pencarian rute berbasis perangkat keras. Berbagai sistem kantor juga dimigrasikan ke jaringan kampus, dan kantor-kantor menjadi paperless.

Pada tahun 1995, IEEE merilis standar IEEE 802.3u Fast Ethernet (FE), menandakan munculnya era Ethernet 100 Mbit/s. Pemanfaatan *bandwidth* yang rendah terbayar, karena menyederhanakan implementasi jaringan. Hal ini juga berarti bahwa mekanisme kompleks seperti *Quality of Service* tidak sepenting yang diharapkan. Untuk mengatasi skala jaringan yang semakin besar, diperkenalkan *Network Management System* menggunakan *Simple Network Management Protocol* (SNMP).

3. Generasi ketiga

Teknologi Wi-Fi muncul sangat awal, penggunaannya terbatas pada jaringan rumah dan jaringan skala kecil lainnya selama lebih dari 10 tahun. Industri selalu berharap untuk memperkenalkan Wi-Fi ke dalam jaringan kampus. Namun harapan ini tidak tercapai terutama karena persyaratan yang tidak memadai, kekhawatiran tentang ancaman keamanan, dan arsitektur yang tidak sesuai. Teknologi Wi-Fi banyak digunakan untuk cakupan hotspot dan jarang diadopsi di jaringan kampus. Seiring dengan semakin populernya seluler pintar, permintaan untuk cakupan Wi-Fi secara menyeluru menjadi lebih kuat. Sehingga sekarang ini sduah banyak yang menerapkan WI-FI untuk jaringan kampus.

c. Aspek Membangan Jaringan Kampus

1. Skala Jaringan

Jaringan kampus dapat diklasifikasikan menjadi tiga jenis: jaringan kampus kecil, menengah, dan besar, masing-masing berbeda dalam jumlah pengguna terminal atau Elemen Jaringan. Kadang-kadang, jaringan kampus kecil dan jaringan kampus menengah secara kolektif disebut jaringan kampus kecil dan menengah. Jaringan kampus yang besar umumnya memiliki persyaratan dan struktur yang kompleks, menghasilkan beban kerja operasi dan pemeliharaan yang berat. Untuk menangani hal ini, tim IT profesional penuh waktu bertanggung jawab atas manajemen IT *end-to-end*, mulai dari perencanaan jaringan

kampus, konstruksi, operasional dan manajemen hingga pemecahan masalah. Tim ini juga membangun platform yang komprehensif untuk memfasilitasi yang efisien.

Berbeda dengan jaringan kampus besar, jaringan kampus kecil atau menengah dibatasi anggaran dan biasanya tidak memiliki tenaga IT profesional penuh waktu atau platform khusus. Biasanya hanya satu karyawan paruh waktu yang bertanggung jawab pada jaringan.

2. Target Layanan

Jika kita melihat jaringan kampus dari perspektif target layanan, kita akan melihat bahwa beberapa jaringan kampus tertutup dan terbatas, hanya mengizinkan pengguna internal, sementara yang lain terbuka untuk pengguna eksternal.

Tabel 1 Kategori Jaringan Kampus

Kategori Jaringan Kampus	Pengguna Terminal	Elemen Jaringan
Jaringan Kampus Kecil	<200	<25
Jaringan Kampus Menengah	200 – 2000	25 – 100
Jaringan Kampus Besar	>2000	>100

Baik pengguna internal maupun eksternal. Sumber ancaman keamanan jaringan berbeda antara jaringan kampus tertutup dan jaringan kampus terbuka. Oleh karena itu, keduanya memiliki persyaratan dan solusi keamanan jaringan yang berbeda. Pengguna pada jaringan kampus tertutup biasanya adalah karyawan internal. Perilaku *online* mereka relatif fleksibel dan dapat dikontrol secara efektif melalui aturan dan regulasi internal serta *reward* dan *punishment*. Oleh karena itu, ancaman terhadap jaringan kampus tertutup terutama berasal dari intrusi eksternal. Untuk alasan ini, jaringan kampus tertutup biasanya menggunakan model benteng untuk mencegah akses yang tidak sah dari jaringan eksternal dan internal. Secara khusus, network admission control (NAC) diperkenalkan untuk mengotentikasi nama pengguna, akun, token, sertifikat, dan kredensial lainnya untuk mencegah pengguna non-internal mengakses jaringan. Selain itu, *firewall* ditempatkan di perbatasan zona keamanan yang berbeda, misalnya, di pintu masuk dan keluar jaringan.

Jaringan kampus terbuka agak berbeda. Jaringan kampus terbuka bertujuan untuk melayani publik sebanyak mungkin. Untuk tujuan ini, otentikasi akses jaringan perlu mengakomodasi akses publik yang nyaman dan identifikasi pengguna yang efektif. Solusi yang layak adalah menggunakan nomor ponsel ditambah kode verifikasi layanan pesan singkat (SMS) atau mengadopsi otentikasi akun sosial. Pendekatan ini dapat menyederhanakan manajemen akun. Namun, akses jaringan publik tidak dapat diprediksi dan mungkin ada banyak ancaman keamanan jaringan. Dengan demikian, sistem kontrol perilaku pengguna sering digunakan di dalam jaringan untuk mencegah perilaku ilegal yang disengaja dan tidak disengaja. Misalnya, jika terminal pengguna terinfeksi virus jaringan, virus dapat menyebar untuk menyerang seluruh sistem jaringan. Untuk menahan serangan, sistem kontrol perilaku pengguna harus mampu mengidentifikasi perilaku pengguna serta

mengisolasi dan membersihkan trafik dari pengguna tersebut. Hal ini memastikan bahwa pengguna dapat mengakses Internet seperti biasa, tanpa mempengaruhi pengguna lain di jaringan.

Dalam situasi dunia nyata, jaringan kampus biasanya memiliki subnet tertutup dan terbuka. Jaringan kampus yang melayani publik selalu mempunyai subnet tertutup untuk keperluan internal dan administrasi. Demikian juga, jaringan kampus yang didesain untuk personil internal biasanya sebagian terbuka untuk orang luar. Sebagai contoh, jaringan kampus perusahaan membuka beberapa bagian dari jaringan untuk tamu dalam meningkatkan komunikasi dan kolaborasi. Beberapa bagian dari jaringan kampus *e-Government* terbuka untuk warga yang akan menikmati layanan pemerintah yang nyaman. Dalam kasus ini, subnet tertutup dan subnet terbuka milik zona keamanan yang berbeda dan harus diisolasi satu sama lain. Metode isolasi yang umum termasuk isolasi fisik, isolasi jaringan logis, dan isolasi firewall. Untuk jaringan yang membutuhkan keamanan yang kuat, umumnya digunakan isolasi fisik, sehingga subnet tertutup dan terbuka tidak dapat berkomunikasi satu sama lain sama sekali.

3. Dukungan Layanan

Jaringan kampus dapat diklasifikasikan menjadi jaringan kampus layanan tunggal dan multi-layanan, tergantung pada layanan yang dibawa. Kompleksitas layanan yang dibawa pada jaringan kampus menentukan kompleksitas jaringan. Pada awalnya, jaringan kampus hanya membawa layanan data, dan layanan lainnya didukung oleh jaringan khusus yang berbeda. Saat ini, sebagian besar perusahaan kecil dan menengah memiliki jumlah layanan jaringan yang terbatas. Sebagai contoh, perusahaan kecil yang menyewa kantor di gedung kantor menggunakan infrastruktur jaringan yang disediakan oleh pemilik gedung kantor. Oleh karena itu, jaringan kampus perusahaan kecil biasanya hanya memerlukan layanan komunikasi data internal. Secara umum, jaringan kampus layanan tunggal memiliki arsitektur yang sederhana.

Jaringan kampus besar yang canggih adalah sangat berbeda. Biasanya melayani kampus besar yang independen, di mana berbagai layanan dasar, seperti manajemen pemadam kebakaran, pengawasan video, manajemen kendaraan, dan kontrol konsumsi energi. Jika jaringan khusus digunakan untuk setiap layanan dasar, biayanya akan sangat tinggi dan akan sangat kompleks. Untuk mengubah ini, teknologi digital dan Ethernet secara bertahap diperkenalkan untuk layanan dasar ini. Melakukan hal itu memfasilitasi penggunaan Ethernet yang matang, dan jaringan kampus secara bertahap dibuat mampu mendukung banyak layanan. Jaringan membawa beberapa layanan dengan persyaratan berbeda, yang terisolasi satu sama lain dan dipastikan secara efektif. Karena ini, arsitektur jaringan kampus menjadi semakin kompleks dan tervirtualisasi.

4. Jenis Akses

Jaringan kampus mempunyai dua mode akses yaitu kabel dan nirkabel. Sebagian besar jaringan kampus saat ini adalah *hybrid* antara kabel dan nirkabel. Jaringan kampus tradisional adalah jaringan kampus berkabel. Dari perspektif pengguna, setiap perangkat di

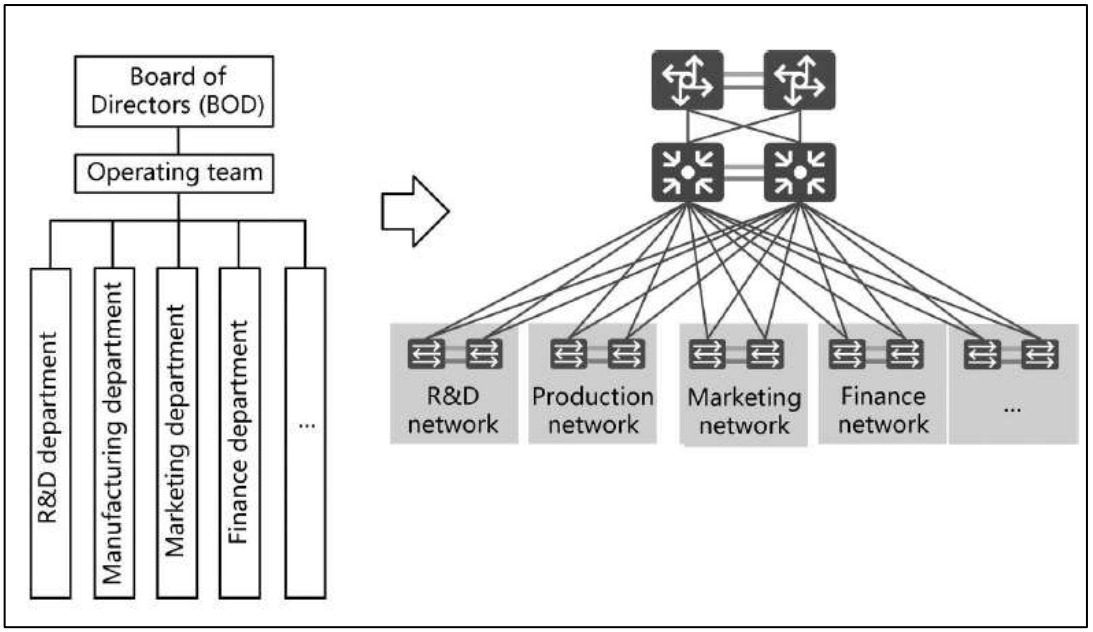
jaringan kampus berkabel terhubung ke port Ethernet di dinding atau di desktop melalui kabel Ethernet. Koneksi ini biasanya tidak saling mempengaruhi. Dengan demikian, arsitektur jaringan kampus kabel biasanya terstruktur dan berlapis, dengan logika yang jelas, manajemen sederhana, dan pemecahan masalah yang mudah.

Jaringan kampus nirkabel, bagaimanapun, sangat berbeda dari jaringan kampus kabel. Biasanya dibangun berdasarkan standar Wi-Fi (standar WLAN). Terminal WLAN terhubung ke Access Point WLAN (AP) menggunakan protokol antarmuka udara seri IEEE 802.11. Penyebaran jaringan dan kualitas instalasi menentukan efek jangkauan jaringan. Optimalisasi jaringan harus dilakukan secara berkala berdasarkan situasi layanan jaringan untuk memastikan kualitas jaringan. Jaringan nirkabel juga rentan terhadap gangguan dari sumber sinyal eksternal, menyebabkan serangkaian ketidaknormalan eksternal, menyebabkan serangkaian kelainan yang sulit ditemukan. Mengingat bahwa koneksi nirkabel tidak terlihat dan terputus-putus, kelainan terjadi secara tiba-tiba dan sulit untuk direproduksi. Untuk alasan ini, personel IT untuk jaringan nirkabel harus memiliki pengetahuan dan keahlian yang cukup terkait dengan *interface wireless*. Untuk alasan-alasan ini, personil IT untuk jaringan nirkabel harus memiliki pengetahuan dan keahlian yang cukup yang berhubungan dengan *interface wireless*.

d. Jenis-jenis Jaringan Kampus

1. Jaringan Kampus Perusahaan

Sebuah jaringan kampus perusahaan mencakup cakupan terbesar dari semua jenis jaringan dan dapat disegmentasi lebih lanjut berdasarkan industri. Jaringan kampus perusahaan yang dijelaskan di sini mengacu pada jaringan kantor perusahaan yang dibangun berdasarkan perangkat *switching* Ethernet. Dalam sebuah perusahaan, arsitektur jaringan kantor umumnya selaras dengan struktur organisasi internal, seperti yang ditunjukkan pada gambar 1. Arsitektur jaringan harus sangat andal dan canggih, cukup untuk terus meningkatkan pengalaman karyawan dan memberikan efisiensi dan kualitas produksi tanpa kompromi.



Gambar 1 Sturktur organisasi dan struktur jaringan

2. Jaringan Kampus Pendidikan

Ada dua jenis jaringan kampus pendidikan yaitu jaringan kampus pendidikan dasar/sekunder dan pendidikan tinggi. Jaringan kampus pendidikan dasar/sekunder ditujukan untuk sekolah dasar dan menengah dengan struktur dan fungsi jaringan internalnya mirip dengan jaringan kampus perusahaan. Jaringan kampus pendidikan tinggi harus melayani mahasiswa universitas/perguruan tinggi, dengan demikian lebih kompleks daripada jaringan kampus pendidikan dasar/sekunder. Jaringan kampus pendidikan tinggi sering terdiri dari beberapa jaringan yang berbeda, termasuk jaringan pengajaran dan penelitian, jaringan pembelajaran siswa, dan jaringan akomodasi operasional. Jaringan kampus pendidikan tinggi juga memiliki persyaratan yang sangat tinggi untuk penyebaran dan pengelolaan jaringan. Jaringan tidak hanya mengirimkan data tetapi juga mengelola perilaku *online* perilaku siswa secara *online* untuk menghindari tindakan ekstrem dan agresif. Mendukung penelitian dan pengajaran adalah prioritas utama. Untuk alasan ini, jaringan harus sangat canggih dan mendukung tuntutan intens teknologi mutakhir.

3. Jaringan Kampus Pemerintahan

Jaringan internal lembaga pemerintah adalah contoh yang baik dari jenis jaringan ini. Karena persyaratan keamanan yang ketat, jaringan internal dan eksternal pada jaringan kampus *e-Government* umumnya terisolasi untuk memastikan keamanan mutlak dari informasi rahasia.

4. Jaringan Kampus Publik

Jenis jaringan ini digunakan di organisasi dan tempat komersial, seperti pusat perbelanjaan, supermarket, hotel, museum, dan taman. Dalam kebanyakan kasus, jaringan

kampus komersial memfasilitasi pekerjaan kantor internal melalui subnet tertutup, tetapi yang paling penting adalah melayani sekelompok besar konsumen, seperti tamu di pusat perbelanjaan, supermarket, dan hotel. Selain menyediakan layanan jaringan, jaringan kampus komersial juga melayani sistem intelijen bisnis. Manfaat yang dihasilkan termasuk meningkatkan pengalaman pelanggan, mengurangi biaya operasional, meningkatkan efisiensi bisnis, dan memberikan nilai lebih dari jaringan.

e. Komponen Jaringan Kampus

1. Jaringa Data Kampus (*Intermediari device*)

Jaringan data kampus dibangun menggunakan teknologi Ethernet atau WLAN. Ini terdiri dari semua perangkat komunikasi data di kampus, termasuk berbagai *Router*, *Switch* Ethernet, *Wireless Access Point* (AP), *Wireless Access Control* (WAC), dan *Firewall*. Semua trafik data internal diteruskan melalui jaringan data kampus. Secara umum, jaringan data kampus terdiri dari beberapa subnet yang membawa layanan yang berbeda. Misalnya, semua kampus memiliki subnet kantor untuk pekerjaan kantor sehari-hari, dan banyak yang memiliki subnet video konferensi secara independen, di mana sambungan khusus digunakan untuk memastikan kualitas vidio konferensi. Subnet jaringan biasanya dikelola oleh satu administrator. Subnet IoT juga akan tersedia di masa depan karena perangkat IoT terhubung ke jaringan data kampus. Karena keragaman teknologi IoT, beberapa subnet IoT akan hidup berdampingan. Selain itu, sebuah kampus biasanya memiliki pusat data internal. Di masa depan, jaringan data kampus mungkin mampu melakukan beberapa layanan pada saat yang bersamaan. Yang artinya jaringan data kampus yang terkonvergensi akan membawa berbagai layanan secara bersamaan seperti data, video, dan audio.

2. Akses Terminal (End User Device)

Pada kebanyakan jaringan, terminal atau perangkat pengguna akhir tidak dianggap sebagai bagian dari keseluruhan jaringan, tetapi sebagai konsumen jaringan. Ini karena pemilik terminal biasanya bukan administrator jaringan. Namun, hal ini tidak berlaku untuk jaringan kampus. Terminal akses sering dianggap sebagai bagian tak terpisahkan dari jaringan kampus. Hal ini karena pemilik akses terminal juga merupakan pemilik jaringan kampus, atau karena administrator jaringan kampus dapat memperoleh ijin terminal melalui manajemen untuk mengelola terminal di jaringan kampus. Dengan cara ini, jaringan data kampus dan akses terminal dapat sepenuhnya berinteraksi satu sama lain, membentuk jaringan *end-to-end*.

Ketika akses terminal dianggap sebagai bagian dari jaringan kampus, administrator jaringan kampus dapat mengelola dan membatasi terminal secara lebih aktif, menyederhanakan seluruh solusi. Misalnya, *software* antivirus yang ditentukan secara paksa diinstal pada terminal. Dengan cara ini, terminal diperiksa secara paksa ketika mereka mencoba mengakses jaringan kampus. Pendekatan ini sangat mengurangi ancaman virus dan menyederhanakan solusi antivirus yang digunakan di seluruh jaringan kampus.

3. Platform Manajemen Jaringan

Platform manajemen jaringan adalah komponen tradisional. Dalam arsitektur jaringan kampus terbaru, posisi dan enabler dari platform manajemen jaringan telah sangat berubah. Perubahan ini adalah kunci untuk menyederhanakan jaringan.

Platform manajemen jaringan tradisional biasanya merupakan rumah bagi berbagai Network Management Systems (NMS) yang menyediakan sejumlah fungsi manajemen dan pemeliharaan jarak jauh untuk jaringan atau perangkat. Namun, platform manajemen jaringan generasi terbaru mengambil peran baru. Platform ini masih memiliki semua fungsi NMS, tetapi yang paling penting menawarkan fungsi manajemen dan pemeliharaan yang berubah secara radikal. Misalnya, manajemen skenario otomatis atau proses umum. Platform manajemen jaringan terbaru adalah fondasi untuk aplikasi layanan. Ini menyediakan *open northbound* dan *southbound Application Programming Interfaces* (API), di mana sistem layanan dapat memanggil sumber daya jaringan.

4. Platform Keamanan

Platform keamanan tingkat lanjut memanfaatkan data besar di seluruh jaringan yang disediakan oleh platform manajemen jaringan untuk bertahan melawan *Advanced Persistent Treats* (APT). Ini juga dapat memanggil *northbound* API yang disediakan oleh platform manajemen jaringan untuk mengisolasi dan secara otomatis membersihkan trafik ancaman.

5. Platform Layanan Aplikasi

Di masa mendatang, banyak layanan aplikasi akan dikembangkan dengan menggunakan basis yang disediakan oleh platform manajemen jaringan. Dengan cara ini, platform layanan aplikasi akan terbentuk di atas jaringan kampus. Misalnya, pada jaringan kampus komersial, mudah untuk memanggil API dari platform manajemen jaringan untuk mendapatkan data posisi jaringan Wi-Fi yang diperlukan dan kemudian mengembangkan aplikasi peta panas pelanggan. Aplikasi semacam itu memberikan referensi untuk penyesuaian di dalam tempat komersial.

f. Perkembangan Teknologi

1. Perusahaan Besar

Menurut wawancara yang diadakan oleh Gartner dengan Chief Information Officers (CIO) perusahaan pada tahun 2018, transformasi digital telah menjadi prioritas strategis perusahaan besar. Hal ini didorong oleh kemajuan teknologi dan tuntutan pengguna serta persaingan eksternal dan tekanan bakat internal. Transformasi digital perusahaan telah bergeser dari fase konseptual ke fase implementasi utama. Perusahaan besar melakukan transformasi digital komprehensif yang berpusat pada pengalaman, biaya, dan efisiensi.

Mobile dan *cloud* sangat menyederhanakan kolaborasi dan komunikasi lintas wilayah. Ahli teknis dapat melakukan operasi dan pemeliharaan dari jarak jauh melalui konferensi video. Para insinyur dapat mengirimkan gambar kesalahan di lokasi dari jarak jauh ke pakar

teknis secara real time. Sumber daya R&D dibagikan di cloud, dan layanan cloud seperti simulasi dan desain cloud.

Banyak perusahaan telah memilih jaringan kampus internal mereka sebagai titik awal untuk transformasi digital. Misalnya di ruang konferensi, orang dapat merasakan layanan cerdas kapan saja. Jika terminal IoT berbasis IP, biaya operasional dapat dikurangi lebih lanjut sampai batas tertentu. Hal ini akan memangkas biaya rata-rata untuk memasang sistem kontrol akses hingga hampir setengahnya. Hal ini bertujuan untuk membuat proses produksi lebih terkendali. Perusahaan dapat secara otomatis menghitung kapan harus membeli bahan mentah dan kuantitas yang diperlukan.

2. Pendidikan

Model pendidikan tradisional difokuskan pada pencapaian pekerjaan siswa. Model pengembangan bakat di masa depan akan berubah dari sekadar mentransfer pengetahuan dan keterampilan menjadi meningkatkan keterampilan sosial dan emosional siswa. Industri pendidikan telah memulai transformasi digital, dengan tujuan mempromosikan pengembangan pendidikan konvergen. Transformasi digital yang sedang berlangsung ini memerlukan jaringan kampus untuk menyediakan koneksi yang lebih luas, memberikan pengalaman layanan yang lebih baik, dan menawarkan data yang lebih mendasar untuk aplikasi.

a. Lingkungan pembelajaran di mana-mana mempromosikan pendidikan berkualitas tinggi untuk semua. Pengajaran seluler dan multimedia telah mulai mengubah model pengajaran tradisional dengan menyediakan metode pembelajaran yang lebih kaya dan fleksibel bagi para siswa. Cloud adalah rumah bagi semua sumber daya layanan pengajaran, termasuk courseware, rekaman, video, reservasi, dan sistem penjadwalan. Siswa dapat mengakses sumber daya ini dari terminal seluler mereka atau di ruang kelas jarak jauh. Dengan cara ini, pengajaran tidak lagi dibatasi oleh ruang, dan siswa bebas belajar di mana saja. *Augmented Reality*/*Virtual Reality* (AR/VR) - pengajaran dengan bantuan dan holografik menawarkan pengalaman yang lebih menarik, intuitif, dan mendalam kepada siswa. Namun, lingkungan belajar di mana-mana, bergantung pada jaringan kampus berkualitas tinggi. Dalam kasus pengajaran dengan bantuan AR/VR, misalnya, setiap terminal pengguna memerlukan *bandwidth* 250 Mbit/s, dan latensi tidak boleh melebihi 15 ms. Jika persyaratan ini tidak terpenuhi, pengguna mungkin akan mengalami pusing dan ketidaknyamanan lainnya.
b. Semakin banyak aplikasi IoT yang digunakan di kampus, membuat kampus cerdas yang sepenuhnya terhubung menjadi kenyataan. Misalnya, kartu *all-in-one* telah menjadi "kartu ID elektronik" bagi para mahasiswa, memungkinkan mereka untuk mengakses berbagai layanan seperti kontrol akses elektronik, *check-in* kehadiran, peminjaman buku, dan perawatan medis. Kartu *all-in-one* ini bisa berupa kartu fisik atau kode QR. Contoh lainnya adalah solusi manajemen aset berdasarkan *Radio Frequency Identification* (RFID). Untuk instrumen di laboratorium sekolah, solusi ini memungkinkan stock opname otomatis sekali klik, berbagi secara *online*, dan menghasilkan alarm pengecualian. Aplikasi IoT, karena

penggunaannya menjadi lebih lazim, dapat memberikan kenyamanan yang lebih besar dalam hal layanan siswa dan mengelola sumber daya pengajaran dengan cara yang lebih halus. Cakupan Wi-Fi penuh merupakan aspek vital bagi sebagian besar kampus. Untuk mencapai kampus pintar yang sepenuhnya terhubung, konvergensi IoT dan Wi-Fi harus dipertimbangkan selama pembangunan jaringan. Hal ini diperlukan untuk mencapai biaya pemasangan kabel yang lebih rendah, penyebaran yang lebih mudah, dan manajemen operasional dan manajemen yang lebih efisien.

c. Konvergensi data pengajaran, pembelajaran, administrasi, dan penelitian membuka jalan untuk merancang jalur pertumbuhan yang cerdas bagi siswa. Paradigma pengajaran dan pengembangan bakat yang baru sepenuhnya memanfaatkan analitik data besar untuk mencapai pembelajaran yang benar-benar dipersonalisasi, melepaskan keahlian dan potensi penuh dari setiap siswa, dan memberikan pendidikan yang berorientasi pada kualitas esensial. Jalur pengembangan dapat disesuaikan untuk setiap siswa berdasarkan berbagai macam data, seperti data ujian masuk perguruan tinggi, data keahlian, data latihan, data penilaian kepribadian, data penilaian minat karier, data komunikasi tatap muka, dan data permintaan bakat eksternal. Jalur pengembangan ini menyediakan jurusan, komunitas, dan pilihan pekerjaan yang direkomendasikan, sehingga memberikan siswa landasan yang kuat untuk merencanakan pengembangan mereka. Selain itu, evaluasi pengajaran yang akurat dapat dilakukan untuk setiap siswa berdasarkan data belajar mandiri, data kehadiran, data kredit, dan data peminjaman buku. Saran pembinaan yang sesuai kemudian ditawarkan kepada siswa, membantu mereka menyelesaikan studi mereka secara efisien.

3. Pemerintahan

Membangun pemerintahan digital harus menjadi salah satu prioritas utama bagi pemerintah di seluruh dunia. Transformasi digital pemerintah melibatkan reformasi model TI *e-Government* tradisional. Transformasi semacam itu akan menciptakan model tata kelola modern yang menampilkan dialog, pengambilan keputusan, layanan, dan inovasi yang diinformasikan data. Pada akhirnya akan mempromosikan layanan publik yang berpusat pada warga, meningkatkan efisiensi manajemen, dan meningkatkan pengalaman layanan.

a. Layanan *e-Government* mencapai persetujuan satu jendela dan penanganan layanan multisaluran. Langkah efektif pertama yang diambil pemerintah dalam perjalanan transformasi digital mereka adalah untuk terus meningkatkan kemampuan mereka dalam menawarkan layanan *e-Government* digital kepada warga negara. Layanan *e-Government* tradisional menghadapi masalah khas seperti layanan yang tersebar dan konstruksi TI yang berulang. Akibatnya, berbagi sumber daya data atau kolaborasi layanan lintas departemen sulit dilakukan. Di masa lalu, warga negara perlu mengunjungi lembaga pemerintah beberapa kali karena terbatasnya saluran yang disediakan lembaga-lembaga ini untuk menangani permintaan layanan. Saat ini, pemerintah memberikan layanan *e-Government* digital melalui jaringan kampus dan membangun pusat data besar *e-Government* berdasarkan platform pertukaran dan berbagi data. Fasilitas baru ini

mencapai pertukaran data yang lebih efisien dan berbagi sumber daya publik di antara departemen. Khususnya, sebagian besar layanan publik tersedia bagi warga negara melalui sejumlah saluran, sehingga sangat mempercepat penanganan layanan permintaan. Model layanan "satu nomor, satu jendela, satu jaringan" mulai terbentuk. Model layanan baru ini memungkinkan data untuk menjalankan tugas bagi masyarakat di seluruh instansi pemerintah. Dalam solusi jaringan *e-Government* tradisional, jaringan pribadi dibangun untuk mencapai isolasi fisik yang lengkap dan memastikan keamanan data pribadi yang mutlak, yang berarti bahwa layanan yang sensitif terhadap keamanan informasi terus dibawa pada jaringan pribadi asli. Untuk jaringan layanan *e-Government* terpadu - jaringan yang membuka banyak saluran penanganan layanan kepada warga - keamanan jaringan akan menjadi tantangan utama dan sesuatu yang harus ditangani.

b. Tata kelola kota digital terbukti produktif untuk koordinasi global dan respons yang cepat. Tata kelola kota digital mencakup tiga aspek, yaitu:
   1. Merampingkan sistem layanan lembaga pemerintah secara horizontal dan mengintegrasikan kemampuan komunikasi audio dan video. Dengan demikian, memungkinkan keterkaitan layanan dan kolaborasi yang efisien antara berbagai departemen, memastikan respons darurat yang cepat. Misalnya, dalam hal respons pemadam kebakaran, platform komando terpadu dapat digunakan untuk mengoordinasikan dan mengirimkan sumber daya pemadam kebakaran dan medis secara terpusat serta memberikan pemberitahuan tentang sumber api dan kondisi jalan secara *real-time*.
   2. Visualisasi, dengan mengintegrasikan teknologi seperti IoT dan GIS, dunia fisik dapat divirtualisasikan ke dalam dunia digital. Di mana keseluruhan status berjalannya perkotaan dapat terus dipantau. Misalnya, petugas memungkinkan untuk mempelajari distribusi sumber daya sanitasi dan tingkat pengumpulan sampah secara real time untuk setiap area di kota.
   3. Menggunakan AI untuk menganalisis status kota dan memberikan peringatan secara real time, mengubah respons pasif menjadi pertahanan proaktif, dan mengoptimalkan proses tata kelola secara komprehensif. Analisis video cerdas telah memainkan peran penting dalam penanganan pelanggaran lalu lintas dan analisis kasus. Contohnya adalah keberhasilan penyelamatan anak yang diculik dalam waktu 10 jam berkat sinopsis video, pengenalan wajah, dan tabrakan data besar.

   Tata kelola kota digital tidak mungkin dilakukan tanpa dukungan jaringan kampus di seluruh kota.

4. Retail

Transformasi digital industri ritel mengharuskan jaringan kampus terbuka di semua lapisan untuk membangun ekosistem aplikasi digital yang diperkaya. Para pemain ritel tradisional secara aktif merangkul perubahan ini, dengan harapan bisa mengambil tempat di era ritel baru di masa depan. Perusahaan *e-commerce* ingin mencapai terobosan bisnis

dengan merampingkan praktik *online* dan *offline* serta memperluas portal lalu lintas ke dalam omni-channel melalui jaringan kampus.

a. Analisis dan penambangan mendalam dari data akses konsumen dalam jumlah besar memfasilitasi pemasaran yang presisi. Model pemasaran tradisional kurang memiliki wawasan yang ditargetkan ke dalam kebutuhan pengguna. Akibatnya, peritel merekomendasikan produk serupa kepada semua pengguna, gagal memenuhi kebutuhan pribadi pengguna dan menyebabkan tingkat konversi pelanggan yang buruk dalam acara pemasaran. Setiap kali pengguna mengakses situs web atau aplikasi peritel, mereka umumnya disajikan dengan produk yang sama, yang mengarah pada pengalaman pengguna yang buruk. Di era ritel baru, jaringan kampus digunakan untuk merampingkan saluran *online* dan *offline* serta menganalisis dan menambang nilai secara mendalam dari sejumlah besar akses konsumen dan data transaksi. Praktik-praktik ini membantu peritel untuk membangun model pengguna yang tepat, melakukan profiling digital untuk setiap pengguna, dan menyediakan layanan yang dipersonalisasi.
b. Aplikasi nilai tambah digital yang berlimpah disediakan dengan cara yang mirip dengan yang ada di toko aplikasi pada *smartphone*. Di mana berbagai macam aplikasi bernilai tambah disediakan untuk meningkatkan pengalaman konsumen, mengurangi biaya operasi, meningkatkan daya saing merek, dan meningkatkan efisiensi operasional. Untuk mengaktifkan skenario ini, arsitektur jaringan harus cukup terbuka untuk saling terhubung dengan aplikasi dari vendor kustomisasi aplikasi pihak ketiga. Dengan cara ini, aplikasi bernilai tambah seperti analisis arus pelanggan dan pemosisian aset dapat dengan cepat dikembangkan dengan menggunakan *Application Programming Interfaces* (API) yang disediakan oleh jaringan. Selain itu, jaringan toko harus mengintegrasikan beberapa kemampuan akses IoT, termasuk Bluetooth, RFID, dan ZigBee.

g. Tantangan Jaringan Kampus dengan Perkembangan Teknologi

1. Koneksi dimana-mana

Penggunaan teknologi Wi-Fi yang meluas di jaringan kampus membebaskan pengguna dari pembatasan kabel dan memungkinkan mereka untuk menikmati gaya kerja seluler yang nyaman. Telah terbukti bahwa penggunaan nirkabel sangat meningkatkan produktivitas dan efisiensi perusahaan, dan jaringan kampus yang serba nirkabel menjadi semakin meluas.

Selain itu, kebangkitan IoT mendorong transformasi jaringan kampus yang mendalam. Indeks konektivitas global terbaru Huawei menunjukkan bahwa pada tahun 2025, akan ada 100 miliar koneksi di seluruh dunia dan IoT akan berkembang pada kecepatan yang dipercepat.

Jaringan kampus masa depan diharapkan tidak hanya menyatukan kabel, nirkabel, dan IoT tetapi juga menyediakan koneksi di mana-mana sambil memberikan layanan yang selalu aktif. Namun, ekspektasi ini akan membawa tantangan bagi jaringan kampus:

Wi-Fi akan menjadi mode akses utama dan perlu mendukung jaringan berskala besar, berkinerja tinggi, dan disesuaikan dengan skenario.

2. **Konstruksi IoT skala besar harus mengatasi masalah seperti biaya tinggi dan gangguan yang parah.**

   a. Layanan Sesuai Permintaan

      Selama transformasi digital, aplikasi berubah dengan cepat dan layanan baru terus bermunculan. Perusahaan berharap bahwa platform layanan lapisan atas dapat dengan mudah memperoleh semua informasi yang diperlukan yang diperlukan dari jaringan yang mendasarinya untuk memberikan layanan bernilai tambah lebih dan menciptakan hasil bisnis yang lebih besar.

      Untuk mencapai kesuksesan bisnis, perusahaan berusaha untuk mempersingkat waktu untuk memasarkan layanan baru dan menerapkan penyediaan aplikasi jaringan kampus sesuai permintaan. Hal ini membutuhkan jaringan kampus untuk memecahkan masalah berikut:

      1. Praktik penyebaran dan manajemen tradisional tidak dapat mendukung penyebaran dan perluasan jaringan yang cepat.
      2. Layanan dan jaringan digabungkan secara erat, sehingga gagal mendukung penyesuaian layanan yang sering.
      3. Kebijakan dan alamat IP digabungkan dengan erat, yang tidak dapat memastikan konsistensi kebijakan dalam skenario kantor bergerak.

   b. *Efficient* dan *Intelligent*

      Dengan perkembangan jaringan kampus yang konstan, jumlah node dan *bandwidth* telah meningkat secara eksponensial. Pada tahun 2010, hanya ada 10 miliar terminal yang mengakses jaringan, sedangkan, diprediksi bahwa pada tahun 2020, angka ini akan mencapai hingga 50 miliar. Lebih lanjut, dengan konvergensi berbagai layanan, jaringan kampus membawa lebih banyak konten dan layanan, mengakomodasi persyaratan yang lebih tinggi pada kualitas layanan, dan menjadi lebih kompleks dari sebelumnya. Kami telah memperhatikan bahwa kesulitan dalam manajemen jaringan berhubungan erat dengan kompleksitas jaringan; keduanya berada dalam variasi langsung. Metode manajemen jaringan tradisional menjadi tidak memadai atau tidak berkelanjutan untuk mengatasi perubahan dalam jaringan kampus karena alasan-alasan utama ini:

      1. Mode manajemen yang berpusat pada perangkat sudah ketinggalan zaman; personel operasional dan manajemen berjuang dengan beban kerja yang berat dan mengelola ratusan perangkat.
      2. Operasional dan manajemen yang didasarkan pada baris perintah tidak efisien; baris perintah tidak berbentuk grafik, sehingga tidak bisa merefleksikan hubungan hirarkis antar layanan.

3. Tidak ada alat untuk mengelola konfigurasi dan sumber daya yang sedang berjalan, atau untuk mengelola konflik yang terjadi selama sistem berjalan.
4. Informasi kesalahan berdasarkan alarm dan log tidak dapat secara efisien mendukung pencarian kesalahan. Menurut statistik, lebih dari 99% alarm dan log tidak ada artinya.
5. Tidak ada sistem indikator kinerja utama atau alat evaluasi untuk layanan.

c. Keamanan

Data adalah inti dari transformasi digital di seluruh industri, dan juga merupakan kunci persaingan bisnis di masa depan. Di dunia digital saat ini, masalah keamanan yang semakin parah telah mendapatkan perhatian global. Dalam beberapa tahun terakhir, serangan *ransomware* yang terkenal telah menjadi peringatan bagi perusahaan akan potensi kerugian langsung dan serius yang disebabkan oleh kerentanan keamanan. Jaringan kampus terutama menghadapi tantangan keamanan berikut ini:

1. Penggunaan terminal nirkabel yang meluas mengaburkan batas jaringan kampus, membuat metode pertahanan perbatasan tradisional tidak efektif.
2. Penggunaan perangkat IoT yang semakin meningkat secara konstan memperluas jaringan dan meningkatkan permukaan serangan.
3. Serangan jaringan baru, seperti serangan APT, membuat metode pertahanan keamanan tradisional tidak efektif dan tidak berkelanjutan.

Untuk mengatasi masalah-masalah sebelumnya, solusi keamanan jaringan kampus yang baru harus diperkenalkan. Solusi baru ini tidak hanya harus menyediakan pertahanan tanpa batas untuk jaringan kampus di mana-mana di masa depan, tetapi juga harus secara efektif mengidentifikasi dan menangani serangan keamanan yang terus berubah dengan menggunakan metode dan teknologi terbaru.

3. Pandangan Industri Terhadap Jaringan di Dunia Digital

Jaringan kampus yang digerakkan secara otonom digerakkan oleh niat dan menonjol dengan memberikan akses yang sepenuhnya terkonvergensi, dukungan multiservice, dan kualitas tinggi. Jaringan ini juga dilengkapi dengan operasional dan manajemen jaringan otomatis dan cerdas serta keamanan yang tidak dapat dipecahkan, dan arsitektur ekosistem terbuka. Banyak organisasi penentu standar, pemimpin industri, dan *influencer* teknologi akhirnya mencapai konsensus tentang pertanyaan ini.

a. Jaringan Pengemudi Otonom Mungkin Menjadi Solusi Utama

Revolusi industri pertama (1760-1870) mendorong masyarakat manusia dari peradaban pertanian ke peradaban industri. Penggunaan mesin uap secara luas sangat meningkatkan produktivitas, membebaskan manusia dari pekerjaan manual yang berat, mempercepat industri manufaktur, dan pada akhirnya meningkatkan produktivitas secara drastis. Revolusi industri kedua (1870-1950) membuat kita bergeser dari era industri ke era kelistrikan, di mana penggunaan tenaga listrik yang meluas memperluas kemajuan yang dibuat dalam revolusi industri pertama dan

meningkatkan produktivitas di lebih banyak industri. Munculnya tenaga listrik mempercepat transportasi dengan kereta api dan mobil. Hal ini, pada gilirannya, menyebabkan perkembangan pesat industri transportasi dan komunikasi antarmanusia dan antarnegara yang lebih sering. Dengan demikian, terbentuklah sistem sosial internasional global.

Revolusi industri ketiga (1950 hingga sekarang) telah berlangsung hampir 70 tahun, memajukan masyarakat manusia dari era listrik ke era informasi. Era ini telah memperluas kemajuan revolusi industri pertama dan kedua. Khususnya, manufaktur otomatis telah muncul, menggandakan produktivitas di berbagai industri. Di era informasi saat ini, komputer elektronik dan jaringan data digunakan secara luas, sangat memperkaya pekerjaan dan kehidupan kita. Orang bisa berkomunikasi satu sama lain kapan saja dan di mana saja. Masyarakat informasi yang kita tinggali saat ini telah mengarah ke globalisasi, di mana informasi terkini dapat ditransmisikan ke seluruh penjuru dunia dalam hitungan detik.

Saat ini, kita berdiri di puncak revolusi industri keempat yang diwakili oleh AI. TIK baru akan membawa kita dari era informasi ke era intelijen, di mana pada saat itu akan diterapkan secara luas ke semua aspek masyarakat kita. AI, sebagai teknologi tujuan umum (GPT), telah meninggalkan fase pertama, di mana eksplorasi teknologi dan aplikasi AI berlangsung dalam skala kecil. Sekarang berada di fase kedua di mana perkembangan teknologi dan lingkungan sosial bertabrakan. Didorong oleh tabrakan yang terus menerus, AI menemukan penggunaan yang semakin meningkat dalam skenario aplikasi industri.

3. Tugas

a. Pemahaman Jaringan Kampus

1. Bacalah modul pembelajaran kegiatan 1 dan buku Chapter 1: Getting To Know A Campus Network (Bab 1: Mengenal Jaringan Kampus) pada tautan berikut ini https://s.id/je-01. Jika Anda mengalami kesulitan membaca dalam bahasa inggris, silahkan klik kanan pada file Chapter 1, kemudian *Open With Google Docs*, setelah file Chapter 1 muncul dengan versi google docs, pada menu Tools pilih Translate Document ke bahasa Indonesia.
2. Setelah Anda memahami modul ini atau materi Chapter 1 pada buku yang berjudul *Getting To Know A Campus Network*, buatlah penjelasan dalam bentuk video dengan resolusi minimal HD tentang apa yang Anda pahami tentang Jaringan Kampus.

   Catatan: Unsur utama yang harus Anda perhatikan pada video ini adalah suara harus jelas dan ketepatan Anda menjelaskan, selebihnya silahkan buat sekreatif kalian yang penting tidak melanggar hak cipta.
3. Upload video Anda ke https://youtube.com dengan *Visibility Public*.
4. Kumpulkan hasil karya Anda pada tautan berikut ini https://s.id/je-as-01.
5. Setiap mahasiswa wajib memberikan masukan yang positif sehingga dapat membangun pemahaman dan konten teman-teman agar dapat berkembang. Adapun linknya dapat di lihat di list berikut ini https://s.id/je-hs-01.

b. Menentukan Topik Proyek (Proyek Team Base)

Setelah memiliki pemahan tentang Jaringan Kampus, setiap kelompok diminta untuk mentukan topik jaringan kampus yang akan dikerjakan dalam 1 semester kedepan. Adapun langkah-langkahnya sebagai berikut:

1. Setiap kelompok harus memiliki objek atau tempat untuk mengerjakan proyek, bisa dicari secara mandiri atau yang telah ditentukan oleh dosen.
2. Kriteria objek proyek
   a) Jaringan Kampus Perusahaan
   b) Jaringan Kampus Pendidikan
   c) Jaringan Kampus Pemerintahan
   d) Jaringan Kampus Publik
3. Pengumpulan Topik pada tautan berikut ini https://s.id/je-pr-1.

Kegiatan Belajar 2
Keamanan dan Network Desain

1. Sub-Capaian Permbelajaran

a. Mampu memahami trend ancaman jaringan kampus, konsep WAN, dan mampu merancang jaringan dengan pendekatan praktik keamanan terbaik
b. Mampu memahami desain jaringan kampus, merancang topologi secara fisik dan logika, serta manajemen pengalamatan IP, serta mampu nenetukan kebuthan jaringan kampus pada proyek.

2. Pokok Bahasan

a. Kondisi Keamanan Saat Ini

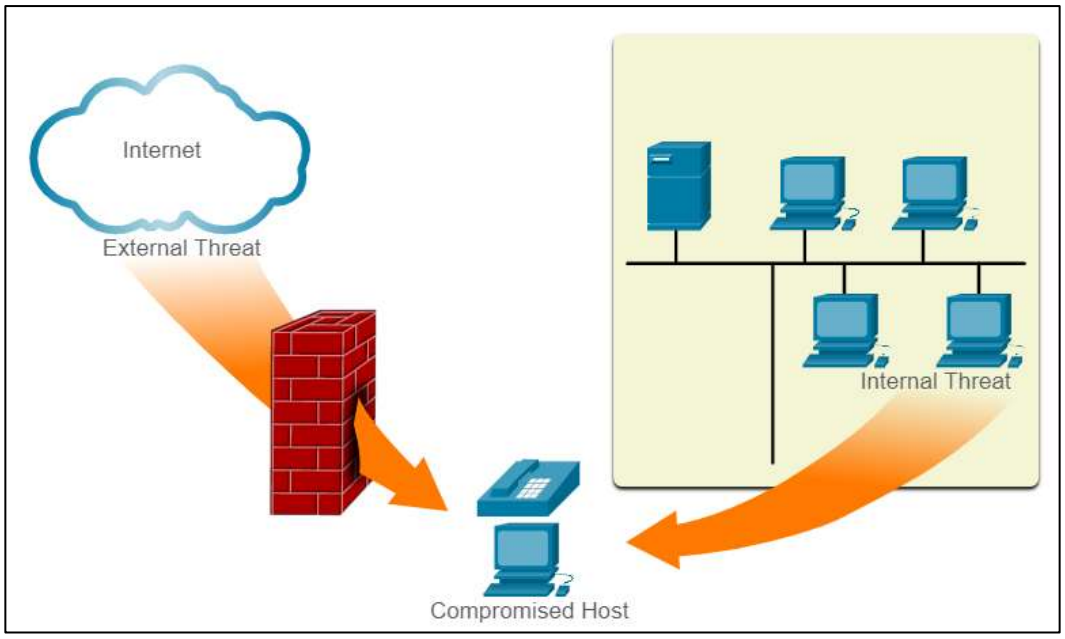
Penjahat dunia maya sekarang memiliki keahlian dan alat yang diperlukan untuk menjatuhkan infrastruktur dan sistem penting. Alat dan teknik mereka terus berkembang. Penjahat siber membawa *malware* ke tingkat kecanggihan dan dampak yang belum pernah terjadi sebelumnya. Mereka menjadi lebih mahir dalam menggunakan teknik siluman dan penghindaran untuk menyembunyikan aktivitas mereka. Penjahat siber mengeksploitasi celah keamanan yang tidak dipertahankan. Pelanggaran keamanan jaringan dapat mengganggu *e-commerce*, menyebabkan hilangnya data bisnis, mengancam privasi orang, dan membahayakan integritas informasi. Pelanggaran ini dapat mengakibatkan hilangnya pendapatan perusahaan, pencurian kekayaan intelektual, tuntutan hukum, dan bahkan dapat mengancam keselamatan publik. Mempertahankan jaringan yang aman memastikan keamanan pengguna jaringan dan melindungi kepentingan komersial. Organisasi membutuhkan individu yang dapat mengenali kecepatan dan skala di mana musuh mengumpulkan dan menyempurnakan persenjataan *cyber* mereka. Semua pengguna harus menyadari istilah keamanan seperti pada tabel 2.

Tabel 2 Istilah Keamanan

Ketentuan Keamanan	Deskripsi
Aset	Segala sesuatu yang bernilai bagi organisasi. Ini mencakup orang, peralatan, sumber daya, dan data.
Kerentanan	Kelemahan dalam sistem, atau desainnya, yang dapat dieksploitasi oleh ancaman.
Ancaman	Potensi bahaya terhadap aset, data, atau fungsionalitas jaringan perusahaan.
Mengeksploitasi	Mekanisme yang memanfaatkan kerentanan.
Mitigasi	Tindakan balasan yang mengurangi kemungkinan atau tingkat keparahan potensi ancaman atau risiko. Keamanan jaringan melibatkan beberapa teknik mitigasi.
Risiko	Kemungkinan ancaman untuk mengeksploitasi kerentanan suatu aset, dengan tujuan mempengaruhi organisasi secara negatif. Risiko diukur dengan menggunakan probabilitas terjadinya suatu peristiwa dan konsekuensinya.

1. Vektor Serangan Jaringan

Vektor serangan adalah jalur di mana pelaku ancaman dapat memperoleh akses ke server, host, atau jaringan. Vektor serangan berasal dari dalam atau luar jaringan perusahaan, seperti yang ditunjukkan pada gambar 2.



Gambar 2 Ancaman dari dalam dan luar

Misalnya, pelaku ancaman dapat menargetkan jaringan melalui internet, untuk mengganggu operasi jaringan dan membuat serangan *denial of service* (DoS). Gambar 2 menunjukkan jaringan ancaman bisa saja berasal dari dalam. Contohnya menghubungkan drive USB yang terinfeksi ke dalam sistem komputer perusahaan. Ancaman internal berpotensi menyebabkan kerusakan yang lebih besar daripada ancaman eksternal karena pengguna internal memiliki akses langsung ke gedung dan perangkat infrastrukturnya. Karyawan mungkin juga memiliki pengetahuan tentang jaringan perusahaan, sumber dayanya, dan data rahasianya. Profesional keamanan jaringan harus mengimplementasikan alat dan menerapkan teknik untuk mengurangi ancaman eksternal dan internal.

2. Kehilangan Data

   Data kemungkinan besar merupakan aset organisasi yang paling berharga. Data organisasi dapat mencakup data penelitian dan pengembangan, data penjualan, data keuangan, data sumber daya manusia dan hukum, data karyawan, data kontraktor, dan data pelanggan. Kehilangan data atau eksfiltrasi data adalah ketika data secara sengaja atau tidak sengaja hilang, dicuri, atau bocor ke dunia luar. Kehilangan data dapat mengakibatkan:

   a. Kerusakan merek dan hilangnya reputasi
   b. Kehilangan keunggulan kompetitif
   c. Kehilangan pelanggan
   d. Kehilangan pendapatan
   e. Litigasi/tindakan hukum yang mengakibatkan denda dan hukuman perdata

f. Biaya dan upaya yang signifikan untuk memberi tahu pihak-pihak yang terkena dampak dan pulih dari pelanggaran

Vektor kehilangan data yang umum ditampilkan dalam tabel 3.

Vektor Kehilangan Data	Deskripsi
Email/Jejaring Sosial	Pesan email atau IM yang disadap bisa ditangkap dan mengungkapkan informasi rahasia.
Perangkat yang Tidak Terenkripsi	Jika data tidak disimpan menggunakan algoritma enkripsi, maka pencuri dapat mengambil data rahasia yang berharga.
Perangkat Penyimpanan Cloud	Data sensitif dapat hilang jika akses ke cloud dikompromikan karena pengaturan keamanan yang lemah.
Media yang Dapat Dilepas	Salah satu risikonya adalah bahwa seorang karyawan bisa melakukan transfer data yang tidak sah ke drive USB. Risiko lainnya adalah, drive USB yang berisi data perusahaan yang berharga bisa hilang.
Hard Copy	Data rahasia harus dihancurkan ketika tidak lagi diperlukan.
Kontrol Akses yang Tidak Tepat	Kata sandi atau kata sandi lemah yang telah dikompromikan dapat memberikan akses mudah kepada pelaku ancaman ke data perusahaan.

Profesional keamanan jaringan harus melindungi data organisasi. Berbagai kontrol Pencegahan Kehilangan Data harus diimplementasikan yang menggabungkan langkah-langkah strategis, operasional dan taktis.

b. Pelaku Ancaman

1. Hacker

Peretas atau biasa disebut *Hacker* adalah istilah umum yang digunakan untuk menggambarkan pelaku ancaman. Awalnya istilah ini merujuk pada seseorang yang ahli komputer yang terampil seperti programmer dan peretasan. Istilah ini kemudian berkembang menjadi seperti yang kita kenal sekarang. Seperti yang ditunjukkan pada tabel 4, istilah *white hat hacker, black hat hacker,* dan *gray hat hacker* sering digunakan untuk menggambarkan jenis peratas.

Tabel 3 Tipe Peretas

Tipe Peretas	Deskripsi
Peretas Topi Putih / *white hat hacker*	Ini adalah peretas etis yang menggunakan keterampilan pemrograman mereka untuk tujuan yang baik, etis, dan legal. *White hat hacker* dapat melakukan tes penetrasi jaringan dalam upaya untuk mengkompromikan jaringan dan sistem dengan menggunakan pengetahuan mereka tentang sistem keamanan komputer untuk menemukan kerentanan jaringan. Kerentanan keamanan dilaporkan kepada pengembang untuk diperbaiki sebelum kerentanan tersebut dapat dieksploitasi.
Peretas Topi Abu-abu / *black hat hacker*	Ini adalah individu yang melakukan kejahatan dan melakukan hal-hal yang bisa dibilang tidak etis, tetapi tidak untuk keuntungan pribadi atau menyebabkan kerusakan. Peretas topi abu-abu dapat mengungkapkan kerentanan kepada organisasi yang terkena dampak setelah membahayakan jaringan mereka.

Peretas Topi Hitam / *black hat hacker*	Ini adalah penjahat tidak etis yang membahayakan keamanan komputer dan jaringan untuk keuntungan pribadi, atau untuk alasan jahat, seperti menyerang jaringan.

2. Evolusi Hacker

Peretasan dimulai pada tahun 1960-an dengan *phone freaking*, atau *phreaking*, yang mengacu pada penggunaan frekuensi audio untuk memanipulasi sistem telepon. Pada saat itu, sakelar telepon menggunakan berbagai nada untuk menunjukkan fungsi yang berbeda. Peretas awal menyadari bahwa dengan meniru nada menggunakan peluit, mereka dapat mengeksploitasi sakelar telepon untuk melakukan panggilan jarak jauh gratis. Pada pertengahan 1980-an, modem *dial-up* komputer digunakan untuk menghubungkan komputer ke jaringan. Hacker menulis program "*war dialing*" yang memutar setiap nomor telepon di area tertentu untuk mencari komputer. Ketika komputer ditemukan, program peretas kata sandi digunakan untuk mendapatkan akses.

Tabel 4 Istilah Peretasan

Istilah Peretasan	Deskripsi
Script Kiddies	Ini adalah remaja atau peretas yang tidak berpengalaman yang menjalankan skrip, alat, dan eksploitasi yang ada, untuk menyebabkan kerusakan, tetapi biasanya tidak untuk mendapatkan keuntungan.
Pialang Kerentanan	Mereka ini biasanya peretas topi abu-abu yang berusaha menemukan eksploitasi dan melaporkannya ke vendor, terkadang untuk mendapatkan hadiah atau imbalan.
Hacktivists	Ini adalah peretas topi abu-abu yang memprotes organisasi atau pemerintah secara publik dengan memposting artikel, video, membocorkan informasi sensitif, dan melakukan serangan jaringan.
Penjahat dunia maya	Mereka adalah peretas topi hitam yang bekerja sendiri atau bekerja untuk organisasi kejahatan siber besar.
Disponsori Negara	Mereka adalah peretas topi putih atau topi hitam yang mencuri rahasia pemerintah, mengumpulkan intelijen, dan menyabotase jaringan. Target mereka adalah pemerintah asing, kelompok teroris, dan perusahaan. Sebagian besar negara di dunia berpartisipasi sampai tingkat tertentu dalam peretasan yang disponsori negara.

c. Alat Pelaku Ancaman

Untuk mengeksploitasi kerentanan, pelaku ancaman harus memiliki teknik atau alat. Selama bertahun-tahun, alat serangan telah menjadi lebih canggih, dan sangat otomatis. Alat-alat baru ini membutuhkan pengetahuan teknis yang lebih sedikit untuk diterapkan.

Peretasan etis melibatkan berbagai jenis alat yang digunakan untuk menguji jaringan dan menjaga keamanan datanya. Untuk memvalidasi keamanan jaringan dan sistemnya, banyak alat pengujian penetrasi jaringan telah dikembangkan. Sangat disayangkan bahwa banyak dari alat ini dapat digunakan oleh peretas topi hitam untuk eksploitasi. Peretas topi hitam juga telah menciptakan banyak alat peretasan. Tools ini dibuat secara eksplisit untuk alasan yang jahat. *White hat hacker* juga harus tahu cara menggunakan *tool-tool* ini ketika melakukan tes penetrasi jaringan. Tabel 5 ini menyoroti kategori alat uji penetrasi yang umum. Perhatikan bagaimana

beberapa alat digunakan oleh *white hat* dan *black hat*. Perlu diingat bahwa daftar ini tidak lengkap karena alat baru selalu dikembangkan.

Tabel 5 Alat Pengujian Penetrasi

Alat Pengujian Penetrasi	Deskripsi
Pemecah Kata Sandi	Alat peretas kata sandi sering disebut sebagai alat pemulihan kata sandi dan dapat digunakan untuk memecahkan atau memulihkan kata sandi. Hal ini dilakukan baik dengan menghapus kata sandi asli, setelah melewati enkripsi data, atau dengan penemuan kata sandi secara langsung. Pemecah kata sandi berulang kali membuat tebakan untuk memecahkan kata sandi. Contoh alat peretas kata sandi termasuk John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, dan Medusa.
Alat Peretasan Nirkabel	Alat peretasan nirkabel digunakan untuk meretas jaringan nirkabel secara sengaja untuk mendeteksi kerentanan keamanan. Contoh alat hacking nirkabel termasuk Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, dan NetStumbler.
Pemindaian Jaringan dan Alat Peretasan	Alat pemindaian jaringan digunakan untuk menyelidiki perangkat jaringan, server, dan host untuk port TCP atau UDP terbuka. Contoh alat pemindaian termasuk Nmap, SuperScan, Angry IP Scanner, dan NetScanTools.
Alat Pembuatan Paket	Alat-alat ini digunakan untuk menyelidiki dan menguji ketahanan *firewall* dengan menggunakan paket-paket palsu yang dibuat secara khusus. Contohnya termasuk Hping, Scapy, Socat, Yersinia, Netcat, Nping, dan Nemesis.
Packet Sniffers	Tools ini digunakan untuk menangkap dan menganalisa paket dalam LAN Ethernet tradisional atau WLAN. Tools termasuk Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, dan SSLstrip.
Detektor Rootkit	Ini adalah pemeriksa integritas direktori dan file yang digunakan oleh white hats untuk mendeteksi root kit yang terinstal. Contoh tool termasuk AIDE, Netfilter, dan PF: OpenBSD Packet Filter.
Fuzzer untuk Mencari Kerentanan	Fuzzer adalah alat yang digunakan oleh pelaku ancaman untuk menemukan kerentanan keamanan komputer. Contoh fuzzer termasuk Skipfish, Wapiti, dan W3af.
Alat Forensik	Alat-alat ini digunakan oleh white hat hacker untuk mengendus jejak bukti yang ada di komputer. Contoh alatnya antara lain Sleuth Kit, Helix, Maltego, dan Encase.
Debugger	Alat-alat ini digunakan oleh black hats untuk merekayasa balik file biner ketika menulis eksploitasi. Mereka juga digunakan oleh white hats ketika menganalisis *malware*. Alat-alat debugging termasuk GDB, WinDbg, IDA Pro, dan Immunity Debugger.
Meretas Sistem Operasi	Ini adalah sistem operasi yang dirancang khusus yang dimuat dengan alat yang dioptimalkan untuk peretasan. Contoh sistem operasi peretasan yang dirancang khusus termasuk Kali Linux, Knoppix, BackBox Linux.
Alat Enkripsi	Alat enkripsi menggunakan skema algoritma untuk menyandikan data untuk mencegah akses yang tidak sah ke data terenkripsi. Contoh dari tool ini termasuk VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN, dan Stunnel.
Alat Eksploitasi Kerentanan	Alat-alat ini mengidentifikasi apakah host jarak jauh rentan terhadap serangan keamanan. Contoh alat eksploitasi

Alat Pengujian Penetrasi	Deskripsi
	kerentanan termasuk Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, dan Netsparker.
Pemindai Kerentanan	Alat-alat ini memindai jaringan atau sistem untuk mengidentifikasi port terbuka. Mereka juga dapat digunakan untuk memindai kerentanan yang diketahui dan memindai VM, perangkat BYOD, dan basis data klien. Contoh alat termasuk Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT, dan Open VAS.

Pelaku ancaman dapat menggunakan alat serangan yang disebutkan sebelumnya, atau kombinasi alat, untuk membuat serangan. Tabel 6 ini menampilkan jenis serangan yang umum. Namun, daftar serangan tidak lengkap karena kerentanan serangan baru terus ditemukan.

Tabel 6 Tipe Serangan

Tipe Serangan	Deskripsi
Serangan Penyadapan	Ini adalah ketika pelaku ancaman menangkap dan "mendengarkan" lalu lintas jaringan. Serangan ini juga disebut sebagai sniffing atau snooping.
Serangan Modifikasi Data	Jika pelaku ancaman telah menangkap lalu lintas perusahaan, mereka dapat mengubah data dalam paket tanpa sepengetahuan pengirim atau penerima.
Serangan Spoofing Alamat IP	Seorang pelaku ancaman membuat paket IP yang tampaknya berasal dari alamat yang valid di dalam intranet perusahaan.
Serangan Berbasis Kata Sandi	Jika pelaku ancaman menemukan akun pengguna yang valid, pelaku ancaman memiliki hak yang sama dengan pengguna yang sebenarnya. Pelaku ancaman bisa menggunakan akun yang valid itu untuk mendapatkan daftar pengguna lain, informasi jaringan, mengubah konfigurasi server dan jaringan, dan memodifikasi, mengubah rute, atau menghapus data.
Penolakan Serangan Layanan	Serangan DoS mencegah penggunaan normal komputer atau jaringan oleh pengguna yang valid. Serangan DoS dapat membanjiri komputer atau seluruh jaringan dengan lalu lintas sampai terjadi shutdown karena kelebihan beban. Serangan DoS juga dapat memblokir lalu lintas, yang mengakibatkan hilangnya akses ke sumber daya jaringan oleh pengguna yang berwenang.
Serangan *Man-in-the-Middle*	Serangan ini terjadi ketika pelaku ancaman telah memposisikan diri mereka di antara sumber dan tujuan. Mereka sekarang dapat secara aktif memantau, menangkap, dan mengendalikan komunikasi secara transparan.
Serangan Kunci yang Dikompromikan	Jika pelaku ancaman mendapatkan kunci rahasia, kunci tersebut disebut sebagai compromised key. Kunci yang dikompromikan dapat digunakan untuk mendapatkan akses ke komunikasi yang aman tanpa pengirim atau penerima menyadari serangan tersebut.
Serangan Sniffer	Sniffer adalah aplikasi atau perangkat yang dapat membaca, memantau, dan menangkap pertukaran data jaringan dan membaca paket jaringan. Jika paket tidak dienkripsi, sniffer menyediakan tampilan penuh dari data di dalam paket.

d. *Malware*

Berbagai jenis *malware* yang digunakan peretas untuk mendapatkan akses ke perangkat akhir. Perangkat akhir sangat rentan terhadap serangan *malware*. Penting untuk mengetahui tentang *malware* karena pelaku ancaman mengandalkan pengguna untuk menginstal *malware* dalam membantu mengeksploitasi celah keamanan.

1. Virus dan Trojan Horses

   Jenis *malware* komputer yang pertama dan paling umum adalah virus. Virus memerlukan tindakan manusia untuk menyebar dan menginfeksi komputer lain. Misalnya, virus dapat menginfeksi komputer ketika korban membuka lampiran email, membuka file pada USB drive, atau mengunduh file. Virus bersembunyi dengan melampirkan dirinya pada kode komputer, perangkat lunak, atau dokumen di komputer. Ketika dibuka, virus mengeksekusi dan menginfeksi komputer. Virus dapat melakukan hal-hal berikut ini:

   a. Mengubah, merusak, menghapus file, atau menghapus seluruh drive.
   b. Menyebabkan masalah booting komputer, dan merusak aplikasi.
   c. Menangkap dan mengirim informasi sensitif kepada pelaku ancaman.
   d. Mengakses dan menggunakan akun email untuk menyebar.
   e. Tidak aktif sampai dipanggil oleh pelaku ancaman.

   Pelaku ancaman menggunakan Trojan horse untuk mengkompromikan host. Trojan horse adalah program yang terlihat berguna tetapi juga membawa kode berbahaya. Trojan horse sering kali disediakan dengan program *online* gratis seperti *game* komputer. Pengguna yang tidak curiga mengunduh dan menginstal *game*, bersama dengan Trojan horse. Ada beberapa jenis Trojan horse seperti yang dijelaskan dalam tabel 7.

Tabel 7 Tipe Trojan Horse

Tipe of Trojan Horse	Deskripsi
Akses jarak jauh	Trojan horse memungkinkan akses jarak jauh yang tidak sah.
Pengiriman data	Trojan horse menyediakan data sensitif kepada pelaku ancaman, seperti kata sandi.
Destruktif	Trojan horse merusak atau menghapus file.
Proxy	Trojan horse akan menggunakan komputer korban sebagai perangkat sumber untuk melancarkan serangan dan melakukan kegiatan ilegal lainnya.
FTP	Trojan horse memungkinkan layanan transfer file yang tidak sah pada perangkat akhir.
Disabler perangkat lunak keamanan	Trojan horse menghentikan program antivirus atau *firewall* agar tidak berfungsi.
Penolakan Layanan (DoS)	Trojan horse memperlambat atau menghentikan aktivitas jaringan.
Keylogger	Trojan horse secara aktif mencoba untuk mencuri informasi rahasia, seperti nomor kartu kredit, dengan merekam goresan kunci yang dimasukkan ke dalam formulir web.

2. Jenis *Malware* Lainnya

   Selain Trojan Horse, terdapat berbagai jenis *malware* lainnya yang dapat di lihat pada tabel 8.

Tabel 8 Jenis-jenis *Malware*

Malware	**Deskripsi**
Adware	*Adware* biasanya didistribusikan dengan mengunduh perangkat lunak *online*. Adware dapat menampilkan iklan yang tidak diminta dengan menggunakan jendela pop-up browser web, *toolbar* baru, atau secara tak terduga mengarahkan halaman web ke situs web yang berbeda. Jendela pop-up mungkin sulit dikendalikan karena jendela baru dapat muncul lebih cepat daripada yang dapat ditutup oleh pengguna.
Ransomware	*Ransomware* biasanya menolak akses pengguna ke file mereka dengan mengenkripsi file dan kemudian menampilkan pesan yang menuntut tebusan untuk kunci dekripsi. Pengguna yang tidak memiliki cadangan terbaru harus membayar tebusan untuk mendekripsi file mereka. Pembayaran biasanya dilakukan menggunakan transfer kawat atau mata uang kripto seperti Bitcoin.
Rootkit	Rootkit digunakan oleh pelaku ancaman untuk mendapatkan akses tingkat akun administrator ke komputer. Rootkit sangat sulit dideteksi karena mereka dapat mengubah *firewall*, proteksi antivirus, file sistem, dan bahkan perintah OS untuk menyembunyikan keberadaannya. Rootkit dapat memberikan backdoor kepada pelaku ancaman yang memberi mereka akses ke PC, dan memungkinkan mereka untuk mengunggah file, dan menginstal perangkat lunak baru untuk digunakan dalam serangan DDoS. Alat penghapus rootkit khusus harus digunakan untuk menghapusnya, atau mungkin diperlukan instalasi ulang OS secara lengkap.
Spyware	Mirip dengan *adware*, tetapi digunakan untuk mengumpulkan informasi tentang pengguna dan mengirimkannya ke pelaku ancaman tanpa persetujuan pengguna. *Spyware* bisa menjadi ancaman rendah, mengumpulkan data penjelajahan, atau bisa juga menjadi ancaman tinggi yang menangkap informasi pribadi dan keuangan.
Worm	Worm adalah program yang mereplikasi diri sendiri yang menyebar secara otomatis tanpa tindakan pengguna dengan mengeksploitasi kerentanan dalam perangkat lunak yang sah. Worm menggunakan jaringan untuk mencari korban lain dengan kerentanan yang sama. Tujuan worm biasanya untuk memperlambat atau mengganggu operasi jaringan.

e. Serangan Jaringan

Seperti yang telah anda pelajari, ada banyak jenis *malware* yang bisa digunakan hacker. Tetapi ini bukan satu-satunya cara mereka bisa menyerang jaringan, atau bahkan organisasi. Ketika *malware* dikirimkan dan diinstal, muatannya dapat digunakan untuk menyebabkan berbagai serangan yang berhubungan dengan jaringan. Untuk memitigasi serangan, sangat berguna untuk memahami jenis-jenis serangan. Dengan mengkategorikan serangan jaringan, maka dimungkinkan untuk mengatasi jenis serangan daripada serangan individual.

1. Serangan Pengintaian

   Pengintaian adalah pengumpulan informasi. Hal ini dianalogikan seperti pencuri yang sedang mensurvei suatu lingkungan dengan pergi dari pintu ke pintu berpura-pura menjual sesuatu. Apa yang sebenarnya dilakukan pencuri adalah mencari rumah yang rentan untuk dibobol, seperti tempat tinggal yang tidak dihuni, tempat tinggal dengan pintu atau jendela yang mudah dibuka, dan tempat tinggal tanpa sistem keamanan atau kamera keamanan. Pelaku ancaman menggunakan serangan pengintaian untuk melakukan penemuan dan pemetaan sistem, layanan, atau kerentanan yang tidak sah. Serangan pengintaian mendahului serangan akses atau serangan DoS. Beberapa teknik yang digunakan oleh pelaku ancaman jahat untuk melakukan serangan pengintaian seperti dijelaskan dalam tabel 9.

   Tabel 9 Teknik Serangan

Teknik	Deskripsi
Melakukan kueri informasi dari target	Pelaku ancaman mencari informasi awal tentang target. Berbagai alat bantu dapat digunakan, termasuk pencarian Google, situs web organisasi, whois, dan banyak lagi.
Memulai sapuan ping dari jaringan target	Permintaan informasi biasanya mengungkapkan alamat jaringan target. Pelaku ancaman sekarang bisa memulai ping sweep untuk menentukan alamat IP mana yang aktif.
Memulai pemindaian port dari alamat IP yang aktif	Ini digunakan untuk menentukan port atau layanan mana yang tersedia. Contoh port scanner termasuk Nmap, SuperScan, Angry IP Scanner, dan NetScanTools.
Jalankan pemindai kerentanan	Ini adalah untuk menanyakan port yang teridentifikasi untuk menentukan jenis dan versi aplikasi dan sistem operasi yang berjalan pada host. Contoh alat termasuk Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT, dan Open VAS.
Menjalankan alat eksploitasi	Aktor ancaman sekarang mencoba menemukan layanan rentan yang dapat dieksploitasi. Berbagai alat eksploitasi kerentanan ada termasuk Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, dan Netsparker.

2. Serangan Akses

   Serangan akses mengeksploitasi kerentanan yang diketahui dalam layanan otentikasi, layanan FTP, dan layanan web. Tujuan dari jenis serangan ini adalah untuk mendapatkan akses masuk ke akun web, database rahasia, dan informasi sensitif lainnya.

   Pelaku ancaman menggunakan serangan akses pada perangkat jaringan dan komputer untuk mengambil data, mendapatkan akses, atau untuk meningkatkan hak akses ke status administrator.

   a. Serangan Kata Sandi

Dalam serangan kata sandi, pelaku ancaman mencoba untuk menemukan kata sandi sistem penting menggunakan berbagai metode. Serangan kata sandi sangat umum terjadi dan dapat diluncurkan menggunakan berbagai alat peretas kata sandi.

b. Serangan *Spoofing*

Dalam serangan *spoofing*, perangkat pelaku ancaman mencoba untuk menyamar sebagai perangkat lain dengan memalsukan data. Serangan spoofing yang umum termasuk IP *spoofing*, MAC *spoofing*, dan DHCP *spoofing*.

c. Eksploitasi kepercayaan

Dalam serangan eksploitasi kepercayaan, pelaku ancaman menggunakan hak istimewa yang tidak sah untuk mendapatkan akses ke sistem, yang mungkin membahayakan target. Klik Play pada gambar untuk melihat contoh eksploitasi kepercayaan.

d. Pengalihan port

Dalam serangan pengalihan port, pelaku ancaman menggunakan sistem yang telah disusupi sebagai basis untuk serangan terhadap target lain. Contoh pada gambar menunjukkan pelaku ancaman menggunakan SSH (port 22) untuk menyambung ke Host A. Host A dipercaya oleh Host B dan, oleh karena itu, pelaku ancaman dapat menggunakan Telnet (port 23) untuk mengaksesnya.

e. Serangan *man-in-the-middle*

Dalam serangan *man-in-the-middle*, pelaku ancaman diposisikan di antara dua entitas yang sah untuk membaca atau memodifikasi data yang lewat di antara kedua pihak. Gambar ini menampilkan contoh serangan man-in-the-middle.

f. Serangan *buffer overflow*

Dalam serangan *buffer overflow*, pelaku ancaman mengeksploitasi memori buffer dan membanjirinya dengan nilai yang tidak terduga. Hal ini biasanya membuat sistem tidak dapat beroperasi, menciptakan serangan DoS. Gambar di atas menunjukkan bahwa pelaku ancaman mengirimkan banyak paket ke korban dalam upaya untuk meluap-luap buffer korban.

3. Serangan Rekaya Sosial

Rekayasa sosial adalah serangan akses yang mencoba memanipulasi individu untuk melakukan tindakan atau membocorkan informasi rahasia. Beberapa teknik rekayasa sosial dilakukan secara langsung sementara yang lain mungkin menggunakan telepon atau internet. Para perekayasa sosial sering mengandalkan kesediaan orang untuk membantu. Mereka juga memangsa kelemahan orang. Misalnya, seorang pelaku ancaman bisa menelepon karyawan yang berwenang dengan masalah mendesak yang membutuhkan akses jaringan segera. Si pelaku ancaman bisa menarik kesombongan karyawan tersebut, meminta otoritas dengan menggunakan teknik menjatuhkan nama, atau menarik keserakahan karyawan tersebut. Informasi tentang teknik rekayasa sosial ditunjukkan dalam tabel 10.

Tabel 10 Rekayasa Serangan Sosial

Serangan Rekayasa Sosial	Deskripsi
Pretexting	Pelaku ancaman berpura-pura membutuhkan data pribadi atau keuangan untuk mengonfirmasi identitas penerima.
Phishing	Pelaku ancaman mengirimkan email penipuan yang disamarkan seolah-olah berasal dari sumber yang sah dan tepercaya untuk mengelabui penerima agar menginstal *malware* di perangkat mereka, atau untuk membagikan informasi pribadi atau keuangan.
Spear phishing	Pelaku ancaman menciptakan serangan phishing yang ditargetkan yang disesuaikan untuk individu atau organisasi tertentu.
Spam	Juga dikenal sebagai junk mail, ini adalah email yang tidak diminta yang sering kali berisi tautan berbahaya, *malware*, atau konten yang menipu.
Sesuatu untuk Sesuatu	Kadang-kadang disebut "Quid pro quo", ini adalah ketika pelaku ancaman meminta informasi pribadi dari suatu pihak dengan imbalan sesuatu seperti hadiah.
Baiting	Seorang pelaku ancaman meninggalkan *flash drive* yang terinfeksi *malware* di lokasi umum. Seorang korban menemukan *flash drive* tersebut dan tanpa curiga memasukkannya ke dalam laptop mereka, tanpa sengaja menginstal *malware*.
Peniruan	Jenis serangan ini adalah di mana pelaku ancaman berpura-pura menjadi seseorang yang bukan dirinya untuk mendapatkan kepercayaan dari korban.
Tailgating	Di sinilah pelaku ancaman dengan cepat mengikuti orang yang berwenang ke lokasi yang aman untuk mendapatkan akses ke area yang aman.
Shoulder surfing	Di sinilah pelaku ancaman secara tidak mencolok melihat dari balik bahu seseorang untuk mencuri kata sandi atau informasi lainnya.
Dumpster diving	Di sinilah pelaku ancaman mengobrak-abrik tempat sampah untuk menemukan dokumen rahasia.

4. Serangan DoS dan DDoS

Serangan *Denial of Service* (DoS) menciptakan semacam gangguan layanan jaringan kepada pengguna, perangkat, atau aplikasi. Jumlah Lalu Lintas yang berlebihan dimana pelaku ancaman mengirimkan data dalam jumlah yang sangat besar dengan kecepatan yang tidak dapat ditangani oleh jaringan, host, atau aplikasi. Hal ini menyebabkan transmisi dan waktu respons melambat. Hal ini juga dapat membuat perangkat atau layanan menjadi *crash*. Paket yang diformat dengan Jahat dimana pelaku ancaman mengirimkan paket yang diformat dengan jahat ke host atau aplikasi dan penerima tidak dapat menanganinya. Hal ini menyebabkan perangkat penerima berjalan sangat lambat atau *crash*.

a. DoS *Attack*

Serangan DoS merupakan risiko besar karena mengganggu komunikasi dan menyebabkan kerugian waktu dan uang yang signifikan. Serangan ini relatif mudah dilakukan, bahkan oleh pelaku ancaman yang tidak terampil.

b. DDoS Attack

Serangan DoS Terdistribusi (DDoS) mirip dengan serangan DoS, tetapi berasal dari beberapa sumber yang terkoordinasi. Misalnya, pelaku ancaman membangun jaringan host yang terinfeksi, yang dikenal sebagai zombie. Pelaku ancaman menggunakan sistem *command and control* (CnC) untuk mengirim pesan kontrol ke zombie. Zombie secara konstan memindai dan menginfeksi lebih banyak host dengan *malware* bot. *Malware* bot dirancang untuk menginfeksi host, menjadikannya zombie yang dapat berkomunikasi dengan sistem CnC. Kumpulan zombie disebut botnet. Ketika sudah siap, pelaku ancaman menginstruksikan sistem CnC untuk membuat botnet zombie melakukan serangan DDoS.

f. Kerentanan dan Ancaman IP

IP tidak memvalidasi apakah alamat IP sumber yang terdapat dalam sebuah paket benar-benar berasal dari sumber tersebut. Karena alasan ini, pelaku ancaman dapat mengirim paket menggunakan alamat IP sumber palsu. Pelaku ancaman juga dapat merusak bidang-bidang lain dalam header IP untuk melakukan serangan mereka. Analis keamanan harus memahami berbagai bidang yang berbeda dalam header IPv4 dan IPv6. Beberapa serangan terkait IP yang lebih umum ditunjukkan dalam tabel 11.

Tabel 11 Teknik Serangan IP

Teknik Serangan IP	Deskripsi
ICMP *attacks*	ICMP *attacks*
Amplification and reflection attacks	Pelaku ancaman berusaha mencegah pengguna yang sah untuk mengakses informasi atau layanan menggunakan serangan DoS dan DDoS.
Address spoofing attacks	Pelaku ancaman memalsukan alamat IP sumber dalam paket IP untuk melakukan blind spoofing atau non-blind spoofing.
Man-in-the-middle attack (MITM)	Pelaku ancaman memposisikan diri mereka di antara sumber dan tujuan untuk memantau, menangkap, dan mengontrol komunikasi secara transparan. Mereka bisa menguping dengan memeriksa paket yang ditangkap, atau mengubah paket dan meneruskannya ke tujuan aslinya.
Session hijacking	Pelaku ancaman mendapatkan akses ke jaringan fisik, dan kemudian menggunakan serangan MITM untuk membajak sesi.

Serangan ICMP merupakan serangan yang dilakukan oleh pelaku ancaman menggunakan ICMP untuk serangan pengintaian dan pemindaian. Mereka dapat meluncurkan serangan pengumpulan informasi untuk memetakan topologi jaringan, menemukan host mana yang aktif (dapat dijangkau), mengidentifikasi sistem operasi host (sidik jari OS), dan menentukan status *firewall*. Pelaku ancaman juga menggunakan ICMP untuk serangan DoS. Jaringan harus memiliki penyaringan daftar kontrol akses (ACL) ICMP yang ketat di tepi jaringan untuk menghindari probing ICMP dari internet. Analis keamanan harus bisa mendeteksi serangan yang berhubungan dengan ICMP dengan melihat lalu lintas yang ditangkap dan file

log. Dalam kasus jaringan besar, perangkat keamanan seperti *firewall* dan sistem deteksi intrusi (IDS) mendeteksi serangan tersebut dan menghasilkan peringatan kepada analis keamanan. Pesan-pesan ICMP umum yang menarik bagi pelaku ancaman tercantum dalam tabel 12.

Pesan ICMP yang digunakan oleh Peretas	Deskripsi
ICMP *echo request and echo reply*	Ini digunakan untuk melakukan verifikasi host dan serangan DoS.
ICMP *unreachable*	Ini digunakan untuk melakukan pengintaian jaringan dan serangan pemindaian.
ICMP *mask reply*	Ini digunakan untuk memetakan jaringan IP internal.
ICMP *redirects*	Ini digunakan untuk memikat host target agar mengirimkan semua lalu lintas melalui perangkat yang disusupi dan menciptakan serangan MITM.
ICMP *Router discovery*	Ini digunakan untuk menyuntikkan entri rute palsu ke dalam tabel *routing* host target.

g. Hierarkis Jaringan

Dunia digital kita sedang berubah. Kemampuan untuk mengakses internet dan jaringan enterprise tidak lagi terbatas pada kantor fisik, lokasi geografis, atau zona waktu. Dalam tempat kerja global saat ini, karyawan dapat mengakses sumber daya dari mana saja di dunia dan informasi harus tersedia pada setiap saat, dan pada perangkat mana pun. Persyaratan ini mendorong kebutuhan untuk membangun jaringan generasi berikutnya yang aman, dapat diandalkan, dan selalu tersedia. Jaringan generasi berikutnya ini tidak hanya mampu mendukung ekspetasi dan peralatan masa kini, tetapi juga harus mampu mengintegrasi platform lama. Bisnis semakin mengandalkan infrastruktur jaringan mereka untuk menyediakan layanan yang sangat penting. Seiring bisnis tumbuh dan berkembang, mereka mempekerjakan lebih banyak karyawan, membuka cabang kantor, dan berekspansi ke pasar global. Perubahan ini secara langsung mempengaruhi persyaratan dari sebuah jaringan yang harus mampu diskalakan untuk memenuhi kebutuhan bisnis.

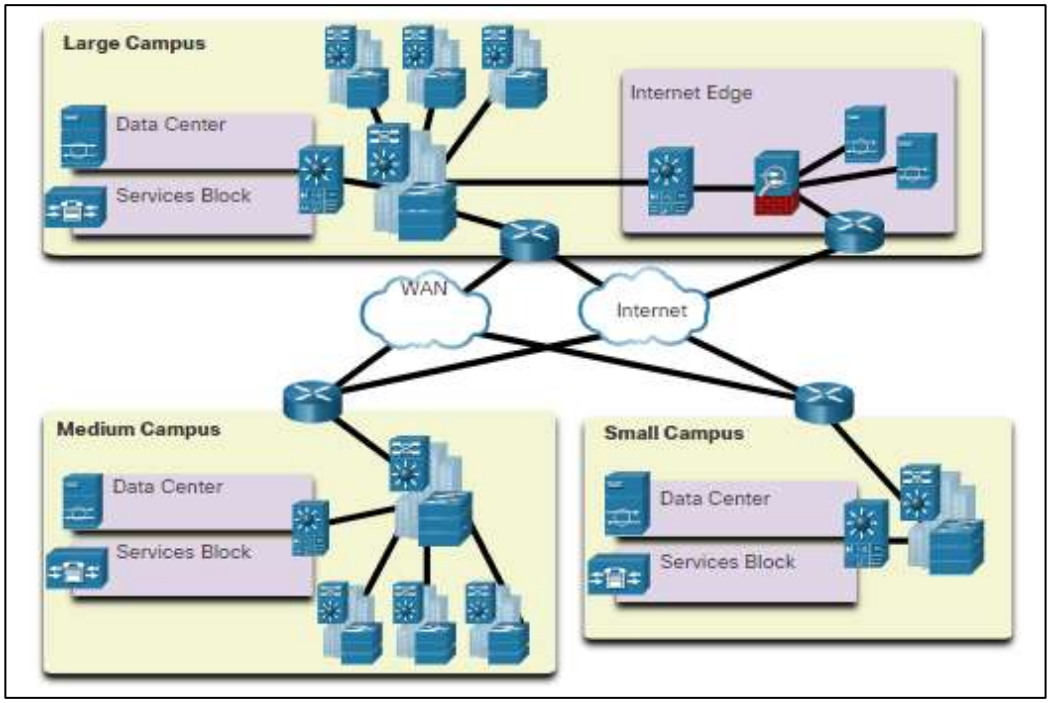
Sebuah jaringan harus mendukung pertukaran dari berbagai jenis *traffic* jaringan, termasuk file data, email, IP telepon, dan aplikasi video untuk berbagai unit bisnis. Semua jaringan enterprise harus mampu melakukan hal berikut :

1. Mendukung aplikasi penting.
2. Mendukung *traffic* jaringan terkonvergensi.
3. Mendukung beragam kebutuhan bisnis.
4. Menyediakan control administratif terpusat.

LAN adalah infrastruktur jaringan yang menyediakan akses pada layanan komunikasi jaringan dan sumber daya untuk pengguna dan perangkat. Pengguna dan perangkat mungkin tersebar di satu lantai atau gedung. Anda membuat jaringan kampus dengan menghubungkan sekelompok LAN yang tersebar di area geografis kecil. Desain jaringan kampus termasuk jaringan kecil yang menggunakan *switch* LAN tunggal, hingga jaringan yang sangat besar dengan ribuan koneksi.

a. Jaringan *Switched* Tanpa Batasan

Dengan meningkatnya tuntutan jaringan konvergen, jaringan harus dikembangkan dengan pendekatan arsitektur yang menanamkan kecerdasan, menyederhanakan operasi, dan dapat diskalakan untuk memenuhi tuntutan masa depan. Salah satu perkembangan terbaru dalam desain jaringan adalah Cisco Borderless Network. Cisco Borderless Network adalah arsitektur jaringan yang menggabungkan inovasi dan desain. Hal ini memungkinkan organisasi untuk mendukung jaringan tanpa batasan yang dapat menghubungkan siapa saja, di mana saja, kapan saja, di perangkat apa saja, dengan aman, andal, dan mulus. Arsitektur ini dirancang untuk mengatasi tantangan IT dan bisnis, seperti mendukung jaringan konvergen dan mengubah pola kerja. Cisco Borderless Network menyediakan kerangka kerja untuk menyatukan akses kabel dan nirkabel, termasuk kebijakan, kontrol akses, dan manajemen kinerja di berbagai jenis perangkat yang berbeda. Dengan menggunakan arsitektur ini, jaringan tanpa batasan, yang ditunjukkan pada gambar, dibangun di atas infrastruktur hierarkis dari perangkat keras yang dapat diskalakan dan tangguh.



Gambar 3 Cisco Borderless Network

Dengan menggabungkan infrastruktur perangkat keras ini dengan solusi perangkat lunak berbasis kebijakan, Cisco Borderless Network menyediakan dua set layanan utama yaitu layanan jaringan, dan layanan pengguna dan layanan *endpoint* di bawah payung solusi manajemen terintegrasi. Ini memungkinkan elemen jaringan yang berbeda untuk bekerja bersama, dan memungkinkan pengguna untuk mengakses sumber daya dari mana saja, kapan saja, sambil memberikan optimalisasi, skalabilitas, dan keamanan.

b. Hierarki dalam Jaringan *Switched* Tanpa Batasan

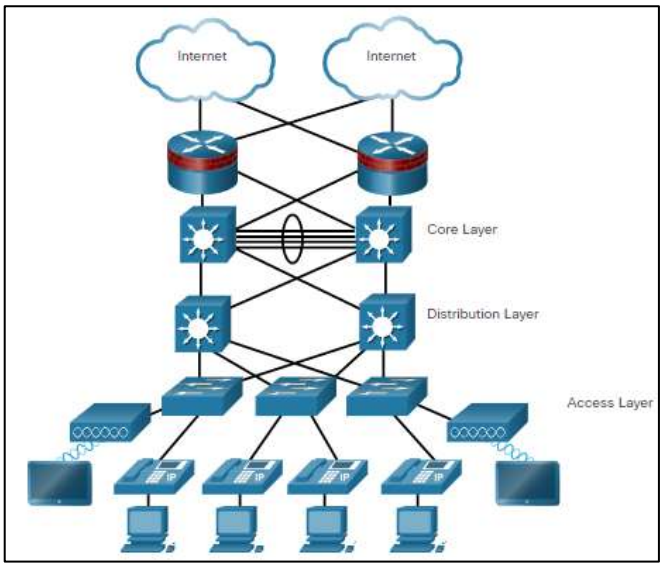
Membuat jaringan *switched* tanpa batasan membutuhkan penggunaan prinsip-prinsip desain jaringan yang baik untuk memastikan ketersediaan, fleksibilitas, keamanan,

dan pengelolaan yang maksimal. Jaringan *switched* tanpa batasan harus memenuhi persyaratan saat ini serta layanan dan teknologi yang dibutuhkan di masa depan. Pedoman desain jaringan *switched* tanpa batasan dibangun berdasarkan prinsip-prinsip berikut:

a. Hierarkis - Desain memfasilitasi pemahaman peran setiap perangkat di setiap tingkat, menyederhanakan penempatan, pengoperasian, dan manajemen, serta mengurangi domain kesalahan di setiap tingkat.
b. Modularitas – Rancangan ini memungkinkan perluasan jaringan tanpa batas yang mulus dan pemberdayaan layanan terintegrasi berdasarkan permintaan.
c. Ketahanan – Rancangan ini memenuhi ekspetasi pengguna untuk menjaga jaringan selalu menyala
d. Fleksibilitas – Rancangan memungkinkan pembagian beban *traffic* yang cerdas dengan menggunakan semua sumber daya jaringan

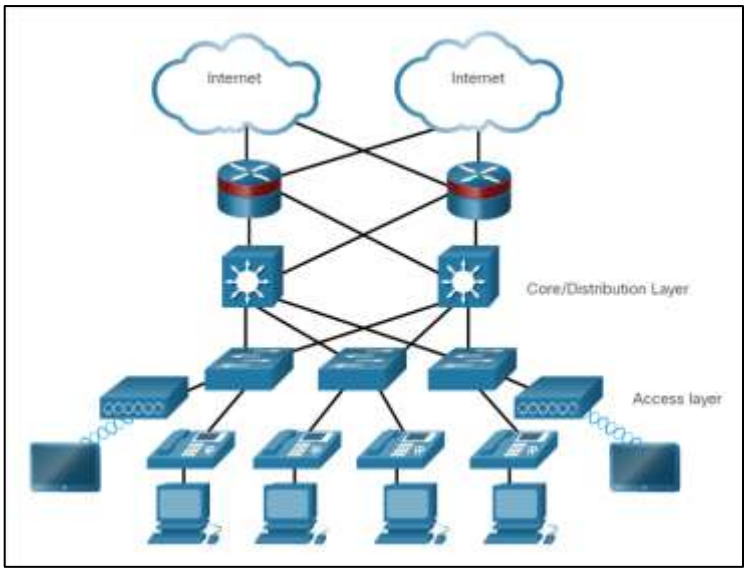
Ini bukan prinsip-prinsip yang berdiri sendiri. Memahami bagaimana setiap prinsip menyesuaikan diri dalam konteks prinsip yang lain sangatlah penting. Merancang jaringan *switched* tanpa batasan dalam gaya hierarkis menciptakan fondasi yang memungkinkan perancang jaringan untuk melapisi fitur keamanan, mobilitas, dan komunikasi terpadu. Dua kerangka kerja desain hirarkis yang telah teruji dan terbukti untuk jaringan kampus adalah lapisan tiga tingkat dan model lapisan dua tingkat. Tiga lapisan penting dalam desain bertingkat ini adalah lapisan akses, distribusi, dan inti. Setiap lapisan dapat dilihat sebagai modul yang terdefinisi dengan baik dan terstruktur, dengan peran dan fungsi khusus dalam jaringan kampus. Memperkenalkan modularitas ke dalam desain hierarkis kampus lebih lanjut memastikan bahwa jaringan kampus tetap tangguh dan cukup fleksibel untuk menyediakan layanan jaringan penting. Modularitas juga membantu memungkinkan pertumbuhan dan perubahan yang terjadi dari waktu ke waktu.

a. Model Tiga Tingkat



Gambar 4 Model Tiga Tingkat

b. Model dua Tingkat



Gambar 5 Model dua Tingkat

c. Fungsi Lapisan Akses, Distribusi, dan Inti.

Lapisan akses, distribusi, dan inti melakukan fungsi-fungsi spesifik dalam desain jaringan hirarkis.

a. Lapisan Akses

Lapisan akses mewakili tepi jaringan, dimana *traffic* masuk atau keluar dari jaringan kampus. Secara tradisional, fungsi utama dari *switch* lapisan akses adalah untuk menyediakan akses jaringan ke pengguna. *Switch* lapisan akses terhubung ke *switch* lapisan distribusi, yang menerapkan teknologi fondasi jaringan seperti *routing*, kualitas layanan, dan keamanan. Untuk memenuhi aplikasi jaringan dan permintaan *end-user*, platform *switch*ing generasi berikutnya sekarang menyediakan layanan yang lebih terkonvergensi, terintegrasi, dan cerdas ke berbagai jenis *endpoints* di tepi jaringan. Membangun kecerdasan ke dalam *switch* lapisan akses memungkinkan aplikasi untuk beroperasi pada jaringan dengan lebih efisien dan aman.

b. Lapisan Distribusi

Lapisan distribusi menghubungkan antara lapisan akses dan lapisan inti untuk menyediakan berbagai fungsi penting, termasuk yang berikut ini:

1. Mengagregasi jaringan closet kabel skala besar.
2. Mengagregasi domain siaran Lapisan 2 dan batas-batas *routing* Lapisan 3
3. Menyediakan intelligent *switching*, *routing*, dan fungsi kebijakan akses jaringan untuk mengakses seluruh jaringan.
4. Menyediakan ketersediaan tinggi dari sakelar lapisan distribusi yang berlebihan ke *end user*, dan jalur biaya yang sama ke inti
5. Menyediakan layanan yang berbeda untuk berbagai kelas aplikasi layanan di tepi jaringan

c. Lapisan Inti

Lapisan inti adalah tulang punggung jaringan. Ia menghubungkan beberapa lapisan jaringan kampus. Lapisan inti berfungsi sebagai agregator untuk semua perangkat lapisan distribusi dan mengikat kampus bersama dengan jaringan lainnya. Tujuan utama dari lapisan inti adalah untuk menyediakan isolasi kesalahan dan konektivitas *backbone* berkecepatan tinggi.

d. Jaringan Berskala

Anda memahami bahwa jaringan Anda akan berubah. Jumlah penggunanya kemungkinan akan meningkat, mereka dapat ditemukan di mana saja, dan mereka akan menggunakan berbagai macam perangkat. Jaringan Anda harus dapat berubah seiring dengan penggunanya. Skalabilitas adalah istilah untuk jaringan yang dapat tumbuh tanpa kehilangan ketersediaan dan keandalan. Untuk mendukung jaringan besar, sedang atau kecil, perancang jaringan harus mengembangkan strategi untuk memungkinkan jaringan agar tersedia dan untuk menskalakan secara efektif dan mudah. Termasuk dalam strategi desain jaringan dasar adalah rekomendasi berikut:

a. Gunakan peralatan modular yang dapat diperluas, atau perangkat berkelompok yang dapat dengan mudah ditingkatkan untuk meningkatkan kemampuan. Modul perangkat dapat ditambahkan ke peralatan yang ada untuk mendukung fitur dan perangkat baru tanpa memerlukan peningkatan peralatan secara besar-besaran. Beberapa perangkat dapat diintegrasikan dalam kluster untuk bertindak sebagai satu perangkat untuk menyederhanakan manajemen dan konfigurasi.
b. Rancang sebuah jaringan hierarkis untuk menyertakan modul-modul yang dapat ditambahkan, diupgrade, dan dimodifikasi, jika perlu, tanpa mempengaruhi rancangan area fungsional lain dari jaringan. Misalnya, membuat lapisan akses terpisah yang dapat diperluas tanpa mempengaruhi distribusi dan lapisan inti dari jaringan kampus.
c. Buat strategi address IPv4 dan IPv6 yang bersifat hierarkis. Perencanaan *address* yang cermat akan menghilangkan kebutuhan untuk meng-*address* ulang jaringan untuk mendukung pengguna dan layanan tambahan.
d. Pilih *Router* atau *switch multilayer* untuk membatasi siaran dan menyaring *traffic* lain yang tidak diinginkan dari jaringan. Gunakan perangkat Lapisan 3 untuk menyaring dan mengurangi *traffic* ke inti jaringan.

e. Perangkat Keras *Switch*

Salah satu cara sederhana untuk membuat jaringan hierarkis dan berskala adalah dengan menggunakan peralatan yang tepat untuk pekerjaan itu. Ada berbagai platform *switch*, faktor bentuk, dan fitur lain yang harus Anda pertimbangkan sebelum memilih *switch*. Ketika mendesain jaringan, penting untuk memilih perangkat keras yang tepat untuk memenuhi persyaratan jaringan saat ini, serta untuk memungkinkan pertumbuhan jaringan. Dalam jaringan enterprise, baik *switch* dan *Router* memainkan peran penting dalam komunikasi jaringan.

a. LAN *Switch* Kampus

Untuk meningkatkan kinerja jaringan di LAN perusahaan, ada sakelar inti, distribusi, akses, dan kompak. Platform sakelar ini bervariasi dari sakelar tanpa kipas dengan delapan port tetap hingga sakelar 13 bilah yang mendukung ratusan port. Platform sakelar LAN kampus termasuk Cisco 2960, 3560, 3650, 3850, 4500, 6500, dan 6800 Series.

Gambar 6 LAN *Switch* Campus

b. *Switch Cloud-Managed*

Switch akses yang dikelola *cloud* Cisco Meraki memungkinkan penumpukan *switch* secara virtual. Mereka memonitor dan mengkonfigurasi ribuan port *switch* melalui web, tanpa campur tangan staf TI di tempat.

Gambar 7 Meraki *Switch*

c. Pusat Data *Switch*

Pusat data harus dibangun berdasarkan *switch* yang mempromosikan skalabilitas infrastruktur, kontinuitas operasional, dan fleksibilitas transportasi. Platform *switch* pusat data termasuk *switch* Cisco Nexus Series.

Gambar 8 Nexus

d. *Switch* Penyedia Layanan

Switch penyedia layanan terbagi dalam dua kategori: *switch* agregasi dan *switch* akses Ethernet. *Switch* agregasi adalah *switch* Ethernet kelas operator yang mengumpulkan lalu lintas di tepi jaringan. *Switch* akses Ethernet penyedia layanan menampilkan kecerdasan aplikasi, layanan terpadu, virtualisasi, keamanan terintegrasi, dan manajemen yang disederhanakan.

Gambar 9 *Switch* Penyedia Layanan

e. Virtual Networking

Jaringan menjadi semakin tervirtualisasi. Platform *switch* jaringan virtual Cisco Nexus menyediakan layanan multi-penyewa yang aman dengan menambahkan teknologi kecerdasan virtualisasi ke jaringan pusat data.

Gambar 10 Virtual Networking

Tabel berikut menyoroti pertimbangan bisnis umum lainnya ketika memilih peralatan *switch*.

Pertimbangan	Deskripsi
Biaya	Biaya *switch* akan tergantung pada jumlah dan kecepatan *interface*, fitur yang didukung, dan kemampuan ekspansi.
Kepadatan Port	*Switch* jaringan harus mendukung jumlah perangkat yang sesuai pada jaringan.
Daya	Sekarang sudah umum untuk memberi daya pada access point, telepon IP, dan pengguna *switch* compact Power over Ethernet (PoE). Selain pertimbangan PoE, beberapa *switch* berbasis sasis mendukung suplai daya yang berlebihan.
Reliabilitas	*Switch* harus menyediakan akses berkelanjutan ke jaringan.
Kecepatan Port	Kecepatan koneksi jaringan menjadi perhatian utama bagi end user.
Frame Buffer	Kemampuan *switch* untuk menyimpan frame penting dalam jaringan di mana mungkin ada port yang padat ke server atau area lain dari jaringan.
Skalabilitas	Jumlah pengguna pada jaringan biasanya bertambah dari waktu ke waktu; oleh karena itu, *switch* harus memberikan kesempatan untuk pertumbuhan.

f. *Router*

Switch bukan satu-satunya komponen jaringan yang dilengkapi dengan berbagai fitur. Pilihan *Router* Anda adalah salah satu keputusan yang sangat penting. *Router* berperan penting dalam jaringan dengan menghubungkan rumah dan bisnis ke internet, menginterkoneksikan beberapa situs dalam jaringan enterprise, menyediakan jalur redundan, dan menghubungkan ISP di internet. *Router* juga dapat bertindak sebagai penerjemah antara berbagai jenis media dan protokol. Misalnya, *Router* dapat menerima

paket dari jaringan Ethernet dan merangkumnya kembali untuk diangkut melalui jaringan serial.

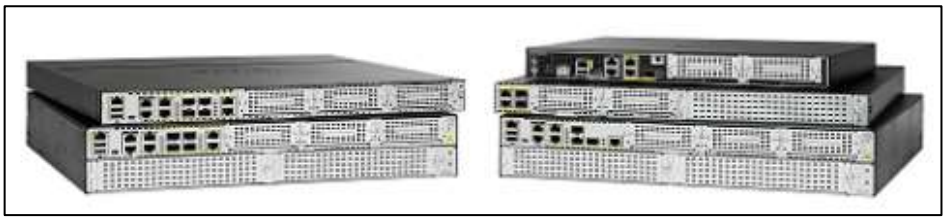
Router menggunakan bagian jaringan (prefix) dari alamat IP tujuan untuk me-route paket ke tujuan yang tepat. Mereka memilih jalur alternatif jika sebuah link mati. Semua host pada jaringan lokal menentukan alamat IP dari *interface Router* lokal dalam konfigurasi IP mereka. *Interface Router* ini adalah *gateway default*. Kemampuan untuk merutekan secara efisien dan pulih dari kegagalan link jaringan sangat penting untuk mengirimkan paket ke tujuan mereka. *Router* juga melayani fungsi-fungsi bermanfaat lainnya sebagai berikut:

a. Mereka menyediakan penahanan siaran dengan membatasi siaran ke jaringan lokal.
b. Mereka menghubungkan lokasi yang terpisah secara geografis.
c. Mereka mengelompokkan pengguna secara logis berdasarkan aplikasi atau departemen dalam perusahaan, berdasarkan kebutuhan umum atau membutuhkan akses ke sumber daya yang sama.
d. Mereka menyediakan keamanan yang lebih baik dengan menyaring lalu lintas yang tidak diinginkan melalui daftar kontrol akses.

Seiring dengan pertumbuhan jaringan, penting untuk memilih *Router* yang tepat untuk memenuhi persyaratannya. Ada berbagai kategori *Router* Cisco.

a. Branch *Routers*

   Router cabang, yang ditunjukkan pada gambar, mengoptimalkan layanan cabang pada satu platform sambil memberikan pengalaman aplikasi yang optimal di seluruh cabang dan infrastruktur WAN. Memaksimalkan ketersediaan layanan di cabang membutuhkan jaringan yang dirancang dengan uptime 24x7x365. Jaringan cabang yang sangat tersedia harus memastikan pemulihan cepat dari kesalahan tipikal, sambil meminimalkan atau menghilangkan dampak pada layanan, dan menyediakan konfigurasi dan manajemen jaringan yang sederhana. Yang ditampilkan adalah *Router* Cisco Integrated Services *Router* (ISR) 4000 Series.



Gambar 11 *Router Branch*

b. *Router* tepi jaringan

   Router tepi jaringan, yang ditunjukkan pada gambar 12, memungkinkan tepi jaringan untuk memberikan layanan berkinerja tinggi, sangat aman, dan andal yang menyatukan kampus, pusat data, dan jaringan cabang. Pelanggan mengharapkan

pengalaman media berkualitas tinggi dan lebih banyak jenis konten daripada sebelumnya. Pelanggan menginginkan interaktivitas, personalisasi, mobilitas, dan kontrol untuk semua konten. Pelanggan juga ingin mengakses konten kapan saja dan di mana saja yang mereka pilih, melalui perangkat apa pun, baik di rumah, di tempat kerja, atau saat bepergian. *Router* tepi jaringan harus memberikan kualitas layanan yang ditingkatkan dan kemampuan video dan seluler tanpa henti. Yang ditampilkan adalah *Router* Cisco Aggregation Services *Router*s (ASR) 9000 Series.

Gambar 12 *Router* Tepi jaringan

c. *Router* Penyedia Layanan

Router penyedia layanan, yang ditunjukkan pada gambar 13, memberikan solusi skalabel ujung ke ujung dan layanan yang sadar pelanggan. Operator harus mengoptimalkan operasi, mengurangi biaya, dan meningkatkan skalabilitas dan fleksibilitas, untuk memberikan pengalaman internet generasi berikutnya di semua perangkat dan lokasi. Sistem ini dirancang untuk menyederhanakan dan meningkatkan operasi dan penyebaran jaringan pengiriman layanan. Yang ditampilkan adalah *Router* Cisco Network Convergence System (NCS) 6000 Series.

Gambar 13 *Router* Pennyedia Layanan

d. Industrial

Router industrial, seperti yang ditunjukkan pada gambar 14, didesain untuk menyediakan fitur-fitur kelas enterprise di lingkungan yang kasar dan keras. Desainnya yang ringkas, modular, dan kokoh sangat baik untuk aplikasi yang sangat penting. Yang ditampilkan adalah *Router* Layanan Terpadu Industri Cisco 1100 Series.

Gambar 14 *Router* Industrial

3. Tugas

Mengidentifikasi kebutuhan dan menentukan desain (Proyek Team Base)

Pada tahapan ini secara berkelompok mengidentifikasi kebuthan jaringan perusahaan yang telah kalian tentukan, kemudian membuat desain jaringan sesuai dengan kebutuhan perusahaan. Desain jaringan meliputi:

1. Topologi Fisik
2. Topologi Logika
3. Dan kebutuhan perangkat dan *software* yang akan di gunakan

Kegiatan Belajar 3
Implementasi

1. Sub-Capaian Pembelajaran

a. Mampu memahami Konsep *Routing* Dimamis, mampu mengimplementasikan protokol *routing* OSPF
b. Mampu memahami dan mengimplementasikan ACL
c. Mampu memahami dan mengimplementasikan NAT
d. Mampu memahami dan mengimplementasikan VPN
e. Mampu memahami dan mengimplementasikan QoS

2. Pokok Bahasan

a. *Open Shortest Path First* (OSPF)

OSPF merupakan protokol *routing* dimanis yang mencakup single-area dan multiarea. OSPFv2 digunakan untuk jaringan IPv4. OSPFv3 digunakan untuk jaringan IPv6. Fokus utama dari pembahasan ini adalah OSPFv2 area tunggal. OSPF adalah protokol *routing link-state* yang dikembangkan sebagai alternatif untuk distance *vector Routing Information Protocol* (RIP). RIP adalah protokol *routing* yang dapat diterima pada masa-masa awal jaringan dan internet. Namun ketergantungan RIP pada *hop count* sebagai satu-satunya metrik untuk menentukan rute terbaik dengan cepat menjadi masalah. Menggunakan *hop count* tidak dapat digunakan dengan baik di jaringan yang lebih besar dengan banyak jalur dengan kecepatan yang berbeda-beda. OSPF memiliki keuntungan yang signifikan dibandingkan RIP karena OSPF menawarkan konvergensi yang lebih cepat dan skala untuk implementasi jaringan yang jauh lebih besar.

OSPF adalah protokol *routing link-state* yang menggunakan konsep area. Seorang administrator jaringan dapat membagi domain *routing* ke dalam area yang berbeda yang membantu mengontrol lalu lintas pembaruan *routing*. Sebuah link adalah sebuah *interface* pada *Router*. Link juga merupakan segmen jaringan yang menghubungkan dua *Router*, atau jaringan rintisan seperti LAN Ethernet yang terhubung ke *Router* tunggal. Informasi tentang keadaan sebuah link dikenal sebagai *link-state*. Semua informasi *link-state* termasuk awalan jaringan, panjang awalan, dan biaya.

Semua protokol *routing* memiliki komponen yang sama. Semuanya menggunakan pesan protokol *routing* untuk bertukar informasi rute. Pesan-pesan tersebut membantu membangun struktur data, yang kemudian diproses menggunakan algoritma *routing*. *Router* yang menjalankan OSPF bertukar pesan untuk menyampaikan informasi *routing* menggunakan lima jenis paket.

1. Pesan Protokol *Routing* (*Routing Protocol Massages*)

   Router yang menjalankan OSPF bertukar pesan untuk menyampaikan informasi perutean menggunakan lima jenis paket, yaitu:

   a. Hello packet
   b. Database description packet

c. *Link-state request packet*
d. *Link-state update packet*
e. *Link-state acknowledgment packet*

2. Struktur Data (*Data Structure*)

   Pesan OSPF digunakan untuk membuat dan memelihara tiga database OSPF, yaitu:

   a. *Adjacency database*, ini menciptakan tabel neighbor.
   b. *Link-state database* (LSDB), ini menciptakan tabel topologi.
   c. *Forwarding database*, ini menciptakan tabel *routing*.

   Tabel-tabel ini berisi daftar *Router* tetangga untuk bertukar informasi *routing*. Tabel-tabel ini disimpan dan dipelihara dalam RAM.

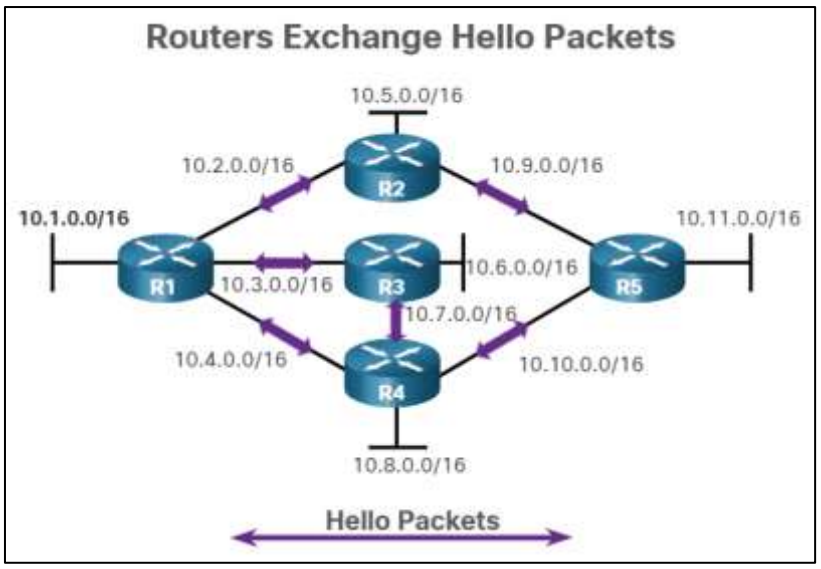
3. Algoritma

   Router membangun tabel topologi menggunakan hasil perhitungan berdasarkan algoritma Dijkstra *shortest-path first* (SPF). Algoritma SPF didasarkan pada biaya kumulatif untuk mencapai tujuan.Algoritma SPF menciptakan pohon SPF dengan menempatkan setiap *Router* pada akar pohon dan menghitung jalur terpendek ke setiap node. Pohon SPF kemudian digunakan untuk menghitung rute terbaik. OSPF menempatkan rute-rute terbaik ke dalam forwarding database, yang digunakan untuk membuat tabel *routing*.

Untuk mempertahankan informasi *routing*, *Router* OSPF menyelesaikan proses *routing link-state* generik untuk mencapai keadaan konvergensi. Gambar 15 menunjukkan topologi lima *Router*. Setiap link di antara *Router* diberi label dengan nilai cost. Dalam OSPF, biaya digunakan untuk menentukan jalur terbaik ke tujuan. Berikut ini adalah langkah-langkah *routing link-state* yang diselesaikan oleh *Router*:

1. Membangun Neighbor Adjacencies (Establish Neighbor Adjacencies)

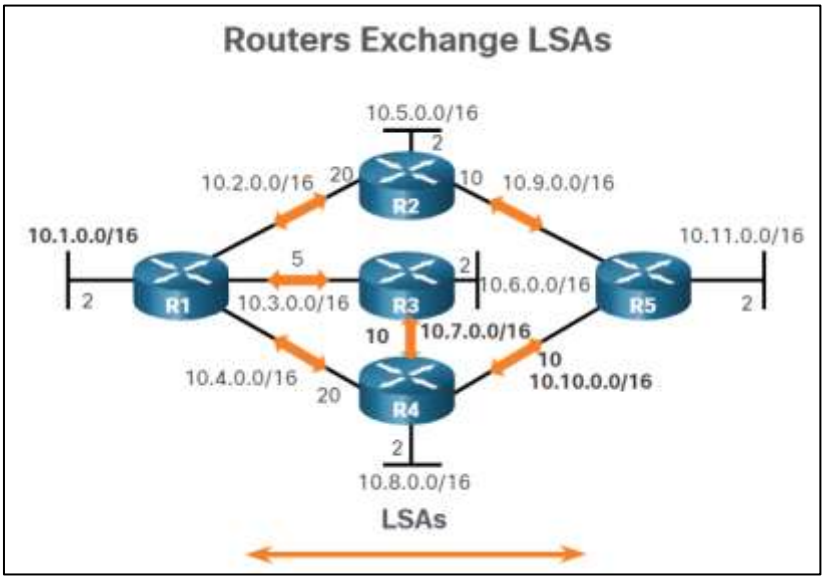
   Router-router yang mendukung OSPF harus mengenali satu sama lain di jaringan sebelum mereka dapat berbagi informasi. *Router* yang mendukung OSPF mengirim paket Hello keluar di semua *interface* yang mendukung OSPF untuk menentukan apakah ada tetangga yang hadir pada link tersebut. Jika ada tetangga yang hadir, *router* yang mendukung OSPF mencoba untuk membangun *Neighbor Adjacencies* dengan tetangganya itu.



Gambar 15 Pertukaran Paket Hello Pada *Router*

2. Pertukaran Iklan *Link-state* (*Exchange Link-state Advertisements*)

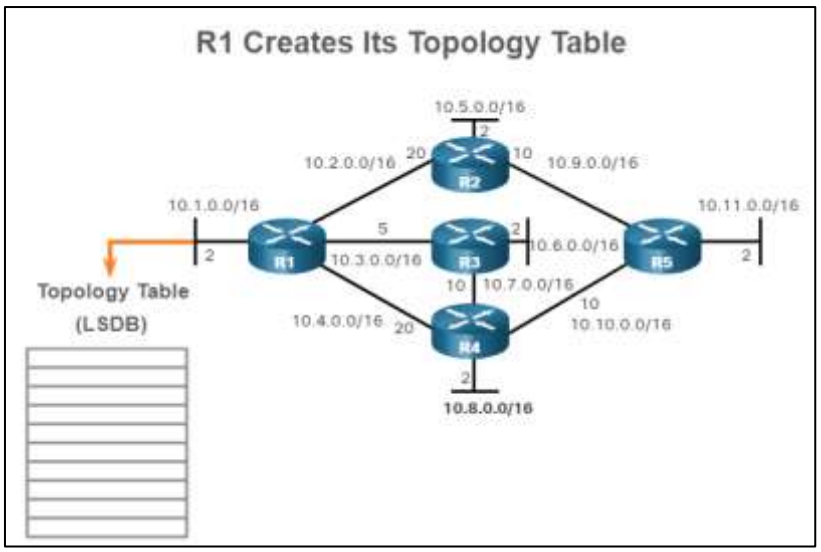
   Setelah *adjacencies* terbentuk, *Router* kemudian bertukar *link-state advertisements* (LSAs). LSAs berisi status dan biaya dari setiap tautan yang terhubung langsung. *Router* membanjiri LSAs mereka ke tetangga yang berdekatan. Tetangga yang berdekatan yang menerima LSAs segera membanjiri LSAs ke tetangga lain yang terhubung langsung, sampai semua *Router* di area tersebut memiliki semua LSAs.



Gambar 16 Pertukaran LSAs

3. Membangun Basis Data *Link State* (*Build the Link State Database*)

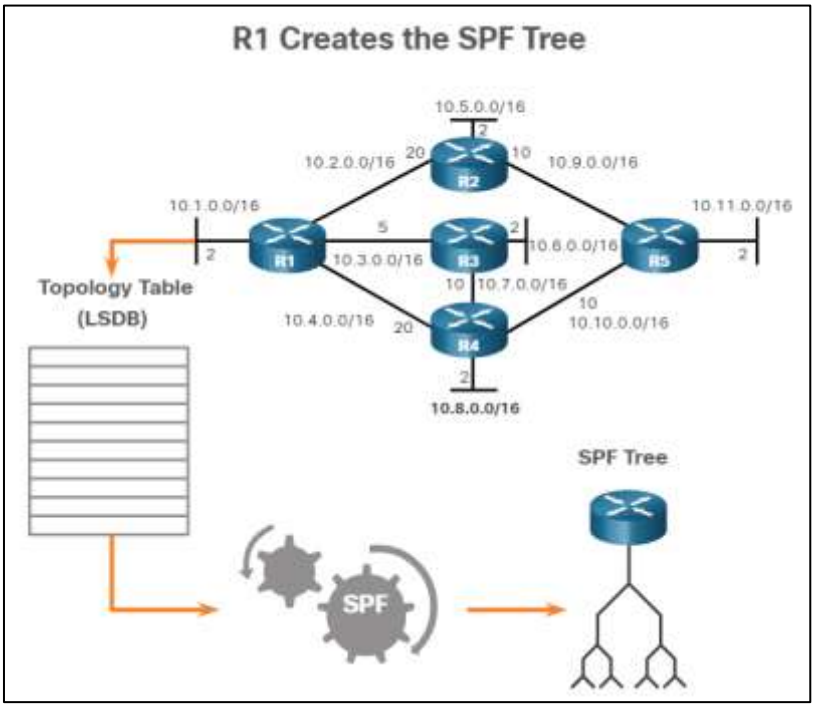
   Setelah LSAs diterima, *Router* yang mendukung OSPF membangun tabel topologi (LSDB) berdasarkan LSAs yang diterima. Database ini pada akhirnya menyimpan semua informasi tentang topologi area.



Gambar 17 Membuat Topologi Tabel

4. Menjalankan Algoritma SPF (*Execute the SPF Algorithm*)

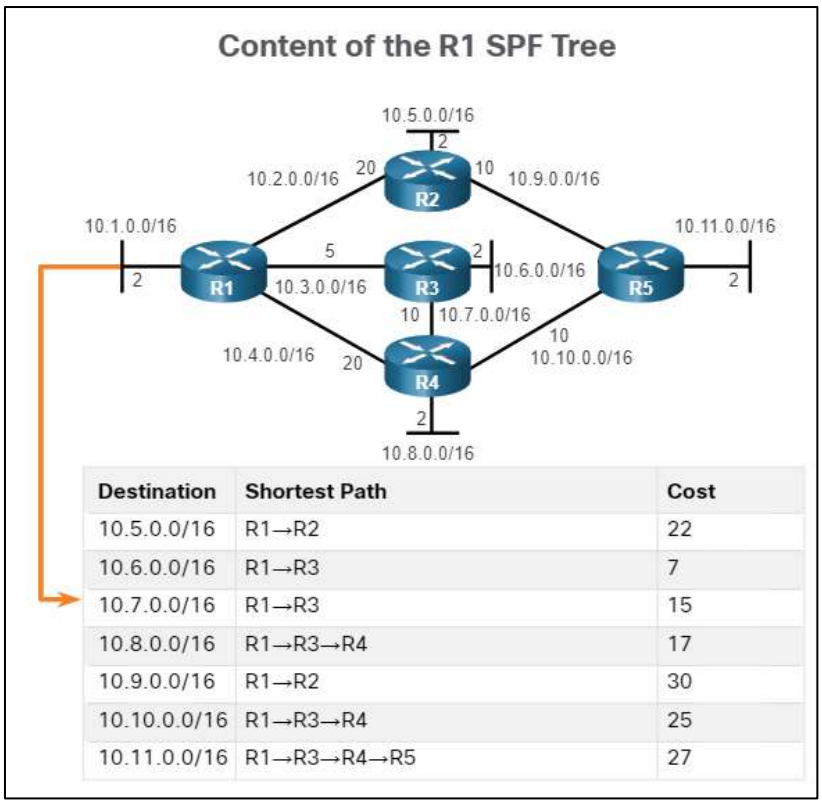
   Router kemudian mengeksekusi algoritma SPF. Roda gigi pada gambar 18, langkah ini digunakan untuk menunjukkan eksekusi algoritma SPF. Algoritma SPF menciptakan pohon SPF.



Gambar 18 Membuat SPF Tree

5. Memilih Rute Terbaik (*Choose the Best Route*)

   Setelah pohon SPF dibangun, jalur terbaik ke setiap jaringan ditawarkan ke tabel *routing* IP. Rute akan dimasukkan ke dalam tabel *routing* kecuali ada sumber rute ke jaringan yang sama dengan jarak administratif yang lebih rendah, seperti rute statis. Keputusan *routing* dibuat berdasarkan entri dalam tabel *routing*.

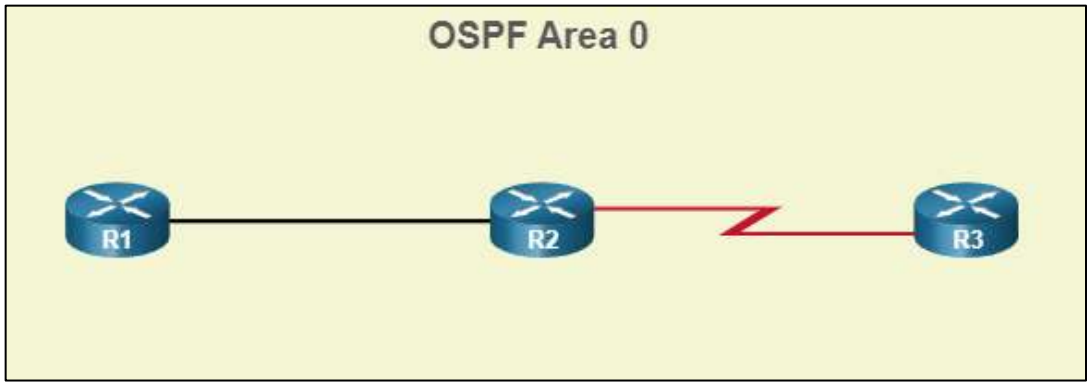


Destination	Shortest Path	Cost
10.5.0.0/16	R1→R2	22
10.6.0.0/16	R1→R3	7
10.7.0.0/16	R1→R3	15
10.8.0.0/16	R1→R3→R4	17
10.9.0.0/16	R1→R2	30
10.10.0.0/16	R1→R3→R4	25
10.11.0.0/16	R1→R3→R4→R5	27

Gambar 19 Pemilihan Jalur Terbaik

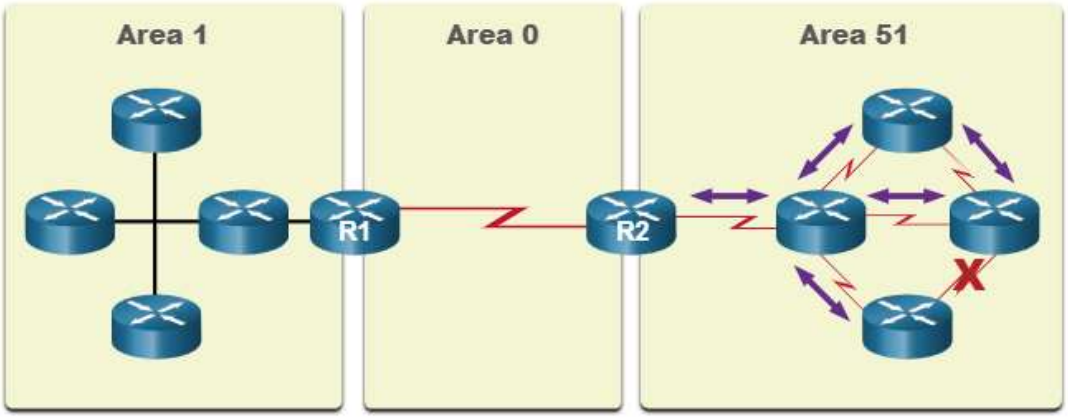
Untuk membuat OSPF lebih efisien dan terukur, OSPF mendukung *routing* hierarkis menggunakan area. Area OSPF adalah sekelompok *Router* yang berbagi informasi *link-state* yang sama dalam LSDB mereka. OSPF dapat diimplementasikan dengan dua cara berikut ini:

1. OSPF Area Tunggal, semua *Router* berada di satu area. Praktik terbaik adalah menggunakan area 0.



Gambar 20 Single Area

2. Multiarea OSPF, OSPF diimplementasikan dengan menggunakan beberapa area, secara hirarkis. Semua area harus terhubung ke area *backbone* (area 0). *Router* yang menghubungkan area-area tersebut disebut sebagai *Area Border Router*s (ABRs).



Gambar 21 Multi Area

Dengan OSPF multiarea, satu domain *routing* yang besar dapat dibagi menjadi area-area yang lebih kecil, untuk mendukung *routing* hierarkis. *Routing* masih terjadi di antara area-area (interarea *routing*), sementara banyak operasi *routing* intensif prosesor, seperti menghitung ulang database, disimpan di dalam area. Misalnya, setiap kali *Router* menerima informasi baru tentang perubahan topologi di dalam area (termasuk penambahan, penghapusan, atau modifikasi link) *Router* harus menjalankan kembali algoritma SPF, membuat pohon SPF baru, dan memperbarui tabel *routing*. Algoritma SPF adalah CPU-intensif dan waktu yang dibutuhkan untuk perhitungan tergantung pada ukuran area. Terlalu banyak *Router* dalam satu area akan membuat LSDB sangat besar dan meningkatkan beban pada CPU. Oleh karena itu, mengatur *Router* ke dalam area-area secara efektif mempartisi basis data yang berpotensi besar menjadi basis data yang lebih kecil dan lebih mudah dikelola.

Opsi desain topologi-hierarkis dengan OSPF multiarea dapat menawarkan keuntungan-keuntungan berikut ini:

a. Tabel *routing* yang lebih kecil, tabel lebih kecil karena ada lebih sedikit entri tabel *routing*. Ini karena alamat jaringan dapat diringkas antar area. Rangkuman rute tidak diaktifkan secara default.
b. Mengurangi *link-state* update overhead, merancang OSPF multiarea dengan area yang lebih kecil meminimalkan pemrosesan dan kebutuhan memori.
c. Mengurangi frekuensi perhitungan SPF, OSPF multiarea melokalisasi dampak perubahan topologi dalam suatu area. Misalnya, OSPF ini meminimalkan dampak pembaruan *routing* karena flooding LSA berhenti di batas area.

OSPF menggunakan paket-paket *link-state* (LSP) berikut ini untuk membangun dan memelihara adjacencies tetangga dan bertukar update *routing*:

1. Tipe 1: Paket Halo, Ini digunakan untuk membangun dan memelihara kedekatan dengan *Router* OSPF lainnya.
2. Tipe 2: Database Description (DBD) packet, Ini berisi daftar singkat LSDB dari *Router* pengirim dan digunakan oleh *Router* penerima untuk memeriksa LSDB lokal. LSDB harus

identik pada semua *Router link-state* dalam suatu area untuk membangun pohon SPF yang akurat.

3. Tipe 3: *Link-state* Request (LSR) packet, *Router* penerima kemudian dapat meminta informasi lebih lanjut tentang entri apa pun di DBD dengan mengirimkan LSR.
4. Tipe 4: *Link-state* Update (LSU) packet, Ini digunakan untuk membalas LSR dan mengumumkan informasi baru. LSU berisi beberapa jenis LSA yang berbeda.
5. Tipe 5: *Link-state* Acknowledgment (LSAck) packet, Ketika LSU diterima, *Router* mengirimkan LSAck untuk mengonfirmasi penerimaan LSU. Bidang data LSAck kosong.

Ketika *Router* OSPF pada awalnya terhubung ke jaringan, *Router* mencoba untuk Membuat adjacencies dengan tetangga, Bertukar informasi *routing*, Menghitung rute terbaik, Mencapai konvergensi. Status yang dilalui OSPF untuk melakukan ini adalah status down, status init, status dua arah, status ExStart, status Exchange, status loading, dan status penuh. Ketika OSPF diaktifkan pada sebuah *interface*, *router* harus menentukan apakah ada tetangga OSPF lain pada link dengan mengirimkan paket Hello yang berisi ID *router*-nya keluar semua *interface* yang diaktifkan OSPF. Paket Hello dikirim ke alamat multicast 224.0.0.0.5 yang dicadangkan All OSPF *Router*s IPv4. Hanya *Router* OSPFv2 yang akan memproses paket-paket ini. Ketika *Router* tetangga yang mendukung OSPF menerima paket Hello dengan ID *router* yang tidak ada dalam daftar tetangganya, *router* penerima mencoba untuk membangun *adjacency* dengan *Router* yang memulai. Setelah keadaan Dua Arah, *router* bertransisi ke keadaan sinkronisasi database, yang merupakan proses tiga langkah yaitu Putuskan *router* Pertama, Pertukaran DBD, Kirim LSR.

Jaringan multiakses dapat menciptakan dua tantangan untuk OSPF mengenai flooding LSAs: penciptaan beberapa *adjacencies* dan *flooding* LSAs yang ekstensif. Peningkatan dramatis dalam jumlah *router* juga secara dramatis meningkatkan jumlah LSA yang dipertukarkan antara *router*. Flooding LSA ini secara signifikan berdampak pada operasi OSPF. Jika setiap *router* dalam jaringan multiakses harus membanjiri dan mengakui semua LSA yang diterima ke semua *router* lain pada jaringan multiakses yang sama, lalu lintas jaringan akan menjadi sangat kacau. Inilah sebabnya mengapa pemilihan DR dan BDR diperlukan. Pada jaringan multiakses, OSPF memilih DR untuk menjadi titik pengumpulan dan distribusi untuk LSA yang dikirim dan diterima. Sebuah BDR juga dipilih jika DR gagal.

Konfigurasi OSPF:

```
Router(config)# router ospf <process-id>
Router(config-router)# network <network-id> <wildcard-mask> area <area-id>
Router(config-router)# network <network-id> <wildcard-mask> area <area-id>
```

Ket:

- network <Network-ID>: untuk advertise network yang terhubung langsung dengan *Router* (directly connected network).
- wildcard-mask: inverse subnet-mask.

b. Access List Control

Router membuat keputusan *routing* berdasarkan informasi dalam header paket. Lalu lintas yang memasuki antarmuka *Router* dirutekan semata-mata berdasarkan informasi dalam tabel *routing*. *Router* membandingkan alamat IP tujuan dengan rute dalam tabel *routing* untuk menemukan kecocokan terbaik dan kemudian meneruskan paket berdasarkan rute yang paling cocok. Proses yang sama dapat digunakan untuk menyaring lalu lintas menggunakan *Access List Control* (ACL). ACL adalah serangkaian perintah yang digunakan untuk memfilter paket berdasarkan informasi yang ditemukan di header paket. Secara default, *Router* tidak memiliki ACL yang dikonfigurasi. Namun, ketika ACL diterapkan ke antarmuka, *Router* melakukan tugas tambahan untuk mengevaluasi semua paket jaringan saat mereka melewati antarmuka untuk menentukan apakah paket tersebut dapat diteruskan. ACL menggunakan daftar berurutan pernyataan izin atau penolakan, yang dikenal sebagai *Access Control Entries* (ACEs).

Ketika lalu lintas jaringan melewati antarmuka yang dikonfigurasi dengan ACL, *Router* membandingkan informasi di dalam paket terhadap setiap ACE, dalam urutan berurutan, untuk menentukan apakah paket tersebut cocok dengan salah satu ACE. Proses ini disebut penyaringan paket. Beberapa tugas yang dilakukan oleh *Router* memerlukan penggunaan ACL untuk mengidentifikasi lalu lintas. Tabel ini mencantumkan beberapa tugas ini dengan contoh-contohnya.

Tugas	Contoh
Membatasi lalu lintas jaringan untuk meningkatkan kinerja jaringan	Kebijakan perusahaan melarang lalu lintas video di jaringan untuk mengurangi beban jaringan. Kebijakan dapat ditegakkan menggunakan ACL untuk memblokir lalu lintas video.
Menyediakan kontrol arus lalu lintas	Kebijakan perusahaan mengharuskan lalu lintas protokol *routing* dibatasi hanya untuk link tertentu. Kebijakan dapat diimplementasikan dengan menggunakan ACL untuk membatasi pengiriman update *routing* hanya yang berasal dari sumber yang diketahui.
Menyediakan tingkat keamanan dasar untuk akses jaringan	Kebijakan perusahaan menuntut agar akses ke jaringan Sumber Daya Manusia dibatasi hanya untuk pengguna yang berwenang. Kebijakan dapat ditegakkan menggunakan ACL untuk membatasi akses ke jaringan tertentu.
Menyaring lalu lintas berdasarkan jenis lalu lintas	Kebijakan perusahaan mensyaratkan bahwa trafik email diijinkan masuk ke jaringan, tetapi akses Telnet ditolak.

	Kebijakan dapat diimplementasikan menggunakan ACL untuk menyaring lalu lintas berdasarkan jenisnya.
Menyaring host untuk mengizinkan atau menolak akses ke layanan jaringan	Kebijakan perusahaan mengharuskan akses ke beberapa jenis file (misalnya, FTP atau HTTP) dibatasi untuk grup pengguna. Kebijakan dapat diimplementasikan dengan menggunakan ACL untuk menyaring akses pengguna ke layanan.
Memberikan prioritas pada kelas lalu lintas jaringan tertentu	Lalu lintas perusahaan menetapkan bahwa lalu lintas suara diteruskan secepat mungkin untuk menghindari gangguan. Kebijakan dapat diimplementasikan dengan menggunakan ACL dan layanan QoS untuk mengidentifikasi lalu lintas suara dan segera memprosesnya.

Ada dua jenis IPv4 ACL:

a. Standard ACLs, ACL ini mengizinkan atau menolak paket hanya berdasarkan alamat IPv4 sumber. ACL nomor 1 sampai 99, atau 1300 sampai 1999 digunakan pada ACL standar.
   Konfigurasi ACL standar:

```
Router(config)# access-list 1 permit/deny source hostname/ip/network
Router(config)# access-list 1 permit/deny any

Router(config)# interface fa0/0
Router(config)# ip access-group 1 in/out
```

   Contoh konfiurasi ACL pada line vty dari network internal dengan ip address 192.168.1.0/24:

```
Router(config)# access-list 12 permit 192.168.1.0 0.0.0.255

Router(config)# line vty 0 4
Router(config)# access-class 12 .in
```

b. Extended ACLs, ACL ini mengizinkan atau menolak paket berdasarkan alamat IPv4 sumber dan alamat IPv4 tujuan, jenis protokol, port TCP atau UDP sumber dan tujuan, dan banyak lagi. ACL nomor 100 sampai 199, atau 2000 sampai 2699 adalah ACL Extended.

```
Router(config)# access-list 100 permit/deny protocol source_IP destination_IP
Router(config)# access-list 100 permit/deny protocol source_IP port
destination_IP port
Router(config)# access-list 100 permit/deny protocol any any

Router(config)# interface fa0/0
Router(config)# ip access-group 1 in/out
```

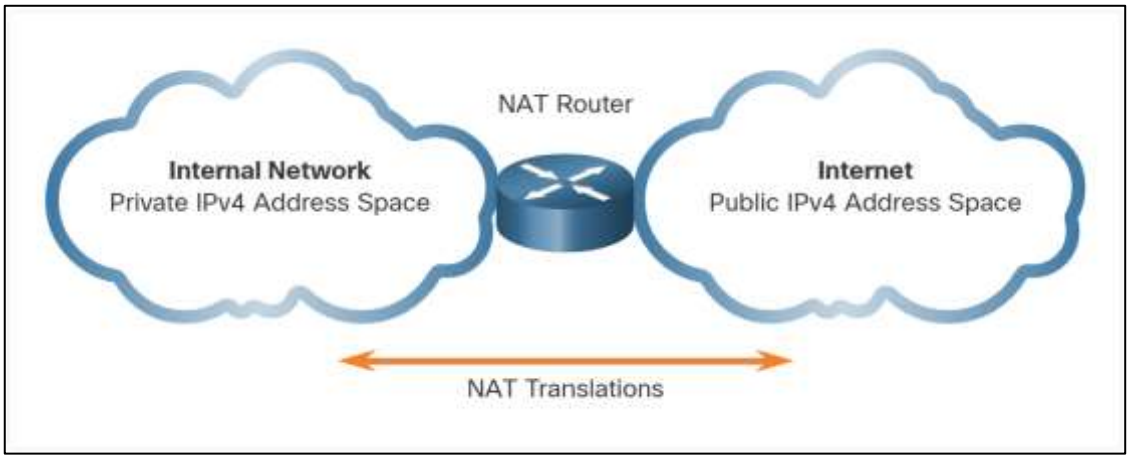
c. Network Access Translation

Seperti yang kita ketahui, alamat IPv4 publik tidak cukup untuk memberikan alamat unik ke setiap perangkat yang terhubung ke internet. Jaringan biasanya diimplementasikan menggunakan alamat IPv4 privat, seperti yang didefinisikan dalam RFC 1918. Rentang alamat yang termasuk dalam RFC 1918 termasuk dalam tabel berikut. Sangat mungkin bahwa komputer yang anda gunakan untuk melihat kursus ini diberi alamat pribadi.

Tabel 12 Tabel IP Private

Class	Rentang Alamat Internal RFC 1918	Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Alamat privat ini digunakan di dalam organisasi atau situs untuk memungkinkan perangkat berkomunikasi secara lokal. Namun, karena alamat-alamat ini tidak mengidentifikasi satu perusahaan atau organisasi, alamat IPv4 privat tidak dapat dirutekan melalui internet. Untuk mengizinkan perangkat dengan alamat IPv4 privat mengakses perangkat dan sumber daya di luar jaringan lokal, alamat privat harus diterjemahkan terlebih dahulu ke alamat publik.



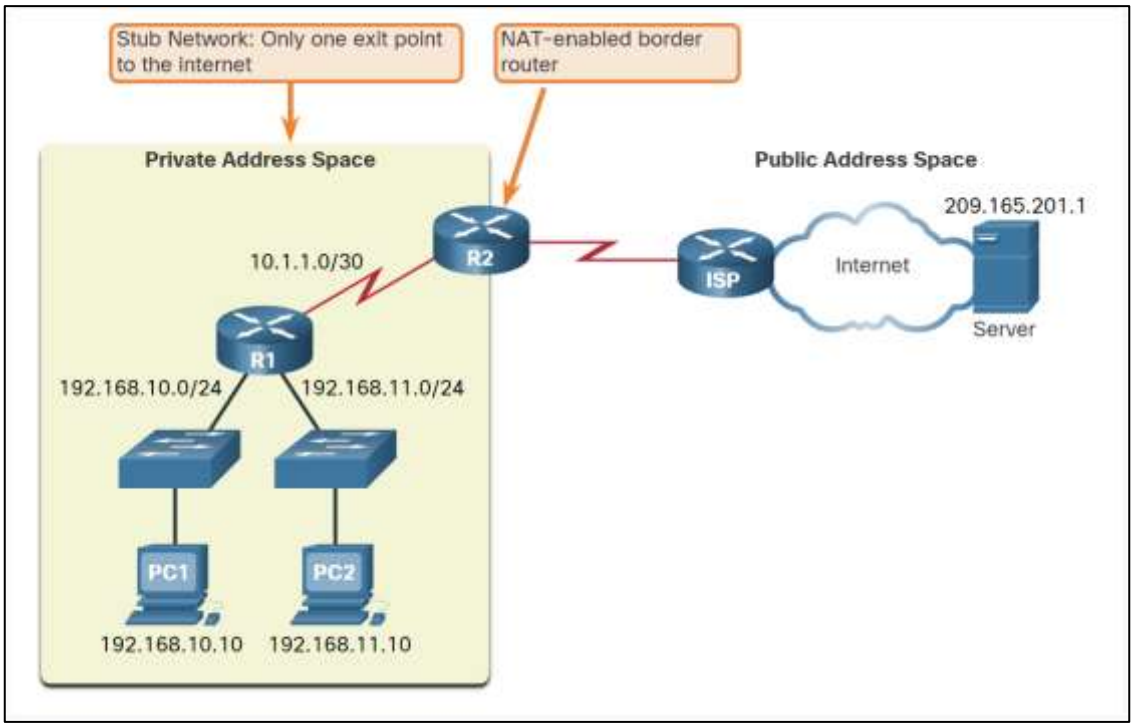
Gambar 22 NAT

NAT menyediakan penerjemahan alamat privat ke alamat publik, seperti yang ditunjukkan pada gambar. Hal ini memungkinkan perangkat dengan alamat IPv4 privat untuk mengakses sumber daya di luar jaringan privat mereka, seperti yang ditemukan di internet. NAT, dikombinasikan dengan alamat IPv4 privat, telah menjadi metode utama untuk menjaga alamat IPv4 publik. Satu alamat IPv4 publik dapat digunakan bersama oleh ratusan, bahkan ribuan perangkat, masing-masing dikonfigurasi dengan alamat IPv4 privat yang unik.

NAT mempunyai banyak kegunaan, tetapi kegunaan utamanya adalah untuk menghemat alamat IPv4 publik. NAT melakukan ini dengan mengizinkan jaringan untuk menggunakan alamat IPv4 pribadi secara internal dan menyediakan terjemahan ke alamat publik hanya bila diperlukan. NAT memiliki manfaat yang dirasakan untuk menambahkan tingkat privasi dan keamanan ke jaringan, karena NAT menyembunyikan alamat IPv4 internal dari jaringan luar.

Router yang mendukung NAT dapat dikonfigurasi dengan satu atau lebih alamat IPv4 publik yang valid. Alamat publik ini dikenal sebagai NAT pool. Ketika sebuah perangkat internal mengirim lalu lintas keluar dari jaringan, *Router* yang mendukung NAT menerjemahkan alamat IPv4 internal perangkat ke alamat publik dari kumpulan NAT. Untuk perangkat luar, semua lalu lintas yang masuk dan keluar jaringan tampaknya memiliki alamat IPv4 publik dari kumpulan alamat yang disediakan.

Router NAT biasanya beroperasi di perbatasan jaringan stub. Jaringan stub adalah satu atau lebih jaringan dengan koneksi tunggal ke jaringan tetangganya, satu arah masuk dan satu arah keluar dari jaringan. Dalam contoh pada gambar, R2 adalah *Router* perbatasan. Seperti yang terlihat dari ISP, R2 membentuk jaringan stub.

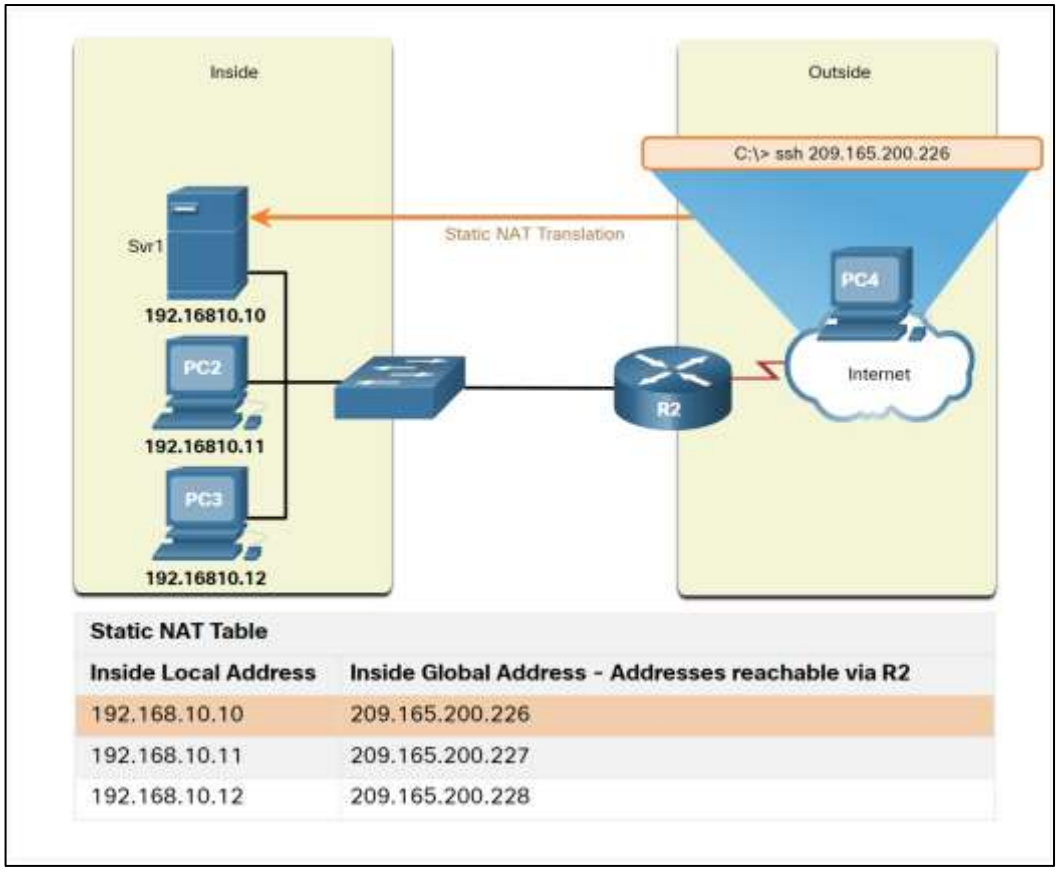


Gambar 23 Skenario NAT

Ketika sebuah perangkat di dalam jaringan rintisan ingin berkomunikasi dengan perangkat di luar jaringannya, paket diteruskan ke *Router* perbatasan. *Router* perbatasan melakukan proses NAT, menerjemahkan alamat pribadi internal perangkat ke alamat publik, luar, yang dapat dirutekan. NAT terbagi menjadi beberapa jenis, yaitu:

1. Statis NAT

   NAT Statis menggunakan pemetaan *one-to-one* dari alamat lokal dan global. Pemetaan ini dikonfigurasi oleh administrator jaringan dan tetap konstan. Dalam gambar 23, R2 dikonfigurasi dengan pemetaan statis untuk alamat lokal dalam Svr1, PC2, dan PC3. Ketika perangkat-perangkat ini mengirim trafik ke internet, alamat lokal dalam mereka diterjemahkan ke alamat global dalam yang dikonfigurasi. Untuk jaringan luar, perangkat-perangkat ini tampak memiliki alamat IPv4 publik.



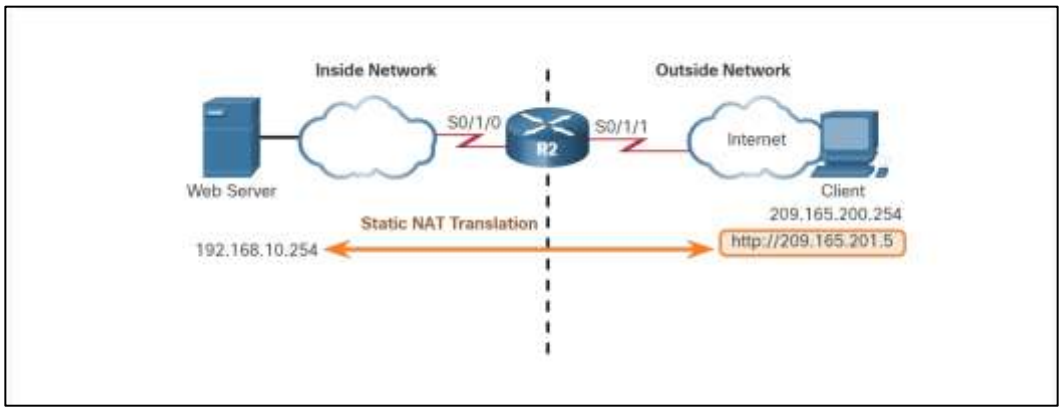
Static NAT Table

Inside Local Address	Inside Global Address - Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

Gambar 24 Statis NAT

NAT statis sangat berguna untuk server web atau perangkat yang harus memiliki alamat yang konsisten yang dapat diakses dari internet, seperti server web perusahaan. Ini juga berguna untuk perangkat yang harus dapat diakses oleh personil yang berwenang ketika berada di luar kantor, tetapi tidak oleh masyarakat umum di internet. Misalnya, administrator jaringan dari PC4 bisa menggunakan SSH untuk mendapatkan akses ke alamat global dalam Svr1 (209.165.200.226). R2 menerjemahkan alamat global dalam ini ke alamat lokal dalam 192.168.10.10 dan menghubungkan sesi ke Svr1.

Berikut ini contoh skenari implementasi statis NAT dan konfigurasinya



Gambar 25 Skenario NAT Statis

Langkah 1. Tugas pertama adalah membuat pemetaan antara alamat lokal dalam dan alamat global dalam. Misalnya, 192.168.10.254 alamat lokal dalam dan 209.165.201.5 alamat global dalam pada gambar dikonfigurasi sebagai terjemahan NAT statis.

```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
```

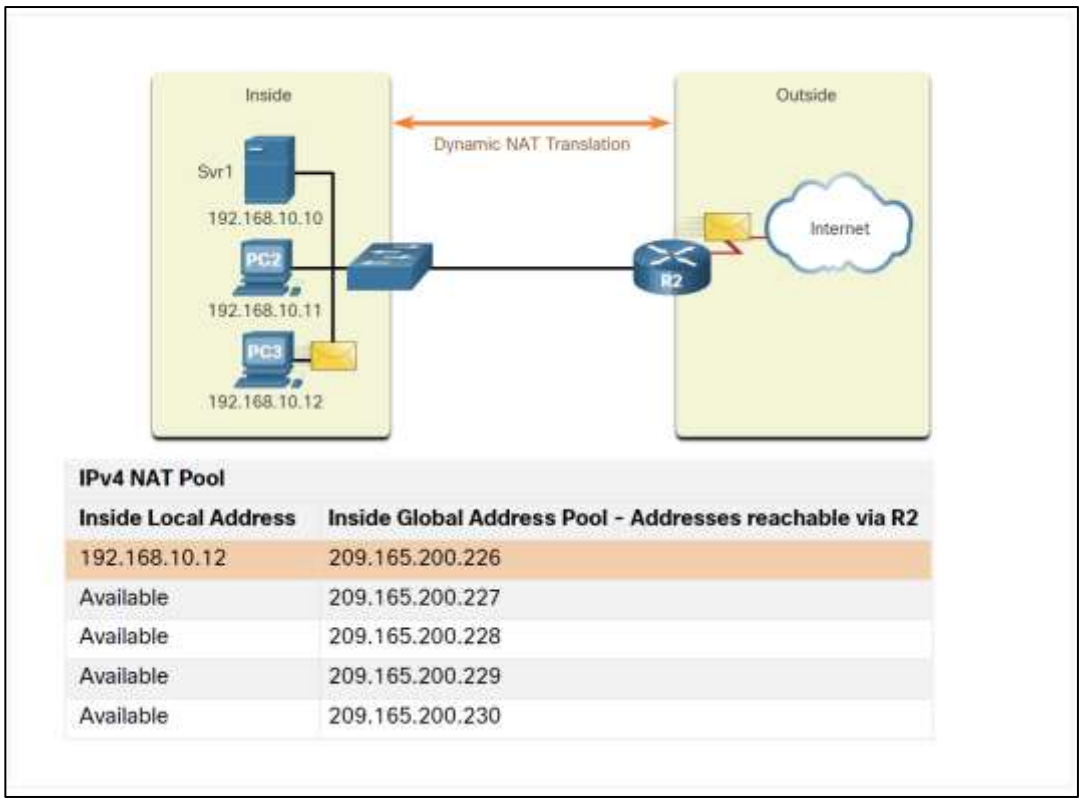
Langkah 2. Setelah pemetaan dikonfigurasi, antarmuka yang berpartisipasi dalam terjemahan dikonfigurasi sebagai di dalam atau di luar relatif terhadap NAT. Dalam contoh, antarmuka R2 Serial 0/1/0 adalah antarmuka di dalam dan Serial 0/1/1 adalah antarmuka luar.

```
R2(config)# interface serial 0/1/0
R2(config-if)# ip address 192.168.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/1/1
R2(config-if)# ip address 209.165.200.1 255.255.255.252
R2(config-if)# ip nat outside
```

Dengan konfigurasi ini, paket-paket yang tiba pada antarmuka dalam R2 (Serial 0/1/0) dari alamat IPv4 lokal dalam yang dikonfigurasi (192.168.10.254) diterjemahkan dan kemudian diteruskan ke jaringan luar. Paket yang tiba pada antarmuka luar R2 (Serial 0/1/1), yang dialamatkan ke alamat IPv4 global dalam yang dikonfigurasi di dalam (209.165.201.5), diterjemahkan ke alamat lokal di dalam (192.168.10.254) dan kemudian diteruskan ke jaringan dalam.

2. NAT Dinamis

NAT Dinamis menggunakan kumpulan alamat publik dan memberikannya berdasarkan siapa cepat dia dapat, siapa cepat dia dapat. Ketika sebuah perangkat di dalam meminta akses ke jaringan luar, NAT dinamis memberikan alamat IPv4 publik yang tersedia dari pool. Pada gambar 26, PC3 telah mengakses internet menggunakan alamat pertama yang tersedia di dalam pool NAT dinamis. Alamat-alamat lain masih tersedia untuk digunakan. Mirip dengan NAT statis, NAT dinamis memerlukan alamat publik yang cukup tersedia untuk memenuhi jumlah total sesi pengguna simultan.

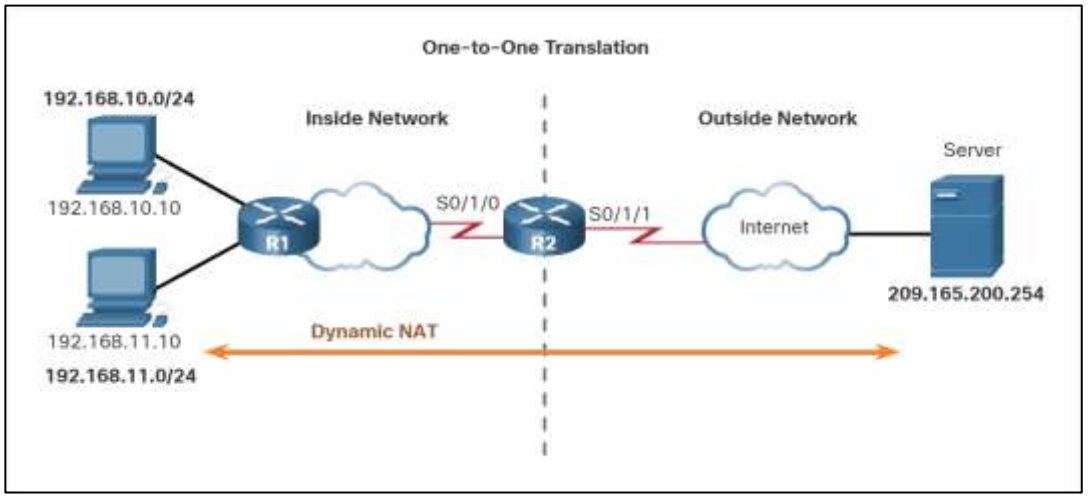


IPv4 NAT Pool

Inside Local Address	Inside Global Address Pool - Addresses reachable via R2
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

Gambar 26 Dinamis NAT

Berikut ini contoh skenario implementasi Dinamis NAT dan konfigurasinya



Gambar 27 Skenario Dinamis NAT

Gambar 27 menunjukkan contoh topologi di mana konfigurasi NAT memungkinkan terjemahan untuk semua host pada jaringan 192.168.0.0/16. Ini termasuk LAN 192.168.10.0 dan 192.168.11.0 ketika host menghasilkan lalu lintas yang memasuki antarmuka S0/1/0 dan keluar dari S0/1/1. Ini termasuk LAN 192.168.10.0 dan 192.168.11.0 ketika host menghasilkan lalu lintas yang masuk ke antarmuka S0/1/0 dan keluar dari S0/1/1. Host di dalam alamat lokal diterjemahkan ke alamat pool yang tersedia dalam kisaran 209.165.200.226 hingga209.165.200.240.

Langkah 1. Tentukan kumpulan alamat yang akan digunakan untuk terjemahan menggunakan perintah ip NAT pool. Kumpulan alamat ini biasanya merupakan kelompok

alamat publik. Alamat didefinisikan dengan menunjukkan alamat IPv4 awal dan alamat IPv4 akhir dari kumpulan alamat tersebut. Kata kunci *netmask* atau prefix-length menunjukkan bit alamat mana yang termasuk jaringan dan bit mana yang termasuk host untuk rentang alamat tersebut. Dalam skenario, tentukan kumpulan alamat IPv4 publik di bawah nama kumpulan NAT-POOL1.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
```

Langkah 2. Konfigurasikan ACL standar untuk mengidentifikasi (mengizinkan) hanya alamat-alamat yang akan diterjemahkan. ACL yang terlalu permisif dapat menyebabkan hasil yang tidak dapat diprediksi. Ingatlah bahwa ada pernyataan deny all yang implisit di akhir setiap ACL. Dalam skenario, tentukan alamat-alamat mana yang memenuhi syarat untuk diterjemahkan.

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Langkah 3. Ikat ACL ke pool, menggunakan sintaks perintah berikut:

***Router*(config)# ip nat inside source list {access-list-number | access-list-name} pool pool-name**

Konfigurasi ini digunakan oleh *Router* untuk mengidentifikasi perangkat mana (daftar) yang menerima alamat mana (pool). Dalam skenario, mengikat NAT-POOL1 dengan ACL 1.

```
R2(config)# ip nat inside source list 1 pool NAT-POOL1
```

Langkah 4. Identifikasi *interface* mana yang berada di dalam, dalam kaitannya dengan NAT; ini akan menjadi *interface* apa pun yang terhubung ke jaringan dalam. Dalam skenario, identifikasi *interface* serial 0/1/0 sebagai *interface* NAT di dalam.

```
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
```

Langkah 5. Identifikasi *interface* mana yang berada di luar, dalam kaitannya dengan NAT; ini akan menjadi *interface* apa pun yang terhubung ke jaringan luar. Dalam skenario, identifikasi *interface* serial 0/1/1 sebagai *interface* NAT luar.

```
R2(config)# interface serial 0/1/1
R2(config-if)# ip nat outside
```

3. PAT

Port Address Translation (PAT), juga dikenal sebagai NAT overload, memetakan beberapa alamat IPv4 privat ke satu alamat IPv4 publik atau beberapa alamat. Inilah yang dilakukan oleh sebagian besar *Router* rumah. ISP memberikan satu alamat ke *Router*, namun beberapa anggota rumah tangga dapat mengakses internet secara bersamaan. Ini adalah bentuk NAT yang paling umum untuk rumah dan perusahaan. Dengan PAT, beberapa alamat dapat dipetakan ke satu atau beberapa alamat, karena setiap alamat pribadi juga dilacak oleh nomor port. Ketika perangkat memulai sesi TCP / IP, ia menghasilkan nilai port sumber TCP atau UDP, atau ID kueri yang ditetapkan secara

khusus untuk ICMP, untuk mengidentifikasi sesi secara unik. Ketika *router* NAT menerima paket dari klien, ia menggunakan nomor port sumbernya untuk secara unik mengidentifikasi terjemahan NAT tertentu. PAT memastikan bahwa perangkat menggunakan nomor port TCP yang berbeda untuk setiap sesi dengan server di internet. Ketika respons kembali dari server, nomor port sumber, yang menjadi nomor port tujuan pada perjalanan pulang, menentukan ke perangkat mana *Router* meneruskan paket. Proses PAT juga memvalidasi bahwa paket yang masuk diminta, sehingga menambahkan tingkat keamanan pada sesi. Saat R2 memproses setiap paket, R2 menggunakan nomor port (1331 dan 1555, dalam contoh ini) untuk mengidentifikasi perangkat dari mana paket tersebut berasal. Alamat sumber (SA) adalah alamat lokal di dalam dengan nomor port yang ditetapkan TCP / UDP ditambahkan. Alamat tujuan (DA) adalah alamat global luar dengan nomor port layanan yang ditambahkan. Dalam contoh ini, port layanan adalah 80, yaitu HTTP. Untuk alamat sumber, R2 menerjemahkan alamat lokal dalam ke alamat global dalam dengan nomor port yang ditambahkan. Alamat tujuan tidak berubah tetapi sekarang disebut sebagai alamat IPv4 global luar. Ketika server web membalas, jalurnya dibalik.

NAT memecahkan masalah kita karena tidak memiliki alamat IPv4 yang cukup, tetapi NAT juga dapat menimbulkan masalah lain. Sehingga NAT dapat memberikan keuntungan dan kerugian NAT. NAT memberikan banyak manfaat, yaitu:

1. NAT melestarikan skema pengalamatan yang terdaftar secara hukum dengan memungkinkan privatisasi intranet. NAT melestarikan alamat melalui *multiplexing* tingkat port aplikasi. Dengan NAT *overload* (PAT), host internal dapat berbagi satu alamat IPv4 publik tunggal untuk semua komunikasi eksternal. Dalam jenis konfigurasi ini, sangat sedikit alamat eksternal yang diperlukan untuk mendukung banyak host internal.
2. NAT meningkatkan fleksibilitas koneksi ke jaringan publik. Beberapa pool, pool cadangan, dan pool *load-balancing* dapat diimplementasikan untuk memastikan koneksi jaringan publik yang handal.
3. NAT menyediakan konsistensi untuk skema pengalamatan jaringan internal. Pada jaringan yang tidak menggunakan alamat IPv4 privat dan NAT, merubah skema alamat IPv4 publik memerlukan penataan ulang semua host di jaringan yang ada. Biaya penataan ulang host dapat menjadi signifikan. NAT memungkinkan skema alamat IPv4 privat yang ada untuk tetap ada sementara memungkinkan perubahan yang mudah ke skema pengalamatan publik yang baru. Ini berarti sebuah organisasi dapat mengubah ISP dan tidak perlu mengubah klien di dalamnya.
4. Dengan menggunakan alamat IPv4 RFC 1918, NAT menyembunyikan alamat IPv4 pengguna dan perangkat lain. Beberapa orang menganggap ini sebagai fitur keamanan; namun, sebagian besar ahli setuju bahwa NAT tidak menyediakan keamanan. *Firewall stateful* adalah apa yang menyediakan keamanan di tepi jaringan.

Selain itu NAT juga memiliki kekurangan. Fakta bahwa host di internet tampak berkomunikasi langsung dengan perangkat yang mendukung NAT, bukan dengan host yang sebenarnya di dalam jaringan pribadi, menciptakan sejumlah masalah. Salah satu kelemahan dari penggunaan NAT berhubungan dengan kinerja jaringan, khususnya untuk protokol real time seperti VoIP. NAT meningkatkan penundaan penerusan karena penerjemahan setiap alamat IPv4 di dalam header paket membutuhkan waktu. Paket pertama selalu diproses-*switched* melalui jalur yang lebih lambat. *Router* harus melihat setiap paket untuk memutuskan apakah paket itu perlu diterjemahkan. *Router* harus mengubah header IPv4, dan mungkin mengubah header TCP atau UDP. Checksum header IPv4, bersama dengan checksum TCP atau UDP harus dihitung ulang setiap kali terjemahan dilakukan. Paket yang tersisa akan melalui jalur fast-*switched* jika ada entri cache; jika tidak, paket-paket tersebut juga tertunda.

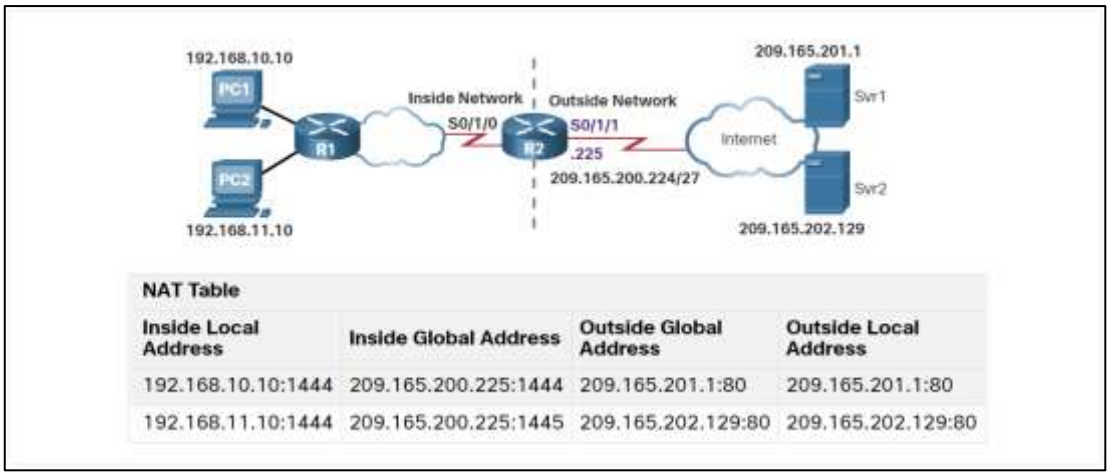
Penundaan penerusan yang disebabkan oleh proses NAT menjadi lebih banyak masalah karena kumpulan alamat IPv4 publik untuk ISP menjadi habis. Banyak ISP yang harus memberikan alamat IPv4 pribadi kepada pelanggan, bukan alamat IPv4 publik. Ini berarti *Router* pelanggan menerjemahkan paket dari alamat IPv4 privatnya ke alamat IPv4 privat ISP. Sebelum meneruskan paket ke penyedia lain, ISP kemudian akan melakukan NAT lagi, menerjemahkan alamat IPv4 pribadinya ke salah satu alamat IPv4 publiknya yang jumlahnya terbatas. Proses dua lapisan terjemahan NAT ini dikenal sebagai *Carrier Grade* NAT (CGN).

Kerugian lain dari penggunaan NAT adalah bahwa pengalamatan *end-to-end* hilang. Ini dikenal sebagai prinsip *end-to-end*. Banyak protokol dan aplikasi internet bergantung pada pengalamatan *end-to-end* dari sumber ke tujuan. Beberapa aplikasi tidak bekerja dengan NAT. Misalnya, beberapa aplikasi keamanan, seperti tanda tangan digital, gagal karena alamat IPv4 sumber berubah sebelum mencapai tujuan. Aplikasi yang menggunakan alamat fisik, bukan nama domain yang memenuhi syarat, tidak mencapai tujuan yang diterjemahkan melintasi *Router* NAT. Kadang-kadang, masalah ini dapat dihindari dengan menerapkan pemetaan NAT statis.

Keterlacakan IPv4 ujung ke ujung juga hilang. Menjadi jauh lebih sulit untuk melacak paket yang mengalami banyak perubahan alamat paket melalui beberapa lompatan NAT, membuat pemecahan masalah menjadi menantang. Menggunakan NAT juga mempersulit penggunaan protokol tunneling, seperti IPsec, karena NAT memodifikasi nilai di header, menyebabkan pemeriksaan integritas gagal.

Layanan yang memerlukan inisiasi koneksi TCP dari jaringan luar, atau protokol stateless, seperti yang menggunakan UDP, dapat terganggu. Kecuali jika *Router* NAT telah dikonfigurasi untuk mendukung protokol tersebut, paket yang masuk tidak dapat mencapai tujuannya. Beberapa protokol dapat mengakomodasi satu contoh NAT antara host yang berpartisipasi (mode pasif FTP, misalnya), tetapi gagal ketika kedua sistem dipisahkan dari internet oleh NAT.

Mengkonfigurasi PAT untuk Menggunakan Alamat IPv4 Tunggal, berikut ini merupakan gambar 28 skenario PAT dengan alamat tunggal



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.11.10:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

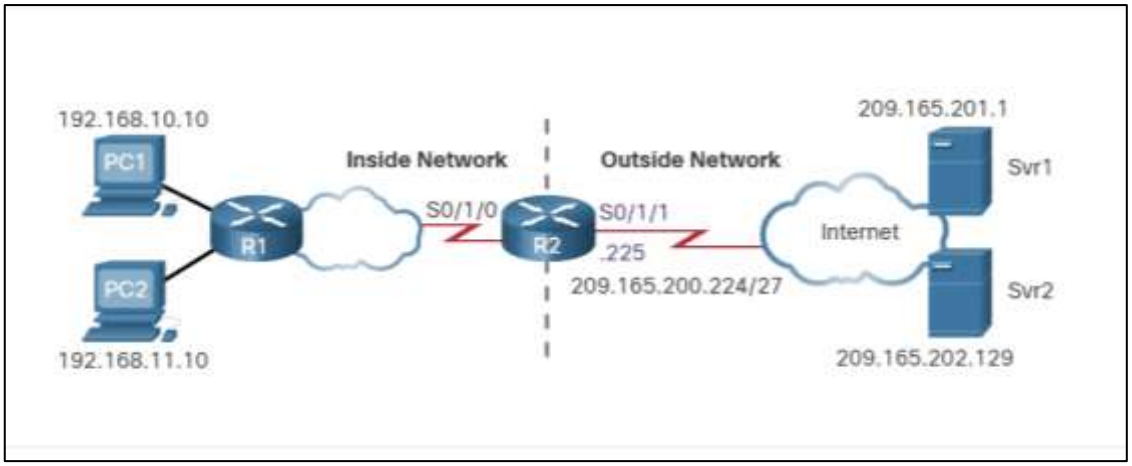
Gambar 28 Skenario PAT

Untuk mengkonfigurasi PAT untuk menggunakan alamat IPv4 tunggal, cukup tambahkan kata kunci overload ke perintah ip nat inside source. Konfigurasi lainnya mirip dengan konfigurasi NAT statis dan dinamis kecuali bahwa dengan PAT, beberapa host dapat menggunakan alamat IPv4 publik yang sama untuk mengakses internet. Dalam contoh, semua host dari jaringan 192.168.0.0/16 (cocok dengan ACL 1) yang mengirim lalu lintas melalui *Router* R2 ke internet akan diterjemahkan ke alamat IPv4 209.165.200.225 (alamat IPv4 dari antarmuka S0/1/1). Arus lalu lintas akan diidentifikasi oleh nomor port dalam tabel NAT karena kata kunci overload dikonfigurasi.

```
R2(config)# ip nat inside source list 1 interface serial 0/1/1 overload
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# interface serial0/1/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface Serial0/1/1
R2(config-if)# ip nat outside
```

Mengkonfigurasi PAT untuk Menggunakan Kumpulan Alamat

ISP dapat mengalokasikan lebih dari satu alamat IPv4 publik ke suatu organisasi. Dalam skenario ini organisasi dapat mengkonfigurasi PAT untuk menggunakan kumpulan alamat publik IPv4 untuk terjemahan. Jika sebuah situs telah mengeluarkan lebih dari satu alamat IPv4 publik, alamat ini dapat menjadi bagian dari kumpulan yang digunakan oleh PAT. Kumpulan kecil alamat dibagi di antara sejumlah besar perangkat, dengan beberapa host menggunakan alamat IPv4 publik yang sama untuk mengakses internet. Untuk mengkonfigurasi PAT untuk kumpulan alamat NAT dinamis, cukup tambahkan kata kunci *overload* ke perintah ip nat *inside source*. Topologi untuk skenario ini diulangi pada gambar untuk kenyamanan Anda.



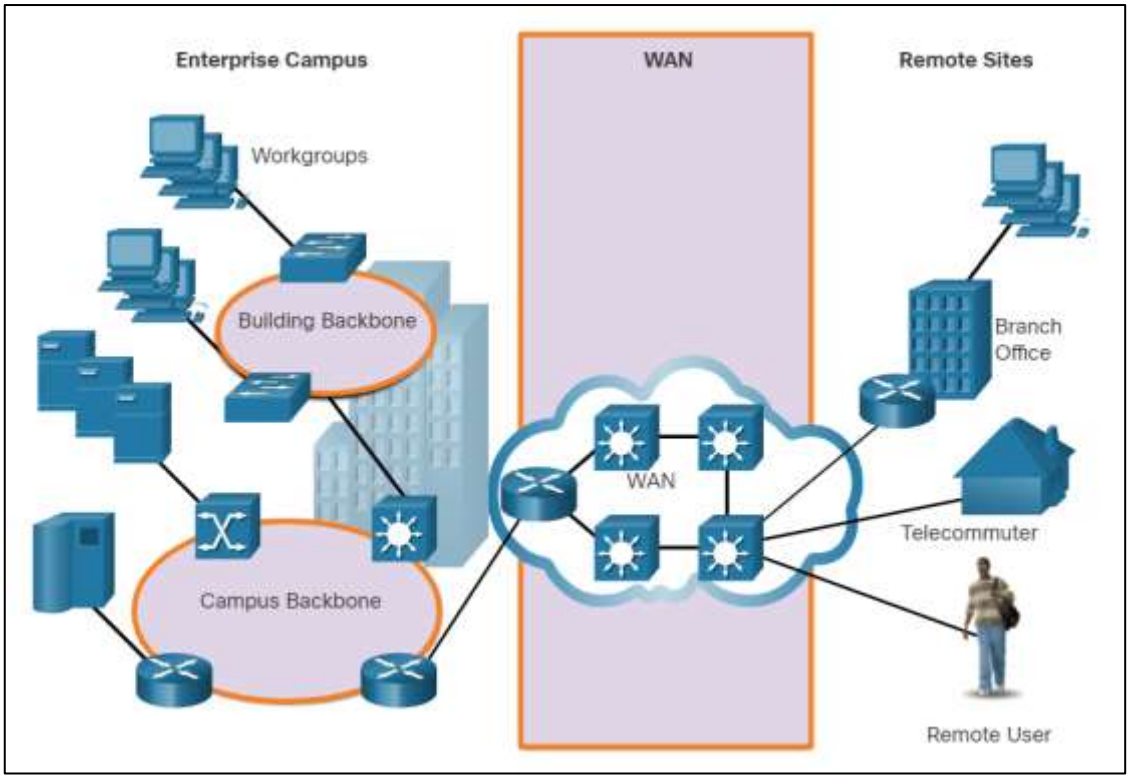
Gambar 29 Skenario PAT 2

Dalam contoh, NAT-POOL2 terikat ke ACL untuk mengizinkan 192.168.0.0/16 untuk diterjemahkan. Host-host ini dapat berbagi alamat IPv4 dari pool karena PAT diaktifkan dengan kata kunci *overload*.

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
R2(config)#
R2(config)# interface serial0/1/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial0/1/1
R2(config-if)# ip nat outside
R2(config-if)# end
R2#
```

d. *Wide Area Network* (WAN)

Baik di tempat kerja atau di rumah, kita semua menggunakan *Local Area Network*s (LAN). Namun, LAN terbatas pada area geografis yang kecil. *Wide Area Network* (WAN) diperlukan untuk menghubungkan di luar batas LAN. WAN adalah jaringan telekomunikasi yang membentang di area geografis yang relatif luas. WAN beroperasi di luar lingkup geografis LAN. Pada gambar 30 dibawah ini, layanan WAN diperlukan untuk menginterkoneksikan jaringan kampus perusahaan ke LAN jarak jauh di situs cabang, situs telecommuter, dan pengguna jarak jauh. Pada gambar tersebut menunjukkan diagram kampus perusahaan dengan beberapa gedung, *router*, *switch*, dan jaringan yang terhubung ke internet WAN yang kemudian terhubung ke berbagai situs dan pengguna jarak jauh.



Gambar 30 WAN

Berikut ini perbedaan jaringan LAN dan WAN

Tabel 13 Perbedaan LAN dan WAN

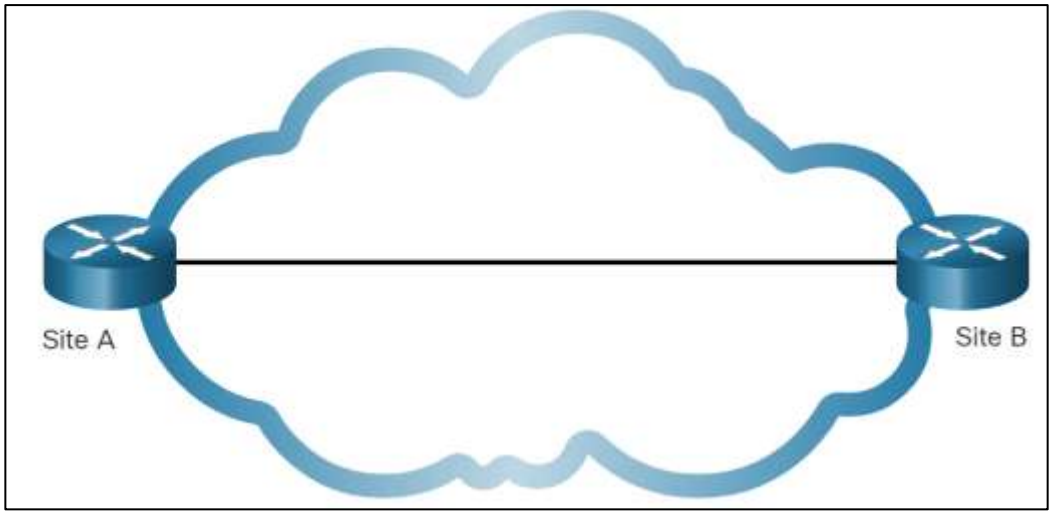
***Local Area Network*s (LAN)**	***Wide Area Networks* (WAN)**
LAN menyediakan layanan jaringan dalam area geografis kecil seperti, jaringan rumah, jaringan kantor, jaringan gedung, atau jaringan kampus.	WAN menyediakan layanan jaringan di area geografis yang luas seperti, di dalam dan di antara kota, negara, dan benua.
LAN digunakan untuk menghubungkan komputer lokal, peripherals, dan perangkat lainnya	WAN digunakan untuk menghubungkan pengguna, dengan jaringan, dan situs jarak jauh.
LAN dimiliki dan dikelola oleh sebuah organisasi atau home user.	WAN dimiliki dan dikelola oleh penyedia layanan internet, telepon, kabel, dan satelit.
Selain biaya infrastruktur jaringan, tidak ada biaya untuk menggunakan LAN.	Layanan WAN disediakan dengan biaya tertentu.
LAN menyediakan kecepatan *bandwidth* tinggi menggunakan kabel Ethernet dan layanan Wi-Fi.	Penyedia WAN menawarkan kecepatan *bandwidth* rendah hingga tinggi, jarak jauh menggunakan jaringan fisik yang kompleks.

Topologi fisik menggambarkan infrastruktur jaringan fisik yang digunakan oleh data ketika data bergerak dari sumber ke tujuan. Topologi fisik WAN yang digunakan dalam WAN adalah kompleks dan sebagian besar, tidak diketahui oleh pengguna. Pertimbangkan seorang pengguna di New York yang membuat panggilan konferensi video dengan pengguna di Tokyo, Jepang. Selain dari koneksi internet pengguna di New York, tidak mungkin untuk mengidentifikasi semua koneksi fisik aktual yang diperlukan untuk mendukung panggilan video. Sebagai gantinya, topologi WAN digambarkan menggunakan topologi logis. Topologi logis menggambarkan koneksi virtual antara sumber dan tujuan. Misalnya, panggilan konferensi video antara pengguna

di New York dan Jepang akan menjadi koneksi *point-to-point* yang logis. Berikut ini jenis-jenis topologi logis yang di gunakan pada WAN.

1. *Point-to-point Topology*

   Topologi *point-to-point*, seperti yang ditunjukkan pada gambar 31, menggunakan sirkuit *point-to-point* antara dua titik akhir.

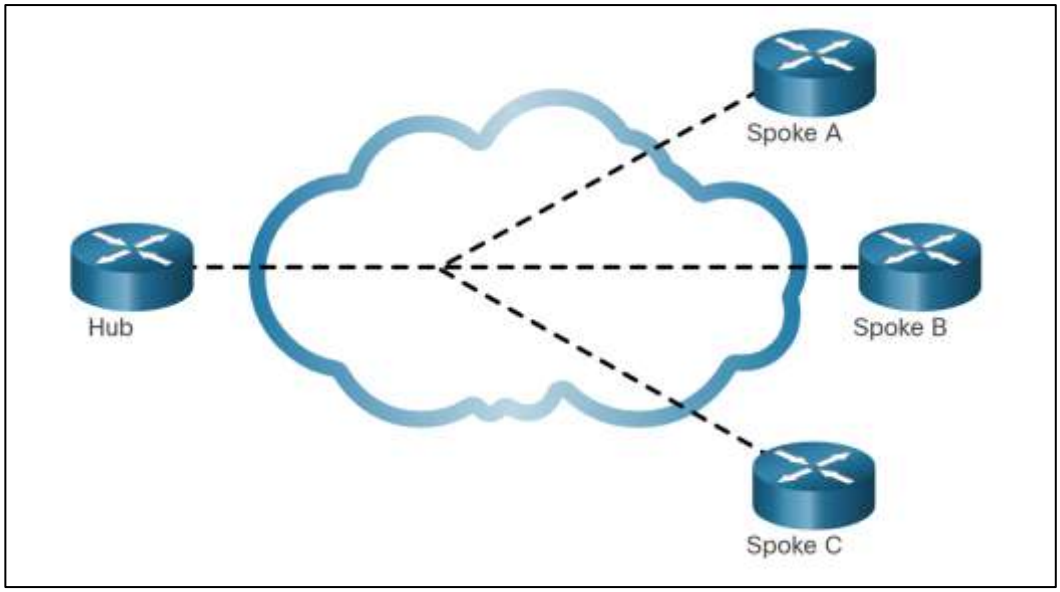


Gambar 31 Topologi *Point-to-point*

Sambungan *point-to-point* sering melibatkan koneksi leased-line khusus dari titik tepi perusahaan ke jaringan penyedia layanan. Koneksi *point-to-point* melibatkan layanan transportasi *Layer* 2 melalui jaringan penyedia layanan. Paket yang dikirim dari satu situs dikirim ke situs lain dan sebaliknya. Koneksi *point-to-point* transparan ke jaringan pelanggan. Tampaknya seolah-olah ada hubungan fisik langsung antara dua titik akhir. Ini bisa menjadi mahal jika banyak koneksi *point-to-point* diperlukan.

2. *Point-to-point* Topology

   Topologi *point-to-point* memungkinkan satu antarmuka pada *Router* hub untuk dibagikan oleh semua sirkuit spoke. *Router* spoke dapat saling berhubungan melalui hub *Router* menggunakan sirkuit virtual dan *subinterfaces* yang dirutekan. Gambar 32 tersebut menampilkan contoh topologi *point-to-point* yang terdiri dari tiga *Router* spoke yang terhubung ke *Router* hub melintasi *cloud* WAN.

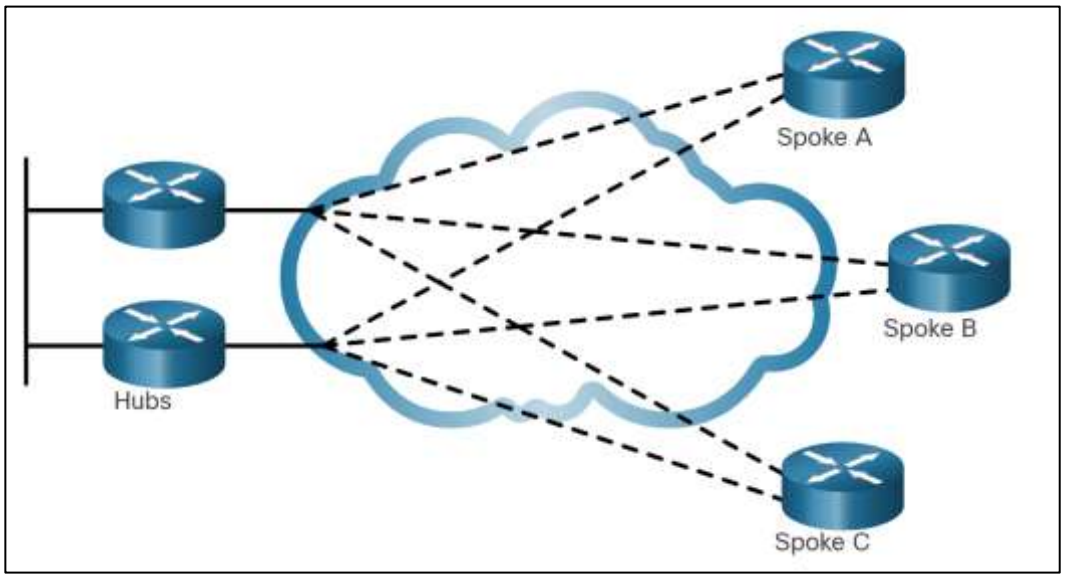


Gambar 32 Topologi Hub-and Spoke

Topologi *point-to-point* adalah topologi single-homed. Hanya ada satu *Router* hub dan semua komunikasi harus melaluinya. Oleh karena itu, *Router* spoke hanya dapat berkomunikasi satu sama lain melalui hub *Router*. Akibatnya, hub *Router* mewakili satu titik kegagalan. Jika gagal, komunikasi antar spoke juga gagal.

3. *Dual-homed Topology*

Topologi *dual-homed* menyediakan *redundancy*. Seperti yang ditunjukkan pada gambar 33, dua *Router* hub dual-homed dan secara redundan melekat pada tiga *Router* spoke di seluruh *cloud* WAN.



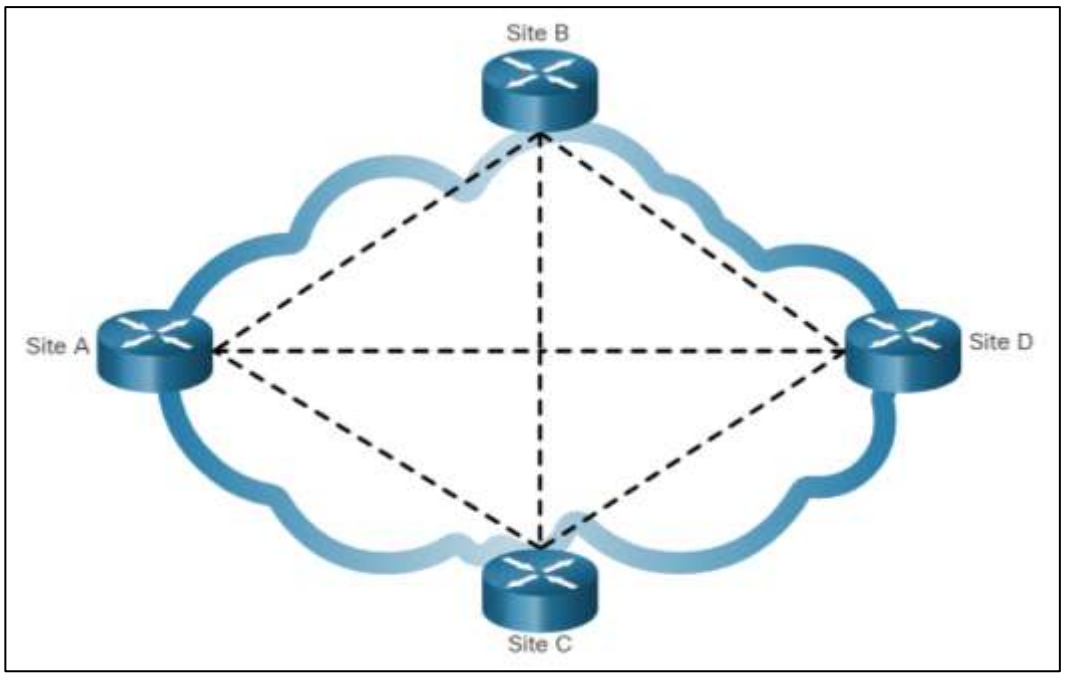
Gambar 33 Topologi *Dual-home*

Keuntungan dari topologi *dual-homed* adalah bahwa mereka menawarkan *redundancy* jaringan yang ditingkatkan, *load balancing*, komputasi dan pemrosesan terdistribusi, dan kemampuan untuk menerapkan koneksi penyedia layanan cadangan. Kerugiannya adalah bahwa mereka lebih mahal untuk diimplementasikan daripada topologi *single-homed*. Ini

karena mereka memerlukan perangkat keras jaringan tambahan, seperti *Router* dan *switch* tambahan. Topologi *dual-homed* juga lebih sulit diimplementasikan karena memerlukan konfigurasi tambahan, dan lebih kompleks.

4. *Fully Meshed Topology*

   Topologi yang sepenuhnya bertautan menggunakan beberapa sirkuit virtual untuk menghubungkan semua situs, seperti yang ditunjukkan pada gambar 34 diabwah ini.

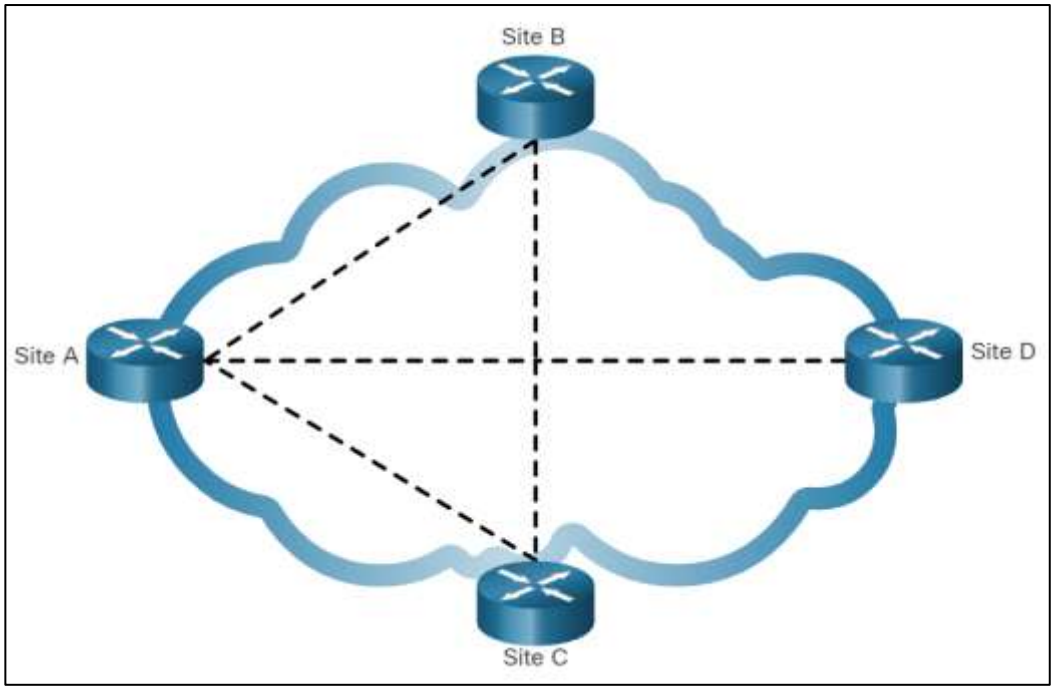


Gambar 34 Topologi Full Mesh

Ini adalah topologi yang paling toleran terhadap kesalahan dari lima topologi yang ditunjukkan. Misalnya, jika situs B kehilangan konektivitas ke situs A, maka dapat mengirim data melalui situs C atau situs D.

5. *Partially Meshed Topology*

   Topologi yang sebagian meshed menghubungkan banyak tetapi tidak semua situs. Misalnya, pada gambar 35, situs A, B, C masih sepenuhnya *meshed*. Situs D harus terhubung ke situs A untuk mencapai situs B dan C.

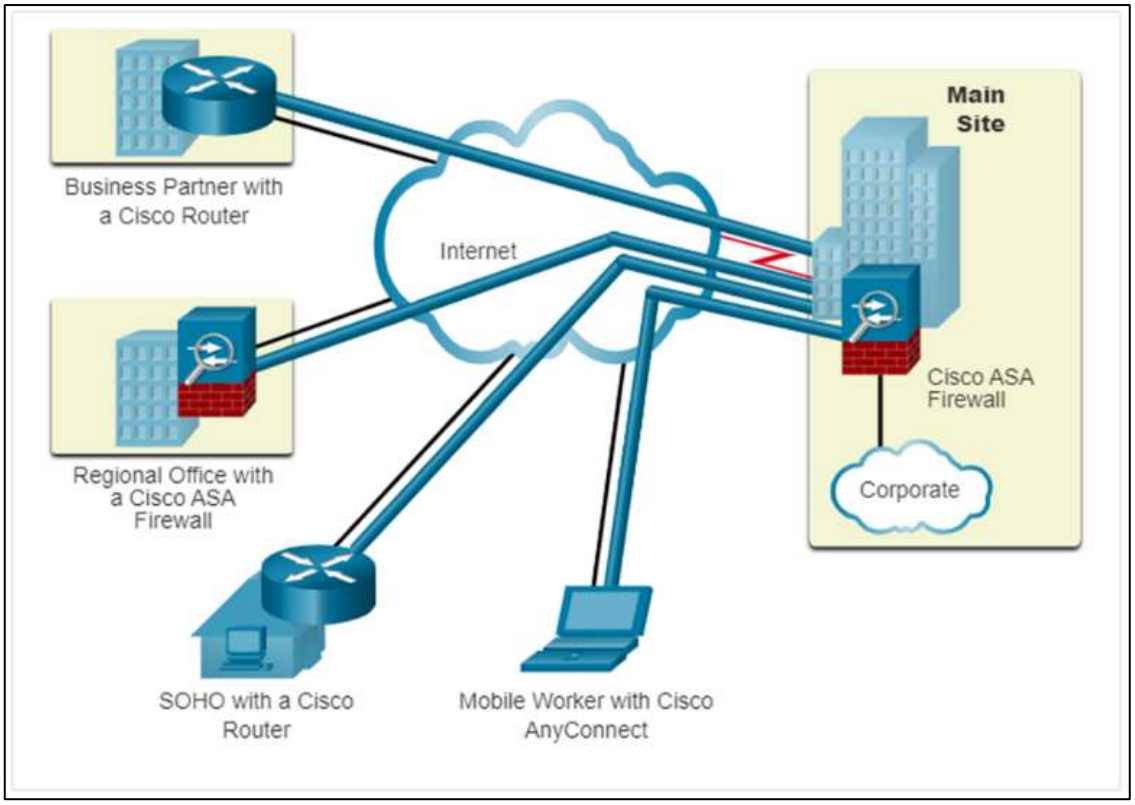


Gambar 35 Topologi partially meshed

e. *Virtual Private Network* (VPN)

Untuk mengamankan lalu lintas jaringan antara situs dan pengguna, organisasi menggunakan *Virtual Private Network* (VPN) untuk membuat koneksi jaringan pribadi ujung ke ujung. VPN bersifat virtual karena membawa informasi dalam jaringan pribadi, tetapi informasi itu sebenarnya diangkut melalui jaringan publik. VPN bersifat pribadi karena lalu lintas dienkripsi untuk menjaga kerahasiaan data saat diangkut melintasi jaringan publik.

Pada gambar Gambar 36 tersebut menunjukkan kumpulan berbagai jenis VPN yang dikelola oleh situs utama perusahaan. Terowongan memungkinkan situs dan pengguna jarak jauh untuk mengakses sumber daya jaringan situs utama dengan aman. Jenis VPN yang pertama adalah tunnel IP secara ketat yang tidak menyertakan autentikasi atau enkripsi data. Misalnya, *Generic Routing Encapsulation* (GRE) adalah protokol tunneling yang dikembangkan oleh Cisco dan yang tidak termasuk layanan enkripsi. GRE digunakan untuk mengenkapsulasi lalu lintas IPv4 dan IPv6 di dalam terowongan IP untuk membuat sambungan titik-ke-titik virtual.



Gambar 36 VPN

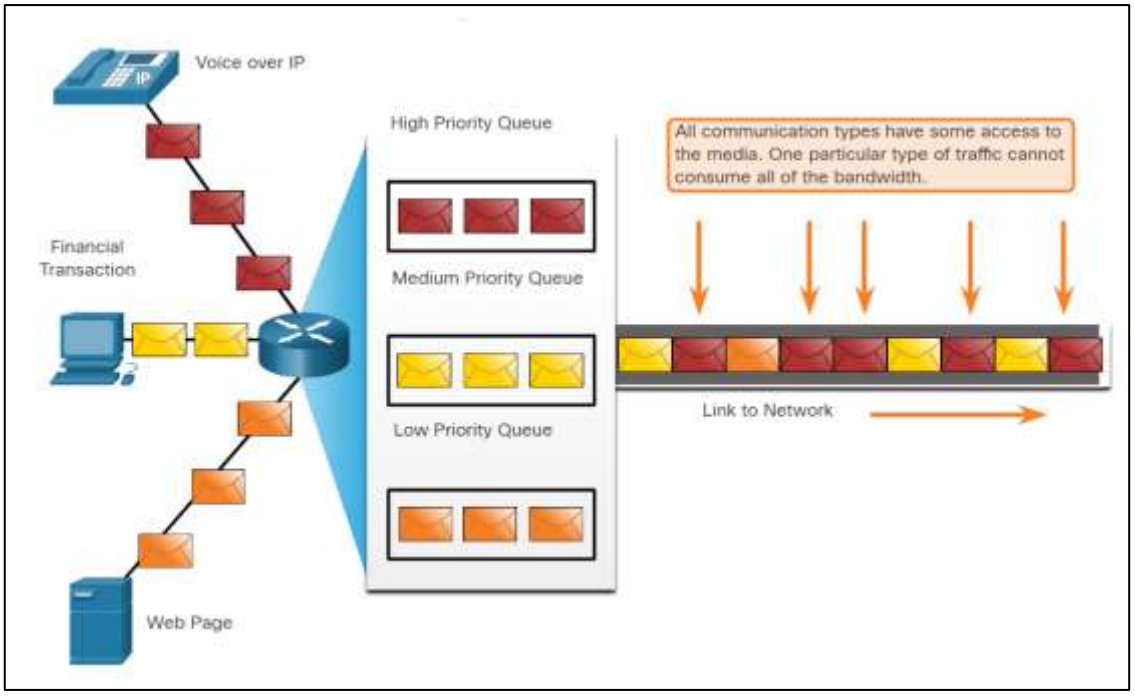
VPN modern sekarang sudah mendukung fitur enkripsi, seperti *Internet Protocol Security* (IPsec) dan *Secure Sockets Layer* (SSL) VPN untuk mengamankan lalu lintas jaringan antar situs. Manfaat utama VPN ditunjukkan pada tabel.

Manfaat	Deskripsi
Hemat Biaya	Dengan munculnya teknologi *bandwidth* tinggi yang hemat biaya, organisasi dapat menggunakan VPN untuk mengurangi biaya konektivitas mereka sekaligus meningkatkan *bandwidth* koneksi jarak jauh.
Keamanan	VPN menyediakan tingkat keamanan tertinggi yang tersedia, dengan menggunakan enkripsi canggih dan protokol otentikasi yang melindungi data dari akses yang tidak sah.
Skalabilitas	VPN memungkinkan organisasi untuk menggunakan internet, sehingga mudah untuk menambah pengguna baru tanpa menambah infrastruktur yang signifikan.
Kecocokan	VPN dapat diimplementasikan di berbagai macam opsi tautan WAN termasuk semua teknologi broadband yang populer. Pekerja jarak jauh dapat memanfaatkan koneksi berkecepatan tinggi ini untuk mendapatkan akses aman ke jaringan perusahaan mereka.

f. QoS

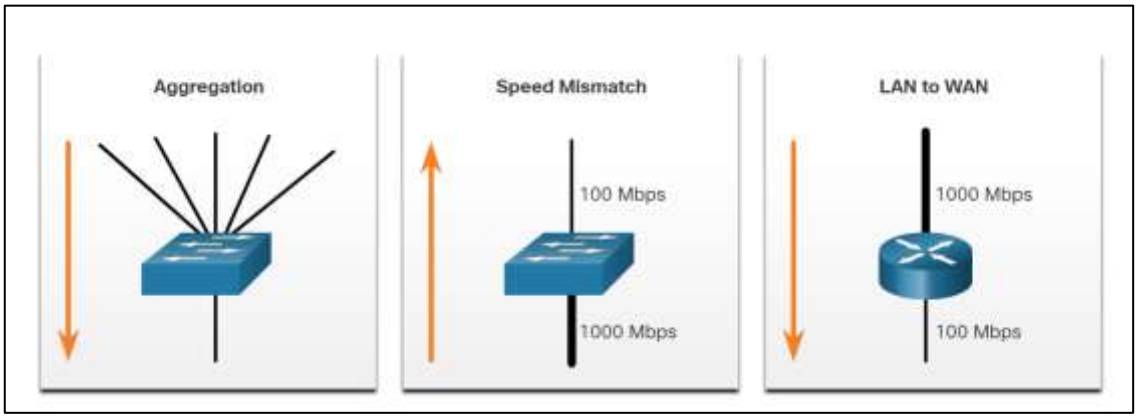
Quality of Service (QoS) adalah persyaratan jaringan yang terus meningkat saat ini. Aplikasi baru, seperti transmisi suara dan video langsung, menciptakan ekspektasi yang lebih tinggi untuk kualitas pengiriman di antara pengguna. Kemacetan terjadi ketika beberapa jalur komunikasi berkumpul ke satu perangkat seperti *router*, dan kemudian banyak dari data itu ditempatkan hanya pada beberapa antarmuka keluar, atau ke antarmuka yang lebih lambat. Kemacetan juga bisa terjadi apabila paket data yang besar mencegah paket yang lebih kecil

ditransmisikan secara tepat waktu. Ketika volume trafik lebih besar dari apa yang dapat diangkut di seluruh jaringan, perangkat mengantri (menahan) paket dalam memori sampai sumber daya tersedia untuk mengirimkannya. Antrian paket menyebabkan penundaan karena paket baru tidak dapat ditransmisikan sampai paket sebelumnya telah diproses. Jika jumlah paket yang harus diantri terus meningkat, memori di dalam perangkat akan terisi dan paket-paket akan dibatalkan. Satu teknik QoS yang dapat membantu dengan masalah ini adalah untuk mengklasifikasikan data ke dalam beberapa antrian, seperti yang ditunjukkan pada gambar 37.



Gambar 37 Antrian paket

Bandwidth jaringan diukur dalam jumlah bit yang dapat ditransmisikan dalam satu detik, atau bit per detik (bps). Misalnya, perangkat jaringan dapat digambarkan untuk memiliki kemampuan untuk melakukan transmisi 10 gigabit per detik (Gbps). Kemacetan jaringan menyebabkan penundaan. Sebuah *interface* mengalami kemacetan ketika ia disajikan dengan lalu lintas yang lebih banyak daripada yang bisa ditangani. Titik-titik kemacetan jaringan adalah kandidat ideal untuk mekanisme QoS. Gambar 38 ini menunjukkan tiga contoh titik kemacetan yang khas.



Gambar 38 Contoh Titik Kemacetan di jaringan

Penundaan atau latensi mengacu pada waktu yang diperlukan paket untuk melakukan perjalanan dari sumber ke tujuan. Dua jenis penundaan adalah tetap dan variabel. Penundaan tetap adalah jumlah waktu tertentu yang dibutuhkan proses tertentu, seperti berapa lama waktu yang dibutuhkan untuk menempatkan bit pada media transmisi. Penundaan variabel membutuhkan waktu yang tidak ditentukan dan dipengaruhi oleh faktor-faktor seperti berapa banyak lalu lintas yang sedang diproses. Sumber-sumber penundaan dapat dilihat dalam tabel.

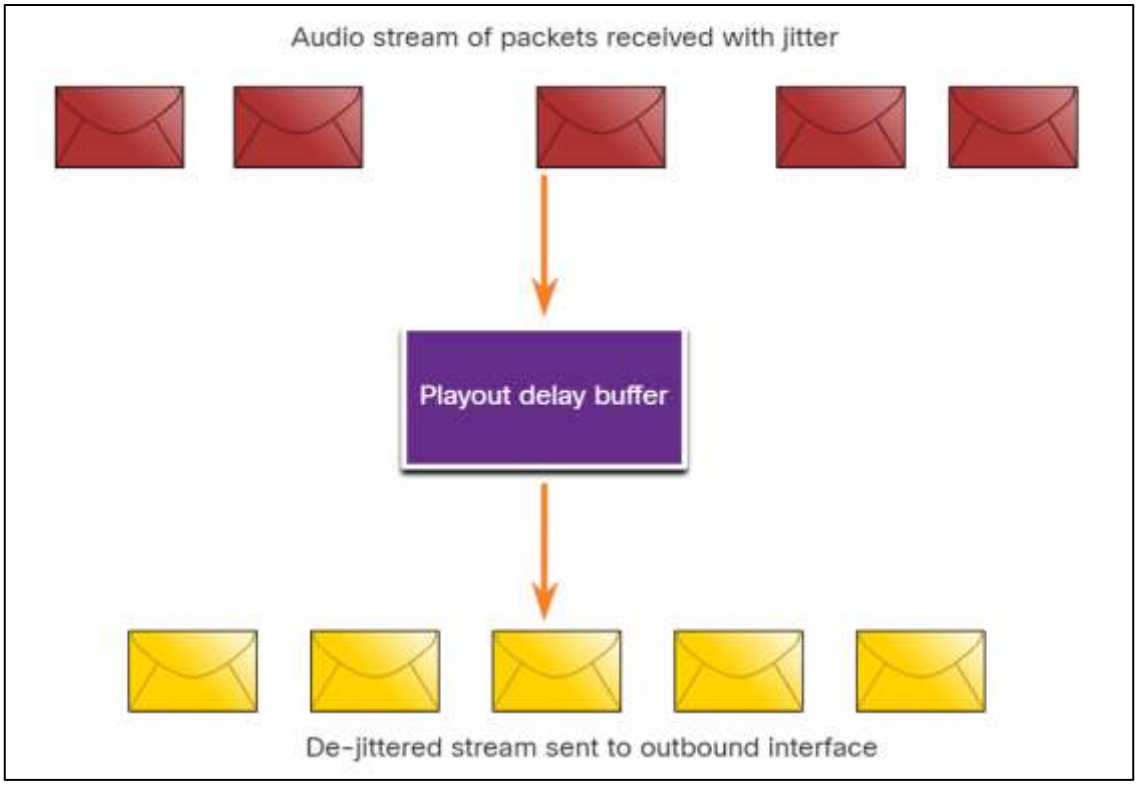
Tabel 14 Sumber penundaan pada jaringan

Penundaan	**Deskripsi**
Penundaan Kode	Jumlah waktu tetap yang diperlukan untuk mengompres data pada sumber sebelum mentransmisikan ke perangkat internetworking pertama, biasanya *switch*.
Penundaan Paket	Waktu tetap yang diperlukan untuk mengenkapsulasi paket dengan semua informasi header yang diperlukan.
Penundaan antrian	Jumlah variabel waktu sebuah frame atau paket menunggu untuk ditransmisikan pada link.
Penundaan serialisasi	Jumlah waktu tetap yang diperlukan untuk mentransmisikan frame ke kawat(wire).
Penundaan propagasi	Jumlah variabel waktu yang diperlukan frame untuk melakukan perjalanan antara sumber dan tujuan.
Penundaan De-jitter	Jumlah waktu tetap yang diperlukan untuk menyangga aliran paket dan kemudian mengirimkannya dalam interval yang berjarak sama.

Jitter adalah variasi dalam penundaan paket yang diterima. Di sisi pengirim, paket dikirim dalam aliran kontinu dengan paket-paket yang berjarak secara merata. Karena kemacetan jaringan, antrian yang tidak tepat, atau kesalahan konfigurasi, penundaan antara setiap paket dapat bervariasi, bukannya tetap konstan. Baik penundaan dan jitter perlu dikontrol dan diminimalkan untuk mendukung lalu lintas *real-time* dan interaktif.

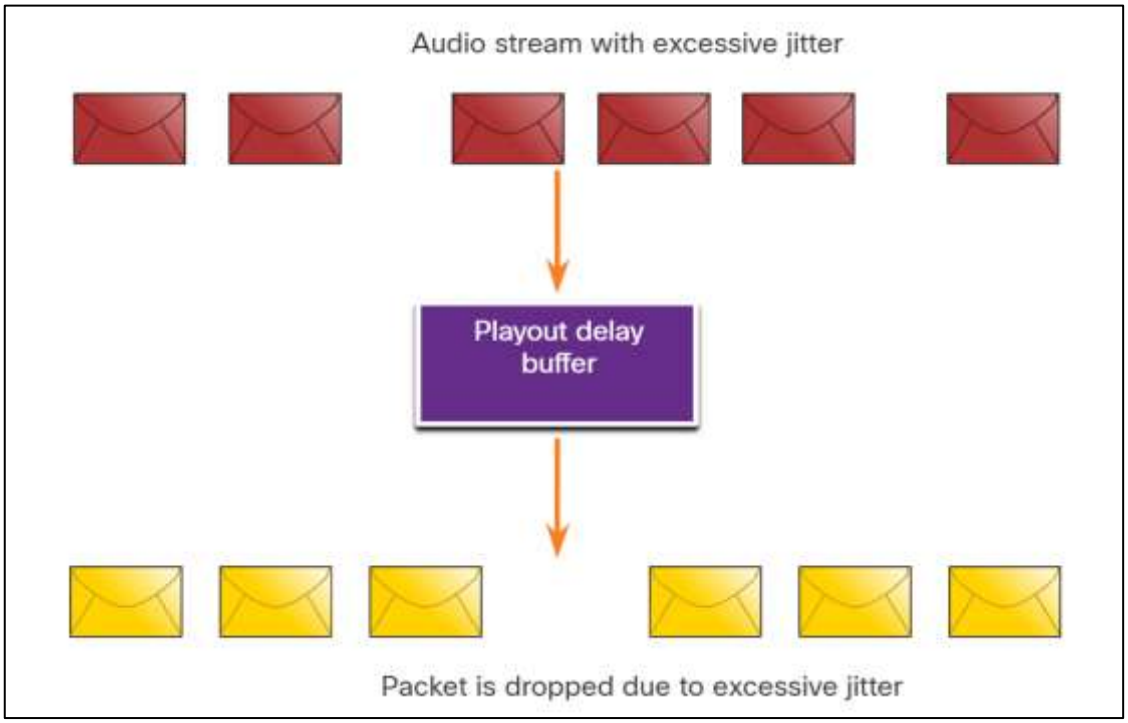
Tanpa mekanisme QoS, paket diproses sesuai urutan penerimaannya. Ketika terjadi kemacetan, perangkat jaringan seperti *router* dan *switch* dapat menjatuhkan paket. Ini berarti bahwa paket yang sensitif terhadap waktu, seperti video dan suara *real-time*, akan dijatuhkan dengan frekuensi yang sama dengan data yang tidak sensitif terhadap waktu, seperti email dan *web browsing*.

Ketika *router* menerima aliran audio digital *Real-Time Protocol* (RTP) untuk *Voice over* IP (VoIP), *Router* harus mengkompensasi jitter yang ditemui. Mekanisme yang menangani fungsi ini adalah *playout delay buffer*. *Playout delay buffer* harus menyangga paket-paket ini dan kemudian mengalirkannya dalam aliran yang stabil, seperti yang ditunjukkan pada gambar 39. Paket digital kemudian dikonversi kembali ke aliran audio analog.



Gambar 39 *Playout Delay Buffer* mengkompensasi Jitter

Jika jitter begitu besar sehingga menyebabkan paket diterima di luar jangkauan buffer ini, paket di luar jangkauan akan dibuang dan putus terdengar dalam audio, seperti ditunjukkan dalam gambar 40.



Gambar 40 Paket Terputus Karena Jitter yang Berlebihan

Untuk kehilangan sekecil satu paket, prosesor sinyal digital (DSP) menginterpolasi apa yang dianggapnya sebagai audio yang seharusnya dan tidak ada masalah yang terdengar oleh

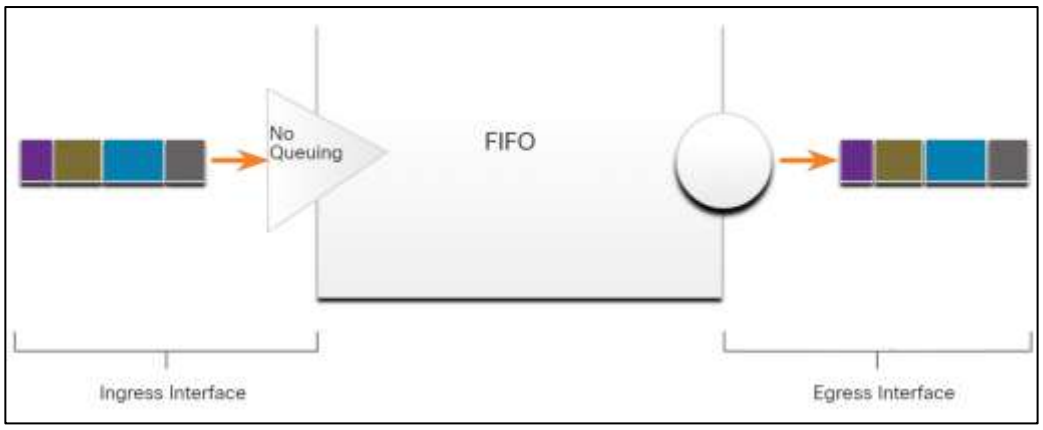
pengguna. Namun demikian, apabila jitter melebihi apa yang dapat dilakukan DSP untuk mengganti paket yang hilang, masalah audio akan terdengar. Packet loss adalah penyebab yang sangat umum dari masalah kualitas suara pada jaringan IP. Dalam jaringan yang dirancang dengan benar, *packet loss* seharusnya mendekati nol. Codec suara yang digunakan oleh DSP dapat mentolerir beberapa tingkat packet loss tanpa efek dramatis pada kualitas suara. Insinyur jaringan menggunakan mekanisme QoS untuk mengklasifikasikan paket suara untuk nol packet loss. *Bandwidth* dijamin untuk panggilan suara dengan memberikan prioritas pada lalu lintas suara di atas lalu lintas yang tidak sensitif terhadap penundaan.

Kebijakan QoS yang diimplementasikan oleh administrator jaringan menjadi aktif ketika terjadi kemacetan pada link. Antrian adalah alat manajemen kemacetan yang dapat menyangga, memprioritaskan, dan jika diperlukan, menyusun ulang paket sebelum ditransmisikan ke tujuan. Berikut ini adalah sejumlah algoritma antrian tersedia. Untuk tujuan kursus ini, kita akan fokus pada yang berikut ini:yang di gunakan untuk QoS.

1. *First In First Out* (FIFO)

   Dalam bentuknya yang paling sederhana, antrian *First In First Out* (FIFO), juga dikenal sebagai antrian yang pertama datang, pertama dilayani, menyangga dan meneruskan paket-paket sesuai urutan kedatangannya. FIFO tidak memiliki konsep prioritas atau kelas trafik dan akibatnya, tidak membuat keputusan tentang prioritas paket. Hanya ada satu antrian, dan semua paket diperlakukan sama. Paket-paket dikirim keluar antarmuka sesuai urutan kedatangannya, seperti yang ditunjukkan pada gambar. Meskipun beberapa trafik mungkin lebih penting atau sensitif terhadap waktu berdasarkan klasifikasi prioritas, perhatikan bahwa trafik dikirim keluar sesuai urutan penerimaannya. Ketika FIFO digunakan, lalu lintas yang penting atau sensitif terhadap waktu dapat didrop ketika ada kemacetan pada *router* atau antarmuka *switch*.

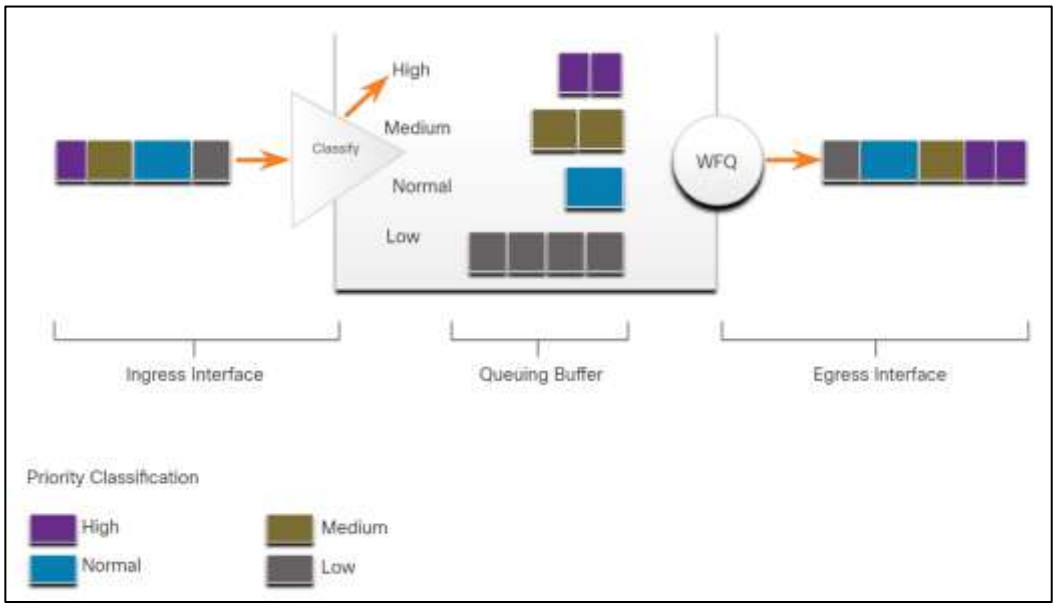
   Ketika tidak ada strategi antrian lain yang dikonfigurasi, semua *interface*, kecuali *interface* serial pada E1 (2.048 Mbps) dan di bawahnya, menggunakan FIFO secara default. (*Interface* serial pada E1 dan di bawahnya menggunakan WFQ secara default). FIFO merupakan metode antrian tercepat, efektif untuk sambungan besar yang mempunyai sedikit penundaan dan kemacetan minimal. Jika sambungan anda mempunyai sedikit kemacetan, antrian FIFO mungkin satu-satunya antrian yang perlu anda gunakan.



Gambar 41 Contoh FIFO

2. *Weighted Fair Queuing* (WFQ)

Weighted Fair Queuing (WFQ) adalah metode penjadwalan otomatis yang menyediakan alokasi *bandwidth* yang adil untuk semua lalu lintas jaringan. WFQ tidak mengijinkan pilihan klasifikasi untuk dikonfigurasi. WFQ menerapkan prioritas, atau bobot, untuk trafik yang teridentifikasi dan mengklasifikasikannya ke dalam percakapan atau aliran, seperti yang ditunjukkan pada gambar 42.



Gambar 42 Contoh WFQ

WFQ kemudian menentukan berapa banyak *bandwidth* yang diizinkan untuk setiap aliran relatif terhadap aliran lainnya. Algoritma berbasis aliran yang digunakan oleh WFQ secara simultan menjadwalkan trafik interaktif ke depan antrian untuk mengurangi waktu respon. Kemudian secara adil membagi *bandwidth* yang tersisa di antara arus *bandwidth* tinggi. WFQ memungkinkan Anda untuk memberikan prioritas pada lalu lintas interaktif bervolume rendah, seperti sesi Telnet dan suara, di bandingkan lalu lintas bervolume tinggi, seperti sesi FTP. Ketika beberapa arus transfer file terjadi secara bersamaan, transfer diberikan *bandwidth* yang sebanding. WFQ mengklasifikasikan lalu lintas ke dalam aliran yang berbeda berdasarkan pengalamatan header paket, termasuk

karakteristik seperti alamat IP sumber dan tujuan, alamat MAC, nomor port, protokol, dan nilai *Type of Service* (ToS). Nilai ToS dalam header IP dapat digunakan untuk mengklasifikasikan lalu lintas.

Arus lalu lintas *bandwidth* rendah, yang merupakan mayoritas lalu lintas, menerima layanan istimewa yang memungkinkan seluruh muatan yang ditawarkan untuk dikirim secara tepat waktu. Arus lalu lintas bervolume tinggi berbagi kapasitas yang tersisa secara proporsional di antara mereka sendiri.

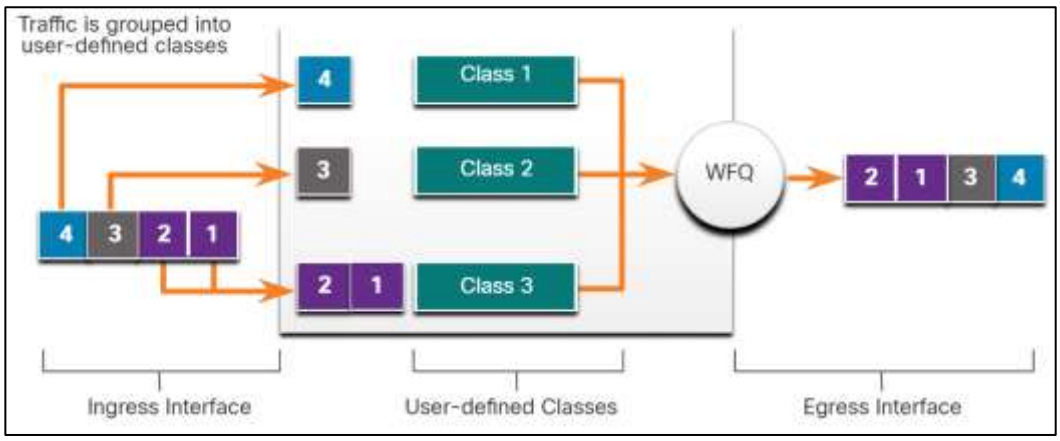
Keterbatasan

WFQ tidak didukung dengan *tunneling* dan enkripsi karena fitur-fitur ini memodifikasi informasi konten paket yang diperlukan oleh WFQ untuk klasifikasi. Meskipun WFQ secara otomatis beradaptasi dengan perubahan kondisi trafik jaringan, WFQ tidak menawarkan tingkat kontrol yang tepat atas alokasi *bandwidth* yang ditawarkan CBWFQ.

3. *Class-Based Weighted Fair Queuing* (CBWFQ)

Class-Based Weighted Fair Queuing (CBWFQ) memperluas fungsionalitas WFQ standar untuk memberikan dukungan bagi kelas lalu lintas yang ditentukan pengguna. Dengan CBWFQ, anda mendefinisikan kelas lalu lintas berdasarkan kriteria kecocokan termasuk protokol, daftar kontrol akses (ACL), dan antarmuka input. Paket-paket yang memenuhi kriteria kecocokan untuk sebuah kelas merupakan trafik untuk kelas tersebut. Antrian FIFO dicadangkan untuk setiap kelas, dan trafik yang termasuk dalam kelas diarahkan ke antrian untuk kelas itu, seperti yang ditunjukkan pada gambar 43.

Ketika kelas telah didefinisikan menurut kriteria kecocokannya, Anda dapat menetapkan karakteristiknya. Untuk mengkarakterisasi kelas, Anda menetapkan *bandwidth*, bobot, dan batas paket maksimum. *Bandwidth* yang ditetapkan ke kelas adalah *bandwidth* terjamin yang dikirimkan ke kelas selama kemacetan. Untuk mengkarakterisasi kelas, Anda juga menentukan batas antrian untuk kelas itu, yang merupakan jumlah maksimum paket yang diizinkan untuk terakumulasi dalam antrian untuk kelas tersebut. Paket-paket yang termasuk dalam kelas tunduk pada *bandwidth* dan batas antrian yang menjadi ciri kelas.

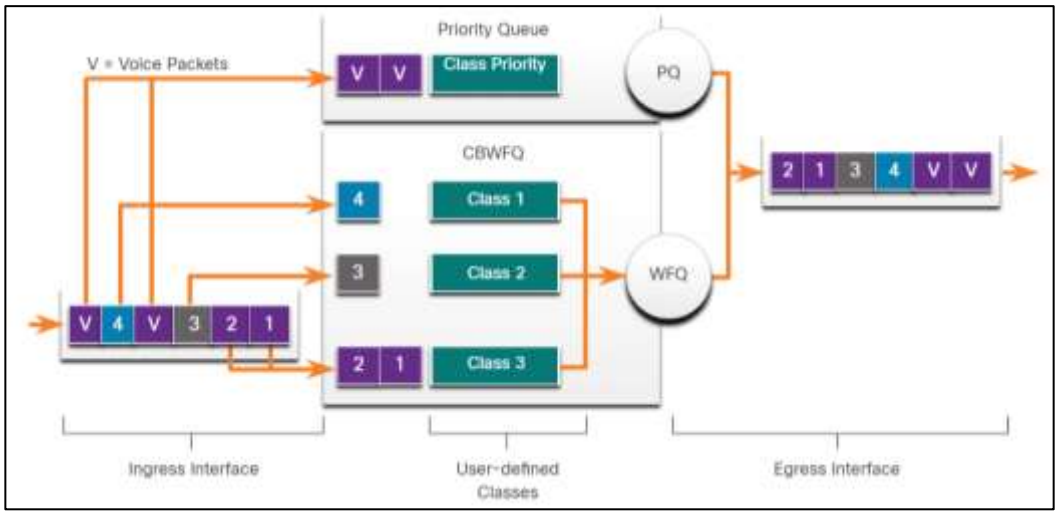


Gambar 43 Contoh CBWFQ

Setelah antrian telah mencapai batas antrian yang dikonfigurasi, menambahkan lebih banyak paket ke kelas menyebabkan tail drop atau packet drop berlaku, tergantung pada bagaimana kebijakan kelas dikonfigurasi. *Tail drop* berarti *router* hanya membuang paket apa pun yang tiba di ujung ekor antrian yang telah sepenuhnya menggunakan sumber daya penahan paketnya. Ini adalah respon antrian default untuk kemacetan. *Tail drop* memperlakukan semua lalu lintas sama dan tidak membedakan antara kelas layanan.

4. *Low Latency Queuing* (LLQ)

Fitur *Low Latency Queuing* (LLQ) membawa antrian prioritas yang ketat (PQ) ke CBWFQ. PQ yang ketat memungkinkan paket-paket yang sensitif terhadap penundaan seperti suara dikirim sebelum paket dalam antrian lainnya. LLQ menyediakan antrian prioritas yang ketat untuk CBWFQ, mengurangi jitter dalam percakapan suara, seperti yang ditunjukkan pada gambar 44.



Gambar 44 Contoh LLQ

Tanpa LLQ, CBWFQ menyediakan WFQ berdasarkan kelas-kelas yang ditentukan tanpa antrian prioritas yang ketat yang tersedia untuk lalu lintas waktu nyata/*real time*. Bobot untuk paket yang termasuk dalam kelas tertentu berasal dari *bandwidth* yang Anda tetapkan ke kelas ketika Anda mengkonfigurasinya. Oleh karena itu, *bandwidth* yang ditetapkan ke paket dari kelas menentukan urutan paket yang dikirim. Semua paket dilayani secara adil berdasarkan berat; tidak ada kelas paket yang dapat diberikan prioritas yang ketat. Skema ini menimbulkan masalah untuk trafik suara yang sebagian besar tidak toleran terhadap penundaan, terutama variasi dalam penundaan. Untuk trafik suara, variasi dalam *delay* memperkenalkan ketidakteraturan transmisi yang bermanifestasi sebagai jitter dalam percakapan yang didengar.

LLQ memungkinkan paket-paket yang sensitif terhadap penundaan seperti suara untuk dikirim terlebih dahulu (sebelum paket-paket dalam antrian lain), memberikan paket-paket yang sensitif terhadap penundaan perlakuan istimewa atas lalu lintas lainnya. Meskipun dimungkinkan untuk mengklasifikasikan berbagai jenis lalu lintas real time ke antrian prioritas yang ketat, Cisco merekomendasikan bahwa hanya lalu lintas suara yang diarahkan ke antrian prioritas.

3. Tugas

Implementasi Proyek (Proyek Team Base)

Pada tahapan ini secara berkelompok melakukan implementasi jaringan kampus, sesuai dengan desain yang telah di buat pada tugas kegiatan belajar 2.

Kegiatan Belajar 4
Operasional

1. Sub-Capaian Pembelajaran

a. Mampu menjelaskan konsep manajemen jaringan, mengimplementasikan manajemen jaringan pada jaringan kampus, dan mampu menganalisa data hasil *monitoring* manajemen jaringan dalam meningkatkan jaringan kampus.

b. Mampu mengimplementasikan tahapan-tahapan dalam melakukan pemeliharaan, dan pemecahan masalah jaringan kampus.

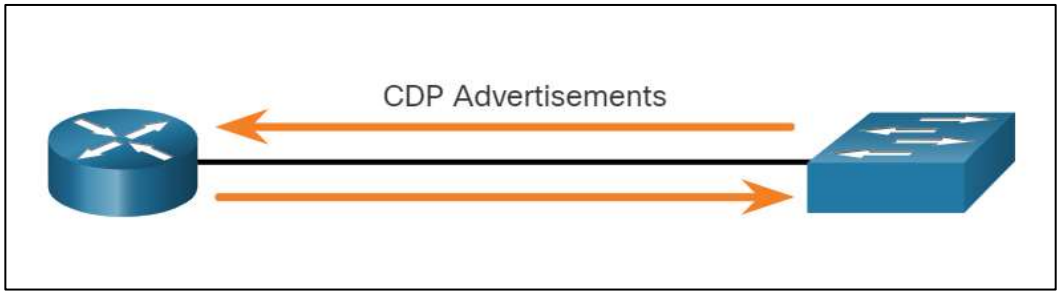
2. Pembahasan

a. Manajemen Jaringan

Jaringan merupakan hal yang kompleks dan perlu dikelola. Untungnya, ada banyak tool yang didesain untuk membuat manajemen jaringan lebih sederhana. Modul ini memperkenalkan beberapa tool dan protokol untuk membantu anda mengelola jaringan.

1. *Cisco Discovery Protocol* (CDP)

CDP adalah protokol *Layer* 2 milik Cisco yang digunakan untuk mengumpulkan informasi tentang perangkat Cisco yang berbagi link data yang sama. CDP adalah media dan protokol independen dan berjalan pada semua perangkat Cisco, seperti *router*, *switch*, dan server akses. Perangkat mengirimkan iklan CDP secara periodik ke perangkat yang terhubung, seperti yang ditunjukkan pada gambar 45.



Gambar 45 CDP Advertisements

Iklan-iklan ini berbagi informasi tentang jenis perangkat yang ditemukan, nama perangkat, dan jumlah serta jenis *interface*. Karena sebagian besar perangkat jaringan terhubung ke perangkat lain, CDP dapat membantu dalam keputusan desain jaringan, pemecahan masalah, dan membuat perubahan pada peralatan. CDP juga dapat digunakan sebagai alat penemuan jaringan untuk menentukan informasi tentang perangkat tetangga. Informasi yang dikumpulkan dari CDP ini dapat membantu membangun topologi logis jaringan ketika dokumentasi tidak ada atau kurang detail.

Untuk menverifikasi CDP dapat menggunakan perintah ***show* cdp**

```
Router# show cdp
Global CDP information:
      Sending CDP packets every 60 seconds
      Sending a holdtime value of 180 seconds
      Sending CDPv2 advertisements is enabled
```

Untuk menonaktifkan CDP dengan perintah **no cdp run**

```
Router(config)# no cdp run
Router(config)# exit
Router# show cdp
CDP is not enabled
Router# configure terminal
Router(config)# cdp run
```

Untuk mengaktifkan CDP pada spesifik *interface* dapat menggunakan perintah berikut ini:

```
Switch(config)# interface gigabitethernet 0/0/1
Switch(config-if)# cdp enable
```

Untuk melihat informasi perangkat tetangga dengan perintah berikut ini:

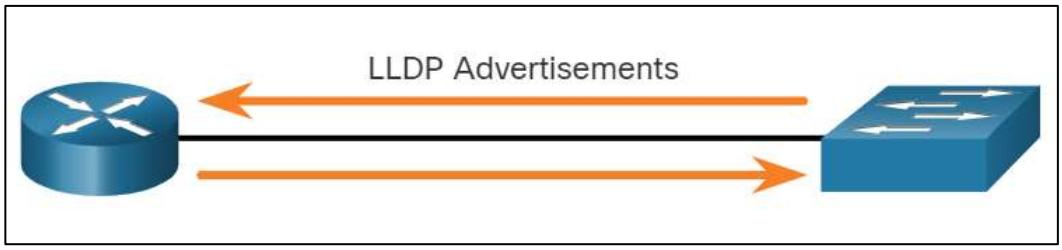
```
Router# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

Total cdp entries displayed : 0
```

2. *Link Layer Discovery Protocol* (LLDP)

Link Layer Discovery Protocol (LLDP) melakukan hal yang sama seperti CDP, tetapi tidak spesifik untuk perangkat Cisco. Sebagai bonus, Anda masih dapat menggunakannya jika Anda memiliki perangkat Cisco. Dengan satu atau lain cara, Anda akan mendapatkan peta jaringan Anda. LLDP adalah protokol penemuan tetangga yang netral-vendor yang mirip dengan CDP. LLDP bekerja dengan perangkat jaringan, seperti *router*, *switch*, dan titik akses LAN nirkabel. Protokol ini mengiklankan identitas dan kemampuannya ke perangkat lain dan menerima informasi dari perangkat *Layer* 2 yang terhubung secara fisik.



Gambar 46 LLDP

Tergantung pada perangkat, LLDP dapat diaktifkan secara default. Untuk mengaktifkan LLDP secara global pada perangkat jaringan Cisco, masukkan perintah **lldp run** dalam mode konfigurasi global. Untuk menonaktifkan LLDP, masukkan perintah **no lldp run** dalam mode konfigurasi global. Mirip dengan CDP, LLDP dapat dikonfigurasi pada *interface* tertentu. Namun, LLDP harus dikonfigurasi secara terpisah untuk mengirim dan menerima paket LLDP. Untuk memverifikasi LLDP telah diaktifkan pada perangkat, masukkan perintah ***show* lldp** dalam mode privileged EXEC.

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
Switch# show lldp
Global LLDP Information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialisation delay is 2 seconds
```

Untuk melihat informasi perangkat tetangga dengan perinta berikut ini:

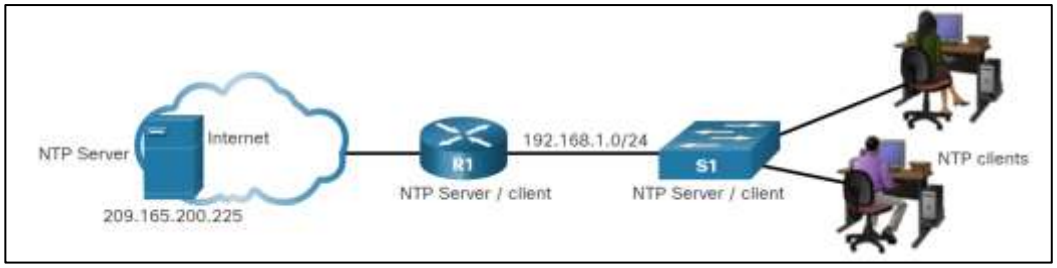
```
S1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
R1                  Fa0/5          117        R               Gi0/0/1
S2                  Fa0/1          112        B               Fa0/1
Total entries displayed: 2
```

3. *Network Time Protocol* (NTP)

Sebelum anda benar-benar mendalami manajemen jaringan, satu hal yang akan membantu anda tetap pada jalurnya adalah memastikan bahwa semua komponen anda diatur ke waktu dan tanggal yang sama. Jam perangkat lunak pada *router* atau *switch* dimulai ketika sistem melakukan *booting*. Ini adalah sumber utama waktu untuk sistem. Penting untuk menyinkronkan waktu di semua perangkat di jaringan karena semua aspek pengelolaan, pengamanan, *troubleshooting*, dan perencanaan jaringan memerlukan *timestamping* yang akurat. Bila waktu tidak disinkronkan antar perangkat, tidak mungkin untuk menentukan urutan kejadian dan penyebab suatu kejadian. Biasanya, pengaturan tanggal dan waktu pada *Router* atau *switch* dapat diatur dengan menggunakan salah satu dari dua metode yaitu secara manual mengkonfigurasi tanggal dan waktu, atau mengkonfigurasi *Network Time Protocol* (NTP).

Seiring dengan berkembangnya jaringan, menjadi sulit untuk memastikan bahwa semua perangkat infrastruktur beroperasi dengan waktu yang tersinkronisasi. Bahkan dalam lingkungan jaringan yang lebih kecil, metode manual tidak ideal. Jika *Router* reboot, bagaimana *router* akan mendapatkan tanggal dan stempel waktu yang akurat?. Oleh karena itu solusi yang lebih baik adalah mengkonfigurasi NTP pada jaringan. Protokol ini memungkinkan *router* pada jaringan untuk menyinkronkan pengaturan waktu mereka dengan server NTP. Sekelompok klien NTP yang memperoleh informasi waktu dan tanggal dari satu sumber memiliki pengaturan waktu yang lebih konsisten. Ketika NTP diimplementasikan dalam jaringan, NTP dapat diatur untuk menyinkronkan ke jam master pribadi, atau dapat menyinkronkan ke server NTP yang tersedia untuk umum di internet. NTP menggunakan port UDP 123 dan didokumentasikan dalam RFC 1305.

Pada gambar menunjukkan topologi yang digunakan untuk mendemonstrasikan konfigurasi dan verifikasi NTP.



Gambar 47 Contoh topologi NTP

Sebelum NTP dikonfigurasi pada jaringan, perintah *show* clock menampilkan waktu saat ini pada jam perangkat lunak. Dengan opsi detail, perhatikan bahwa sumber waktu adalah konfigurasi pengguna. Itu berarti waktu dikonfigurasi secara manual dengan perintah clock.

```
R1# show clock detail
20:55:10.207 UTC Fri Nov 15 2019
Time source is user configuration
```

Perintah **ntp server ip-address** dikeluarkan dalam modus konfigurasi global untuk mengkonfigurasi 209.165.200.225 sebagai server NTP untuk R1. Untuk memverifikasi sumber waktu diatur ke NTP, gunakan perintah *show* clock detail. Perhatikan bahwa sekarang sumber waktu adalah NTP.

```
R1(config)# ntp server 209.165.200.225
R1(config)# end
R1# show clock detail
21:01:34.563 UTC Fri Nov 15 2019
Time source is NTP
```

Dalam contoh berikut, perintah *show* ntp *associations* dan *show* ntp status digunakan untuk memverifikasi bahwa R1 disinkronkan dengan server NTP di 209.165.200.225. Perhatikan bahwa R1 disinkronkan dengan server NTP stratum 1 di 209.165.200.225, yang disinkronkan dengan jam GPS. Perintah *show* ntp status menampilkan bahwa R1 sekarang adalah perangkat stratum 2 yang disinkronkan dengan server NTP di 209.165.220.225.

```
R1# show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
*~209.165.200.225 .GPS.           1     61     64   377  0.481   7.480  4.261
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
ntp uptime is 589900 (1/100 of seconds), resolution is 4016
reference time is DA088DD3.C4E659D3 (13:21:23.769 PST Fri Nov 15 2019)
clock offset is 7.0883 msec, root delay is 99.77 msec
root dispersion is 13.43 msec, peer dispersion is 2.48 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000001803 s/s
system poll interval is 64, last update was 169 sec ago.
```

Selanjutnya, jam pada S1 dikonfigurasi untuk melakukan sinkronisasi ke R1 dengan perintah ntp server dan kemudian konfigurasi diverifikasi dengan perintah *show* ntp *associations*, seperti yang ditampilkan.

```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
*~192.168.1.1     209.165.200.225  2     12     64   377  1.066  13.616  3.840
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Output dari perintah *show* ntp *associations* memverifikasi bahwa jam pada S1 sekarang disinkronkan dengan R1 di 192.168.1.1 melalui NTP. R1 adalah perangkat stratum 2 dan server NTP untuk S1. Sekarang S1 adalah perangkat stratum 3 yang dapat menyediakan layanan NTP ke perangkat lain dalam jaringan, seperti perangkat akhir.

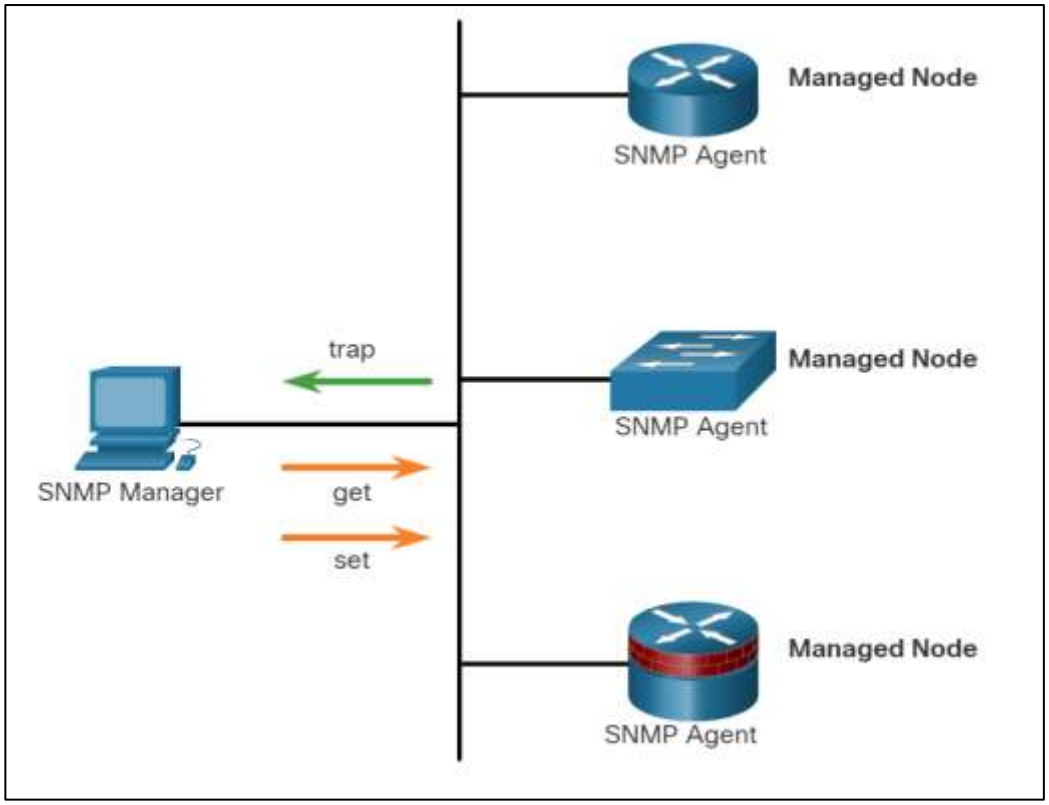
```
S1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2**17
reference time is DA08904B.3269C655 (13:31:55.196 PST Tue Nov 15 2019)
clock offset is 18.7764 msec, root delay is 102.42 msec
root dispersion is 38.03 msec, peer dispersion is 3.74 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000003925 s/s
system poll interval is 128, last update was 178 sec ago.
```

4. *Simple Network Management Protocol* (SNMP)

SNMP dikembangkan untuk memungkinkan administrator mengelola node seperti server, *workstation*, *router*, *switch*, dan peralatan keamanan, pada jaringan IP. SNMP memungkinkan administrator jaringan untuk memonitor dan mengelola kinerja jaringan, menemukan dan memecahkan masalah jaringan, dan merencanakan pertumbuhan jaringan. SNMP adalah protokol lapisan aplikasi yang menyediakan format pesan untuk komunikasi antara manajer dan agen. Sistem SNMP terdiri dari tiga elemen:

1. Manajer SNMP
2. Agen SNMP (node yang dikelola)
3. Basis Informasi Manajemen (Management Information Base (MIB))

Untuk mengkonfigurasi SNMP pada perangkat jaringan, pertama-tama perlu mendefinisikan hubungan antara manajer dan agen. Manajer SNMP adalah bagian dari sistem manajemen jaringan (NMS). Manajer SNMP menjalankan perangkat lunak manajemen SNMP. Seperti yang ditunjukkan pada gambar 49, manajer SNMP dapat mengumpulkan informasi dari agen SNMP dengan menggunakan aksi "get" dan dapat mengubah konfigurasi pada agen dengan menggunakan aksi "set". Selain itu, agen SNMP dapat meneruskan informasi langsung ke manajer jaringan dengan menggunakan "traps(perangkap)”.



Gambar 48 SNMP

Agen SNMP dan MIB berada pada perangkat klien SNMP. Perangkat jaringan yang harus dikelola, seperti *switch*, *router*, server, *firewall*, dan workstation, dilengkapi dengan modul perangkat lunak agen SNMP. MIB menyimpan data tentang perangkat dan statistik operasional dan dimaksudkan untuk tersedia bagi pengguna jarak jauh yang diautentikasi. Agen SNMP bertanggung jawab untuk menyediakan akses ke MIB lokal. SNMP mendefinisikan bagaimana informasi manajemen dipertukarkan antara aplikasi manajemen jaringan dan agen manajemen. Manajer SNMP melakukan polling pada agen dan menanyakan MIB untuk agen SNMP pada port UDP 161. Agen SNMP mengirim setiap perangkap SNMP ke manajer SNMP pada port UDP 162.

Agen SNMP yang berada pada perangkat yang dikelola mengumpulkan dan menyimpan informasi tentang perangkat dan operasinya. Informasi ini disimpan oleh agen secara lokal dalam MIB. Manajer SNMP kemudian menggunakan agen SNMP untuk mengakses informasi dalam MIB. Ada dua permintaan manajer SNMP utama, get dan set. Permintaan get digunakan oleh NMS untuk meminta data dari perangkat. Permintaan set digunakan oleh NMS untuk mengubah variabel konfigurasi dalam perangkat agen. Permintaan set juga dapat memulai tindakan dalam perangkat. Misalnya, satu set dapat menyebabkan *router* untuk reboot, mengirim file konfigurasi, atau menerima file konfigurasi. Manajer SNMP menggunakan tindakan get dan set untuk melakukan operasi yang dijelaskan dalam tabel 15.

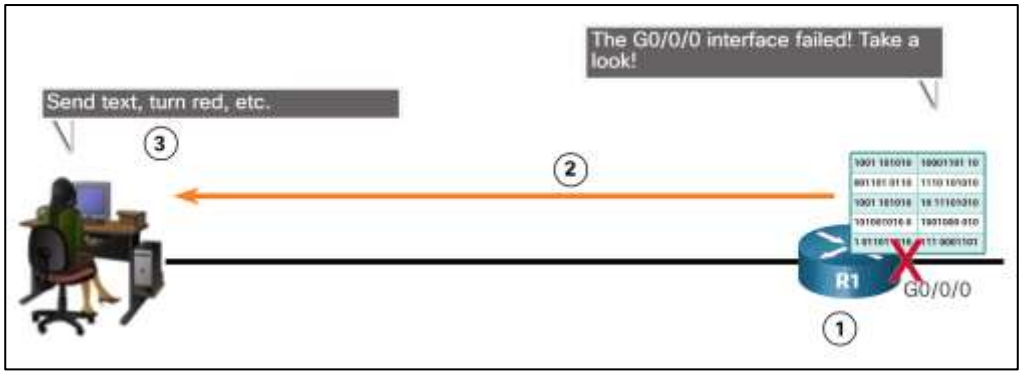
Tabel 15 Operasi SNMP

Operasi	Deskripsi
get-request	Mengambil nilai dari variabel tertentu.
get-next-request	Mengambil nilai dari variabel dalam tabel; manajer SNMP tidak perlu mengetahui nama variabel yang tepat. Pencarian berurutan dilakukan untuk menemukan variabel yang dibutuhkan dari dalam tabel.
get-bulk-request	Mengambil blok data yang besar, seperti beberapa baris dalam tabel, yang jika tidak, akan memerlukan transmisi banyak blok data kecil. (Hanya berfungsi dengan SNMPv2 atau yang lebih baru).
get-response	Balasan ke get-request, get-next-request, dan set-request yang dikirim oleh NMS.
set-request	Menyimpan nilai dalam variabel tertentu.

a. Perangkap Agen SNMP (SNMP Agent Traps)

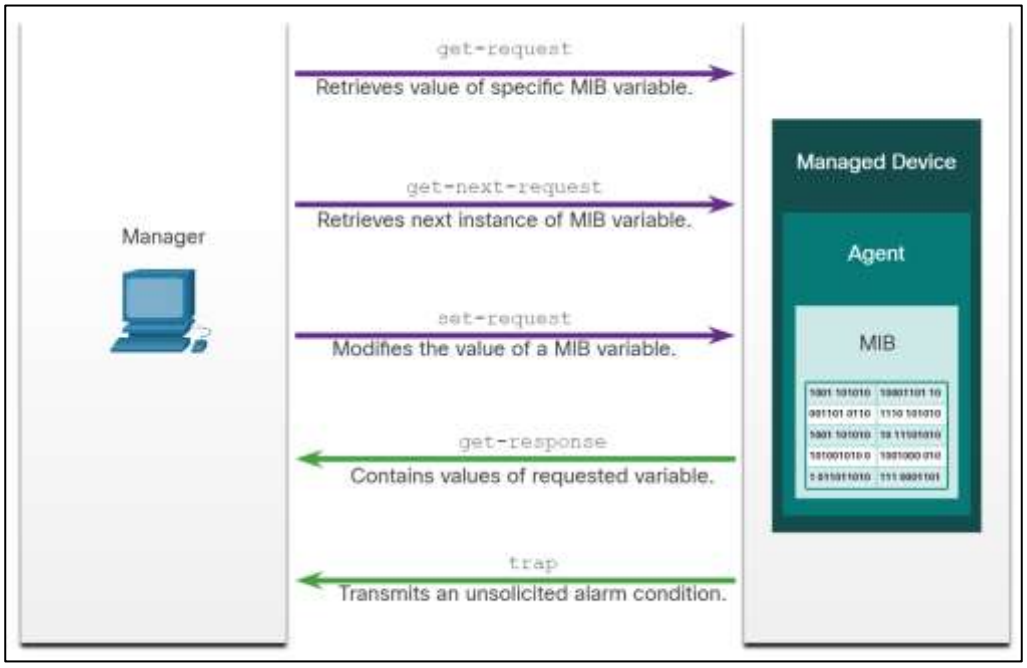
NMS secara berkala melakukan polling agen SNMP yang berada pada perangkat yang dikelola menggunakan permintaan get. NMS menanyakan data kepada perangkat. Dengan menggunakan proses ini, aplikasi manajemen jaringan dapat mengumpulkan informasi untuk memantau beban lalu lintas dan untuk memverifikasi konfigurasi perangkat dari perangkat yang dikelola. Informasi dapat ditampilkan melalui GUI pada NMS. Rata-rata, minimum, atau maksimum dapat dihitung. Data dapat dibuat grafik, atau ambang batas dapat diatur untuk memicu proses pemberitahuan ketika ambang batas terlampaui. Misalnya, NMS dapat memantau pemanfaatan CPU dari *Router* Cisco. Manajer SNMP mengambil sampel nilai secara berkala dan menyajikan informasi ini dalam grafik untuk digunakan administrator jaringan dalam membuat *baseline*, membuat laporan, atau melihat informasi waktu nyata.

Polling SNMP periodik memang memiliki kelemahan. Pertama, ada penundaan antara waktu kejadian dan waktu kejadian itu diketahui (melalui polling) oleh NMS. Kedua, ada *trade-off* antara frekuensi polling dan penggunaan *bandwidth*. Untuk mengurangi kerugian ini, bagi agen SNMP untuk menghasilkan dan mengirim jebakan untuk segera menginformasikan NMS tentang peristiwa tertentu. Perangkap adalah pesan yang tidak diminta yang memperingatkan manajer SNMP terhadap suatu kondisi atau peristiwa di jaringan. Contoh kondisi perangkap termasuk, tetapi tidak terbatas pada, otentikasi pengguna yang tidak tepat, *restart*, status tautan (naik atau turun), pelacakan alamat MAC, penutupan koneksi TCP, kehilangan koneksi ke tetangga, atau peristiwa penting lainnya. Pemberitahuan yang diarahkan perangkap mengurangi sumber daya jaringan dan agen dengan menghilangkan kebutuhan untuk beberapa permintaan polling SNMP.



Gambar 49 Ilustrasi Penggunaan SNMP Traps

Gambar tersebut mengilustrasikan penggunaan perangkap SNMP untuk memberitahu administrator jaringan bahwa *interface* G0/0/0 telah gagal. Perangkat lunak NMS dapat mengirim pesan teks kepada administrator jaringan, memunculkan jendela pada perangkat lunak NMS, atau mengubah ikon *Router* menjadi merah di NMS GUI.



Gambar 50 Pertukaran data pada SNMP

b. Versi SNMP

Saat ini ada beberapa versi SNMP, yaitu:

1. SNMPv1 - Ini adalah *Simple Network Management Protocol*, Standar Internet Lengkap, yang didefinisikan dalam RFC 1157.
2. SNMPv2c - Ini didefinisikan dalam RFCs 1901 hingga 1908. SNMPv2c menggunakan Kerangka Kerja Administratif berbasis komunitas-string.
3. SNMPv3 - Ini adalah protokol berbasis standar yang dapat dioperasikan yang awalnya didefinisikan dalam RFC 2273 hingga 2275. SNMPv3 menyediakan akses aman ke perangkat dengan mengautentikasi dan mengenkripsi paket

melalui jaringan. Protokol ini mencakup fitur-fitur keamanan ini: integritas pesan untuk memastikan bahwa paket tidak dirusak dalam perjalanan, otentikasi untuk menentukan bahwa pesan berasal dari sumber yang valid, dan enkripsi untuk mencegah isi pesan dibaca oleh sumber yang tidak sah.

c. Sting Komunitas

Agar SNMP dapat beroperasi, NMS harus memiliki akses ke MIB. Untuk memastikan bahwa permintaan akses valid, beberapa bentuk otentikasi harus ada. SNMPv1 dan SNMPv2c menggunakan string komunitas yang mengontrol akses ke MIB. String komunitas adalah kata sandi plaintext. String komunitas SNMP mengotentikasi akses ke objek MIB. Ada dua jenis string komunitas:

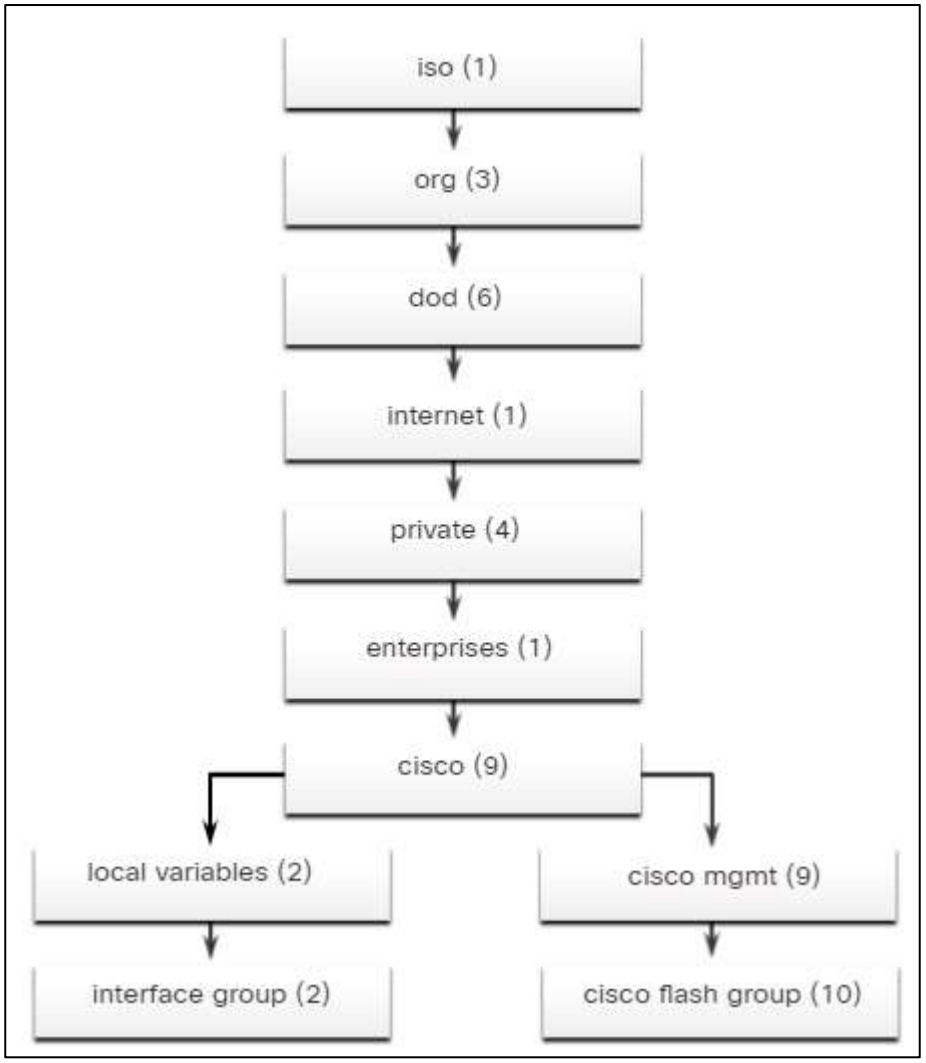
1. Read-only (ro) - Tipe ini menyediakan akses ke variabel MIB, tetapi tidak mengizinkan variabel ini diubah, hanya dibaca. Karena keamanan minimal di versi 2c, banyak organisasi menggunakan SNMPv2c dalam mode read-only.
2. Read-write (rw) - Tipe ini menyediakan akses baca dan tulis ke semua objek di MIB.

Untuk melihat atau mengatur variabel MIB, pengguna harus menentukan string komunitas yang sesuai untuk akses baca atau tulis.

d. ID Objek MIB

MIB mengatur variabel secara hierarkis. Variabel MIB memungkinkan perangkat lunak manajemen untuk memantau dan mengontrol perangkat jaringan. Secara formal, MIB mendefinisikan setiap variabel sebagai ID objek (OID). OIDs secara unik mengidentifikasi objek yang dikelola dalam hierarki MIB. MIB mengatur OIDs berdasarkan standar RFC ke dalam hierarki OIDs, biasanya ditampilkan sebagai pohon. Pohon MIB untuk perangkat tertentu mencakup beberapa cabang dengan variabel yang umum untuk banyak perangkat jaringan dan beberapa cabang dengan variabel khusus untuk perangkat atau vendor tersebut.

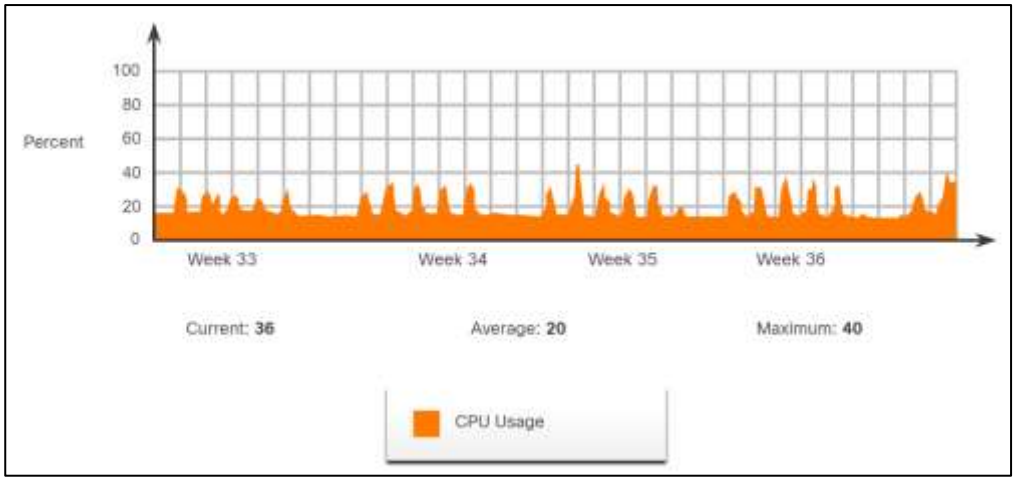
RFC mendefinisikan beberapa variabel publik umum. Kebanyakan perangkat mengimplementasikan variabel MIB ini. Selain itu, vendor peralatan jaringan, seperti Cisco, dapat mendefinisikan cabang pribadi mereka sendiri dari pohon untuk mengakomodasi variabel baru yang spesifik untuk perangkat mereka. Gambar 51 menunjukkan bagian dari struktur MIB yang didefinisikan oleh Cisco. Perhatikan bagaimana OID dapat dijelaskan dalam kata-kata atau angka untuk membantu menemukan variabel tertentu di pohon. OID milik Cisco, diberi nomor sebagai berikut: .iso (1).org (3).dod (6).internet (1).private (4).enterprises (1).cisco (9). Oleh karena itu, OID adalah 1.3.6.1.4.1.9.



Gambar 51 Contoh MIB

e. Skenario Polling

SNMP dapat digunakan untuk mengamati utilisasi CPU selama periode waktu tertentu dengan melakukan polling perangkat. Statistik CPU kemudian dapat dikompilasi pada NMS dan dibuat grafiknya. Ini menciptakan garis dasar untuk administrator jaringan. Nilai ambang batas kemudian dapat diatur relatif terhadap garis dasar ini. Ketika utilisasi CPU melebihi ambang batas ini, pemberitahuan akan dikirim. Gambar 52 ini mengilustrasikan sampel 5 menit dari utilisasi CPU *router* selama periode beberapa minggu. Data diambil melalui utilitas snmpget, yang dikeluarkan pada NMS. Dengan menggunakan utilitas snmpget, Anda dapat secara manual mengambil data real-time, atau meminta NMS menjalankan laporan. Laporan ini akan memberi Anda periode waktu yang dapat Anda gunakan data untuk mendapatkan rata-rata. Utilitas snmpget memerlukan versi SNMP, komunitas yang benar, alamat IP dari perangkat jaringan untuk *query*, dan nomor OID yang ditetapkan. Gambar ini mendemonstrasikan penggunaan utilitas *freeware* snmpget, yang memungkinkan pengambilan informasi dengan cepat dari MIB.

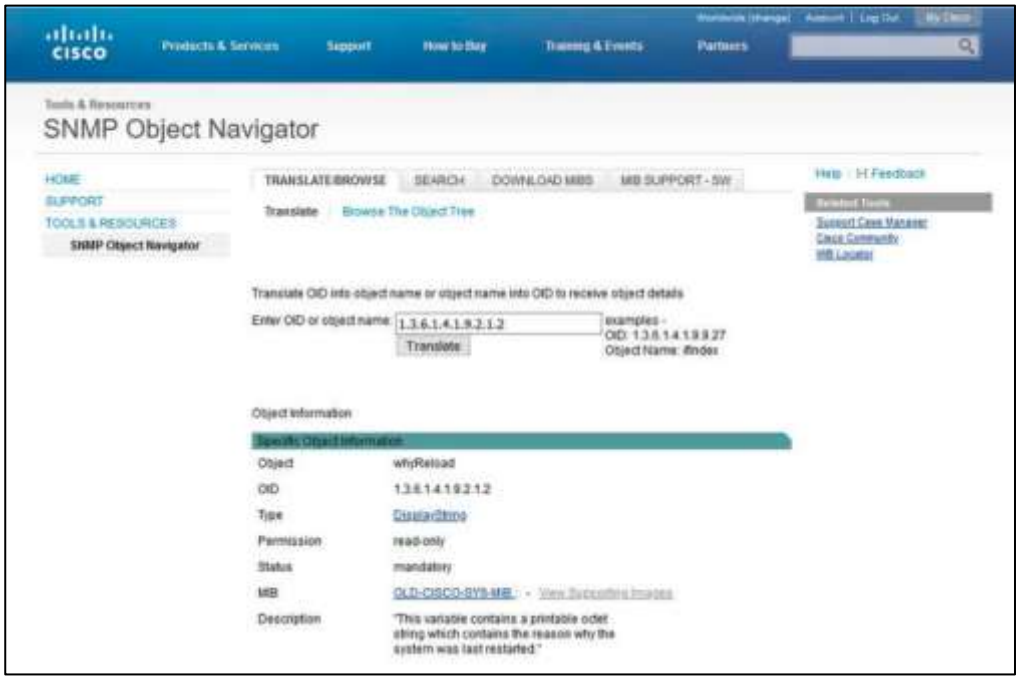


Gambar 52 SNMP Pooling (CPU Utilization)

f. Navigator Objek SNMP

Utilitas snmpget memberikan beberapa wawasan tentang mekanisme dasar bagaimana SNMP bekerja. Namun, bekerja dengan nama variabel MIB yang panjang seperti 1.3.6.1.4.1.9.2.1.58.0 bisa menjadi masalah bagi pengguna rata-rata. Lebih umum, staf operasi jaringan menggunakan produk manajemen jaringan dengan GUI yang mudah digunakan, yang membuat seluruh penamaan variabel data MIB transparan bagi pengguna.

Cari "Cisco SNMP *Object Navigator tool*" untuk menemukan alat Cisco yang memungkinkan administrator jaringan untuk meneliti rincian tentang OID tertentu. Gambar menampilkan contoh penggunaan navigator untuk meneliti informasi OID untuk objek **whyReload**.

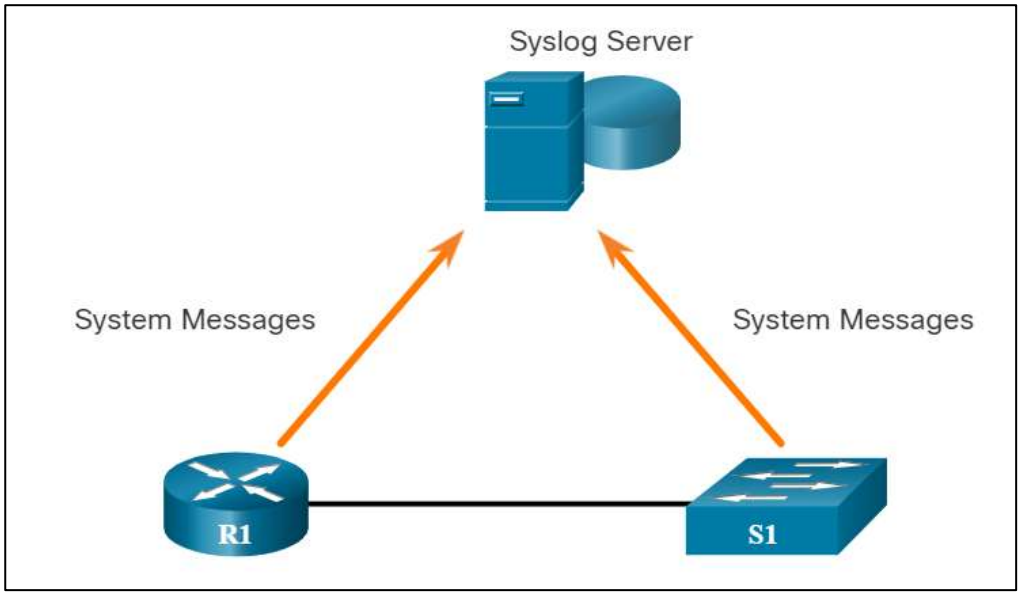


Gambar 53 Cisco SNMP Navigator

g. Syslog

Seperti lampu *Check Engine* di dashboard mobil Anda, komponen-komponen dalam jaringan Anda dapat memberi tahu Anda jika ada sesuatu yang salah. Protokol syslog dirancang untuk memastikan bahwa Anda dapat menerima dan memahami pesan-pesan ini. Ketika peristiwa tertentu terjadi pada jaringan, perangkat jaringan memiliki mekanisme terpercaya untuk memberitahu administrator dengan pesan sistem yang rinci. Pesan-pesan ini dapat berupa pesan yang tidak kritis atau signifikan. Administrator jaringan mempunyai berbagai pilihan untuk menyimpan, menginterpretasikan, dan menampilkan pesan-pesan ini. Mereka juga bisa diberitahu pesan-pesan yang bisa mempunyai dampak terbesar pada infrastruktur jaringan. Metode yang paling umum untuk mengakses pesan sistem adalah dengan menggunakan protokol yang disebut syslog.

Syslog adalah istilah yang digunakan untuk mendeskripsikan suatu standar. Istilah ini juga digunakan untuk menggambarkan protokol yang dikembangkan untuk standar itu. Protokol syslog dikembangkan untuk sistem UNIX pada tahun 1980-an tetapi pertama kali didokumentasikan sebagai RFC 3164 oleh IETF pada tahun 2001. Syslog menggunakan port UDP 514 untuk mengirim pesan notifikasi peristiwa di seluruh jaringan IP ke pengumpul pesan peristiwa, seperti yang ditunjukkan pada gambar 54.



Gambar 54 Ilustrtasi Syslog

Pada perangkat jaringan Cisco, protokol syslog dimulai dengan mengirimkan pesan sistem dan output debug ke proses logging lokal internal ke perangkat. Bagaimana proses logging mengelola pesan dan output ini didasarkan pada konfigurasi perangkat. Misalnya, pesan syslog dapat dikirim melintasi jaringan ke server syslog eksternal. Pesan-pesan ini dapat diambil tanpa perlu mengakses perangkat yang sebenarnya. Pesan log dan output yang disimpan pada server eksternal dapat ditarik ke dalam berbagai laporan untuk memudahkan pembacaan.

Sebagai alternatif, pesan syslog dapat dikirim ke buffer internal. Pesan yang dikirim ke buffer internal hanya dapat dilihat melalui CLI perangkat. Terakhir, administrator jaringan dapat menentukan bahwa hanya jenis pesan sistem tertentu yang dikirim ke berbagai tujuan. Misalnya, perangkat dapat dikonfigurasi untuk meneruskan semua pesan sistem ke server syslog eksternal. Namun, pesan tingkat debug diteruskan ke buffer internal dan hanya dapat diakses oleh administrator dari CLI.

Perangkat Cisco menghasilkan pesan syslog sebagai hasil dari peristiwa jaringan. Setiap pesan syslog berisi tingkat keparahan dan fasilitas. Tingkat numerik yang lebih kecil adalah alarm syslog yang lebih kritis. Tingkat keparahan pesan dapat diatur untuk mengontrol di mana setiap jenis pesan ditampilkan (yaitu pada konsol atau tujuan lainnya). Daftar lengkap level syslog ditunjukkan dalam tabel 16.

Tabel 16 Level Syslog

Nama Tingkat Keparahan	Tingkat Keparahan	Penjelasan
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

b. Pemecahan Masala pada Jaringan

Yang benar adalah bahwa satu-satunya cara untuk menjadi *troubleshooter* jaringan yang baik adalah selalu memecahkan masalah. Perlu waktu untuk menjadi ahli dalam hal ini. Untuk mahir dibidang ini ada beberapa hal yang harus anda pahami, yaitu:

1. Dokumentasi jaringan

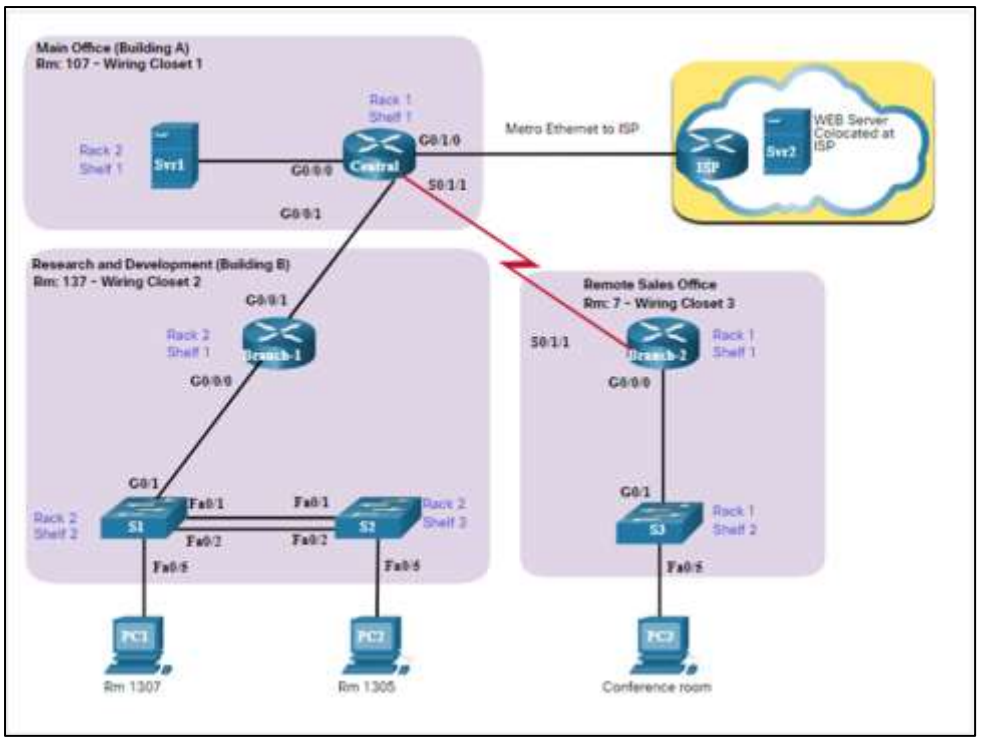
   Seperti halnya aktivitas kompleks seperti *troubleshooting* jaringan, anda perlu mulai dengan dokumentasi yang baik. Dokumentasi jaringan yang akurat dan lengkap diperlukan untuk memonitor dan *troubleshooting* jaringan secara efektif.

   Dokumentasi jaringan umum mencakup yang berikut ini:

   a. Diagram topologi jaringan fisik dan logis

      Diagram topologi jaringan melacak lokasi, fungsi, dan status perangkat di jaringan. Ada dua jenis diagram topologi jaringan: topologi fisik dan topologi logis. Topologi jaringan fisik menunjukkan tata letak fisik dari perangkat yang terhubung ke jaringan. Anda perlu mengetahui bagaimana perangkat-perangkat terhubung secara fisik untuk memecahkan masalah lapisan fisik. Informasi yang dicatat pada topologi fisik biasanya termasuk yang berikut ini:

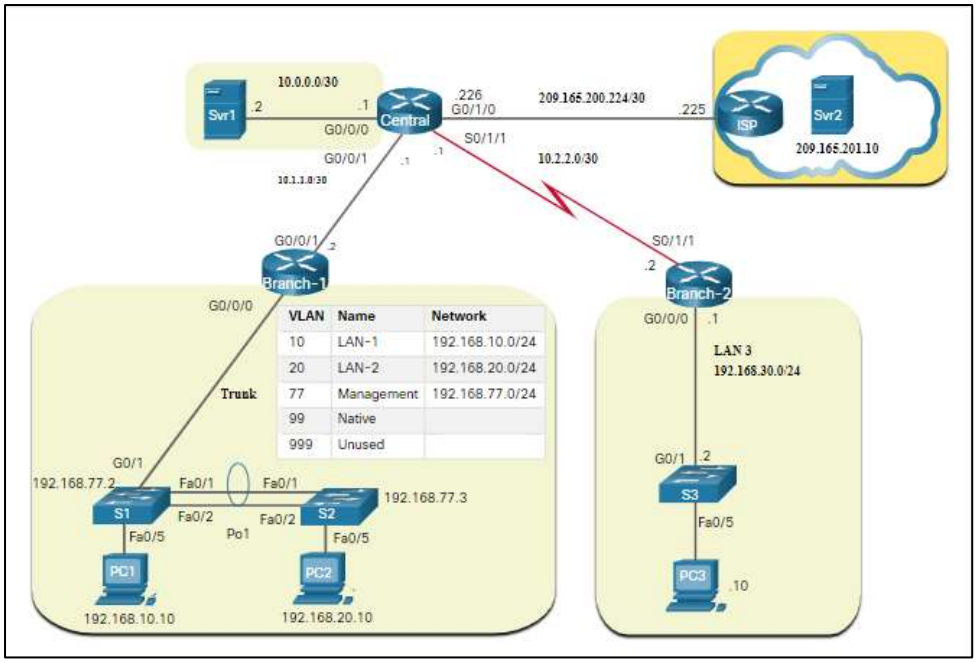
      1. Nama perangkat
      2. Lokasi perangkat (alamat, nomor ruangan, lokasi rak)
      3. *Interface* dan port yang digunakan
      4. Jenis kabel



Gambar 55 Topologi Fisik

Topologi jaringan logis mengilustrasikan bagaimana perangkat secara logis terhubung ke jaringan. Ini mengacu pada bagaimana perangkat mentransfer data di seluruh jaringan ketika berkomunikasi dengan perangkat lain. Simbol digunakan untuk mewakili komponen jaringan, seperti *router*, *switch*, server, dan host. Selain itu, koneksi antara beberapa situs dapat ditampilkan, tetapi tidak mewakili lokasi fisik yang sebenarnya. Informasi yang direkam pada topologi jaringan logis dapat mencakup yang berikut ini:

1. Pengidentifikasi perangkat
2. Alamat IP dan panjang prefix
3. Pengidentifikasi *interface*
4. Protokol *routing* / rute statis
5. Informasi Lapisan 2 (yaitu, VLAN, trunk, EtherChannels)



Gambar 56 Topologi Logis

b. Dokumentasi perangkat jaringan yang mencatat semua informasi perangkat terkait Dokumentasi perangkat jaringan harus berisi catatan yang akurat dan terbaru dari perangkat keras dan perangkat lunak jaringan. Dokumentasi harus menyertakan semua informasi terkait tentang perangkat jaringan. Banyak organisasi membuat dokumen dengan tabel atau spreadsheet untuk menangkap informasi perangkat yang relevan.

Tabel 17 Contoh dokumentasi perangkat *Router*

Perangkat	**Model**	**Deskripsi**	**Lokasi**	**IOS**	**Lisensi**
Central	ISR 4321	Central Edge *Router*	Building A Rm: 137	Cisco IOS XE Software, Version 16.09.04 flash:isr4300 universalk9_ias.16.09.04.SPA.bin	ipbasek9 securityk9
Interface	Deskripsi	Address IPv4	Address IPv6	MAC Address	*Routing*
G0/0/0	Connects to SVR-1	10.0.0.1/30	2001:db8:acad:1::1/64	a03d.6fe1.e180	OSPF
G0/0/1	Connects to Branch-1	10.1.1.1/30	2001:db8:acad:a001::1/64	a03d.6fe1.e181	OSPFv3
G0/1/0	Connects to ISP	209.165.200.226/30	2001:db8:feed:1::2/64	a03d.6fc3.a132	Default
S0/1/1	Connects to Branch-2	10.1.1.2/24	2001:db8:acad:2::1/64	n/a	OSPFv3

Tabel 18 Contoh dokumentasi perangkat *Switch*

Perangkat	**Model**	**Deskripsi**	**Address Mgt. IP**	**IOS**			**VTP**	
S1	Cisco Catalyst WS-C2960-24TC-L	Branch-1 LAN1 *switch*	192.168.77.2/24	IOS: 15.0(2)SE7 Image: C2960-LANBASEK9-M			Domain: CCNA Mode: Server	
Port	Deskripsi		Access	VLAN	Trunk	Ether Channel	Native	Enabled
Fa0/1	Port Channel 1 trunk to S2 Fa0/1		-	-	Yes	Port-Channel 1	99	Yes
Fa0/2	Port Channel 1 trunk to S2 Fa0/2		-	-	Yes	Port-Channel 1	99	Yes
Fa0/3	*** Not in use ***		Yes	999	-	-		Shut
Fa0/4	*** Not in use ***		Yes	999	-	-		Shut
Fa0/5	Access port to user		Yes	10	-	-		Yes
…					-	-		-
Fa0/24	Access port to user		Yes	20	-	-		Yes
Fa0/24	*** Not in use ***		Yes	999	-	-		Shut
G0/1	Trunk link to Branch – 1		-	-	Yes	-	99	Yes
G0/2	*** Not in use ***		Yes	999		-		

Tabel 19 Contoh dokumentasi perangkat end user

Perangkat	**OS**	**Layanan**	**MAC Address**	**IPv4 / IPv6 Addresses**	**Default Gateway**	**DNS**
SRV1	MS Server 2016	SMTP, POP3, File services, DHCP	5475.d08e.9ad8	10.0.0.2/30	10.0.0.1	10.0.0.1
				2001:db8:acad:1::2/64	2001:db8:acad:1::1	2001:db8:acad:1::1
SRV2	MS Server 2016	HTTP, HTTPS	5475.d07a.5312	209.165.201.10	209.165.201.1	209.165.201.1
				2001:db8:feed:1::10/64	2001:db8:feed:1::1	2001:db8:feed:1::1
PC1	MS Windows 10	HTTP, HTTPS	5475.d017.3133	192.168.10.10/24	192.168.10.1	192.168.10.1
				2001:db8:acad:1::251/64	2001:db8:acad:1::1	2001:db8:acad:1::1

c. Dokumentasi *baseline* kinerja jaringan

Tujuan dari pemantauan jaringan adalah untuk melihat kinerja jaringan dibandingkan dengan *baseline* yang telah ditentukan sebelumnya. *Baseline* digunakan untuk menetapkan kinerja jaringan atau sistem normal untuk menentukan "kepribadian" jaringan dalam kondisi normal. Menetapkan *baseline* kinerja jaringan memerlukan pengumpulan data kinerja dari port dan perangkat yang penting untuk operasi jaringan. *Baseline* jaringan harus menjawab pertanyaan-pertanyaan berikut:

1. Bagaimana kinerja jaringan selama hari normal atau rata-rata?

2. Di mana kesalahan paling banyak terjadi?
3. Bagian mana dari jaringan yang paling banyak digunakan?
4. Bagian jaringan mana yang paling jarang digunakan?
5. Perangkat mana yang harus dimonitor dan ambang peringatan apa yang harus ditetapkan?
6. Dapatkah jaringan memenuhi kebijakan yang telah diidentifikasi?

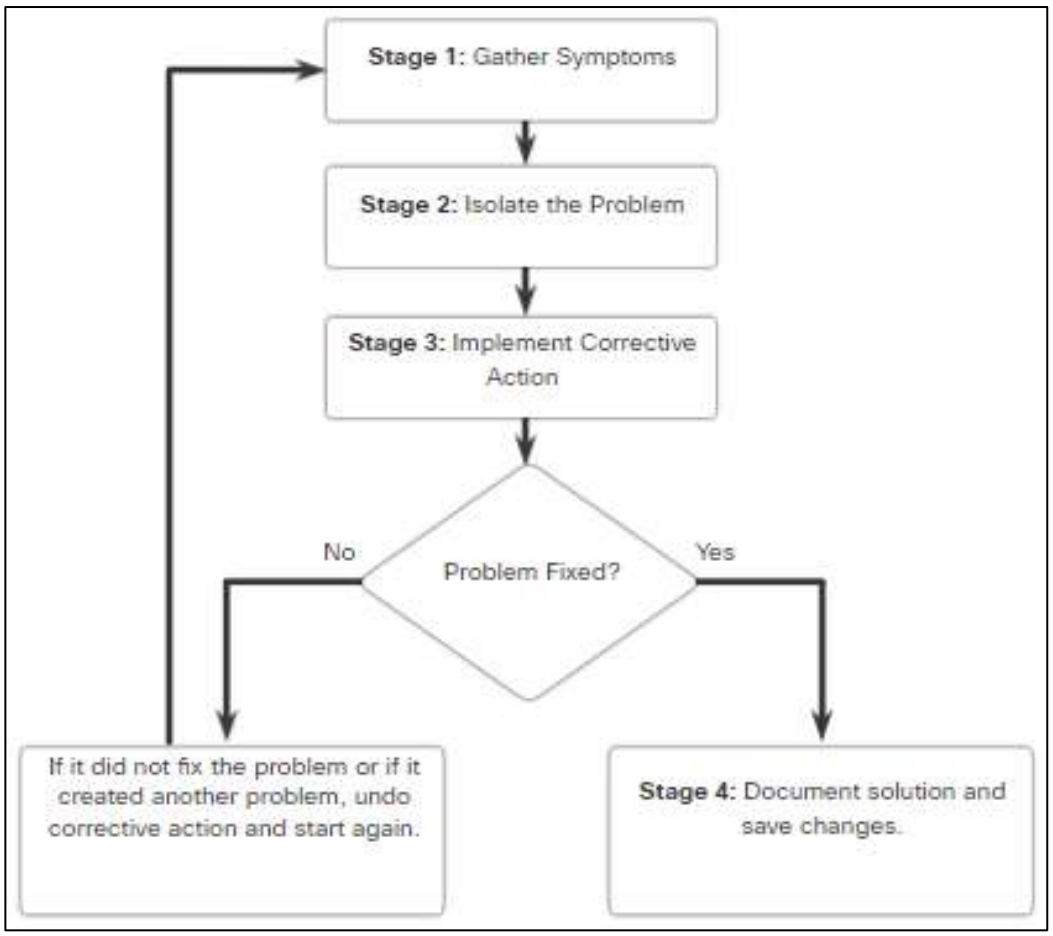
Mengukur kinerja awal dan ketersediaan perangkat dan tautan jaringan penting memungkinkan administrator jaringan untuk menentukan perbedaan antara perilaku abnormal dan kinerja jaringan yang tepat, seiring pertumbuhan jaringan, atau perubahan pola *traffic*. *Baseline* juga memberikan wawasan apakah rancangan jaringan saat ini dapat memenuhi persyaratan bisnis. Tanpa *baseline*, tidak ada standar yang ada untuk mengukur sifat optimal dari lalu lintas jaringan dan tingkat kemacetan. Analisis setelah *baseline* awal juga cenderung untuk mengungkapkan masalah tersembunyi. Data yang terkumpul menunjukkan sifat sebenarnya dari kemacetan atau potensi kemacetan dalam jaringan. Hal ini juga dapat mengungkapkan area dalam jaringan yang kurang dimanfaatkan, dan sering kali dapat mengarah pada upaya perancangan ulang jaringan, berdasarkan pengamatan kualitas dan kapasitas. *Baseline* kinerja jaringan awal menetapkan tahap untuk mengukur efek dari perubahan jaringan dan upaya pemecahan masalah selanjutnya. Oleh karena itu, penting untuk merencanakannya dengan hati-hati.

Semua dokumentasi jaringan harus disimpan di satu lokasi, baik dalam bentuk *hard copy* atau di jaringan pada server yang dilindungi. Dokumentasi cadangan harus dipelihara dan disimpan di lokasi terpisah.

2. Proses *Troubleshooting*

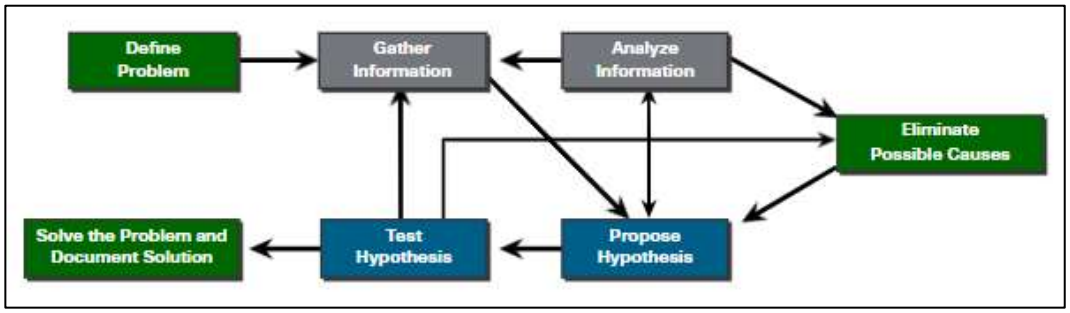
Troubleshooting dapat memakan waktu karena jaringan berbeda, masalah berbeda, dan pengalaman *troubleshooting* bervariasi. Namun, administrator yang berpengalaman tahu bahwa menggunakan metode *troubleshooting* yang terstruktur akan mempersingkat waktu *troubleshooting* secara keseluruhan. Oleh karena itu, proses *troubleshooting* harus dipandu oleh metode terstruktur. Ini memerlukan prosedur *troubleshooting* yang terdefinisi dan terdokumentasi dengan baik untuk meminimalkan waktu yang terbuang yang terkait dengan *troubleshooting hit-and-miss* yang tidak menentu. Namun, metode-metode ini tidak statis. Langkah-langkah pemecahan masalah yang diambil untuk memecahkan masalah tidak selalu sama atau dieksekusi dalam urutan yang sama persis.

Ada beberapa proses pemecahan masalah yang bisa digunakan untuk memecahkan masalah. Gambar 57 di bawah menampilkan diagram alir logika dari proses pemecahan masalah tiga tahap yang disederhanakan. Namun, proses yang lebih rinci mungkin lebih membantu untuk memecahkan masalah jaringan.



Gambar 57 Pemecahan masalah 3 langkah

Selain itu terdapat proses pemecehan masalah lain seperti pada gambar 58. Gambar ini menampilkan proses pemecahan masalah tujuh langkah yang lebih rinci. Perhatikan bagaimana beberapa langkah saling berhubungan. Hal ini karena, beberapa teknisi mungkin bisa melompat di antara langkah-langkah berdasarkan tingkat pengalaman mereka.



Gambar 58 Pemecahan masalah 7 langkah

a. Tentukan Masalahnya

Tujuan dari tahap ini adalah untuk memverifikasi bahwa ada masalah dan kemudian mendefinisikan dengan benar apa masalahnya. Masalah biasanya diidentifikasi oleh gejala (misalnya, jaringan lambat atau berhenti bekerja). Gejala jaringan dapat muncul dalam berbagai bentuk, termasuk peringatan dari sistem manajemen jaringan, pesan konsol, dan keluhan user. Sewaktu mengumpulkan gejala, penting

untuk mengajukan pertanyaan dan menyelidiki masalah untuk melokalisasi masalah ke kisaran kemungkinan yang lebih kecil. Misalnya, apakah masalahnya terbatas pada satu perangkat, sekelompok perangkat, atau seluruh subnet atau jaringan perangkat?. Dalam sebuah organisasi, masalah biasanya ditugaskan ke teknisi jaringan sebagai *trouble ticket*. *Ticket-ticket* ini dibuat dengan menggunakan *software trouble ticketing* yang melacak kemajuan dari setiap *ticket*. *Software trouble ticketing* juga bisa termasuk portal pengguna swalayan untuk mengirimkan *ticket*, akses ke basis pengetahuan *trouble ticketing* yang bisa dicari, kemampuan *remote control* untuk memecahkan masalah *end-user*, dan banyak lagi.

b. Mengumpulkan Informasi

   Dalam langkah ini, target (yaitu, host, perangkat) yang akan diselidiki harus diidentifikasi, akses ke perangkat target harus diperoleh, dan informasi dikumpulkan. Selama langkah ini, teknisi dapat mengumpulkan dan mendokumentasikan lebih banyak gejala, tergantung pada karakteristik yang diidentifikasi. Jika masalahnya berada di luar batas kendali organisasi (misalnya, kehilangan konektivitas internet di luar sistem otonom), hubungi administrator untuk sistem eksternal sebelum mengumpulkan gejala jaringan tambahan.

c. Analisa Informasi

   Kemungkinan penyebab harus diidentifikasi. Informasi yang terkumpul diinterpretasikan dan dianalisa dengan menggunakan dokumentasi jaringan, *baseline* jaringan, mencari basis pengetahuan organisasi, mencari di internet, dan berbicara dengan teknisi lain.

d. Hilangkan Penyebab Yang Mungkin

   Jika beberapa penyebab teridentifikasi, maka daftarnya harus dikurangi dengan mengeliminasi secara progresif penyebab yang mungkin untuk akhirnya mengidentifikasi penyebab yang paling mungkin. Pengalaman pemecahan masalah sangat berharga untuk mengeliminasi penyebab secara cepat dan mengidentifikasi penyebab yang paling mungkin.

e. Mengajukan Hipotesis

   Apabila penyebab yang paling mungkin telah diidentifikasi, solusi harus dirumuskan. Pada tahap ini, pengalaman pemecahan masalah sangat berharga ketika mengusulkan rencana.

f. Uji Hipotesis

   Sebelum menguji solusi, penting untuk menilai dampak dan urgensi masalah. Misalnya, dapatkah solusi memiliki efek buruk pada sistem atau proses lain? Tingkat keparahan masalah harus ditimbang terhadap dampak solusi. Misalnya, jika server atau *Router* yang penting harus *offline* untuk waktu yang signifikan, mungkin lebih baik menunggu sampai akhir hari kerja untuk mengimplementasikan perbaikan. Kadang-kadang, solusi dapat dibuat sampai masalah yang sebenarnya teratasi. Buat rencana rollback yang mengidentifikasi cara membalikkan solusi dengan

cepat. Hal ini mungkin terbukti diperlukan jika solusi gagal. Implementasikan solusi dan verifikasi bahwa solusi tersebut telah memecahkan masalah. Kadang-kadang sebuah solusi menimbulkan masalah yang tidak terduga. Oleh karena itu, penting agar solusi diverifikasi secara menyeluruh sebelum melanjutkan ke langkah berikutnya. Jika solusi gagal, solusi yang dicoba didokumentasikan dan perubahannya dihapus. Teknisi sekarang harus kembali ke langkah mengumpulkan informasi dan mengisolasi masalah.

g. Pecahkan Masalahnya

Ketika masalah sudah terpecahkan, informasikan kepada pengguna dan siapa saja yang terlibat dalam proses pemecahan masalah bahwa masalah telah teratasi. Anggota tim TI lainnya harus diberitahu tentang solusinya. Dokumentasi yang tepat tentang penyebab dan perbaikan akan membantu teknisi dukungan lainnya dalam mencegah dan memecahkan masalah serupa di masa mendatang.

2. Alat *Troubleshooting*

Seperti yang anda ketahui, jaringan terdiri dari perangkat lunak dan perangkat keras. Oleh karena itu, baik perangkat lunak maupun perangkat keras memiliki *tool* masing-masing untuk *troubleshooting*. Topik ini membahas *tool troubleshooting* yang tersedia untuk keduanya. Berbagai macam perangkat lunak dan perangkat keras tersedia untuk mempermudah pemecahan masalah. *Tool-tool* ini dapat digunakan untuk mengumpulkan dan menganalisa gejala-gejala masalah jaringan. Mereka sering menyediakan fungsi pemantauan dan pelaporan yang dapat digunakan untuk membuat *baseline* jaringan.

a. Network Manajement System

Alat sistem manajemen jaringan (NMS) termasuk pemantauan tingkat perangkat, konfigurasi, dan alat manajemen kesalahan. *Tool-tool* ini dapat digunakan untuk menginvestigasi dan memperbaiki masalah jaringan. Perangkat lunak pemantauan jaringan secara grafis menampilkan tampilan fisik perangkat jaringan, memungkinkan manajer jaringan untuk memantau perangkat jarak jauh secara terus menerus dan otomatis. Perangkat lunak manajemen perangkat menyediakan status perangkat dinamis, statistik, dan informasi konfigurasi untuk perangkat jaringan utama.

b. Berbasis Pengetahuan

Basis pengetahuan vendor perangkat jaringan *online* telah menjadi sumber informasi yang sangat diperlukan. Ketika basis pengetahuan berbasis vendor digabungkan dengan mesin search engine, administrator jaringan memiliki akses ke kumpulan informasi berbasis pengalaman yang luas. Sebagai contoh, halaman Cisco Tools & Resources dapat ditemukan di http://www.cisco.com di bawah menu Support. Halaman ini menyediakan alat yang dapat digunakan untuk perangkat keras dan perangkat lunak Cisco.

c. Alat *baseline*

Banyak *tool* untuk mengotomatisasi dokumentasi jaringan dan proses baselining tersedia. Alat *baselining* membantu dengan tugas-tugas dokumentasi umum. Misalnya, mereka bisa menggambar diagram jaringan, membantu menjaga dokumentasi *software* dan hardware jaringan tetap *up-to-date*, dan membantu mengukur penggunaan *bandwidth* jaringan *baseline* secara efektif.

d. Multimeter digital

   Multimeter digital (DMM) adalah alat uji yang digunakan untuk secara langsung mengukur nilai listrik dari tegangan, arus, dan resistansi. Dalam *troubleshooting* jaringan, kebanyakan tes yang memerlukan multimeter melibatkan pengecekan level tegangan catu daya dan memverifikasi bahwa perangkat jaringan menerima daya.

e. Penguji kabel

   Penguji kabel adalah perangkat genggam khusus yang dirancang untuk menguji berbagai jenis kabel komunikasi data. Penguji kabel dapat digunakan untuk mendeteksi kabel yang putus, kabel yang bersilangan, koneksi yang korslet, dan koneksi yang tidak dipasangkan dengan benar. Perangkat ini bisa berupa penguji kontinuitas yang murah, penguji kabel data dengan harga sedang, atau reflektometer domain-waktu (TDR) yang mahal. TDR digunakan untuk menentukan jarak ke putusnya kabel. Perangkat ini mengirimkan sinyal di sepanjang kabel dan menunggu sinyal tersebut dipantulkan. Waktu antara pengiriman sinyal dan penerimaannya kembali diubah menjadi pengukuran jarak. Fungsi TDR biasanya dikemas dengan penguji pemasangan kabel data. TDR yang digunakan untuk menguji kabel serat optik dikenal sebagai *optical time-domain reflectometers* (OTDRs).

f. Penganalisis kabel

   Penganalisis kabel adalah perangkat genggam multifungsi yang digunakan untuk menguji dan mengesahkan kabel tembaga dan serat untuk berbagai layanan dan standar. Alat yang lebih canggih mencakup diagnostik pemecahan masalah tingkat lanjut yang mengukur jarak ke cacat kinerja seperti *near-end crosstalk* (NEXT) atau *return loss* (RL), mengidentifikasi tindakan korektif, dan secara grafis menampilkan perilaku *crosstalk* dan impedansi. Penganalisis kabel juga biasanya menyertakan perangkat lunak berbasis PC. Setelah data lapangan dikumpulkan, data dari perangkat genggam dapat diupload sehingga administrator jaringan dapat membuat laporan terbaru.

g. Penganilisis jaringan portabel jaringan

   Perangkat portabel digunakan untuk pemecahan masalah jaringan *switched* dan VLAN. Dengan mencolokkan penganalisis jaringan di mana saja di jaringan, seorang insinyur jaringan dapat melihat port *switch* yang terhubung dengan perangkat, dan pemanfaatan rata-rata dan puncak. Penganalisis juga dapat digunakan untuk menemukan konfigurasi VLAN, mengidentifikasi pembicara

jaringan teratas (host yang menghasilkan lalu lintas paling banyak), menganalisis *traffic* jaringan, dan melihat detail antarmuka. Perangkat ini biasanya dapat mengeluarkan output ke PC yang memiliki perangkat lunak pemantauan jaringan yang diinstal untuk analisis dan pemecahan masalah lebih lanjut.

3. Tugas

Operasional Proyek (Proyek Team Base)

Pada tahapan ini secara berkelompok melakukan mastikan proyek jaringan kampus, berjalan sesuai dengan baik.

Kegiatan Belajar 5
Penulisan Laporan

1. Sub-Capaian Pembelajaran

a. Mampu menyeusn laporan proyek dalam bentuk Artikel Ilmiah / Laporan PkM
b. Mampu memaparkan hasil Proyek ke Peserta

2. Pembahasan

a. Pendahuluan

Pada bagian pendahuluan berisi kejelasan **BIG Idea** (Fakta-fakta yang diungkapkan untuk mendukung penjelasan tentang keberadaan problem/challenge yang akan diselesaikan berdasarkan sumber-sumber materi scientific yang valid/sahih seperti artikel jurnal) yang berhubungan dengan proyek yang telah di kerjakan. Selain ini harus besi Kejelasan **Rumusan Masalah/*Challenge Statement*** berdasarkan fakta yang diungkap. Pada pendahuluan juga harus berisi Kejelasan **Tujuan Penelitian** (Apa solution concept yang diajukan untuk menyelesaikan masalah) serta Kejelasan Scope/Batasan Masalah.

b. Tinjauan Pustaka

Pada bagian tinjauan pustaka berisi ***Fundamental Theory*** (Termasuk di dalamnya basic definition, model, etc.) serta hasil riset-riset sebelumnya yang relevan dengan penelitian yang direncanakan dengan menggunakan sumber-sumber materi scientific yang valid/sahih: artikel jurnal 80%, buku dan lainnya 20%.

c. Metode

Pada bagian metode berisi tentang informasi detail tentang bagaimana merealisasikan solution concept yang akan dirancang (Jika membuat hardware/system: bagaimana diagram blok yang menjelaskan sistem kerjanya; bagaimana setiap blok dirancang; Apa kebutuhan alat dan bahannya, dsb.), serta timeline (ganttchart) untuk rencana pengerjaan setiap blok (sub bagian) dari project skripsi yang akan dikerjakan

d. Implementasi dan Pembahasan

Pada bagian Implementasi akan membuat Informasi detail tahapan tahapan dan implementasi yang dilakukan dalam implementasi proyek yang di kerjakan. Implementasi mencakup konfigurasi, serta pengujian yang telah di lakukan, serta penjelasan setiap tahapan dan hasil yang di dapatkan.

e. Kesimpulan dan Saran

Kesimpulan dan saran adalah bagian penutup dari proyek yang telah dibuat isi dari proyek telah dijabarkan dalam Bab sebelumnya. Pada bagian kesimpuan akan dijelaskan secara singkat mengenai hasil proyek yang telah dikerjakan. Pada bagian saran akan mennguraikan saran rasa perlu dikembangkan.

f. Plagiarism checker

Deteksi plagiarisme adalah proses pencarian bagian yang diduga plagiat dari sebuah karya. Dalam hal ini, karya tidak hanya terbatas pada dokumen, tetapi juga desain baik gambar atau video, dan kode program. Meskipun kasus yang umum terjadi pada tulisan ilmiah baik berupa esai atau laporan. Dengan perkembangan komputer dan internet menjadikan orang mudah untuk memplagiat kaya seseorang. Pendeteksian plagiarisme dapat dilakukan baik secara manual atau otomatis menggunakan perangkat lunak. Deteksi plagiarisme secara manual memerlukan usaha yang besar disertai dengan ingatan yang baik, mengingat banyaknya dokumen yang harus bandingkan. Oleh karena itu, pendeteksian menggunakan perangkat lunak akan lebih memudahkan tugas ini. Berikut ini adalah tools yang bisa di gunakan untuk melakukan pengecekan plagiarisme

1. Turnitin (https://www.turnitin.com/)

   Turnitin merupakan salah satu aplikasi cek plagiat yang paling populer, khususnya dalam dunia akademik. Aplikasi ini akan memeriksa hasil tulisanmu dengan memastikan ia tidak memiliki kesamaan dengan dokumen lain yang ada di internet, situs web, buku, artikel, dan lain-lain. Aplikasi ini tidak bisa digunakan secara gratis (berbayar).
2. DupliChecker (https://www.duplichecker.com/)

   Ini merupakan aplikasi cek plagiat yang gratis. Memiliki tampilannya sederhana, namun akurasi pengecekannya cukup tinggi. Untuk menggunakan aplikasi ini harus membuat akun untuk mendapatkan 50 pengecekan plagiarisme gratis per hari. Tampa membuat akun hanya memperbolehkan pengecekan satu dokumen saja.
3. Grammarly (https://www.grammarly.com/)

   Aplikasi ini populer sebagai aplikasi pemeriksa grammar bahasa Inggris, namun aplikasi ini juga memiliki aplikasi cek plagiat yang dapat di gunakan secara gratis dan berbayar. Dalam penggunaanya Anda hanya perlu memasukkan teks yang ingin diperiksa dan Grammarly akan memrosesnya dengan database yang ia miliki.

3. Tugas

Penulisan laporan akhir proyek dalam bentuk artikel ilmiah (Proyek Team Base)

Pada tahapan ini secara berkelompok melakukan penulisan artikel sesuai dengan yang telah dibahas pada module ini. Untuk template artikel dapay di download pada tautan ini https://s.id/templt-artikel. Untuk plagiat tidak boleh lebih dari **24 %**.

Daftar Pustaka

Shen, N.,Yu, B., Huang, M., Xu, H. 2021. Campus Network Architectures and Technologies. CRC Press

Network Academy. 2020.Enterprise Networking, Security, and Automation Companion Guide (CCNAv7). Cisco Press

Network Academy. 2020.Enterprise Networking, Security, and Automation Labs and Study Guide (CCNAv7). Cisco Press

Network Academy. 2020.Enterprise Networking, Security, and Automation Course Booklet (CCNAv7). Cisco Press