

JARINGAN KOMPUTER



DAFTAR ISI

BAB 1 MENJELAJAHI JARINGAN	14
1.1 HUBUNGAN GLOBAL.....	14
• JARINGAN DALAM KEHIDUPAN	14
• TEKNOLOGI SAATINI.....	14
• TANPA BATAS.....	14
• JARINGAN MENDUKUNG BELAJAR.....	15
• JARINGAN MENDUKUNG KOMUNIKASI.....	15
• JARINGAN MENDUKUNG PEKERJAAN.....	16
• JARINGAN MENDUKUNG PERMAINAN.....	16
• JARINGAN DALAM BERBAGAI UKURAN	16
• Clients dan Server	17
• Peer to Peer	17
1.2 LAN, WAN dan INTERNET.....	19
❖ KOMPONEN JARINGAN	19
• (END DEVICE) Perangkat akhir	19
• (INTERMEDIARY NETWORK DEVICE) Perantara Perangkat Jaringan	20
• MEDIA JARINGAN.....	20
• REPRESENTASI JARINGAN	21
• TOPOLOGI DIAGRAM	22
❖ LANs & WANs.....	23
• Tipe Jaringan	23
• LAN	24
• WAN	25
❖ Internet, Intranets, dan Extranets	26
• INTERNET	26
• INTRANET & EXTRANET.....	26
❖ Hubungan Internet.....	27
• TEKNOLOGI AKSES INTERNET.....	27
• KONEKSI INTERNET RUMAH DAN KANTOR SEDERHANA.....	27
• BISNIS KONEKSI INTERNET	29
1.3 JARINGAN SEBAGAI PLATFORM	30
❖ KONVERGENSI JARINGAN	30
• Jaringan Terpisah Tradisional.....	30
❖ Jaringan Konvergen.....	30

❖ JARINGAN YANG HANDAL.....	31
● Arsitektur Jaringan	31
● Toleransi Kesalahan	31
● Skalabilitas.....	32
● Kualitas Layanan.....	33
● Keamanan	33
1.4 MERUBAH LINGKUNGAN JARINGAN.....	35
❖ TREND JARINGAN.....	35
● Tren Baru.....	35
● Bawa Perangkat sendiri.....	35
● Kolaborasi Online	35
● Komunikasi Video.....	36
● Komputasi Awan	36
❖ TEKNOLOGI JARINGAN UNTUK RUMAH	37
● Tren Teknologi untuk Rumah.....	37
● Jaringan Powerline	37
● Wireless Broadband	38
❖ KEAMANAN JARINGAN	39
● Ancaman Keamanan	39
● Solusi Keamanan	40
LATIHAN SOAL 1	42
BAB 2 Konfigurasi sistem operasi jaringan	43
2.1 PENGANTAR	43
❖ CISCO IOS	43
● OPERATING SISTEM.....	43
● TUJUAN OPERATING SISTEM	44
● METODE AKSES	45
● PROGRAM EMULASI TERMINAL.....	46
● CISCO IOS MODE OPERASI	47
● MODE PERINTAH UTAMA	47
● KONFIGURASI MODE PERINTAH	48
● NAVIGASI ANTARA MODE IOS	49
● STRUKTUR PERINTAH DASAR IOS.....	50
● IOS COMMAND SYNTAX.....	50
● IOS Fitur HELP.....	51

• HotKeys & Shorcuts.....	51
❖ KONFIGURASI DASAR ALAT.....	53
• NAMA ALAT (DEVICE).....	53
• KONFIGURASI HOSTNAME.....	54
• AKSES PERANGKAT YANG AMAN	55
• KONFIGURASI PASSWORD	55
• ENKRIPSI PASSWORD	56
• PESAN BANNER / PEMBERITAHUAN	57
• SYNTAX CHECKER - Membatasi Akses ke Switch	58
• SIMPAN FILE KONFIGURASI YANG BERJALAN	58
• SETELAH KONFIGURASI BERJALAN.....	59
• MENYIMPAN KONFIGURASI KE FILE TEKS	60
❖ SKEMA PENGALAMATAN	62
• IP ADDRESS.....	62
• TAMPILAN DAN PORTS	63
• KONFIGURASI MANUAL ALAMAT IP UNTUK PERANGKAT	64
• KONFIGURASI ALAMAT IP OTOMATIS UNTUK PERANGKAT	65
• SWITCH VIRTUAL INTERFACE CONFIGURATION	66
• SYNTAX CHECKER - CONFIGURING A SWITCH VIRTUAL INTERFACE	67
• INTERFACE ADDRESSING VERIFICATION	67
LATIHAN SOAL 2	68
BAB 3 PROTOKOL JARINGAN DAN KOMUNIKASI.....	69
3.1 PENGANTAR	69
❖ ATURAN DALAM BERKOMUNIKASI	69
• DASAR-DASAR BERKOMUNIKASI.....	69
• ATURAN PEMBENTUKAN	70
• ENCODING PESAN	71
• FORMAT PESAN DAN ENKAPSULASI	71
• UKURAN PESAN.....	73
• WAKTU PESAN	73
• PILIHAN PENGIRIMAN PESAN	74
❖ PROTOKOL JARINGAN DAN STANDARD	74
• ATURAN YANG MENGATUR KOMUNIKASI.....	74
• PROTOKOL JARINGAN	75
• INTERAKSI PROTOKOL.....	77

• STANDART PROTOKOL DAN STANDART INDUSTRI	78
• PERKEMBANGAN TCP/IP	79
• TCP/ IP PROTOKOL SUITE	79
• TCP/ IP PROSES KOMUNIKASI	81
• STANDART TERBUKA.....	82
• STANDART INTERNET	83
• STANDART ORGANISASI KOMUNIKASI DAN ELEKTRONIK	84
• KEUNTUNGAN MENGGUNAKAN LAYERED MODEL	84
• MODEL REFERENSI OSI.....	85
• TCP/IP PROTOCOL MODEL.....	86
• PERBANDINGAN OSI MODEL DAN TCP / IP MODEL.....	87
❖ PENGIRIMAN DATA DIDALAM JARINGAN	88
• SEGMENTASI PESAN.....	88
• PROTOCOL DATA UNIT.....	89
• CONTOH ENKAPSULASI	89
• DE-ENKAPSULASI.....	90
• ALAMAT JARINGAN	90
• ALAMAT DATALINK	91
• PERANGKAT PADA JARINGAN YANG SAMA	92
• PERANGKAT DI JARINGAN JARAK JAUH	93
LATIHAN SOAL 3	95
BAB 4 AKSES JARINGAN	96
4.1 PENGANTAR	96
4.2 PROTOKOL LAYER FISIK	96
❖ KONEKSI LAYER FISIK.....	96
• TIPE KONEKSI.....	96
• NETWORK INTERFACE CARD	97
❖ TUJUAN PROTOKOL LAYER FISIK	98
• LAYER FISIK.....	98
• MEDIA LAYER FISIK.....	99
• STANDART LAYER FISIK	100
❖ KARAKTERISTIK LAYER FISIK	101
• FUNCTION	101
• BANDWIDTH	102
• THROUGHPUT	103

•	TIPE MEDIA FISIK.....	103
4.3	MEDIA JARINGAN.....	104
❖	COPPER CABLING	104
•	KARAKTERISTIK KABEL COPER.....	104
•	MEDIA KABEL COPER.....	105
•	KABEL TWISTED-PAIR UNSHIELDED	106
•	KABEL SHIELDED TWISTED-PAIR	107
•	KABEL COAXIAL	107
•	KEAMANAN KABEL COPPER / TEMBAGA	108
❖	UTP Cabling	109
•	PROPERTI KABEL UTP	109
•	STANDART KABEL UTP	109
•	KONEKTOR KABEL UTP	110
•	TIPE KABEL UTP	111
•	TESTING KABEL UTP	112
❖	FIBER-OPTIC CABLING	112
•	PROPERTI FIBER-OPTIC KABEL	112
•	DESAIN KABEL MEDIA FIBER	113
•	TIPE MEDIA FIBER.....	114
•	FIBER OPTIC KONEKTOR.....	115
•	TESTING FIBER KABEL.....	117
•	FIBER VS TEMBAGA.....	118
❖	MEDIA WIRELESS.....	118
•	PROPERTI MEDIA WIRELESS.....	118
•	TIPE MEDIA WIRELESS.....	119
•	WIRELESS LAN	120
4.4	DATA LINK LAYER PROTOCOL.....	120
❖	TUJUAN DATA LINK LAYER	120
•	DATA LINK LAYER	120
•	DATA LINK SUBLAYER	121
•	MEDIA AKSES CONTROL.....	122
•	PENYEDIAAN AKSES KE MEDIA.....	123
•	STANDARISASI DATA LINK LAYER.....	124
4.5	KENDALI AKSES MEDIA.....	124
❖	TOPOLOGIES.....	124

• PENGENDALIAN AKSES KE MEDIA.....	124
• TOPOLOGI FISIK DAN LOGIKA	125
❖ WAN TOPOLOGIES	126
• TOPOLOGI FISIK WAN SECARA UMUM	126
• TOPOLOGI POINT – TO – POINT FISIK	127
• TOPOLOGI POINT – TO – POINT LOGIS	127
❖ LAN TOPOLOGIES	128
• TOPOLOGI FISIK LAN SECARA UMUM	128
• HALF DAN FULL DUPLEX.....	129
• METODE AKSES KONTROL MEDIA.....	130
❖ DATA LINK FRAME.....	131
• FRAME.....	131
• FRAME FIELDS	131
LATIHAN SOAL 4.....	133
BAB 5 ETHERNET	134
5.1 PENGANTAR	134
5.2 ETHERNET PROTOCOL.....	134
❖ ETHERNET FRAME	134
• ETHERNET ENCAPSULATION	134
• MAC SUBLAYER	136
• ETHERNET EVOLUTION	136
• ETHERNET FRAME FIELDS	137
• ETHERNET MAC ADDRESSES	137
• MAC ADDRESSES : IDENTITAS ETHERNET	138
• FRAME PROCESSING	139
• MAC ADDRESS REPRESENTATIONS	140
• UNICAST MAC ADDRESS.....	141
• BROADCAST MAC ADDRESS.....	142
• MULTICAST MAC ADDRESS	142
5.3 LAN SWITCHES	143
❖ MAC ADDRESS TABEL.....	143
• FUNDAMENTAL SWITCH	143
• BELAJAR ALAMAT MAC	144
• MEMFILTER FRAME.....	146
❖ SWITCH FORWARDING METHODS.....	147

• METODE FRAME FORWARDING PADA CISCO SWITCHES	147
• CUT – THROUGH SWITCHING	147
• MEMORY BUFFERING ON SWITCHES.....	147
❖ SETTING PORT SWITCH	148
• DUPLEX AND SPEED SETTINGS.....	148
• AUTO – MIDX	150
5.4 ADDRESS RESOLUTION PROTOCOL.....	150
❖ MAC AND IP	150
• TUJUAN PADA JARINGAN YANG SAMA.....	150
❖ ARP	151
• PENGENALAN ARP.....	151
• FUNGSI ARP.....	152
❖ MASALAH ARP.....	154
• ARP BROADCAST	154
• ARP SPOOFING	154
LATIHAN SOAL 5	155
BAB 6 NETWORK LAYER	156
6.1 PENGANTAR	156
6.2 PROTOKOL LAPISAN JARINGAN	156
❖ KOMUNIKASI LAPISAN JARINGAN.....	156
• LAPISAN JARINGAN	156
• PROTOKOL LAPISAN JARINGAN	157
❖ KARAKTERISTIK IP PROTOKOL.....	157
• ENKAPSULASI IP	157
• KARAKTERISTIK IP.....	158
• IP TANPA KONEKSI	159
• IP BEST EFFORT DELIVERY	159
• IP MEDIA INDEPENDENT	160
❖ IPv4 PAKET	161
• IPV4 PACKET HEADER.....	161
❖ IPv6 PAKET	162
• KETERBATASAN IPv4	162
• PERKENALAN IPv6	163
• ENCAPSULASI IPv6.....	163
• IPv6 PACKET HEADER	165

6.3	ROUTING	166
❖	HOW a HOST ROUTES	166
•	HOST FORWARDING DECISION	166
•	DEFAULT GATEWAY	167
•	MENGGUNAKAN DEFAULT GATEWAY	167
•	HOST ROUTING TABLE	168
❖	ROUTER ROUTING TABLE.....	168
•	ROUTER PACKET FORWADING DECISION	168
•	IPv4 ROUTER ROUTING TABLE	169
•	DIRECTLY CONNECTED ROUTING TABLE ENTRIES.....	170
•	REMOTE CONNECTED ROUTING TABLE ENTRIES.....	171
•	NEXT HOP ADDRESS	171
6.4	ROUTERS	172
❖	ANATOMI ROUTER.....	172
•	ROUTER ADALAH KOMPUTER.....	172
•	ROUTER CPU DAN OS.....	173
•	ROUTER MEMORY.....	173
•	DIDALAM SEBUAH ROUTER	174
•	KONEKSI KE ROUTER	175
•	LAN & WAN INTERFACE	175
❖	ROUTER BOOT-UP.....	176
•	BOOTSET FILES	176
•	ROUTER BOOTUP PROCESS.....	176
6.5	CONFIGURE ROUTERS	178
❖	CONFIGURE INITIAL SETTINGS	178
•	BASIC SWITCH CONFIGURATION STEPS	178
•	BASIC ROUTER CONFIGURATION STEPS.....	180
❖	CONFIGURE INTERFACE	182
•	CONFIGURE ROUTER INTERFACE	182
•	VERIFIKASI INTERFACE CONFIGURE	184
❖	CONFIGURE THE DEFAULT GATEWAY.....	185
•	DEFAULT GATEWAY FOR A HOST	185
•	DEFAULT GATEWAY FOR SWITCH	186
	LATIHAN SOAL 6	188
	BAB 7 IP ADDRESSING	189

7.1	PENGANTAR	189
7.2	IPv4 NETWORK ADDRESSES	189
❖	BINARY & DESIMAL CONVERSION.....	189
●	IPV4 ADDRESSES.....	189
●	POSITIONAL NATION.....	190
●	KONVERSI BINARY KE DECIMAL	192
●	KONVERSI DECIMAL KE BINARY	194
●	CONTOH KONVERSI DECIMAL KE BINARY	194
❖	IPv4 STRUKTUR ALAMAT.....	195
●	NETWORK AND HOST PORTION.....	195
●	SUBNET MASK	196
●	ANDing	197
●	PANJANG PREFIX.....	198
●	NETWORK, HOST AND BROADCAST ADDRESSES	199
❖	IPv4 UNICAST, BROADCAST, AND MULTICAST.....	201
●	STATISTIC IPV4 ADDRESS ASSIGNMENT TO A HOST	201
●	DYNAMIC IPV4 ADDRESS ASSIGNMENT TO A HOST	202
●	KOMUNIKASI IPV4.....	203
●	UNICAST TRANSMISSION	204
●	BROADCAST TRANSMISSION.....	204
●	MULTICAST TRANSMISSION.....	205
❖	TIPE PENGALAMATAN IPv4.....	205
●	PUBLIC AND PRIVATE ADDRESSES	205
●	SPESIAL USER IPV4 ADDRESSES.....	206
●	PENANGANAN CLASSICAL LEGACY.....	207
●	PENGALAMATAN TANPA KELAS.....	208
●	ASSIGNMENT OF IP ADDRESSES.....	209
7.3	IPv6 NETWORK ADDRESSES	210
❖	MASALAH IPV4.....	210
●	KEBUTUHAN AKAN IPV6.....	210
●	KOEKSTENSISI IPV4 DAN IPv6	210
❖	PENGALAMATAN IPv6.....	212
●	REPRESENTASI PENGALAMATAN IPV6.....	212
●	RULE 1 – OMIT LEADING OS.....	213
●	RULE 2 – OMIT ALL 0 SEGMENTS	214

❖ TIPE PENGALAMATAN IPv6.....	216
● TIPE ALAMAT IPV6	216
● PANJANG PREFIX IPV6.....	217
● IPv6 UNICAST ADDRESSES.....	217
● IPv6 LINK- LOCAL UNICAST ADDRESSES.....	218
❖ IPv6 UNICAST ADDRESSES.....	220
● STRUKTUR IPv6 GLOBAL UNICAST ADDRESSES.....	220
● STATIC CONFIGURATION OF A GLOBAL UNICAST ADDRESSES	222
● DYNAMIC CONFIGURATION – SLAAC.....	224
● EUI-64 PROCESS AND RANDOMLY GENERATED	225
● DYNAMIC LINK-LOCAL ADDRESSES	228
● STATIC LINK-LOCAL ADDRESSES.....	229
● VERIFIKASI IPv6 ADDRESS CONFIGURATION.....	230
❖ IPv6 MULTICAST ADDRESSES	232
● ASSIGNED IPv6 MULTICAST ADDRESSES.....	232
● SOLICITED-NODE IPv6 MULTICAST ADDRESSES.....	233
7.4 VERIFIKASI KONEKTIFITAS	234
❖ ICMP	234
● ICMPv4 DAN ICMPv6.....	234
● ICMPv6 ROUTER SOLICITATION AND ROUTER ADVERTISEMENT MESSAGES.....	235
❖ TESTING & VERIFIKASI.....	237
● PING – TESTING LOCAL STACK	237
● PING – TESTING CONNECTIVITY TO THE LOCAL LAN	238
● PING – TESTING CONNECTIVITY TO REMOTE	239
LATIHAN SOAL 7	240
BAB 8 SUBNETTING IP NETWORKS	241
8.1 PENGANTAR	241
8.2 SUBNETTING IPv4 NETWORK	241
❖ NETWORK SEGMENTATION	241
● BROADCAST DOMAINS	241
● PROBLEM WITH LARGE BROADCAST DOMAINS	242
● REASONS FOR SUBNETTING.....	243
❖ SUBNETTING IPv4 NETWORK.....	244
● OCTET BOUNDARIES	244
● SUBNETTING ON THE OCTET BOUNDARIES	245

• CLASSLESS SUBNETTING	246
• CLASSLESS SUBNETTING EXAMPLE	247
• CREATING 2 SUBNETS	249
• SUBNETTING FORMULAS	251
• CREATING 4 SUBNETS	252
❖ SUBNETTING a/16 AND /8 PREFIX	254
• CREATING SUBNETS WITH a/16 PREFIX.....	254
• CREATING 100 SUBNETS WITH a/16 NETWORK	255
• CALCULATING THE HOSTS.....	256
❖ SUBNETTING TO MEET REQUIREMENTS.....	257
• SUBNETTING BASED ON HOST REQUIREMENTS.....	257
• SUBNETTING BASED ON NETWORK REQUIREMENTS.....	258
• NETWORK REQUIREMENTS EXAMPLE	258
❖ BENEFITS OF VARIABLE LENGTH SUBNET MASKING.....	260
• TRADITIONAL SUBNETTING WASTES ADDRESSES.....	260
• VARIABEL LENGTH SUBNET MASKS	262
• BASIC VLSM	263
• VLSM IN PRACTICE	264
• VLSM CHART	265
8.3 ADDRESSING SCHEMES	267
❖ STRUCTURED DESIGN.....	267
• NETWORK ADDRESSING PLANNING	267
• PLANNING TO ADDRESS THE NETWORK.....	267
• ASSIGNING ADDRESSES TO DEVICES.....	268
8.4 DESIGN CONSIDERATIONS FOR IPv6	269
❖ SUBNETTING AN IPv6 NETWORK	269
• THE IPv6 GLOBAL UNICAST ADDRESS	269
• SUBNETTING USING THE SUBNET ID.....	270
• IPv6 SUBNET ALLOCATION	271
LATIHAN SOAL 8	273
BAB 9 TRANSPORT LAYER	274
9.1 PENGANTAR	274
9.2 TRANSPORT LAYER PROTOCOLS	274
❖ TRANSPORT OF DATA.....	274
• ROLE OF THE TRANSPORT LAYER.....	274

• TRANSPORT LAYER RESPONSIBILITIES	275
• CONVERSATION MULTIPLEXING	277
• TRANSPORT LAYER RELIABILITY	277
• UDP	278
• THE RIGHT TRANSPORT LAYER PROTOCOL FOR THE RIGHT APPLICATION.....	279
❖ TCP DAN UDP OVERVIEW	280
• TCP FEATURES.....	280
• TCP HEADER	281
• UDP FEATURES	282
• UDP HEADER	282
• MULTIPLE SEPARATE CONVERSATIONS	283
• PORT NUMBERS	283
• SOCKET PAIRS.....	284
• PORT NUMBER GROUPS	285
• THE NETSTAT COMMAND.....	286
9.3 TCP DAN UDP	287
❖ TCP COMMUNICATION PROCESS.....	287
• TCP SERVER PROCESSES.....	287
• TCP CONNECTION ESTABLISHMENT	288
• TCP SESSION TERMINATION	289
• TCP THREE-WAY HANDSHAKE ANALYSIS	289
❖ UDP COMMUNICATION PROCESS.....	290
• UDP LOW OVERHEAD VERSUS RELIABILITY	290
• UDP DATAGRAM REASSEMBLY	291
• UDP SERVER PROCESSES AND REQUEST.....	291
• UDP CLIENT PROCESSES	292
❖ TCP ATAU UDP	293
• APPLICATION THAT USE TCP	293
• APPLICATION THAT USE UDP	294
LATIHAN SOAL 9	295
BAB 10 APPLICATION LAYER	296
10.1 PENGANTAR	296
10.2 APPLICATION LAYER PROTOCOLS	296
❖ APPLICATION, PRESENTATION AND SESSION	296
• APPLICATION LAYER	296

• PRESENTATION AND SESSION LAYER.....	297
• TCP / IP APPLICATION LAYER PROTOCOLS.....	297
❖ HOW APPLICATION PROTOCOLS INTERACT WITH END-USER APPLICATIONS.....	298
• CLIENT-SERVER MODEL.....	298
• PEER-TO-PEER NETWORKS.....	298
• PEER-TO-PEER APPLICATIONS.....	299
• COMMON P2P APPLICATIONS	300
10.3 WELL-KNOWN APPLICATION LAYER PROTOCOLS AND SERVICES.....	301
❖ WEB AND EMAIL PROTOCOLS.....	301
• HYPertext Transfer Protocol And Hypertext Markup Language	301
• HTTP AND HTTPS.....	301
• EMAIL PROTOCOLS.....	302
• SMTP OPERATION	303
• POP OPERATION.....	304
• IMAP OPERATION.....	304
❖ IP ADDRESSING SERVICES	305
• DOMAIN NAME SERVICE.....	305
• DNS MESSAGE FORMAT.....	305
• DNS HIERARCHY	306
• NSLOOKUP COMMAND.....	307
• DYNAMIC HOST CONFIGURATION PROTOCOL	308
• DHCP OPERATION	309
❖ FILE SHARING SERVICES	310
• FILE TRANSFER PROTOCOL.....	310
• SERVER MESSAGE BLOCK	310
LATIHAN SOAL 10.....	312

BAB 1 MENJELAJAHI JARINGAN

1.1 HUBUNGAN GLOBAL

Kita sekarang berdiri di titik balik kritis dalam penggunaan teknologi untuk memperluas dan memberdayakan kemampuan kita untuk berkomunikasi. Globalisasi Internet telah berhasil lebih cepat dari yang bisa dibayangkan siapa pun. Cara interaksi sosial, komersial, politik dan pribadi terjadi dengan cepat berubah untuk mengikuti evolusi jaringan global ini. Pada tahap selanjutnya, inovator akan menggunakan Internet sebagai titik awal untuk usaha mereka, menciptakan produk dan layanan baru yang dirancang khusus untuk memanfaatkan kemampuan jaringan. Sebagai pengembang mendorong batas dari apa yang mungkin, kemampuan jaringan yang saling berhubungan yang membentuk Internet akan memainkan peran yang semakin meningkat dalam keberhasilan proyek-proyek ini.

Bab ini memperkenalkan platform jaringan data yang dengannya hubungan sosial dan bisnis kita semakin bergantung. Materi tersebut meletakkan dasar untuk mengeksplorasi layanan, teknologi, dan masalah yang dihadapi oleh profesional jaringan saat mereka merancang, membangun, dan memelihara jaringan modern.

- **JARINGAN DALAM KEHIDUPAN**

Di antara semua hal penting bagi eksistensi manusia, kebutuhan untuk berinteraksi dengan orang lain berada di bawah kebutuhan kita untuk mempertahankan kehidupan. Komunikasi hampir sama pentingnya bagi kita sebagai ketergantungan kita pada udara, air, makanan, dan tempat tinggal.

Di dunia sekarang ini, melalui penggunaan jaringan, kita terhubung tidak seperti sebelumnya. Orang dengan ide bisa berkomunikasi seketika dengan orang lain untuk membuat gagasan itu menjadi kenyataan. Berita acara dan penemuan dikenal di seluruh dunia dalam hitungan detik. Individu bahkan bisa terhubung dan bermain game dengan teman yang dipisahkan oleh samudra dan benua.

- **TEKNOLOGI SAATINI**

Bayangkan sebuah dunia tanpa internet. Tidak ada lagi Google, YouTube, instant messaging, Facebook, Wikipedia, game online, Netflix, iTunes, dan akses mudah ke informasi terkini. Tidak ada situs perbandingan harga lainnya, hindari jalur dengan belanja online, atau dengan cepat mencari nomor telepon dan arahkan peta ke berbagai lokasi dengan sekali klik. Seberapa berbedanya hidup kita tanpa semua ini? Itulah dunia yang kita tinggali hanya dalam 15 sampai 20 tahun yang lalu. Namun selama bertahun-tahun, jaringan data telah berkembang perlahan dan telah diperbaiki untuk memperbaiki kualitas hidup orang-orang di mana-mana.

- **TANPA BATAS**

Kemajuan teknologi jaringan mungkin merupakan perubahan paling signifikan di dunia saat ini. Mereka membantu menciptakan dunia di mana batas-batas nasional, jarak geografis, dan keterbatasan fisik menjadi kurang relevan sehingga menghadirkan hambatan yang terus berkurang.

Internet telah mengubah cara interaksi sosial, komersial, politik, dan pribadi. Sifat langsung

komunikasi melalui Internet mendorong terciptanya komunitas global. Komunitas global memungkinkan interaksi sosial yang tidak bergantung pada lokasi atau zona waktu. Penciptaan komunitas online untuk pertukaran gagasan dan informasi berpotensi meningkatkan peluang produktivitas di seluruh dunia.

- **JARINGAN MENDUKUNG BELAJAR**

Jaringan telah mengubah cara kita belajar. Akses ke pengajaran berkualitas tinggi tidak lagi terbatas pada siswa yang tinggal di tempat dimana instruksi tersebut disampaikan. Pembelajaran jarak jauh online telah menghilangkan hambatan geografis dan meningkatkan kesempatan siswa. Jaringan yang tangguh dan terpercaya mendukung dan memperkaya pengalaman belajar siswa. Mereka memberikan materi pembelajaran dalam berbagai format termasuk aktivitas interaktif, penilaian, dan umpan balik

- **JARINGAN MENDUKUNG KOMUNIKASI**

Globalisasi Internet telah mengantar bentuk komunikasi baru yang memberdayakan individu untuk menciptakan informasi yang dapat diakses oleh khalayak global.

- **Bentuk Komunikasi**

Beberapa bentuk komunikasi meliputi:

- ✓ **Texting** - Texting memungkinkan komunikasi real-time instan antara dua orang atau lebih.
- ✓ **Media Sosial** - Media sosial terdiri dari situs web interaktif tempat orang dan komunitas membuat dan berbagi konten buatan pengguna dengan teman, keluarga, rekan kerja, dan dunia.
- ✓ **Alat Kolaborasi** - Tanpa batasan lokasi atau zona waktu, alat kolaborasi memungkinkan individu untuk berkomunikasi satu sama lain, seringkali di video interaktif real-time. Distribusi jaringan data yang luas berarti bahwa orang-orang di lokasi terpencil dapat berkontribusi atas dasar kesetaraan dengan orang-orang di jantung pusat populasi yang besar.
- ✓ **Blog** - Blogs, yang merupakan kependekan dari kata "weblog", adalah halaman web yang mudah untuk diupdate dan diedit. Tidak seperti situs komersial, blog memberi orang sarana untuk mengkomunikasikan pemikiran mereka ke pemirsa global tanpa pengetahuan teknis tentang desain web.
- ✓ **Wikis** - Wikis adalah halaman web yang dapat diedit dan dilihat oleh orang-orang. Sedangkan sebuah blog lebih bersifat individual, jurnal pribadi, sebuah wiki adalah sebuah kelompok penciptaan. Dengan demikian, mungkin akan ditinjau dan diedit lebih ekstensif. Banyak bisnis menggunakan wiki sebagai alat kolaborasi internal mereka.
- ✓ **Podcasting** - Podcasting memungkinkan orang untuk memberikan rekaman audio mereka ke khalayak luas. File audio ditempatkan di situs web (atau blog atau wiki) tempat orang lain dapat mengunduhnya dan memutar rekaman di komputer, laptop, dan perangkat seluler lainnya.
- ✓ **Peer-to-Peer (P2P) File Sharing** - Berbagi file peer-to-peer memungkinkan orang berbagi file satu sama lain tanpa harus menyimpan dan mendownloadnya dari server pusat. Pengguna bergabung dengan jaringan P2P hanya dengan menginstal perangkat

Iunak P2P. Berbagi file P2P belum dipeluk oleh semua orang. Banyak orang khawatir melanggar hukum materi berhak cipta.

- **JARINGAN MENDUKUNG PEKERJAAN**

Di dunia bisnis, jaringan data pada awalnya digunakan oleh perusahaan untuk mencatat dan mengelola informasi keuangan, informasi pelanggan, dan sistem penggajian karyawan secara internal. Jaringan bisnis ini berevolusi untuk memungkinkan transmisi berbagai jenis layanan informasi, termasuk email, video, pesan, dan telepon.

Penggunaan jaringan untuk memberikan pelatihan karyawan yang efisien dan hemat biaya semakin meningkat dalam penerimaan. Peluang belajar online dapat mengurangi perjalanan yang memakan waktu dan mahal, namun tetap memastikan bahwa semua karyawan dilatih secara memadai untuk melakukan pekerjaan mereka dengan cara yang aman dan produktif.

- **JARINGAN MENDUKUNG PERMAINAN**

Internet digunakan untuk bentuk hiburan tradisional. Kami mendengarkan rekaman artis, melihat pratinjau atau melihat gambar gerak, membaca keseluruhan buku, dan mendownload materi untuk akses offline di masa mendatang. Acara olah raga dan konser live dapat dialami saat terjadi, atau dicatat dan dilihat berdasarkan permintaan.

Jaringan memungkinkan terciptanya bentuk hiburan baru, seperti game online. Pemain berpartisipasi dalam kompetisi online apapun yang bisa dibayangkan para perancang game. Kami bersaing dengan teman dan musuh di seluruh dunia seolah-olah kami semua berada di ruangan yang sama.

Bahkan aktivitas offline pun ditingkatkan dengan menggunakan layanan kolaborasi jaringan. Komunitas minat global berkembang dengan pesat. Kami berbagi pengalaman dan hobi yang umum di luar lingkungan, kota, atau wilayah setempat. Penggemar olahraga berbagi pendapat dan fakta tentang tim favorit mereka. Kolektor menampilkan koleksi berharga dan mendapatkan umpan balik ahli tentang mereka

- **JARINGAN DALAM BERBAGAI UKURAN**

Jaringan datang dalam segala ukuran. Mereka dapat berkisar dari jaringan sederhana yang terdiri dari dua komputer ke jaringan yang menghubungkan jutaan perangkat.

Jaringan sederhana yang dipasang di rumah memungkinkan berbagi sumber daya, seperti printer, dokumen, gambar dan musik antara beberapa komputer lokal.

Jaringan kantor rumah dan jaringan kantor kecil sering kali disiapkan oleh individu yang bekerja dari rumah atau kantor terpencil dan perlu terhubung ke jaringan perusahaan atau sumber terpusat lainnya. Selain itu, banyak wiraswasta menggunakan kantor rumah dan jaringan kantor kecil untuk mengiklankan dan menjual produk, memesan persediaan dan berkomunikasi dengan pelanggan.

Dalam bisnis dan organisasi besar, jaringan dapat digunakan dalam skala yang lebih luas lagi untuk menyediakan konsolidasi, penyimpanan, dan akses terhadap informasi pada server jaringan. Jaringan juga memungkinkan komunikasi yang cepat seperti email, pesan instan, dan kolaborasi antar karyawan. Selain manfaat internal, banyak organisasi menggunakan jaringan

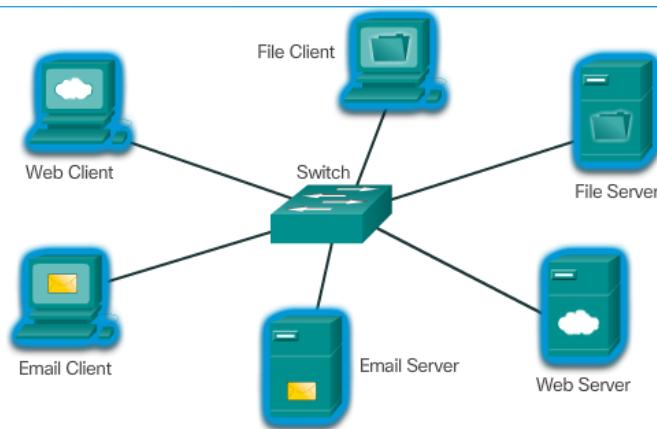
mereka untuk menyediakan produk dan layanan kepada pelanggan melalui koneksi mereka ke internet. Internet adalah jaringan terbesar yang ada. Sebenarnya, istilah internet berarti 'jaringan jaringan'. Internet secara harfiah merupakan kumpulan jaringan pribadi dan publik yang saling berhubungan, seperti yang dijelaskan di atas.

- **Clients dan Server**

Semua komputer yang terhubung ke jaringan yang berpartisipasi secara langsung dalam komunikasi jaringan dikelompokkan sebagai host. Host juga disebut perangkat akhir.

Server adalah komputer dengan perangkat lunak yang memungkinkan mereka memberikan informasi, seperti email atau halaman web, ke perangkat akhir lainnya di jaringan. Setiap layanan memerlukan perangkat lunak server terpisah. Misalnya, server memerlukan perangkat lunak server web untuk memberikan layanan web ke jaringan. Komputer dengan perangkat lunak server dapat memberikan layanan secara bersamaan kepada satu atau banyak klien. Selain itu, satu komputer dapat menjalankan beberapa jenis perangkat lunak server. Di rumah atau usaha kecil, mungkin diperlukan satu komputer untuk bertindak sebagai server file, server web, dan server email.

Klien adalah komputer dengan perangkat lunak yang diinstal yang memungkinkan mereka untuk meminta dan menampilkan informasi yang diperoleh dari server. Contoh perangkat lunak klien adalah browser web, seperti Chrome atau FireFox. Satu komputer juga dapat menjalankan beberapa jenis perangkat lunak klien. Misalnya, pengguna bisa mengecek email dan melihat halaman web sembari instant messaging dan mendengarkan radio internet.



Contoh Client & server

- **Peer to Peer**

Perangkat lunak client dan server biasanya berjalan di komputer terpisah, namun juga memungkinkan satu komputer untuk menjalankan kedua peran pada saat bersamaan. Di usaha kecil dan rumah, banyak komputer berfungsi sebagai server dan klien di jaringan. Jenis jaringan ini disebut jaringan peer-to-peer.

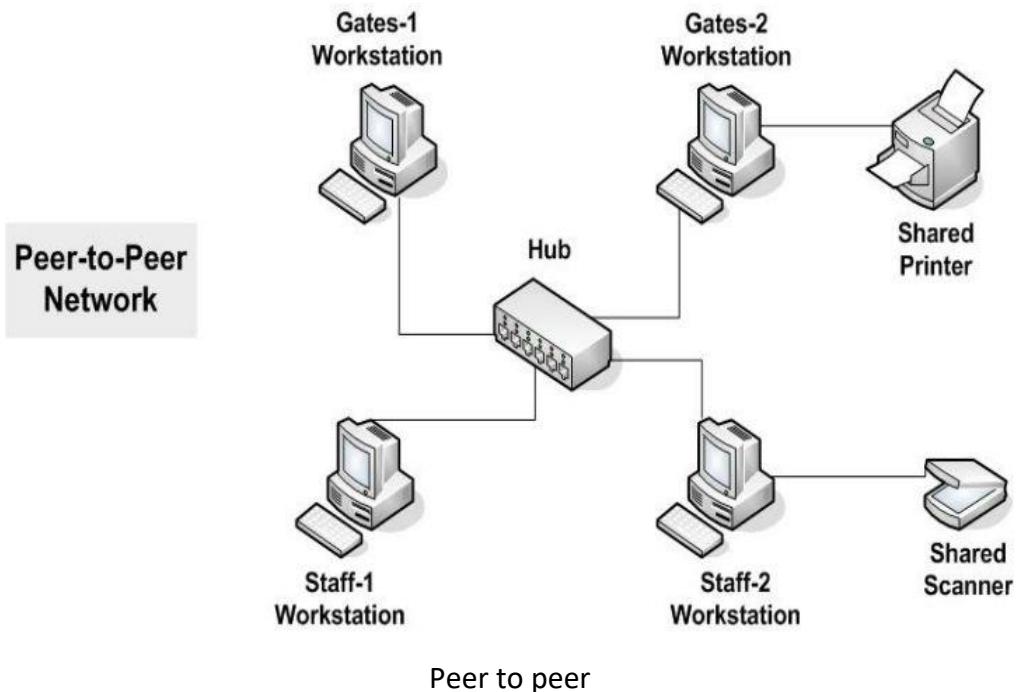
Keuntungan jaringan peer-to-peer:

- ✓ Mudah dipasang
- ✓ Kurang Kompleksitas

- ✓ Turunkan biaya karena perangkat jaringan dan dedicated server mungkin tidak diperlukan
- ✓ Bisa digunakan untuk tugas sederhana seperti mentransfer file dan sharing printer

Kelemahan jaringan peer-to-peer:

- ✓ Tidak ada administrasi terpusat
- ✓ Tidak aman
- ✓ Tidak terukur
- ✓ Semua perangkat dapat bertindak baik sebagai klien maupun server yang dapat memperlambat kinerja mereka



1.2 LAN, WAN dan INTERNET

❖ KOMPONEN JARINGAN

Jalur yang diambil pesan dari sumber ke tujuan bisa sesederhana satu kabel yang menghubungkan satu komputer dengan komputer lain, atau sekompleks kumpulan jaringan yang secara harfiah menjangkau dunia. Infrastruktur jaringan ini menyediakan saluran yang stabil dan andal dimana komunikasi ini terjadi.

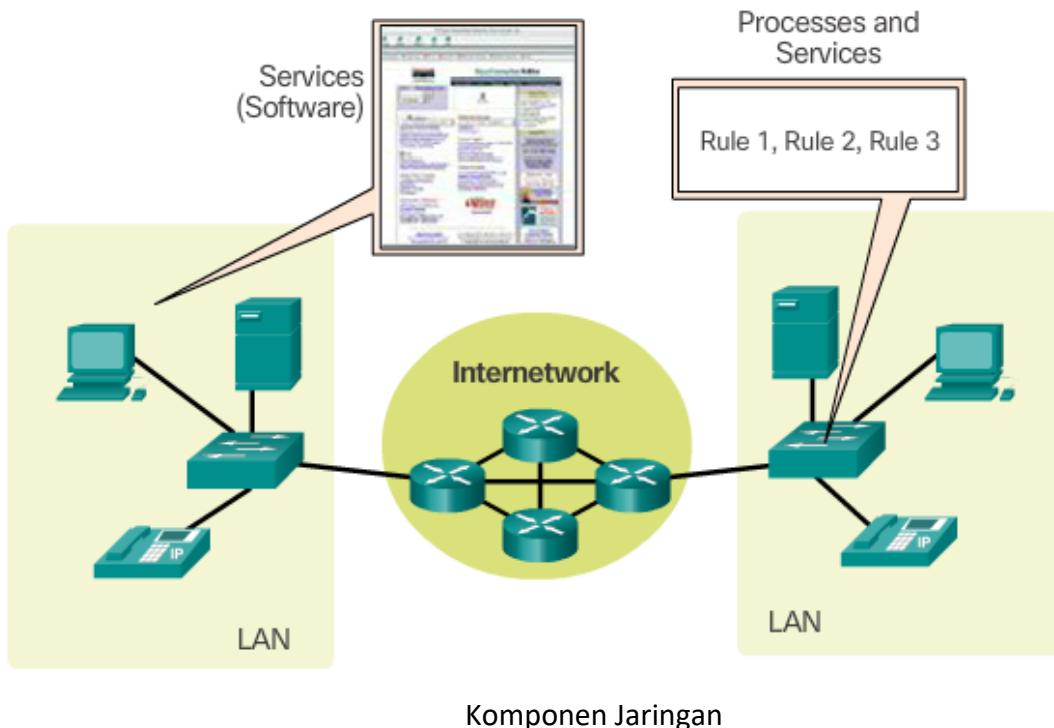
Tiga kategori komponen jaringan:

- ✓ Device / Perangkat
- ✓ Media
- ✓ Service / Layanan

Perangkat dan media adalah elemen fisik, atau perangkat keras, dari jaringan. Perangkat keras seringkali merupakan komponen yang terlihat dari platform jaringan seperti laptop, PC, switch, router, jalur akses nirkabel, atau kabel yang digunakan untuk menghubungkan perangkat.

Layanan mencakup banyak aplikasi jaringan umum yang digunakan orang setiap hari, seperti layanan email hosting dan layanan web hosting. Proses menyediakan fungsionalitas yang mengarahkan dan memindahkan pesan melalui jaringan.

Prosesnya kurang jelas bagi kita namun sangat penting untuk pengoperasian jaringan.



• (END DEVICE) Perangkat akhir

Perangkat jaringan yang paling dikenal orang disebut perangkat akhir. Beberapa contoh perangkat akhir ditunjukkan pada Gambar dibawah.

Perangkat akhir adalah sumber atau tujuan pesan yang dikirimkan melalui jaringan. Untuk membedakan satu perangkat ujung dari yang lain, setiap perangkat akhir pada jaringan diidentifikasi oleh sebuah alamat. Bila perangkat akhir memulai komunikasi, perangkat akan menggunakan alamat perangkat tujuan akhir untuk menentukan lokasi pesan yang akan dikirim.

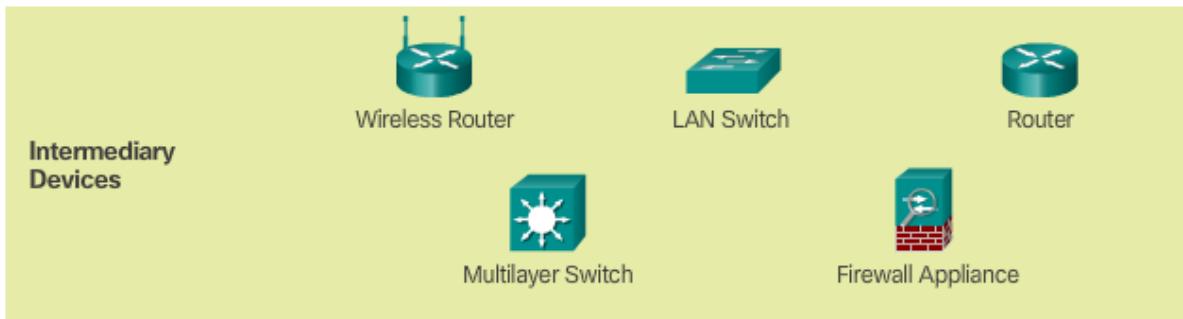


Perangkat Akhir

• (INTERMEDIARY NETWORK DEVICE) Perantara Perangkat Jaringan

Perantara perangkat menghubungkan perangkat akhir individu ke jaringan dan dapat menghubungkan beberapa jaringan individu untuk membentuk sebuah internetwork. Perangkat perantara ini menyediakan konektivitas dan memastikan arus data melintasi jaringan.

Perangkat perantara menggunakan alamat perangkat tujuan akhir, bersamaan dengan informasi tentang interkoneksi jaringan, untuk menentukan jalur yang harus diambil pesan melalui jaringan. Contoh perangkat perantara yang lebih umum dan daftar fungsi ditunjukkan pada gambar.



Perantara Perangkat jaringan

Fungsi perantara perangkat jaringan:

- meregenerasi dan mentransmisikan kembali sinyal data
- Pertahankan informasi tentang jalur apa yang ada melalui jaringan dan internetwork
- memberitahukan perangkat kesalahan dan kegagalan komunikasi lainnya
- Data langsung sepanjang jalur alternatif bila terjadi kegagalan tautan
- klasifikasikan dan pesan langsung sesuai prioritas
- mengizinkan atau menolak arus data, berdasarkan pengaturan keamanan

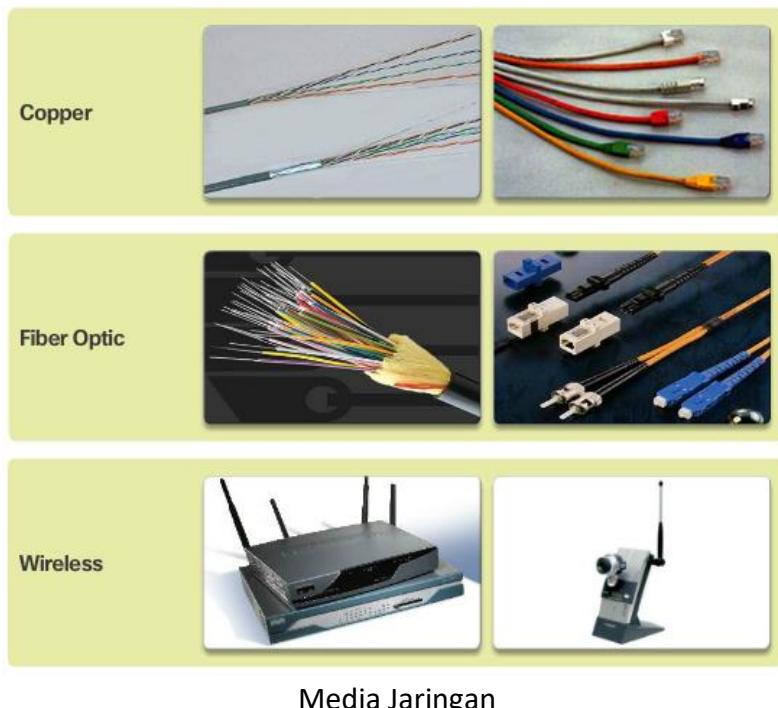
• MEDIA JARINGAN

Komunikasi antar jaringan dilakukan melalui media. Media menyediakan saluran tempat pesan berpindah dari sumber ke tujuan. Jaringan modern terutama menggunakan tiga jenis

media untuk menghubungkan perangkat dan untuk menyediakan jalur di mana data dapat ditransmisikan. Seperti ditunjukkan pada Gambar, media ini adalah:

- ✓ **Kabel logam dalam kabel** - data dikodekan menjadi impuls listrik
- ✓ **Serat kaca atau plastik** (kabel serat optik) - data dikodekan sebagai pulsa cahaya
- ✓ **Transmisi nirkabel** - data dikodekan menggunakan panjang gelombang dari spektrum elektromagnetik

Berbagai jenis media jaringan memiliki fitur dan manfaat yang berbeda. Tidak semua media jaringan memiliki karakteristik yang sama, dan juga tidak semuanya cocok untuk tujuan yang sama.



• REPRESENTASI JARINGAN

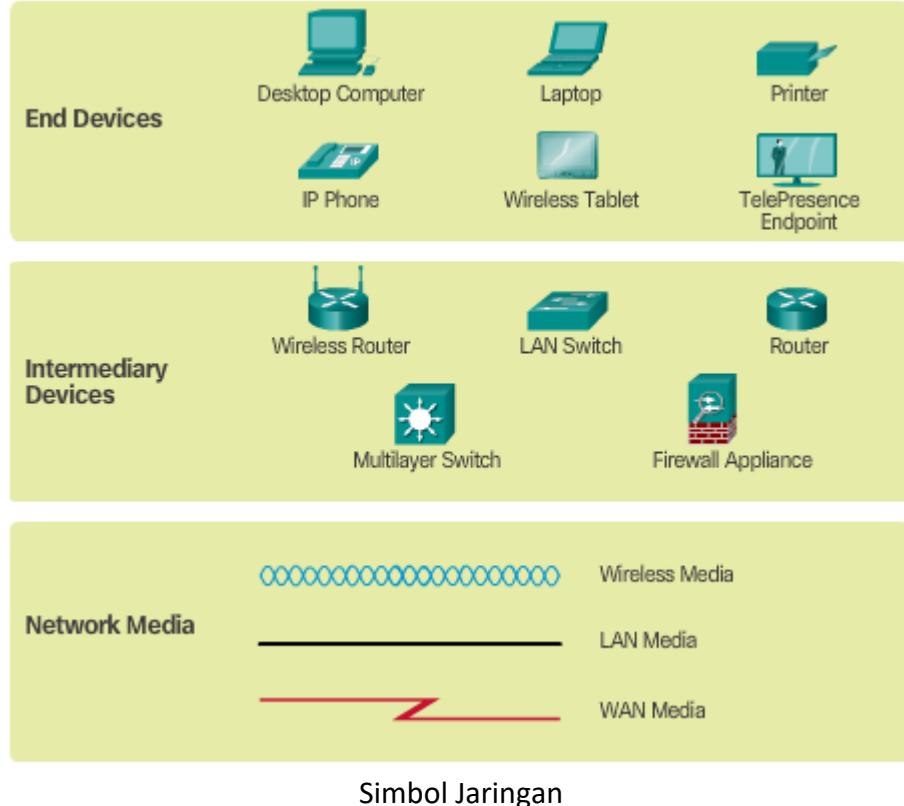
Diagram jaringan sering menggunakan simbol, seperti yang ditunjukkan pada Gambar, untuk mewakili berbagai perangkat dan koneksi yang membentuk jaringan. Diagram menyediakan cara mudah untuk memahami bagaimana perangkat dalam jaringan besar terhubung. Jenis "gambar" jaringan ini dikenal sebagai diagram topologi. Kemampuan untuk mengenali representasi logis dari komponen jaringan fisik sangat penting untuk dapat memvisualisasikan organisasi dan pengoperasian jaringan.

Selain representasi ini, istilah khusus digunakan saat membahas bagaimana masing-masing perangkat dan media terhubung satu sama lain. Hal penting yang harus diingat adalah:

- ✓ **Network Interface Card** - Adaptor NIC atau LAN, menyediakan koneksi fisik ke jaringan pada PC atau perangkat akhir lainnya. Media yang menghubungkan PC ke perangkat jaringan, langsung terhubung ke NIC.
- ✓ **Port Fisik** - Konektor atau outlet pada perangkat jaringan tempat media terhubung ke perangkat akhir atau perangkat jaringan lainnya.

- ✓ **Interface** - Port khusus pada perangkat jaringan yang terhubung ke jaringan individual. Karena router digunakan untuk interkoneksi jaringan, port pada router disebut sebagai antarmuka jaringan.

Catatan: Seringkali, istilah port dan interface digunakan secara bergantian.



• TOPOLOGI DIAGRAM

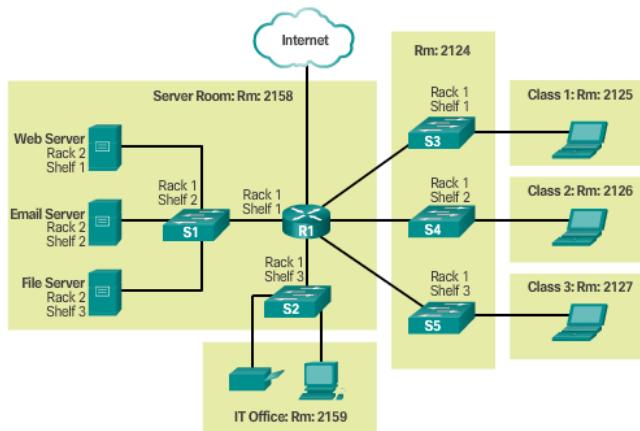
Diagram topologi wajib bagi siapa saja yang bekerja dengan jaringan.

Mereka menyediakan peta visual tentang bagaimana jaringan terhubung.

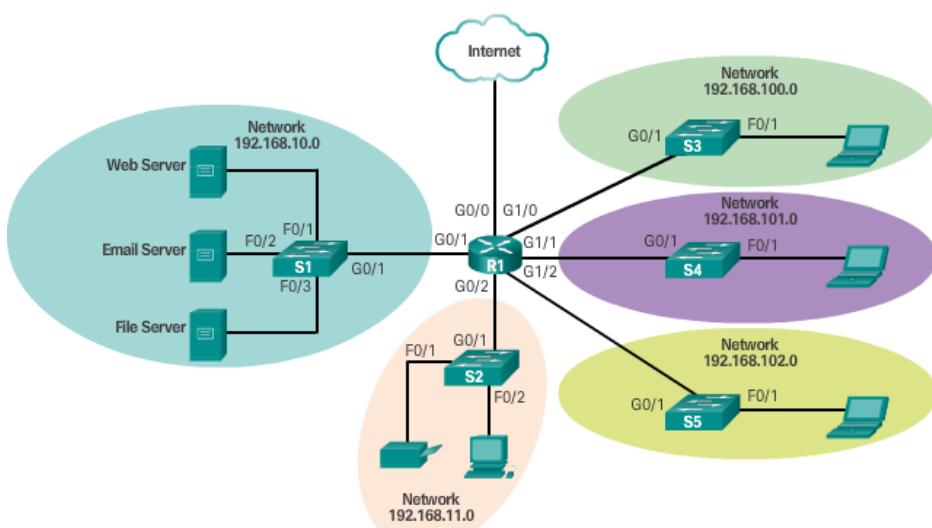
Ada dua jenis diagram topologi:

- ✓ Diagram topologi fisik - Identifikasi lokasi fisik perangkat perantara dan pemasangan kabel.
- ✓ Diagram topologi logis - Identifikasi perangkat, port, dan skema pengalaman.

Topologi yang ditunjukkan dalam diagram fisik dan logika sesuai untuk tingkat pemahaman Anda pada saat ini. Cari di Internet untuk "diagram topologi jaringan" untuk melihat beberapa contoh yang lebih kompleks. Jika Anda menambahkan "Cisco" ke frasa pencarian Anda, Anda akan menemukan banyak topologi menggunakan ikon serupa dengan apa yang telah Anda lihat di bab ini.



Topologi Fisik



Topologi Logis

❖ LANs & WANs

• Tipe Jaringan

Infrastruktur jaringan dapat sangat bervariasi dalam hal:

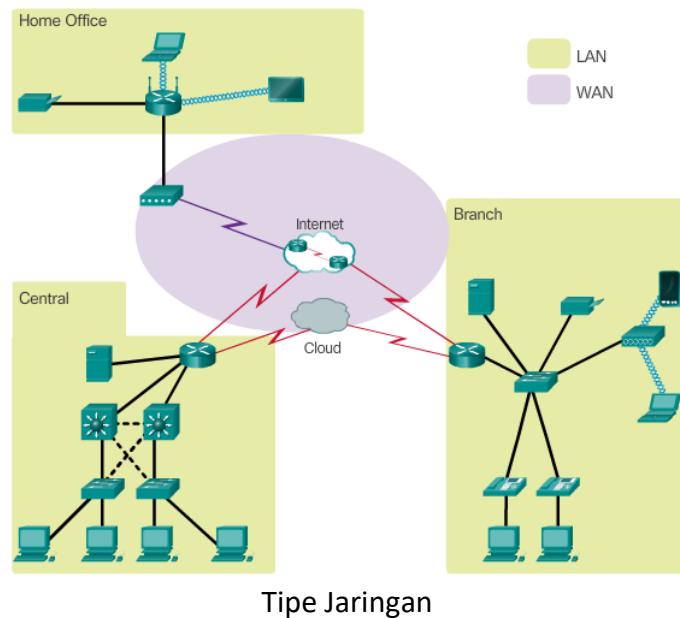
- ✓ Ukuran area tertutup
- ✓ Jumlah pengguna yang terhubung
- ✓ Jumlah dan jenis layanan yang tersedia
- ✓ Area tanggung jawab

Angka tersebut menggambarkan dua jenis infrastruktur jaringan yang paling umum:

- ✓ **Local Area Network (LAN)** - Infrastruktur jaringan yang menyediakan akses ke pengguna dan perangkat akhir di wilayah geografis kecil, yang biasanya merupakan jaringan perusahaan, rumah, atau usaha kecil yang dimiliki dan dikelola oleh departemen perorangan atau TI.
- ✓ **Wide Area Network (WAN)** - Infrastruktur jaringan yang menyediakan akses ke jaringan lain di wilayah geografis yang luas, yang biasanya dimiliki dan dikelola oleh penyedia layanan telekomunikasi.

Jenis jaringan lainnya meliputi:

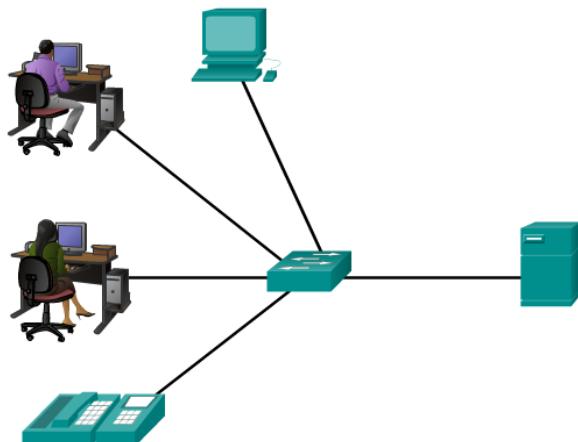
- ✓ **Metropolitan Area Network (MAN)** - Infrastruktur jaringan yang mencakup area fisik yang lebih besar daripada LAN namun lebih kecil dari WAN (mis., Kota). MAN biasanya dioperasikan oleh satu kesatuan seperti organisasi besar.
- ✓ **Wireless LAN (WLAN)** - Serupa dengan LAN namun secara nirkabel menghubungkan pengguna dan titik akhir di area geografis yang kecil.
- ✓ **Storage Area Network (SAN)** - Infrastruktur jaringan yang dirancang untuk mendukung server file dan menyediakan penyimpanan data, pengambilan, dan replikasi.



- **LAN**

LAN adalah infrastruktur jaringan yang membentang di wilayah geografis yang kecil. Fitur khusus LAN meliputi:

- ✓ LAN saling menghubungkan perangkat akhir di area terbatas seperti rumah, sekolah, gedung perkantoran, atau kampus.
- ✓ LAN biasanya dikelola oleh satu organisasi atau individu. Kontrol administratif yang mengatur kebijakan keamanan dan pengendalian akses diberlakukan di tingkat jaringan.
- ✓ LAN menyediakan bandwidth berkecepatan tinggi ke perangkat akhir internal dan perangkat perantara.



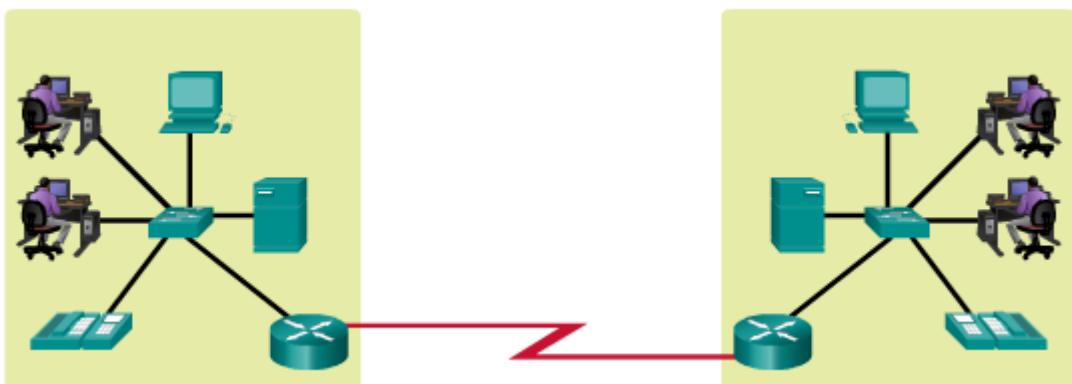
Jaringan LAN

- **WAN**

WAN adalah infrastruktur jaringan yang membentang luas di wilayah geografis. WAN biasanya dikelola oleh penyedia layanan (SP) atau Internet Service Providers (ISP).

Fitur khusus WAN meliputi:

- ✓ WAN menghubungkan LAN melalui wilayah geografis yang luas seperti antara kota, negara bagian, provinsi, negara, atau benua.
- ✓ WAN biasanya dikelola oleh beberapa penyedia layanan.
- ✓ WAN biasanya menyediakan hubungan kecepatan yang lebih lambat antar LAN.



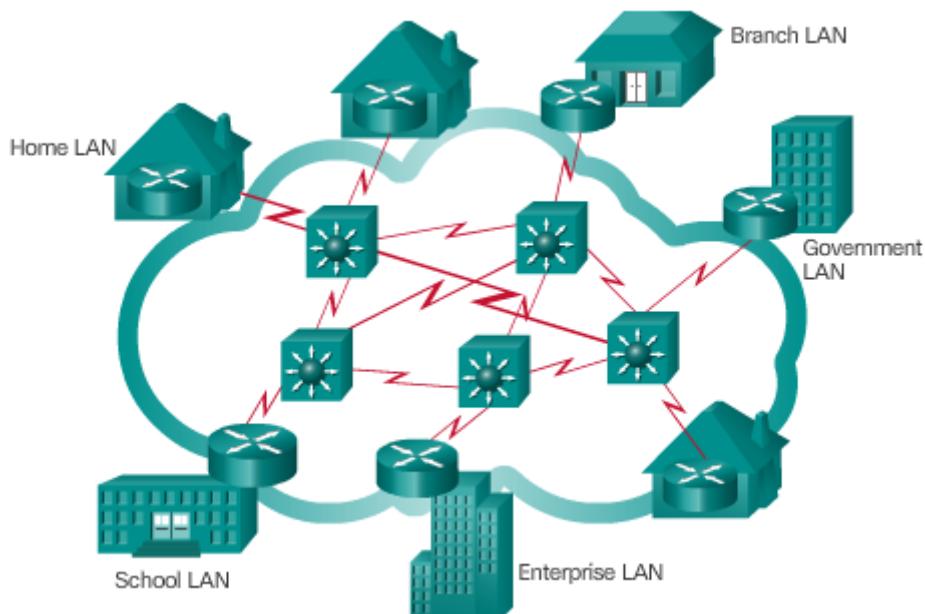
Jaringan WAN

❖ Internet, Intranets, dan Extranets

• INTERNET

Internet adalah kumpulan jaringan interkoneksi di seluruh dunia (internetwork atau internet singkatnya). Angka tersebut menunjukkan satu cara untuk melihat internet sebagai kumpulan LAN dan WAN yang saling berhubungan. Beberapa contoh LAN terhubung satu sama lain melalui koneksi WAN. WAN kemudian dihubungkan satu sama lain. Garis koneksi WAN merah mewakili semua variasi cara kita menghubungkan jaringan. WAN dapat terhubung melalui kabel tembaga, kabel serat optik, dan transmisi nirkabel (tidak diperlihatkan).

Internet tidak dimiliki oleh individu atau kelompok manapun. Untuk Memastikan komunikasi yang efektif di seluruh infrastruktur yang beragam ini memerlukan penerapan teknologi dan standar yang konsisten dan umum dan juga kerjasama dari banyak agen administrasi jaringan. Ada organisasi yang telah dikembangkan untuk membantu menjaga struktur dan standarisasi protokol dan proses Internet. Organisasi-organisasi ini termasuk Internet Engineering Task Force (IETF), Internet Corporation untuk Ditugaskan Nama dan Nomor (ICANN), dan Internet Architecture Board (IAB), ditambah banyak lainnya.



Kumpulan hubungan Internet dengan LAN dan WAN

• INTRANET & EXTRANET

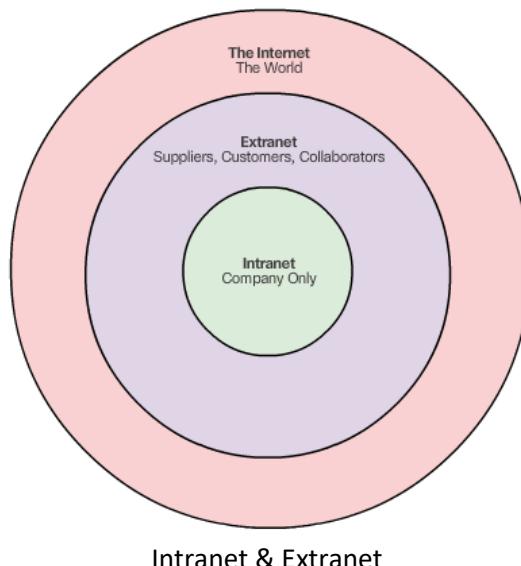
Ada dua istilah lain yang mirip dengan istilah internet:

- ✓ Intranet
- ✓ Ekstranet

Intranet adalah istilah yang sering digunakan untuk merujuk pada koneksi pribadi LAN dan WAN yang termasuk dalam sebuah organisasi, dan dirancang agar dapat diakses hanya oleh anggota organisasi, karyawan, atau pihak lain yang memiliki otorisasi.

Suatu organisasi dapat menggunakan ekstranet untuk memberikan akses yang aman dan aman kepada individu yang bekerja untuk organisasi yang berbeda, namun memerlukan akses ke data organisasi. Contoh Extranet meliputi:

- ✓ Perusahaan yang menyediakan akses ke pemasok dan kontraktor luar.
- ✓ Rumah sakit yang menyediakan sistem pemesanan ke dokter sehingga mereka bisa membuat janji temu untuk pasien mereka.
- ✓ Sebuah kantor pendidikan lokal yang menyediakan informasi anggaran dan personil ke sekolah-sekolah di kabupatenannya.



❖ Hubungan Internet

• TEKNOLOGI AKSES INTERNET

Ada banyak cara untuk menghubungkan pengguna dan organisasi ke Internet. Pengguna rumahan, teleworker (pekerja jarak jauh), dan kantor kecil biasanya memerlukan koneksi ke Internet Service Provider (ISP) untuk mengakses Internet. Pilihan koneksi sangat bervariasi antara ISP dan lokasi geografis. Namun, pilihan populer termasuk kabel broadband, broadband digital subscriber line (DSL), WAN nirkabel, dan layanan mobile.

Organisasi biasanya memerlukan akses ke situs perusahaan lain dan Internet. Koneksi cepat diperlukan untuk mendukung layanan bisnis termasuk telepon IP, konferensi video, dan penyimpanan data center.

Interkoneksi kelas bisnis biasanya disediakan oleh penyedia layanan (SP). Layanan kelas bisnis yang populer mencakup bisnis DSL, leased line, dan Metro Ethernet.

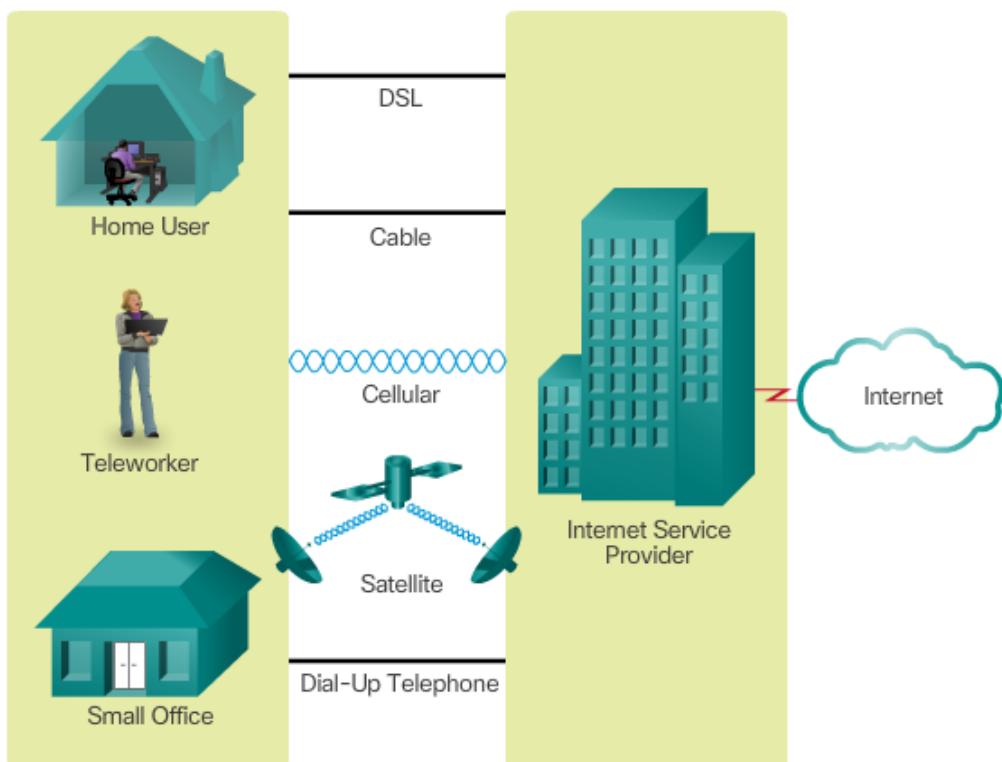
• KONEKSI INTERNET RUMAH DAN KANTOR SEDERHANA

Pilihan koneksi umum untuk pengguna kantor kecil dan kantor rumahan:

- ✓ **Kabel** - Biasanya ditawarkan oleh penyedia layanan televisi kabel, sinyal data internet dibawa pada kabel yang sama dengan kabel televisi kabel. Ini menyediakan bandwidth yang tinggi, selalu terhubung ke Internet.
- ✓ **DSL** - **Digital Subscriber Lines** menyediakan bandwidth yang tinggi, selalu terhubung ke Internet. DSL berjalan melalui saluran telepon. Secara umum, kantor kecil dan pengguna rumahan terhubung menggunakan Asymmetrical DSL (ADSL), yang berarti kecepatan download lebih cepat dari kecepatan upload.
- ✓ **Seluler** - Akses Internet seluler menggunakan jaringan seluler untuk menghubungkan. Dimanapun Anda bisa mendapatkan sinyal seluler, Anda bisa mendapatkan akses Internet seluler. Kinerja akan dibatasi oleh kemampuan ponsel dan menara sel yang terhubung.
- ✓ **Satelite** - Ketersediaan akses Internet satelit adalah keuntungan nyata di area yang seharusnya tidak memiliki konektivitas internet sama sekali. Piring satelit membutuhkan garis pandang yang jelas ke satelit.
- ✓ **Telepon Dial-up** - Pilihan murah yang menggunakan saluran telepon dan modem. Bandwidth rendah yang disediakan oleh koneksi modem dial-up biasanya tidak cukup untuk transfer data yang besar, walaupun berguna untuk akses mobile saat bepergian.

Banyak rumah dan kantor kecil lebih sering terhubung langsung dengan kabel serat optik. Ini memungkinkan ISP menyediakan kecepatan bandwidth yang lebih tinggi dan mendukung lebih banyak layanan seperti Internet, telepon, dan TV.

Pilihan koneksi bervariasi tergantung lokasi geografis dan ketersediaan penyedia layanan.



Pilihan koneksi jaringan

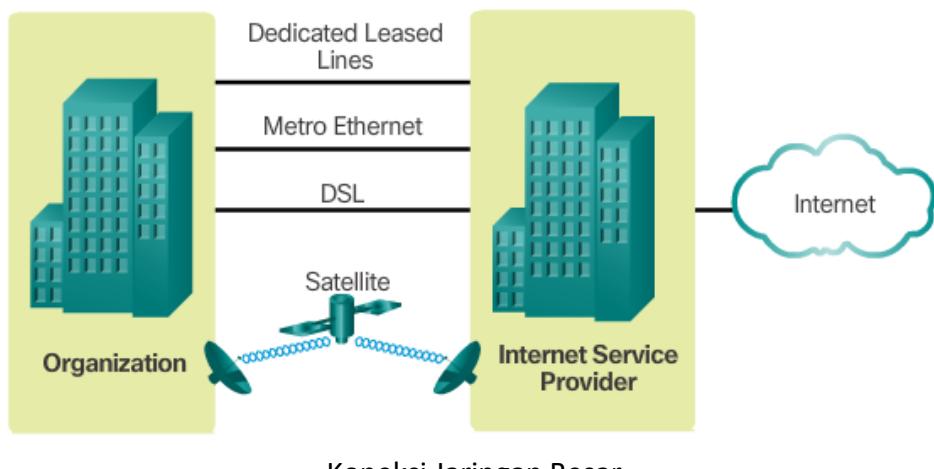
- **BISNIS KONEKSI INTERNET**

Pilihan koneksi perusahaan berbeda dari pilihan pengguna rumahan. Bisnis mungkin memerlukan bandwidth yang lebih tinggi, dedicated bandwidth, dan managed services. Pilihan koneksi yang tersedia berbeda tergantung pada jenis penyedia layanan yang berada di dekatnya.

Beberapa pilihan koneksi umum untuk bisnis:

- ✓ **Dedicated Leased Line** - Leased line sebenarnya merupakan sirkuit yang tersimpan dalam jaringan penyedia layanan yang menghubungkan kantor-kantor yang terpisah secara geografis untuk jaringan suara dan / atau data pribadi. Sirkuit biasanya disewa dengan tarif bulanan atau tahunan. Mereka bisa mahal.
- ✓ **WAN Ethernet** - Ethernet WANs memperluas teknologi akses LAN ke WAN. Ethernet adalah teknologi LAN yang akan Anda pelajari di bab selanjutnya. Manfaat Ethernet sekarang diperluas ke WAN.
- ✓ **DSL** - Bisnis DSL tersedia dalam berbagai format. Pilihan populer adalah Symmetric Digital Subscriber Lines (SDSL) yang mirip dengan versi konsumen DSL, namun menyediakan upload dan download pada kecepatan yang sama.
- ✓ **Satelite** - Serupa dengan pengguna kantor kecil dan kantor rumahan, layanan satelit dapat menyediakan koneksi saat solusi kabel tidak tersedia.

Pilihan koneksi bervariasi tergantung lokasi geografis dan ketersediaan penyedia layanan.

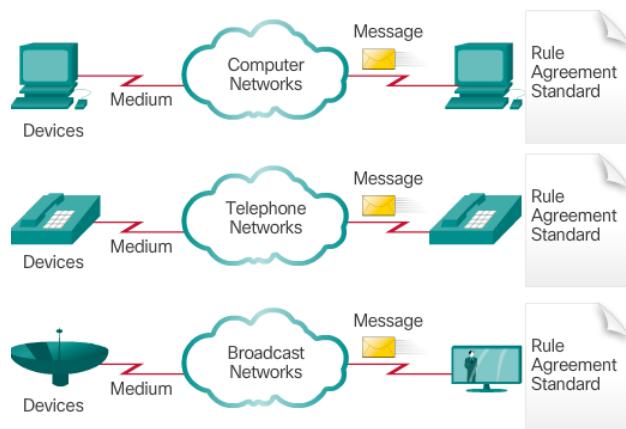


1.3 JARINGAN SEBAGAI PLATFORM

❖ KONVERGENSI JARINGAN

• Jaringan Terpisah Tradisional

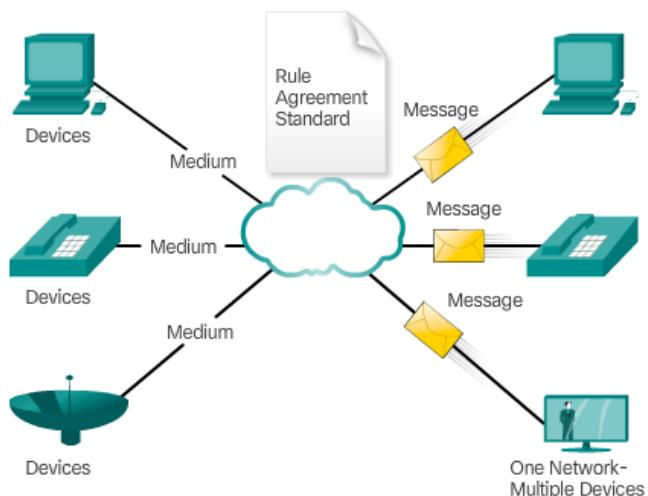
Contoh sebuah sekolah yang dibangun tiga puluh tahun yang lalu. Saat itu, beberapa ruang kelas dipasang untuk jaringan data, jaringan telepon, dan jaringan video untuk televisi. Jaringan terpisah ini tidak bisa saling berkomunikasi, seperti yang ditunjukkan pada gambar. Setiap jaringan menggunakan teknologi yang berbeda untuk membawa sinyal komunikasi. Setiap jaringan memiliki seperangkat peraturan dan standar untuk memastikan komunikasi yang berhasil.



Beberapa Jaringan

❖ Jaringan Konvergen

Saat ini, jaringan data, telepon, dan video terpisah saling terhubung. Tidak seperti jaringan khusus, jaringan konvergensi mampu menghadirkan data, suara, dan video di antara berbagai jenis perangkat melalui infrastruktur jaringan yang sama, seperti yang ditunjukkan pada gambar. Infrastruktur jaringan ini menggunakan seperangkat aturan, kesepakatan, dan standar implementasi yang sama.



Jaringan konvergen

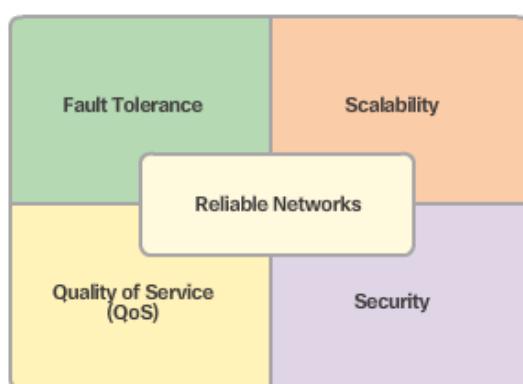
❖ JARINGAN YANG HANDAL

• Arsitektur Jaringan

Jaringan harus mendukung berbagai aplikasi dan layanan, serta mengoperasikan lebih dari berbagai jenis kabel dan perangkat, yang merupakan infrastruktur fisik. Istilah arsitektur jaringan, dalam konteks ini, mengacu pada teknologi yang mendukung infrastruktur dan layanan dan peraturan terprogram, atau protokol, yang memindahkan data ke seluruh jaringan.

Seiring berkembangnya jaringan, kita menemukan bahwa ada empat karakteristik dasar yang harus ditangani oleh arsitektur mendasar agar dapat memenuhi harapan pengguna:

- ✓ Toleransi kesalahan
- ✓ Skalabilitas
- ✓ Kualitas Layanan (QoS)
- ✓ Keamanan



Dukungan arsitektur jaringan

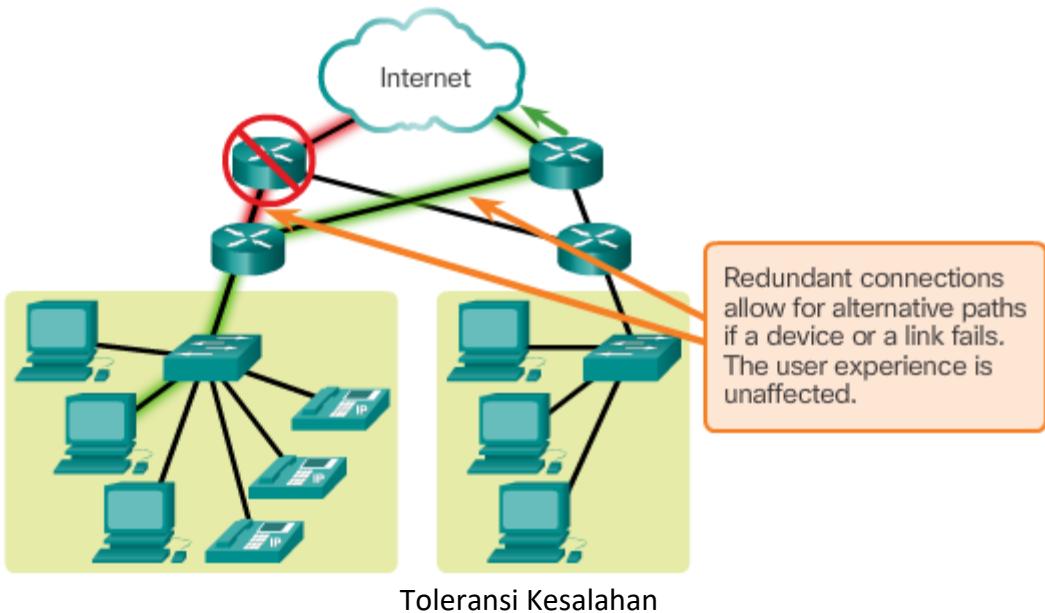
• Toleransi Kesalahan

Harapannya adalah bahwa internet selalu tersedia bagi jutaan pengguna yang mengandalkannya. Hal ini membutuhkan arsitektur jaringan yang dibangun agar menjadi fault tolerant. Jaringan toleransi kesalahan adalah salah satu yang membatasi dampak kegagalan, sehingga jumlah perangkat yang paling sedikit terpengaruh. Hal ini juga dibangun dengan cara yang memungkinkan pemulihan cepat saat terjadi kegagalan seperti itu. Jaringan ini bergantung pada beberapa jalur antara sumber dan tujuan pesan. Jika satu jalan gagal, pesan bisa langsung dikirim melalui tautan yang berbeda. Memiliki banyak jalur ke tujuan dikenal sebagai redundansi.

Salah satu cara jaringan yang handal memberikan redundansi adalah dengan menerapkan packet-switched network. Packet switching membagi lalu lintas menjadi paket yang diarahkan melalui jaringan bersama. Satu pesan, seperti email atau aliran video, dipecah menjadi beberapa blok pesan, disebut paket. Setiap paket memiliki informasi pengalaman yang diperlukan dari sumber dan tujuan pesan. Router dalam jaringan akan mengganti paket berdasarkan kondisi jaringan pada saat itu. Ini berarti bahwa semua paket dalam satu pesan bisa menempuh jalur yang sangat berbeda ke tujuan. Pada gambar, pengguna tidak sadar dan tidak terpengaruh oleh router yang secara dinamis mengubah rute saat link gagal.

Ini tidak terjadi pada jaringan circuit-switched yang biasa digunakan untuk komunikasi suara. Jaringan circuit-switched adalah sirkuit yang membentuk sirkuit khusus antara sumber dan

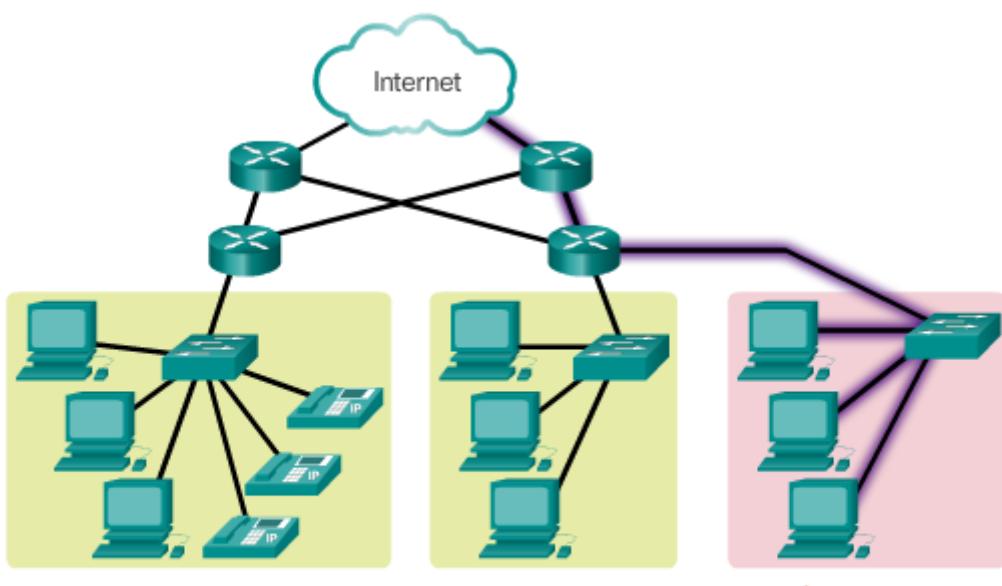
tujuan sebelum pengguna dapat berkomunikasi. Jika panggilan tiba-tiba dihentikan, pengguna harus melakukan koneksi baru.



Toleransi Kesalahan

- **Skalabilitas**

Jaringan terukur dapat berkembang dengan cepat untuk mendukung pengguna dan aplikasi baru tanpa mempengaruhi kinerja layanan yang dikirimkan ke pengguna lama. Angka tersebut menunjukkan bagaimana jaringan baru dapat dengan mudah ditambahkan ke jaringan yang ada. Selain itu, jaringan bersifat skalabel karena para desainer mengikuti standar dan protokol yang diterima. Hal ini memungkinkan vendor perangkat lunak dan perangkat keras untuk fokus pada peningkatan produk dan layanan tanpa khawatir merancang seperangkat aturan baru untuk beroperasi dalam jaringan.



Additional users and whole networks can be connected to the Internet without degrading performance for existing users.

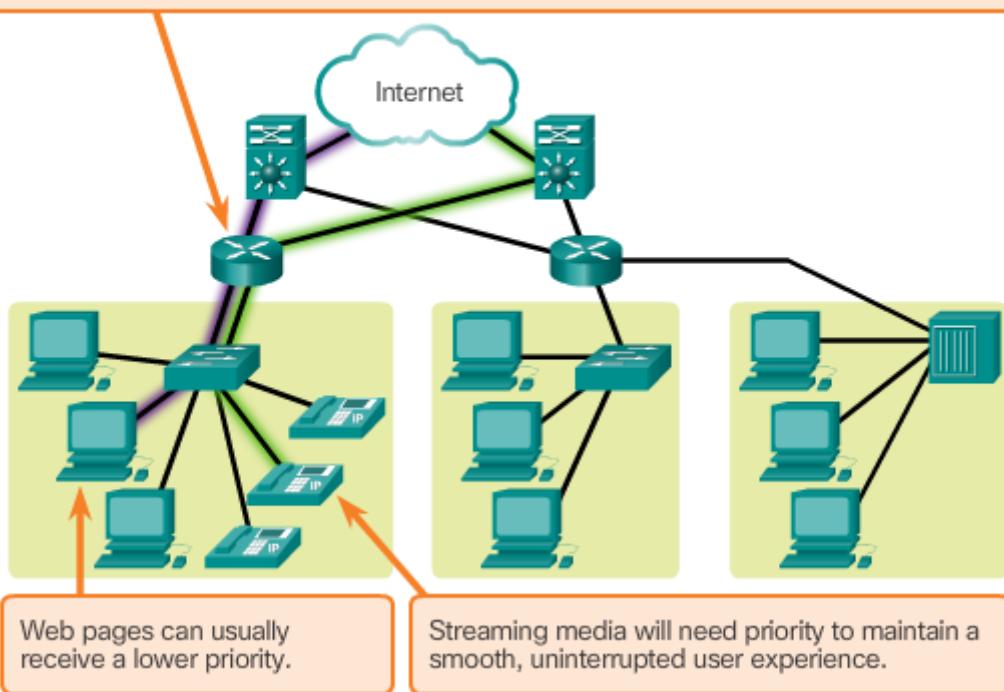
- **Kualitas Layanan**

Quality of Service (QoS) juga merupakan kebutuhan jaringan yang semakin meningkat saat ini. Aplikasi baru tersedia bagi pengguna melalui jaringan internal, seperti transmisi suara dan video langsung, menciptakan harapan yang lebih tinggi untuk kualitas layanan yang diberikan. Pernahkah Anda mencoba menonton video dengan jeda dan jeda yang konstan? Seiring data, suara, dan konten video terus berkumpul ke jaringan yang sama, QoS menjadi mekanisme utama untuk mengelola kemacetan dan memastikan pengiriman konten yang dapat diandalkan ke semua pengguna.

Kemacetan terjadi ketika permintaan bandwidth melebihi jumlah yang tersedia. Bandwidth jaringan diukur dalam jumlah bit yang dapat ditransmisikan dalam satu detik, atau bit per detik (bps). Ketika komunikasi simultan dicoba di seluruh jaringan, permintaan akan bandwidth jaringan dapat melebihi ketersediannya, menciptakan kemacetan jaringan.

Bila volume lalu lintas lebih besar daripada yang dapat diangkut melintasi jaringan, perangkat antrian, atau tahan, paket dalam memori sampai sumber daya tersedia untuk mengirimkannya. Pada gambar, satu pengguna meminta halaman web dan yang lainnya sedang melakukan panggilan telepon. Dengan adanya kebijakan QoS, router dapat mengatur arus lalu lintas data dan suara, memprioritaskan komunikasi suara jika jaringan mengalami kemacetan.

Quality of Service, managed by the router, ensures that priorities are matched with the type of communication and its importance to the organization.

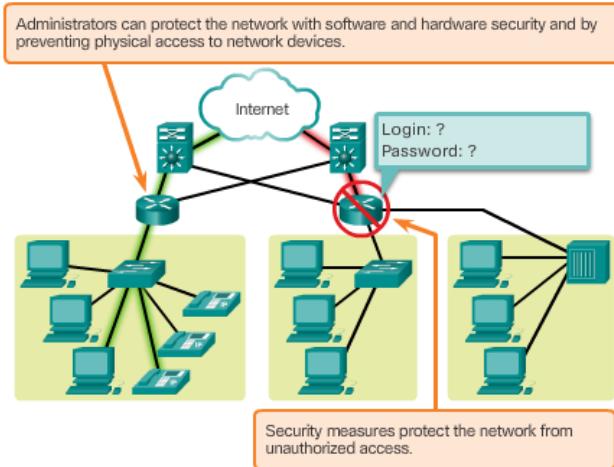


Kualitas Layanan

- **Keamanan**

Infrastruktur jaringan, layanan, dan data yang terdapat pada perangkat yang terpasang pada jaringan sangat penting aset pribadi dan bisnis. Ada dua jenis masalah keamanan jaringan yang harus diperhatikan: keamanan infrastruktur jaringan dan keamanan informasi.

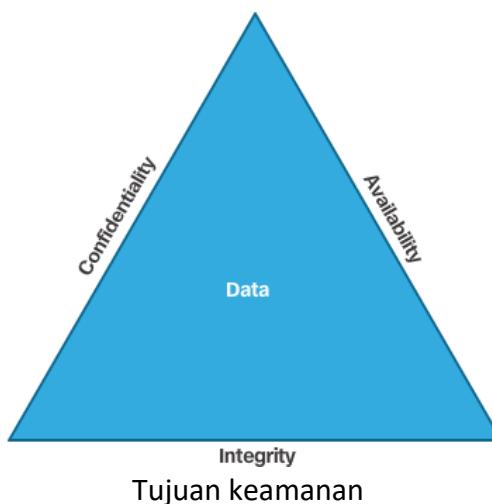
Mengamankan infrastruktur jaringan mencakup pengamanan fisik perangkat yang menyediakan koneksi jaringan, dan mencegah akses yang tidak sah ke perangkat lunak manajemen yang berada pada mereka.



Keamanan infrastruktur

Keamanan informasi mengacu pada melindungi informasi yang terdapat dalam paket yang dikirim melalui jaringan dan informasi yang tersimpan pada perangkat jaringan terpasang. Untuk mencapai tujuan keamanan jaringan, ada tiga persyaratan utama;

- ✓ **Kerahasiaan** - kerahasiaan data berarti hanya penerima yang berhak dan berwenang yang dapat mengakses dan membaca data.
- ✓ **Integritas** - Integritas data berarti memiliki kepastian bahwa informasi tersebut belum diubah dalam transmisi, dari asal ke tujuan.
- ✓ **Ketersediaan** - Ketersediaan data berarti memiliki kepastian akses yang tepat waktu dan dapat diandalkan terhadap layanan data untuk pengguna yang berwenang.



1.4 MERUBAH LINGKUNGAN JARINGAN

❖ TREND JARINGAN

- Tren Baru**

Seiring teknologi baru dan perangkat pengguna akhir masuk ke pasar, bisnis dan konsumen harus terus menyesuaikan diri dengan lingkungan yang senantiasa berubah ini. Peran jaringan berubah untuk memungkinkan koneksi antara orang, perangkat, dan informasi. Ada beberapa tren jaringan baru yang akan mempengaruhi organisasi dan konsumen. Beberapa tren teratas meliputi:

- ✓ Bawa Perangkat Anda Sendiri (BYOD)
- ✓ Kolaborasi online
- ✓ Komunikasi video
- ✓ Komputasi awan (cloud)

- Bawa Perangkat sendiri**

Konsep perangkat apa pun, untuk konten apa pun, dengan cara apa pun, adalah tren global utama yang memerlukan perubahan signifikan terhadap cara perangkat digunakan. Tren ini dikenal dengan nama Bring Your Own Device (BYOD).

BYOD adalah tentang pengguna akhir yang memiliki kebebasan untuk menggunakan alat pribadi untuk mengakses informasi dan berkomunikasi di seluruh jaringan bisnis atau kampus. Dengan pertumbuhan perangkat konsumen, dan penurunan biaya, karyawan dan siswa terkait dapat diharapkan memiliki beberapa alat komputasi dan jaringan paling canggih untuk penggunaan pribadi. Alat pribadi ini meliputi laptop, netbook, tablet, smartphone, dan e-reader. Ini bisa berupa perangkat yang dibeli oleh perusahaan atau sekolah, dibeli oleh individu, atau keduanya.

BYOD berarti perangkat apa pun, dengan kepemilikan apa pun, digunakan di mana saja. Misalnya, di masa lalu, seorang siswa yang perlu mengakses jaringan kampus atau internet harus menggunakan salah satu komputer sekolah. Perangkat ini biasanya terbatas dan dilihat sebagai alat hanya untuk pekerjaan yang dilakukan di kelas atau di perpustakaan. Konektivitas yang diperluas melalui akses mobile dan remote ke jaringan kampus memberi siswa fleksibilitas yang luar biasa dan lebih banyak kesempatan belajar bagi siswa.

- Kolaborasi Online**

Individu ingin terhubung ke jaringan, tidak hanya untuk akses ke aplikasi data, tapi juga untuk berkolaborasi satu sama lain. Kolaborasi didefinisikan sebagai "tindakan bekerja dengan orang lain atau orang lain dalam sebuah proyek bersama." Alat kolaborasi, seperti Cisco WebEx yang ditunjukkan pada gambar tersebut, memberi karyawan, siswa, guru, pelanggan, dan mitra cara untuk segera terhubung, berinteraksi, dan mencapai tujuan mereka.

Untuk bisnis, kolaborasi adalah prioritas penting dan strategis yang digunakan oleh organisasi untuk tetap kompetitif. Kolaborasi juga menjadi prioritas dalam pendidikan. Siswa perlu berkolaborasi untuk saling membantu dalam belajar, untuk mengembangkan keterampilan tim yang digunakan dalam angkatan kerja, dan untuk bekerja sama dalam proyek berbasis tim.

- **Komunikasi Video**

Kecenderungan lain dalam jaringan yang sangat penting bagi upaya komunikasi dan kolaborasi adalah video. Video digunakan untuk komunikasi, kolaborasi, dan hiburan. Panggilan video dapat dilakukan ke dan dari manapun dengan koneksi Internet.

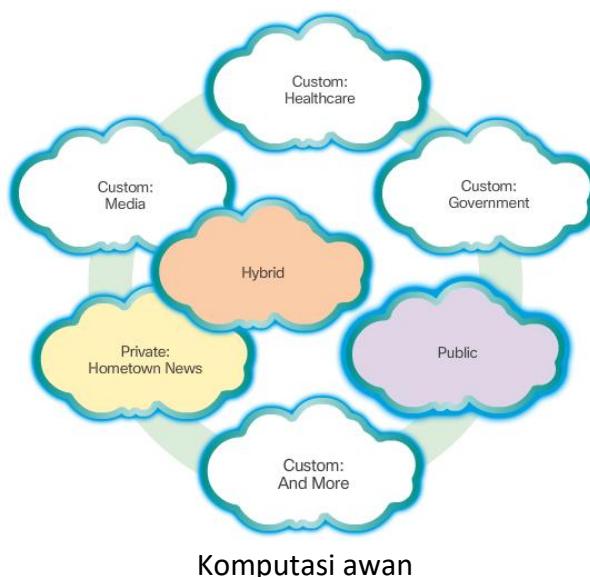
Video conferencing adalah alat yang ampuh untuk berkomunikasi dengan orang lain dari kejauhan, baik lokal maupun global. Video menjadi persyaratan penting untuk kolaborasi yang efektif seiring perluasan organisasi lintas batas geografis dan budaya. Klik Putar di gambar untuk melihat bagaimana TelePresence dapat digabungkan ke dalam kehidupan sehari-hari dan bisnis.

- **Komputasi Awan**

Komputasi awan adalah tren global lainnya yang mengubah cara kita mengakses dan menyimpan data. Komputasi awan memungkinkan kita menyimpan file pribadi, bahkan membackup seluruh hard disk drive kita di server melalui Internet. Aplikasi seperti pengolah kata dan pengeditan foto bisa diakses menggunakan Cloud.

Untuk bisnis, komputasi Cloud memperluas kemampuan TI tanpa memerlukan investasi di infrastruktur baru, melatih personil baru, atau memberi lisensi perangkat lunak baru. Layanan ini tersedia sesuai permintaan dan dikirimkan secara ekonomis ke perangkat mana pun di dunia tanpa mengorbankan keamanan atau fungsinya.

Ada empat tipe utama Awan, seperti yang ditunjukkan pada gambar: Awan Publik, Awan Pribadi, Awan Hibrid, dan Awan Kustom. Klik setiap Awan untuk mempelajari lebih lanjut. Komputasi awan dimungkinkan karena adanya pusat data. Pusat data adalah fasilitas yang digunakan untuk sistem komputer rumah dan komponen terkait. Sebuah pusat data dapat menempati satu ruangan sebuah bangunan, satu atau lebih lantai, atau keseluruhan bangunan. Pusat data biasanya sangat mahal untuk dibangun dan dipelihara. Untuk alasan ini, hanya organisasi besar yang menggunakan pusat data pribadi untuk menampung data mereka dan memberikan layanan kepada pengguna. Organisasi yang lebih kecil yang tidak mampu mempertahankan pusat data pribadi mereka sendiri dapat mengurangi keseluruhan biaya kepemilikan dengan menyewakan layanan server dan penyimpanan dari organisasi pusat data yang lebih besar di Awan.



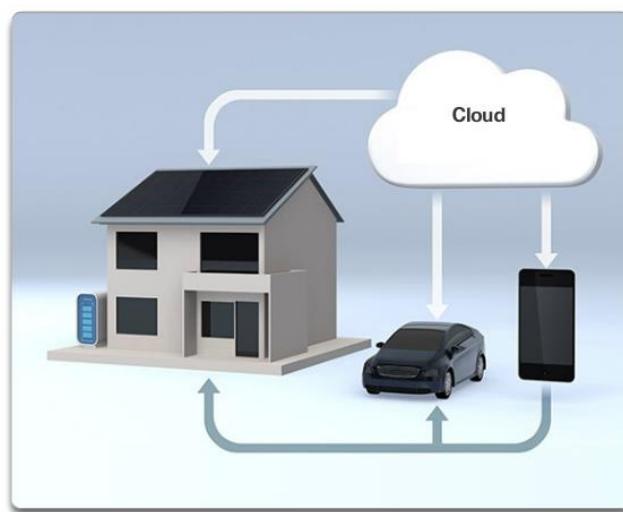
❖ TEKNOLOGI JARINGAN UNTUK RUMAH

• Tren Teknologi untuk Rumah

Tren jaringan tidak hanya mempengaruhi cara kita berkomunikasi di tempat kerja dan di sekolah, juga mengubah hampir setiap aspek rumah.

Tren rumah terbaru termasuk 'teknologi rumah pintar'. Teknologi rumah pintar adalah teknologi yang terintegrasi ke dalam peralatan sehari-hari yang memungkinkan mereka untuk saling berhubungan dengan perangkat lain, membuat mereka lebih 'cerdas' atau otomatis. Misalnya, bayangkan bisa menyiapkan piring dan meletakkannya di oven untuk memasak sebelum meninggalkan rumah pada hari itu. Bayangkan jika oven 'sadar' dari masakan yang dimasaknya dan terhubung dengan 'kalender acara Anda' sehingga bisa menentukan jam berapa Anda harus siap makan, dan menyesuaikan waktu mulai dan lama memasak sesuai kebutuhan. Bahkan bisa menyesuaikan waktu memasak dan suhu berdasarkan perubahan jadwal. Selain itu, koneksi smartphone atau tablet memungkinkan pengguna kemampuan untuk terhubung ke oven secara langsung, untuk melakukan penyesuaian yang diinginkan. Bila sajinya "tersedia", oven mengirimkan pesan peringatan ke perangkat pengguna akhir yang ditentukan bahwa piring itu telah selesai dan pemanasan.

Skenario ini tidak lama lagi. Padahal, teknologi rumah pintar saat ini sedang dikembangkan untuk semua ruangan di dalam sebuah rumah. Teknologi rumah pintar akan menjadi lebih nyata karena jaringan rumahan dan teknologi internet berkecepatan tinggi menjadi semakin meluas. Teknologi jaringan rumah baru dikembangkan setiap hari untuk memenuhi kebutuhan teknologi yang berkembang ini.

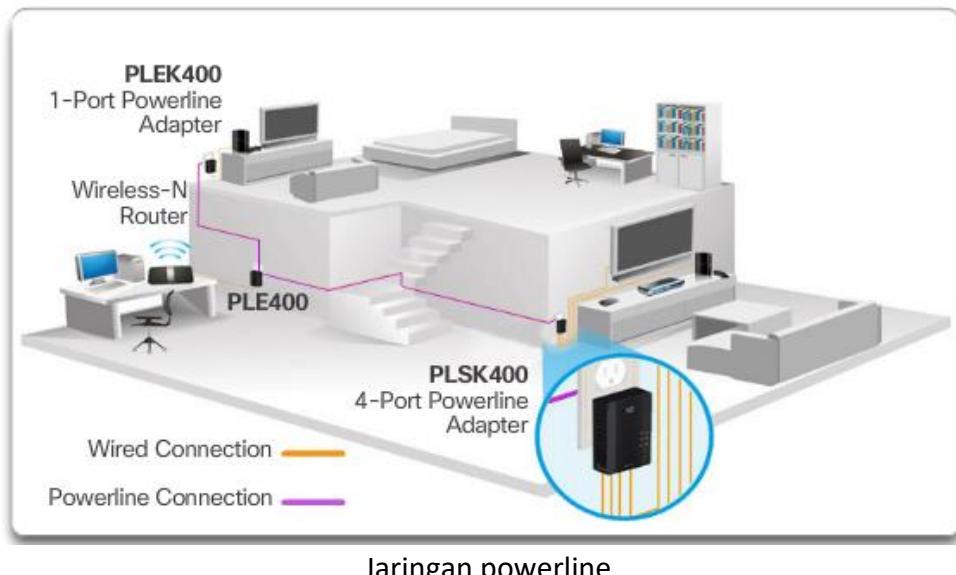


Teknologi Rumah Pintar

• Jaringan Powerline

Jaringan Powerline adalah tren yang muncul untuk jaringan rumah yang menggunakan kabel listrik yang ada untuk menghubungkan perangkat, berarti kemampuan untuk menghubungkan perangkat ke jaringan dimanapun ada stopkontak listrik. Ini menghemat biaya pemasangan kabel data dan tanpa biaya tambahan pada tagihan listrik. Dengan menggunakan kabel yang sama yang menghasilkan listrik, jaringan listrik mengirimkan informasi dengan mengirimkan data pada frekuensi tertentu.

Dengan menggunakan adaptor powerline standar, perangkat dapat terhubung ke LAN dimanapun ada stopkontak listrik. Jaringan powerline sangat berguna saat titik akses nirkabel tidak dapat digunakan atau tidak bisa menjangkau semua perangkat di rumah. Jaringan powerline tidak dirancang untuk menjadi pengganti pemasangan kabel khusus di jaringan data. Namun, ini adalah alternatif bila kabel data jaringan atau komunikasi nirkabel bukanlah pilihan yang tepat.



• Wireless Broadband

Menghubungkan ke Internet sangat penting dalam teknologi rumah pintar. DSL dan kabel adalah teknologi umum yang digunakan untuk menghubungkan rumah dan usaha kecil ke Internet. Namun, wireless mungkin pilihan lain di banyak daerah. Penyedia Layanan Internet Nirkabel (WISP) Penyedia Layanan Internet Nirkabel (WISP) adalah ISP yang menghubungkan pelanggan ke jalur akses atau hot spot yang ditunjuk menggunakan teknologi nirkabel serupa yang ditemukan di jaringan area lokal nirkabel (WLAN). WISP lebih umum ditemukan di lingkungan pedesaan dimana layanan DSL atau kabel tidak tersedia.

Meskipun menara transmisi terpisah dapat dipasang untuk antena, biasanya antena dilekatkan pada struktur tinggi yang ada, seperti menara air atau menara radio. Piring atau antena kecil dipasang di atap pelanggan di kisaran pemancar WISP. Unit akses pelanggan terhubung ke jaringan kabel di dalam rumah. Dari sudut pandang pengguna rumahan, pengaturannya tidak jauh berbeda dengan DSL atau layanan kabel. Perbedaan utamanya adalah koneksi dari rumah ke ISP bersifat nirkabel dan bukan kabel fisik. Layanan Broadband Nirkabel

Solusi nirkabel lainnya untuk rumah dan usaha kecil adalah broadband nirkabel, seperti yang ditunjukkan pada gambar. Ini menggunakan teknologi seluler yang sama yang digunakan untuk mengakses Internet dengan ponsel cerdas atau tablet. Antena dipasang di luar rumah yang menyediakan konektivitas nirkabel atau kabel untuk perangkat di rumah. Di banyak daerah, broadband nirkabel rumahan bersaing langsung dengan layanan DSL dan kabel.



Wireless Broadband Service

❖ KEAMANAN JARINGAN

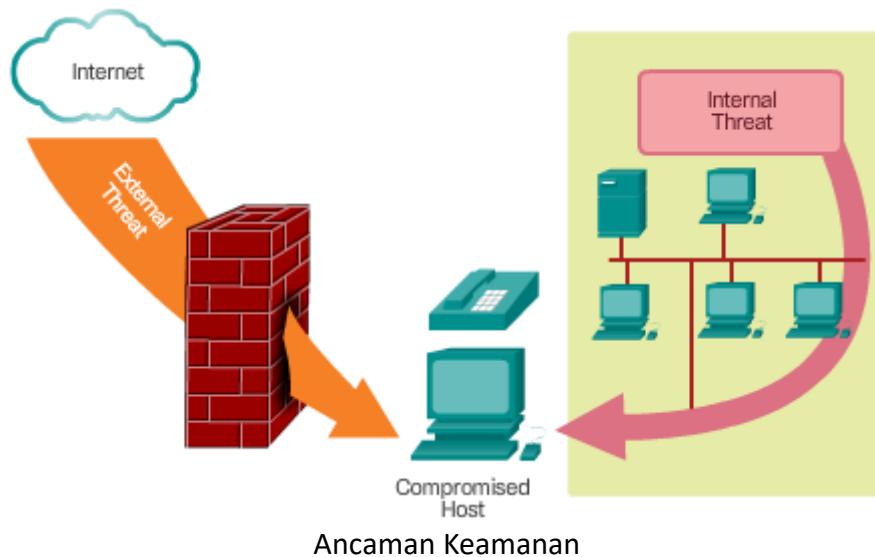
• Ancaman Keamanan

Keamanan jaringan merupakan bagian integral dari jaringan komputer, terlepas dari apakah jaringan tersebut terbatas pada lingkungan rumah dengan satu koneksi ke Internet atau sebesar korporasi dengan ribuan pengguna. Keamanan jaringan yang diimplementasikan harus memperhitungkan lingkungan, serta alat dan persyaratan jaringan. Ini harus bisa mengamankan data sambil tetap memungkinkan untuk kualitas layanan yang diharapkan dari jaringan. Mengamankan jaringan melibatkan protokol, teknologi, perangkat, peralatan, dan teknik untuk mengamankan data dan mengurangi ancaman. Ancaman vektor mungkin eksternal atau internal. Banyak ancaman keamanan jaringan eksternal saat ini tersebar di Internet.

Ancaman eksternal yang paling umum terhadap jaringan meliputi:

- ✓ Virus, worm, dan trojan horse - perangkat lunak berbahaya dan kode sewenang-wenang yang berjalan pada perangkat pengguna.
- ✓ Spyware dan adware - perangkat lunak yang diinstal pada perangkat pengguna yang secara diam-diam mengumpulkan informasi tentang pengguna.
- ✓ Serangan zero-day, juga disebut serangan zero-hour - sebuah serangan yang terjadi pada hari pertama bahwa kerentanan diketahui.
- ✓ Serangan hacker - serangan oleh orang yang berpengetahuan ke perangkat pengguna atau sumber daya jaringan.
- ✓ Serangan denial of service - serangan yang dirancang untuk memperlambat atau merusak aplikasi dan proses pada perangkat jaringan.
- ✓ Pengambilan data dan pencurian data - sebuah serangan untuk menangkap informasi pribadi dari jaringan organisasi
- ✓ Pencurian identitas - serangan untuk mencuri kredensial masuk pengguna untuk mengakses data pribadi

Hal yang sama pentingnya untuk mempertimbangkan ancaman internal. Ada banyak penelitian yang menunjukkan bahwa pelanggaran data yang paling umum terjadi karena pengguna internal jaringan. Hal ini dapat dikaitkan dengan perangkat yang hilang atau dicuri, penyalahgunaan yang tidak disengaja oleh karyawan, dan lingkungan bisnis, bahkan karyawan berbahaya sekalipun. Dengan strategi BYOD yang berkembang, data perusahaan jauh lebih rentan. Oleh karena itu, saat mengembangkan kebijakan keamanan, penting untuk mengatasi ancaman keamanan eksternal maupun internal.



• Solusi Keamanan

Tidak ada solusi tunggal yang bisa melindungi jaringan dari beragam ancaman yang ada. Untuk alasan ini, keamanan harus diterapkan di beberapa lapisan, menggunakan lebih dari satu solusi keamanan. Jika satu komponen keamanan gagal mengidentifikasi dan melindungi jaringan, yang lain masih berdiri.

Implementasi keamanan jaringan rumah biasanya agak mendasar. Hal ini umumnya diimplementasikan pada perangkat penghubung akhir, serta pada titik koneksi ke Internet, dan bahkan dapat mengandalkan layanan kontrak dari ISP.

Sebaliknya, implementasi keamanan jaringan untuk jaringan perusahaan biasanya terdiri dari banyak komponen yang dibangun ke dalam jaringan untuk memantau dan menyaring lalu lintas. Idealnya, semua komponen bekerja sama, yang meminimalkan perawatan dan meningkatkan keamanan.

Komponen keamanan jaringan untuk jaringan rumah atau kantor kecil harus mencakup, minimal:

- ✓ **Antivirus dan antispyware** - Ini digunakan untuk melindungi perangkat akhir agar tidak terinfeksi perangkat lunak berbahaya.
- ✓ **Penyaringan firewall** - Ini digunakan untuk memblokir akses tidak sah ke jaringan. Ini mungkin termasuk sistem firewall berbasis host yang diterapkan untuk mencegah akses yang tidak sah ke perangkat akhir, atau layanan penyaringan dasar di router rumah untuk mencegah akses yang tidak sah dari dunia luar ke jaringan.

Selain hal di atas, jaringan dan jaringan perusahaan yang lebih besar seringkali memiliki persyaratan keamanan lainnya:

- ✓ **Sistem firewall khusus** - Ini digunakan untuk memberikan kemampuan firewall yang lebih canggih yang dapat memfilter sejumlah besar lalu lintas dengan rincian lebih banyak.
- ✓ **Daftar kontrol akses (ACL)** - Ini digunakan untuk lebih memfilter akses dan penerusan lalu lintas.
- ✓ **Sistem pencegahan intrusi (IPS)** - Ini digunakan untuk mengidentifikasi ancaman penyebaran cepat, seperti serangan zero-day atau zero-hour.
- ✓ **Jaringan pribadi virtual (VPN)** - Ini digunakan untuk memberikan akses yang aman kepada pekerja jarak jauh.

Persyaratan keamanan jaringan harus memperhitungkan lingkungan jaringan, serta berbagai aplikasi, dan kebutuhan komputasi. Baik lingkungan rumah maupun bisnis harus bisa mengamankan datanya meski tetap memungkinkan untuk kualitas layanan yang diharapkan dari masing-masing teknologi. Selain itu, solusi keamanan yang diterapkan harus disesuaikan dengan tren dan perubahan jaringan yang terus meningkat.

Studi tentang ancaman keamanan jaringan dan teknik mitigasi dimulai dengan pemahaman yang jelas mengenai infrastruktur peralihan dan perutean yang mendasarinya yang digunakan untuk mengatur layanan jaringan.

LATIHAN SOAL 1

- 1) Jelaskan yang dimaksud dengan internet
- 2) berikan contoh perkembangan teknologi internet
- 3) Sebutkan manfaat internet dalam kehidupan sehari-hari
- 4) sebutkan dan jelaskan komponen-komponen jaringan
- 5) sebutkan dan jelaskan bentuk-bentuk komunikasi
- 6) jelaskan yang dimaksud dengan peer to peer
- 7) sebutkan perangkat intermediary device
- 8) sebutkan jenis media jaringan
- 9) jelaskan perbedaan antara LAN, WAN, MAN, WLAN, SAN
- 10) buatlah topologi jaringan disebuah rumah dan kampus

BAB 2 Konfigurasi sistem operasi jaringan

2.1 PENGANTAR

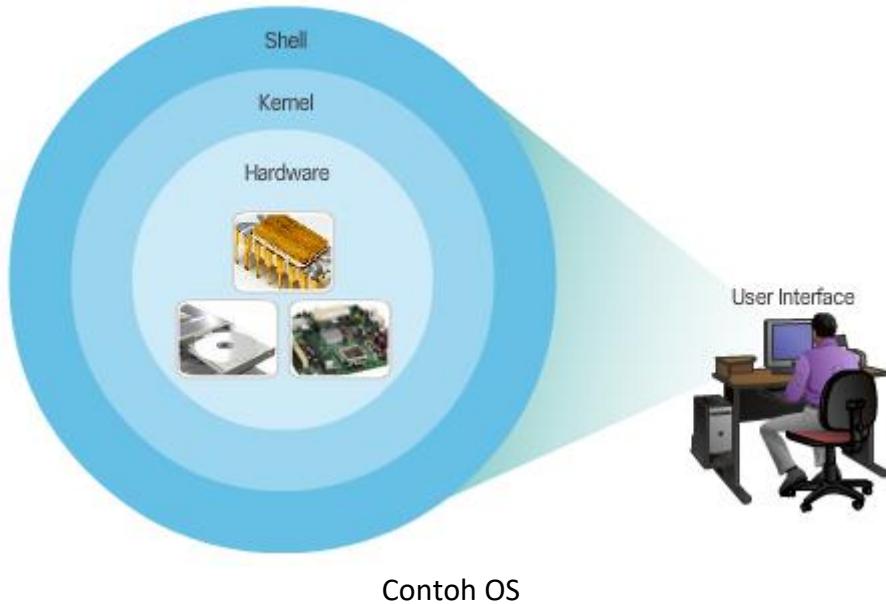
Setiap komputer memerlukan sebuah sistem operasi untuk berfungsi, termasuk perangkat jaringan berbasis komputer seperti switch, router, access point, dan firewall. Perangkat jaringan ini menggunakan sistem operasi yang disebut sistem operasi jaringan.

Sistem operasi jaringan memungkinkan perangkat keras perangkat berfungsi dan menyediakan antarmuka bagi pengguna untuk berinteraksi.

❖ CISCO IOS

• OPERATING SISTEM

Semua perangkat akhir dan perangkat jaringan memerlukan sistem operasi (OS). Seperti ditunjukkan pada Gambar , bagian dari OS yang berinteraksi langsung dengan perangkat keras komputer dikenal dengan nama kernel. Bagian yang berinteraksi dengan aplikasi dan pengguna dikenal sebagai shell. Pengguna dapat berinteraksi dengan shell menggunakan command-line interface (CLI) atau antarmuka pengguna grafis (GUI).



Contoh OS

Saat menggunakan CLI seperti yang ditunjukkan pada Gambar, pengguna berinteraksi langsung dengan sistem di lingkungan berbasis teks dengan memasukkan perintah pada keyboard pada prompt perintah. Sistem mengeksekusi perintah, sering memberikan output tekstual. CLI membutuhkan overhead yang sangat sedikit untuk beroperasi. Namun, hal itu mengharuskan pengguna memiliki pengetahuan tentang struktur dasar yang mengendalikan sistem.

```
[root@danscentos-s5 ~]# ls
bin dev home lib64 media opt root selinux sus usr
boot etc lib lost+found mnt proc sbin srv tmp var
[root@danscentos-s5 ~]# _
```

Comand line interface

Antarmuka GUI seperti Windows, OS X, Apple iOS, atau Android memungkinkan pengguna untuk berinteraksi dengan sistem menggunakan ikon grafis, menu, dan jendela grafis. Untuk alasan ini, banyak orang mengandalkan lingkungan GUI.

Namun, GUI mungkin tidak selalu dapat menyediakan semua fitur yang tersedia di CLI. GUI juga bisa gagal, macet, atau tidak beroperasi seperti yang ditentukan. Untuk alasan ini, perangkat jaringan biasanya diakses melalui CLI. CLI kurang resource intensive dan sangat stabil jika dibandingkan dengan GUI.

Sistem operasi jaringan yang digunakan pada perangkat Cisco disebut Cisco Internetwork Operating System (IOS). Cisco IOS digunakan untuk sebagian besar perangkat Cisco terlepas dari jenis atau ukuran perangkat.

Catatan: Sistem operasi pada router rumah biasanya disebut firmware. Metode yang paling umum untuk mengkonfigurasi router rumah adalah dengan menggunakan GUI berbasis browser web.

- **TUJUAN OPERATING SISTEM**

Sistem operasi jaringan mirip dengan sistem operasi PC. Melalui GUI, sistem operasi PC memungkinkan pengguna untuk:

- ✓ Menggunakan mouse untuk membuat pilihan dan menjalankan program
- ✓ Masukkan perintah text dan text-based
- ✓ Melihat output pada monitor

Sistem operasi jaringan berbasis CLI seperti Cisco IOS pada switch atau router memungkinkan teknisi jaringan untuk:

- ✓ Menggunakan keyboard untuk menjalankan program jaringan berbasis CLI
- ✓ Menggunakan keyboard untuk memasukkan teks dan perintah berbasis teks
- ✓ Melihat output pada monitor

Perangkat jaringan Cisco menjalankan versi tertentu dari Cisco IOS. Versi IOS tergantung pada jenis perangkat yang digunakan dan fitur yang dibutuhkan. Sementara semua perangkat hadir dengan rangkaian iOS dan fitur default, Anda dapat mengunggah versi atau rangkaian fitur IOS untuk mendapatkan kemampuan tambahan.

- **METODE AKSES**

Switch Cisco IOS dapat diimplementasikan tanpa konfigurasi dan masih mengaktifkan data antar perangkat yang terhubung. Dengan menghubungkan dua PC ke switch, PC tersebut akan langsung terhubung satu sama lain.

Meskipun switch Cisco akan berfungsi dengan segera, mengkonfigurasi pengaturan awal adalah praktik terbaik yang direkomendasikan. Ada beberapa cara untuk mengakses lingkungan CLI dan mengkonfigurasi perangkat. Metode yang paling umum adalah:

- ✓ **Console** - Ini adalah port manajemen fisik yang menyediakan akses out-of-band ke perangkat Cisco. Akses out-of-band mengacu pada akses melalui saluran pengelolaan khusus yang hanya digunakan untuk tujuan perawatan perangkat.

Keuntungan menggunakan port konsol adalah perangkat dapat diakses meski tidak ada layanan jaringan yang dikonfigurasi, seperti saat melakukan konfigurasi awal perangkat jaringan. Saat melakukan konfigurasi awal, komputer yang menjalankan perangkat lunak emulasi terminal terhubung ke port konsol perangkat menggunakan kabel khusus. Perintah konfigurasi untuk mengatur switch atau router dapat dimasukkan pada komputer yang terhubung.

- ✓ **Secure Shell (SSH)** - SSH adalah metode untuk jarak jauh membuat koneksi CLI yang aman melalui antarmuka virtual, melalui jaringan. Tidak seperti koneksi konsol, koneksi SSH memerlukan layanan jaringan aktif pada perangkat termasuk antarmuka aktif yang dikonfigurasi dengan sebuah alamat.

SSH adalah metode yang disarankan untuk manajemen jarak jauh karena menyediakan koneksi yang aman. SSH menyediakan otentikasi password terenkripsi dan pengangkutan data sesi. Hal ini membuat ID pengguna, kata sandi, dan rincian sesi manajemen bersifat pribadi. Sebagian besar versi Cisco IOS menyertakan server SSH dan klien SSH yang dapat digunakan untuk membuat sesi SSH dengan perangkat lain.

- ✓ **Telnet** - Telnet adalah metode yang tidak aman untuk membangun sesi CLI dari jarak jauh melalui antarmuka virtual, melalui jaringan. Tidak seperti SSH, Telnet tidak menyediakan koneksi yang terenkripsi dengan aman. Otentikasi pengguna, kata sandi, dan perintah dikirim melalui jaringan di plaintext.

Praktik terbaik menentukan penggunaan SSH alih-alih Telnet untuk koneksi remote management CLI. Cisco IOS menyertakan server Telnet dan klien Telnet yang dapat digunakan untuk membuat sesi Telnet dengan perangkat lain.

Beberapa perangkat, seperti router, mungkin juga mendukung port pelengkap warisan yang digunakan untuk membuat sesi CLI dari jarak jauh menggunakan modem. Serupa dengan koneksi konsol, port AUX tidak beroperasi dan tidak memerlukan layanan jaringan untuk dikonfigurasi atau tersedia.

- **PROGRAM EMULASI TERMINAL**

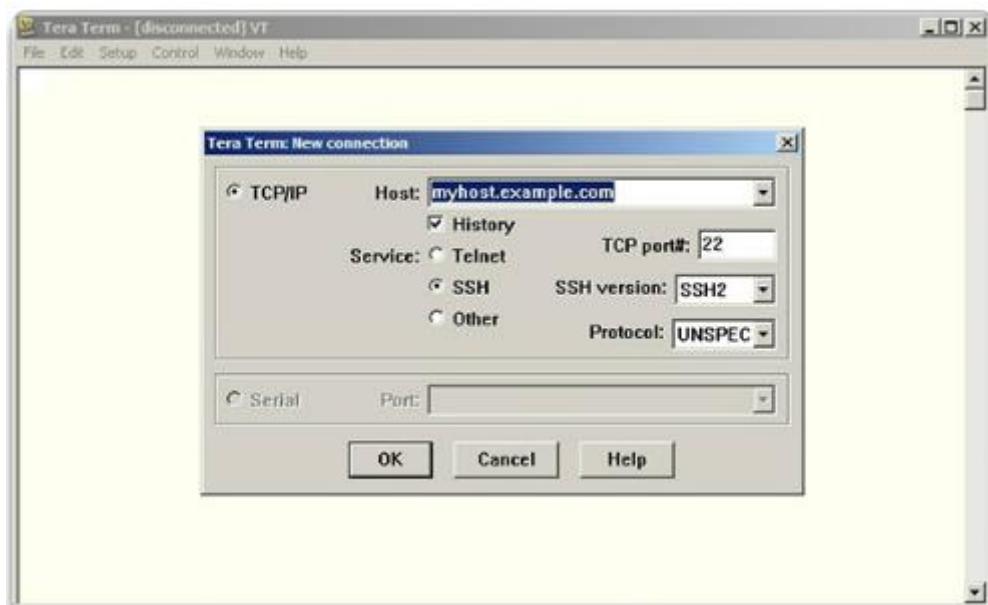
Ada sejumlah program emulasi terminal yang bagus yang tersedia untuk terhubung ke perangkat jaringan baik dengan koneksi serial melalui port konsol atau koneksi SSH / Telnet. Beberapa di antaranya meliputi:

- ✓ **PuTTY**



Putty

- ✓ **Tera Term**



Tera Term

- ✓ **SecureCRT**

```
# df
Filesystem      1K-blocks   Used Available Use% Mounted on
/dev/sda6        585605   171696   387805  36% /
/dev/sda2        77772    25621    48135  35% /boot
/dev/sda9       30115468  23596276  4989396  83% /home
none            1832324     0   1832324  0% /dev/shm
/dev/sda5        256667    9122    234293  4% /tmp
/dev/sda8       3099268  2838228  183688  97% /usr
/dev/sda3        381121    99189   262333  28% /var
#
```

SecureCRT

- ✓ **OS X Terminal**

Program ini memungkinkan Anda meningkatkan produktivitas dengan menyesuaikan ukuran jendela, mengubah ukuran font, dan mengubah skema warna.

- **CISCO IOS MODE OPERASI**

Untuk awalnya mengkonfigurasi perangkat Cisco, koneksi konsol harus dibuat. Setelah tersambung, teknisi jaringan harus menavigasi melalui berbagai mode perintah dari IOS CLI. Mode Cisco IOS menggunakan struktur hirarkis dan sangat mirip untuk switch dan router.

- **MODE PERINTAH UTAMA**

Sebagai fitur keamanan, perangkat lunak Cisco IOS memisahkan akses manajemen ke dua mode perintah berikut:

- ✓ **Mode User EXEC** - Modus ini memiliki kemampuan terbatas tapi berguna untuk operasi dasar. Ini hanya mengizinkan sejumlah perintah pemantauan dasar namun tidak memungkinkan pelaksanaan perintah yang mungkin mengubah konfigurasi perangkat. Mode user EXEC dikenali oleh prompt CLI yang diakhiri dengan simbol >
- ✓ **Mode Privileged EXEC** - Untuk menjalankan perintah konfigurasi, administrator jaringan harus mengakses mode privilege EXEC. Modus konfigurasi yang lebih tinggi,

seperti mode konfigurasi global, hanya dapat dicapai dari mode priviledge EXEC. Mode priviledge EXEC dapat diidentifikasi dengan prompt yang diakhiri dengan simbol #

Command Mode	Description	Default Device Prompt
User Exec Mode	<ul style="list-style-type: none"> Mode allows access to only a limited number of basic monitoring commands. It is often referred to as “view-only” mode. 	Switch> Router>
Privileged EXEC Mode	<ul style="list-style-type: none"> Mode allows access to all commands and features. The user can use any monitoring commands and execute configuration and management commands. 	Switch# Router#

Perintah Utama

- **KONFIGURASI MODE PERINTAH**

Untuk mengkonfigurasi perangkat, pengguna harus masuk ke Global Configuration Mode, yang biasa disebut global config mode.

Dari mode konfigurasi global, perubahan konfigurasi CLI dibuat yang mempengaruhi pengoperasian perangkat secara keseluruhan. Modus konfigurasi global diidentifikasi dengan sebuah prompt yang diakhiri dengan (config) # setelah nama perangkat, seperti Switch (config) #.

Modus konfigurasi global diakses sebelum mode konfigurasi spesifik lainnya. Dari mode konfigurasi global, pengguna bisa masuk ke mode sub-konfigurasi yang berbeda. Masing-masing mode ini memungkinkan konfigurasi bagian atau fungsi tertentu dari perangkat iOS. Dua mode konfigurasi umum yang umum termasuk:

- ✓ **Line Configuration Mode** - Digunakan untuk mengkonfigurasi akses konsol, SSH, Telnet, atau AUX.
- ✓ **Interface Configuration Mode** - Digunakan untuk mengkonfigurasi port switch atau interface jaringan router.

Saat menggunakan CLI, mode ini dikenali oleh command-line prompt yang unik untuk mode itu. Secara default, setiap prompt dimulai dengan nama perangkat. Mengikuti namanya, sisa prompt menunjukkan mode. Misalnya, prompt default untuk mode konfigurasi baris adalah Switch (config-line) # dan prompt default untuk mode konfigurasi antar muka adalah Switch (config-if) #.

- **NAVIGASI ANTARA MODE IOS**

Berbagai perintah digunakan untuk masuk dan keluar dari perintah prompt. Untuk berpindah dari mode user EXEC pengguna ke mode privileged EXEC, gunakan perintah enable. Gunakan perintah mode privileged EXEC yang dinonaktifkan untuk kembali ke mode user EXEC. Mode privileged EXEC terkadang disebut mode enable.

Untuk pindah dan keluar dari mode konfigurasi global, gunakan perintah terminal privileged EXEC yang di configure terminal. Untuk kembali ke mode privileged EXEC, masukkan perintah exit global mode config.

Ada banyak mode sub-konfigurasi yang berbeda. Misalnya, untuk masuk ke baris sub-configuration mode, Anda menggunakan line command yang diikuti oleh jenis baris manajemen dan nomor yang ingin Anda akses. Untuk keluar dari mode sub-konfigurasi dan kembali ke mode konfigurasi global, gunakan exit command. Perhatikan perubahan pada command prompt.

```
Switch(config)# line console 0
```

```
Switch(config-line)#
```

Untuk berpindah dari mode konfigurasi sub-mode konfigurasi global ke mode satu langkah di atasnya dalam hierarki mode, masukkan ke exit command.

```
Switch(config-line)# exit
```

```
Switch(config)#
```

Untuk beralih dari mode sub-konfigurasi ke mode privileged EXEC, masukkan end command atau masukkan kombinasi tombol Ctrl + Z.

```
Switch(config-line)# end
```

```
Switch#
```

Anda juga dapat berpindah langsung dari satu mode sub-konfigurasi ke mode sub-konfigurasi lainnya. Perhatikan bagaimana setelah nama perangkat jaringan, command prompt berubah dari (config-line) # menjadi (config-if) #.

```
Switch(config-line)# interface FastEthernet 0/1
```

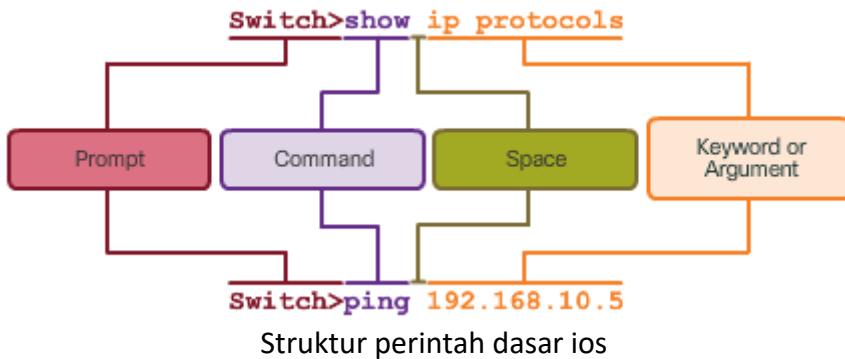
```
Switch(config-if)#
```

- **STRUKTUR PERINTAH DASAR IOS**

Perangkat Cisco IOS mendukung banyak perintah. Setiap perintah IOS memiliki format atau sintaks tertentu dan hanya bisa dijalankan dalam mode yang sesuai. Sintaks umum untuk sebuah perintah adalah perintah yang diikuti oleh *keyword* dan *argumen* yang sesuai.

- ✓ **Keyword** - parameter spesifik yang ditentukan dalam sistem operasi (ip protocols)
- ✓ **Argumen** - not predefined; nilai atau variabel yang ditentukan oleh pengguna (192.168.10.5)

Setelah memasukkan setiap perintah lengkap, termasuk kata kunci dan argumen, tekan tombol Enter untuk mengirimkan perintah ke command interpreter.



- **IOS COMMAND SYNTAX**

Perintah mungkin memerlukan satu atau lebih argumen. Untuk menentukan *keyword* dan *argumen* yang dibutuhkan untuk sebuah perintah, simak sintaks perintahnya. Sintaksnya menyediakan pola atau format yang harus digunakan saat memasukkan perintah.

Seperti yang teridentifikasi dalam tabel pada gambar, *boldface* menunjukkan perintah dan kata kunci yang dimasukkan seperti gambar di bawah ini. *italics* menunjukkan argumen dimana pengguna memberikan nilainya.

Misalnya, sintaks untuk menggunakan perintah deskripsi adalah *description string*. Argumennya adalah *string value* yang diberikan oleh pengguna. Perintah deskripsi biasanya digunakan untuk mengidentifikasi tujuan sebuah antarmuka. Misalnya, memasukkan perintah, deskripsi Menghubungkan ke *switch* kantor pusat utama, menjelaskan di mana perangkat lain berada di akhir koneksi.

Konvensi	Deskripsi
boldface	teks menunjukkan <i>command</i> dan <i>keyword</i> yang Anda masukkan secara harfiah seperti yang ditunjukkan
<i>italics</i>	teks miring menunjukkan argumen yang anda berikan nilai
[x]	Tanda kurung siku menunjukkan elemen opsional (<i>keyword</i> atau <i>argument</i>)
{x}	Kurung kurawal menunjukkan elemen yang dibutuhkan (<i>keyword</i> atau <i>argument</i>)

[x {y x}]	Kurung kurawal dan garis vertikal dengan kurung siku menunjukkan elemen yang dibutuhkan dengan element opsional
-------------	---

Contoh berikut menunjukkan konvensi yang digunakan untuk mendokumentasikan dan menggunakan perintah IOS.

- ✓ ping ip-address - Perintahnya adalah ping dan argumen yang ditetapkan pengguna adalah ip-address dari perangkat tujuan. Misalnya ping 10.10.10.5.
- ✓ traceroute ip-address - Perintahnya adalah traceroute dan argumen yang ditetapkan pengguna adalah ip-address dari perangkat tujuan. Misalnya, traceroute 192.168.254.254.

Cisco IOS Command Reference adalah sumber informasi utama untuk perintah IOS tertentu.

- **IOS Fitur HELP**

IOS memiliki dua bentuk bantuan yang tersedia:

- ✓ Context-Sensitive Help
- ✓ Command Syntax Check

Bantuan yang sensitif konteks memungkinkan Anda menemukan perintah yang tersedia di setiap mode perintah dengan cepat, perintahnya dimulai dengan karakter atau kelompok karakter tertentu, dan argumen dan *keyword* mana yang tersedia untuk perintah tertentu. Untuk mengakses bantuan peka konteks, cukup masukkan tanda tanya, ?, Di CLI.

Cek sintaks perintah memverifikasi bahwa perintah yang valid telah dimasukkan oleh pengguna. Saat sebuah perintah masuk, *the command line interpreter* mengevaluasi perintah dari kiri ke kanan. Jika *interpreter* memahami perintah, tindakan yang diminta dijalankan, dan CLI kembali ke prompt yang sesuai. Namun, jika *interpreter* tidak dapat memahami perintah yang dimasukkan, maka akan memberikan umpan balik yang menggambarkan apa yang salah dengan perintah tersebut.

- **HotKeys & Shortcuts**

IOS CLI menyediakan hot keys dan shortcut yang membuat konfigurasi, monitoring, dan troubleshooting lebih mudah, seperti yang ditunjukkan pada gambar.

Command dan *keyword* dapat disingkat dengan jumlah karakter minimum yang mengidentifikasi pilihan unik. Sebagai contoh, perintah *configure* dapat disingkat menjadi *conf* karena *configure* adalah satu-satunya perintah yang dimulai dengan *conf*. Sebuah singkatan dari *con* tidak akan bekerja karena lebih dari satu perintah dimulai dengan *con*. Kata kunci juga bisa disingkat.

CLI Line Editing

Tab	Melengkapi perintah parsial / tidak lengkap yang dimasukkan
BackSpace	Hapus karakter ke kiri dari kursor
Ctrl-D	Hapus karakter pada kursor
Ctrl-K	Hapus semua karakter dari letak kursor hingga akhir baris perintah
Esc D	Hapus semua karakter dari letak kursor hingga akhir kata
Ctrl-U or Ctrl-X	Hapus semua karakter dari letak kursor kembali ke awal baris perintah
Ctrl-W	Hapus semua kata ke kiri dari kursor
Ctrl-A	Pindahkan kursor ke awal dari baris
Left Arrow or Ctrl-B	Pindahkan kursor 1 karakter ke kiri
Esc B	Pindahkan kursor kembali 1 kata ke kiri
Esc F	Pindahkan kursor kedepan 1 kata ke kanan
Right Arrow or Ctrl-F	Pindahkan kursor 1 karakter ke kanan
Ctrl-E	Pindahkan kursor ke akhir baris perintah
Up Arrow or Ctrl-P	Memanggil kembali perintah yang pernah dimasukkan dari history, dimulai dengan perintah terakhir
Ctrl-R or Ctrl-I or Ctrl-L	Menampilkan ulang system prompt dan baris komentar setelah pesan diterima

At the " -----More-----" prompt

Enter Key	Displays the next line.
Space Bar	Displays the next screen.
Any Key	Ends the display string, returning to privileged EXEC mode.

Break Keys

Ctrl-C	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode. When in setup mode, aborts back to the command prompt.
Ctrl-Z	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Shift-6	All-purpose break sequence. Use to abort DNS lookups, traceroutes, pings.

NOTE: **Control** keys - Press and hold the <Ctrl> key and then press the specified letter key.
Escape sequences - Press and release the <Esc> key, and then press the letter key.

- ❖ **KONFIGURASI DASAR ALAT**
 - **NAMA ALAT (DEVICE)**

Saat mengkonfigurasi perangkat jaringan, salah satu langkah pertama adalah mengkonfigurasi nama perangkat atau nama host yang unik. Nama host yang muncul dalam petunjuk CLI dapat digunakan dalam berbagai proses otentifikasi antar perangkat, dan harus digunakan pada diagram topologi.

Jika nama perangkat tidak dikonfigurasi secara eksplisit, nama default yang ditetapkan pabrik digunakan oleh Cisco IOS. Nama default untuk switch Cisco IOS adalah "Switch." Jika semua perangkat jaringan ditinggalkan dengan nama default mereka, akan sulit untuk mengidentifikasi perangkat tertentu. Misalnya, saat mengakses perangkat jarak jauh menggunakan SSH, penting untuk memastikan bahwa Anda terhubung ke perangkat yang tepat.

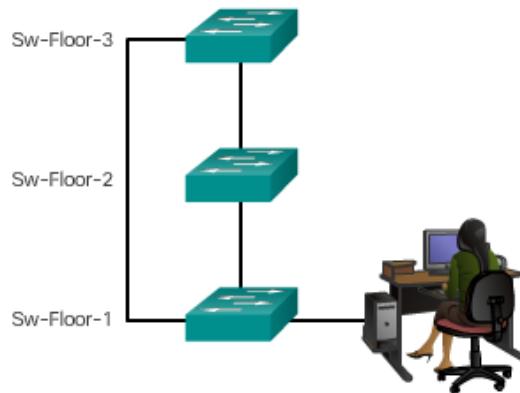
Dengan memilih nama dengan bijak, lebih mudah mengingat, mendokumentasikan, dan mengidentifikasi perangkat jaringan. Panduan untuk konfigurasi hostname tercantum pada Gambar.

Nama host yang digunakan pada perangkat IOS ditampilkan berupa huruf kapital dan huruf kecil. Oleh karena itu, memungkinkan Anda untuk memanfaatkan nama seperti biasanya. Ini sangat kontras dengan skema penamaan Internet, di mana huruf besar dan huruf kecil diperlakukan sama.

Panduan untuk memilih Hostname :

- ✓ Dimulai dengan huruf
- ✓ Tidak terdapat spasi
- ✓ Diakhiri dengan huruf atau digit
- ✓ Hanya menggunakan huruf, digit dan penghubung
- ✓ Kurang dari 64 karakter

Contohnya, pada Gambar, tiga switch, yang mencakup tiga lantai yang berbeda, saling berhubungan satu sama lain dalam sebuah jaringan. Konvensi penamaan yang digunakan mempertimbangkan lokasi dan tujuan masing-masing perangkat. Dokumentasi jaringan harus menjelaskan bagaimana nama-nama ini dipilih sehingga perangkat tambahan dapat diberi nama sesuai dengan itu.



Konfigurasi nama device

- **KONFIGURASI HOSTNAME**

Setelah konvensi penamaan telah diidentifikasi, langkah selanjutnya adalah menerapkan nama ke perangkat menggunakan CLI.

Seperti ditunjukkan pada Gambar, dari mode privileged EXEC, akses mode konfigurasi global dengan memasukkan perintah `configure terminal`. Perhatikan perubahan pada command prompt.

```

Switch# configure terminal
Switch(config)# hostname SW-Floor-1
Sw-Floor-1(config)#

```

Konfigurasi hostname

Dari mode konfigurasi global, masukkan perintah `hostname` diikuti dengan nama switch dan tekan Enter. Perhatikan perubahan nama command prompt.

Catatan: Untuk menghapus nama host yang dikonfigurasi dan mengembalikan pengalihan ke prompt default, gunakan perintah konfigurasi global `hostname`.

Selalu pastikan dokumentasi diperbarui setiap kali perangkat ditambahkan atau diubah. Identifikasi perangkat di dokumentasi menurut lokasi, tujuan, dan alamat mereka.

Gunakan Pemeriksa Sintaks pada Gambar untuk berlatih memasukkan nama host di switch.

Configure the Switch Hostname

Enter the configuration mode and configure the switch hostname to be 'Sw-Floor-1'.

```

Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#

```

You have successfully configured the switch hostname.

Konfigurasi nama switch

- AKSES PERANGKAT YANG AMAN

Penggunaan kata kunci yang lemah atau mudah tebak terus menjadi isu keamanan di banyak sisi dunia bisnis. Perangkat jaringan, termasuk router nirkabel rumahan, harus selalu memiliki kata sandi yang dikonfigurasi untuk membatasi akses administratif.

Cisco IOS dapat dikonfigurasi untuk menggunakan kata sandi mode hierarkis untuk memungkinkan hak akses yang berbeda ke perangkat jaringan.

Semua perangkat jaringan harus membatasi akses. Gunakan password yang kuat yang tidak mudah ditebak. Pertimbangkan poin-poin kunci

Securing Administrative Access <ul style="list-style-type: none">• Secure privileged EXEC access with a password• Secure user EXEC access with a password• Secure remote Telnet access with a password Other tasks <ul style="list-style-type: none">• Encrypt all passwords• Provide legal notification	When Choosing Passwords: <ul style="list-style-type: none">• Use passwords that are more than 8 characters in length.• Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.• Avoid using the same password for all devices.• Don't use common words because these are easily guessed.
---	---

- KONFIGURASI PASSWORD

Kata sandi yang paling penting untuk dikonfigurasi adalah akses ke mode *privileged EXEC*. Untuk mengamankan akses *privileged EXEC*, gunakan perintah config password rahasia yang aktif.

```
Sw-Floor-1> enable
Sw-Floor-1#
Sw-Floor-1# conf terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
Sw-Floor-1# disable
Sw-Floor-1> enable
Password: ← Class
Sw-Floor-1#
```

Untuk mengamankan akses *user EXEC*, port konsol harus dikonfigurasi. Masukkan mode konfigurasi konsol baris menggunakan konsol baris 0 perintah konfigurasi global. Angka nol digunakan untuk mewakili antarmuka konsol pertama (dan dalam kebanyakan kasus satu-satunya). Selanjutnya, tentukan *user mode EXEC* password menggunakan perintah password password. Akhirnya, aktifkan akses pengguna EXEC dengan menggunakan perintah masuk. Akses konsol sekarang akan memerlukan kata sandi sebelum mendapatkan akses ke mode EXEC pengguna.

```
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# exit
Sw-Floor-1(config)#

```

Saluran VTY memungkinkan akses jarak jauh ke perangkat. Untuk mengamankan jalur VTY yang digunakan untuk SSH dan Telnet, masukkan mode VTY line menggunakan perintah konfigurasi global vty 0 15. Banyak switch Cisco mendukung hingga 16 jalur VTY yang diberi nomor 0 sampai 15. Selanjutnya, tentukan password VTY dengan menggunakan perintah password password. Terakhir, aktifkan akses VTY menggunakan perintah masuk.

```
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)#

```

- **ENKRIPSI PASSWORD**

File startup-config dan running-config menampilkan sebagian besar kata kunci dalam plaintext. Ini adalah ancaman keamanan karena siapapun bisa melihat password yang digunakan jika mereka memiliki akses ke file-file ini.

Untuk mengenkripsi kata sandi, gunakan perintah konfigurasi enkripsi password-password global. Perintah tersebut menggunakan enkripsi yang lemah untuk semua password yang tidak terenkripsi. Enkripsi ini hanya berlaku untuk kata sandi dalam file konfigurasi, bukan dengan kata sandi karena dikirim melalui jaringan. Tujuan dari perintah ini adalah untuk menjaga individu yang tidak berwenang melihat kata kunci dalam file konfigurasi.

```
Enter the command to encrypt the plaintext passwords.
Switch(config)# service password-encryption
Exit global configuration mode and view the running configuration.
Switch(config)# exit

Switch# show running-config
!
<output omitted>
!
line con 0
password 7 094F471A1A0A
login
!
line vty 0 4
password 7 03095A0F034F38435B49150A1819
login
!
!
end

Switch#
You successfully encrypted the plaintext passwords.
```

• PESAN BANNER / PEMBERITAHUAN

Meskipun menggunakan kata sandi adalah salah satu cara untuk menjaga personil yang tidak diotorisasi keluar dari jaringan, sangat penting untuk menyediakan metode untuk menyatakan bahwa hanya petugas yang berwenang yang harus berusaha masuk ke perangkat. Untuk melakukan ini, tambahkan pemberitahuan informasi ke keluaran perangkat. informasi bisa menjadi bagian penting dari proses hukum jika seseorang diadili karena membobol perangkat. Beberapa sistem hukum tidak mengizinkan penuntutan, atau bahkan pemantauan pengguna, kecuali jika pemberitahuan tersebut terlihat.

Untuk membuat pesan pemberitahuan hari ini pada perangkat jaringan, gunakan banner motd # pesan hari # perintah konfigurasi global. The "#" dalam sintaks perintah disebut karakter pembatas. Ini dimasukkan sebelum dan sesudah pesan. Karakter pembatas bisa berupa karakter apapun asalkan tidak terjadi pada pesan. Untuk alasan ini, simbol seperti "#" sering digunakan. Setelah perintah dijalankan, banner akan ditampilkan pada semua usaha selanjutnya untuk mengakses perangkat sampai banner dilepas.

Karena spanduk bisa dilihat oleh siapa saja yang mencoba masuk, pesannya harus dituliskan dengan sangat hati-hati. Konten atau kata-kata spanduk yang tepat bergantung pada hukum setempat dan kebijakan perusahaan. pemberitahuan harus menyatakan bahwa hanya petugas yang berwenang yang diizinkan mengakses perangkat. Setiap kata yang menyiratkan login adalah "welcome" atau "invite" tidak sesuai. Selanjutnya, banner tersebut dapat mencakup shutdown sistem terjadwal dan informasi lainnya yang mempengaruhi semua pengguna jaringan.

- **SYNTAX CHECKER - Membatasi Akses ke Switch**

Limit access to a switch.

- Encrypt all passwords.
- Secure the privileged EXEC access.
- Secure the console access.
- Secure the VTY access.

Encrypt all passwords.

```
Sw-Floor-1(config)# service password-encryption  
Sw-Floor-1(config)#{
```

Secure the privileged EXEC access with the password. Cla55.

```
Sw-Floor-1(config)# enable secret Cla55  
Sw-Floor-1(config)#{
```

Secure the console line.

- Use the password Cisc0.
- Allow login.

```
Sw-Floor-1(config)# line con 0  
Sw-Floor-1(config-line)# password Cisc0  
Sw-Floor-1(config-line)# login  
Sw-Floor-1(config-line)#{
```

Secure the first 16 VTY lines.

- Use the password Cisc0.
- Allow login.

```
Sw-Floor-1(config)# line vty 0 15  
Sw-Floor-1(config-line)# password Cisc0  
Sw-Floor-1(config-line)# login  
Sw-Floor-1(config-line)#{
```

You have successfully limited access to a switch.

- **SIMPAN FILE KONFIGURASI YANG BERJALAN**

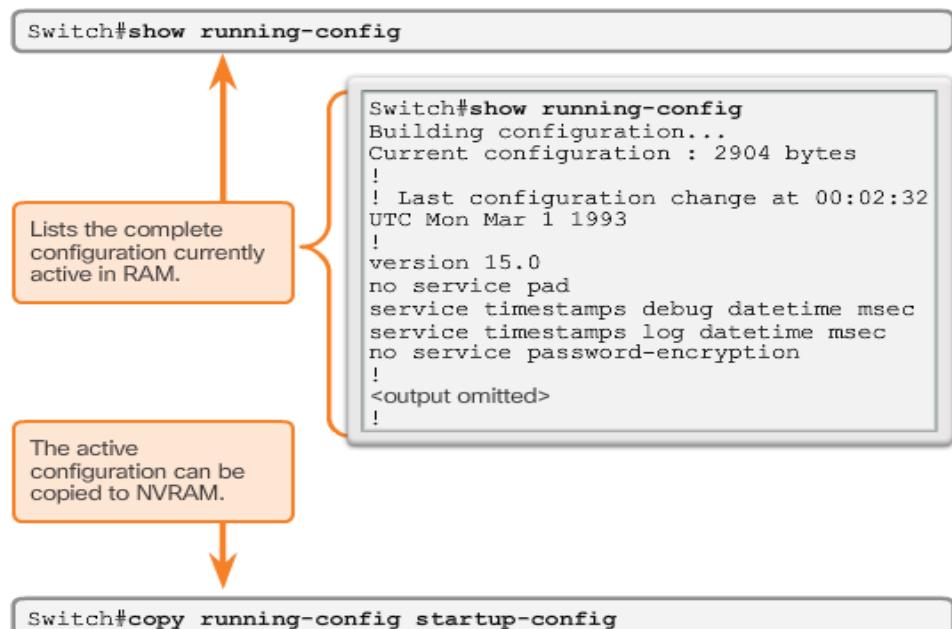
Berikut adalah dua file sistem yang menyimpan konfigurasi perangkat:

- ✓ **startup-config** - File yang tersimpan dalam Non-volatile Random Access Memory (NVRAM) yang berisi semua perintah yang akan digunakan oleh perangkat saat startup atau reboot. NVRAM tidak kehilangan isinya saat perangkat dimatikan.
- ✓ **running-config** - File yang tersimpan dalam Random Access Memory (RAM) yang mencerminkan konfigurasi saat ini. Mengubah konfigurasi yang sedang berjalan akan mempengaruhi pengoperasian perangkat Cisco dengan segera. RAM adalah memori yang mudah menguap. Ini kehilangan semua kontennya saat perangkat dimatikan atau dihidupkan ulang.

gunakan perintah running-config privileged EXEC mode untuk melihat file konfigurasi yang sedang berjalan. Untuk melihat file konfigurasi startup, gunakan perintah EXEC startup-config privilege.

Jika daya ke perangkat hilang atau jika perangkat di-restart, semua perubahan konfigurasi akan hilang kecuali jika telah disimpan. Untuk menyimpan perubahan yang dibuat pada

konfigurasi yang berjalan ke file konfigurasi startup, gunakan perintah running mode config-config startup-config privileged EXEC.



• SETELAH KONFIGURASI BERJALAN

Jika perubahan yang dilakukan pada konfigurasi yang berjalan tidak memiliki efek yang diinginkan dan file running-config belum disimpan, Anda dapat:

- ✓ Kembalikan perangkat ke konfigurasi sebelumnya dengan menghapus perintah yang diubah satu per satu.
- ✓ Salin file konfigurasi startup ke konfigurasi yang sedang berjalan dengan perintah startup config-config running-config privileged EXEC mode.
- ✓ Muat ulang perangkat menggunakan perintah reload mode privilege EXEC

Kelemahan untuk menggunakan perintah reload untuk menghapus konfigurasi yang belum disimpan adalah jumlah waktu perangkat akan offline, menyebabkan downtime jaringan.

Saat memulai reload, IOS akan mendeteksi bahwa konfigurasi yang berjalan memiliki perubahan yang tidak tersimpan pada konfigurasi startup. Sebuah prompt akan muncul untuk menanyakan apakah akan menyimpan perubahan. Untuk membuang perubahan, masukkan n atau tidak.

Sebagai alternatif, jika perubahan yang tidak diinginkan disimpan ke konfigurasi startup, mungkin perlu menghapus semua konfigurasi. Ini memerlukan penghapusan konfigurasi startup dan memulai ulang perangkat. Konfigurasi startup dihapus dengan menggunakan perintah perintah EXEC startup-config privilege. Setelah perintah dikeluarkan, switch akan meminta konfirmasi Anda. Tekan Enter untuk menerima.

Setelah menghapus konfigurasi startup dari NVRAM, muat ulang perangkat untuk menghapus file konfigurasi yang sedang berjalan dari RAM. Pada reload, sebuah switch akan memuat konfigurasi startup default yang awalnya dikirimkan bersama perangkat.

- **MENYIMPAN KONFIGURASI KE FILE TEKS**

File konfigurasi juga bisa disimpan dan diarsipkan ke dokumen teks. Urutan langkah ini memastikan salinan file konfigurasi kerja tersedia untuk diedit atau digunakan kembali nanti. Sebagai contoh, asumsikan bahwa sebuah saklar telah dikonfigurasi, dan konfigurasi yang berjalan telah tersimpan pada perangkat.

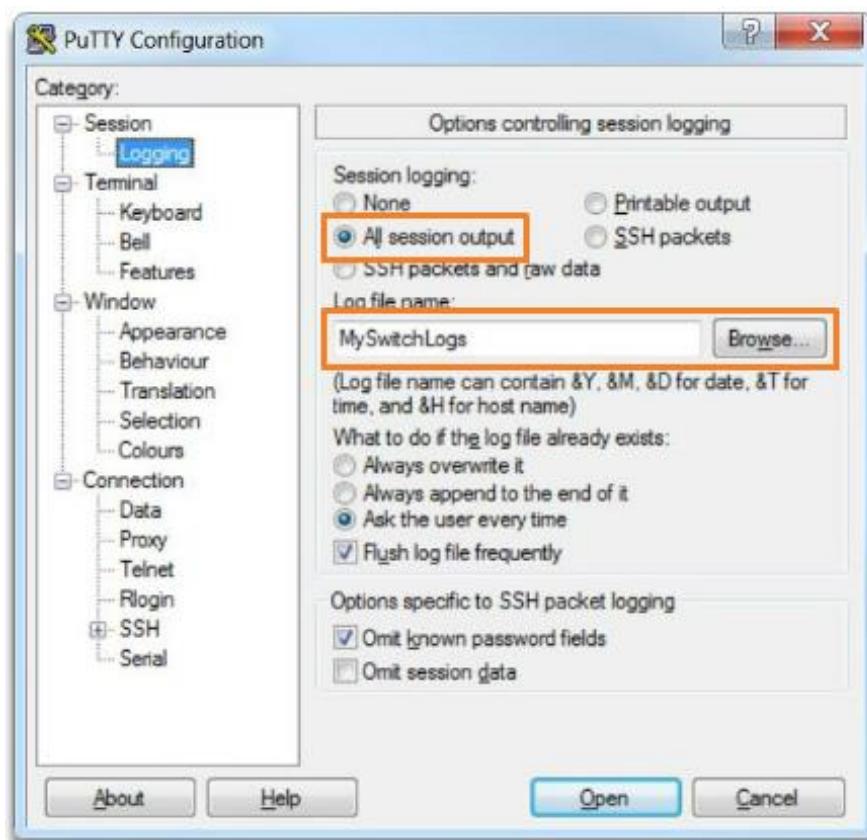
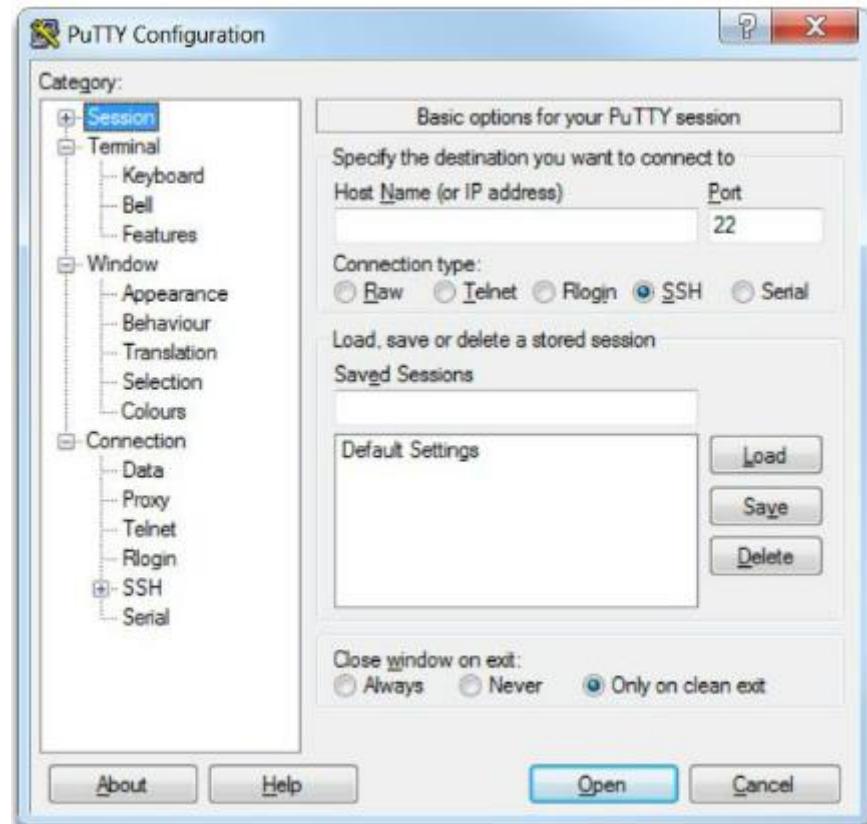
- ✓ Buka perangkat lunak emulasi terminal seperti Putty atau Tera Term (Gambar 1) yang terhubung ke switch.
- ✓ Aktifkan logging di perangkat lunak terminal, seperti Putty atau Tera Term, dan tetapkan nama dan lokasi file untuk menyimpan file log. Gambar 2 menampilkan bahwa Semua output sesi akan ditangkap ke file yang ditentukan (yaitu, MySwitchLogs).
- ✓ Jalankan acara running-config atau tampilkan perintah startup-config pada prompt privilege EXEC. Teks yang ditampilkan di jendela terminal akan ditempatkan pada file yang dipilih.

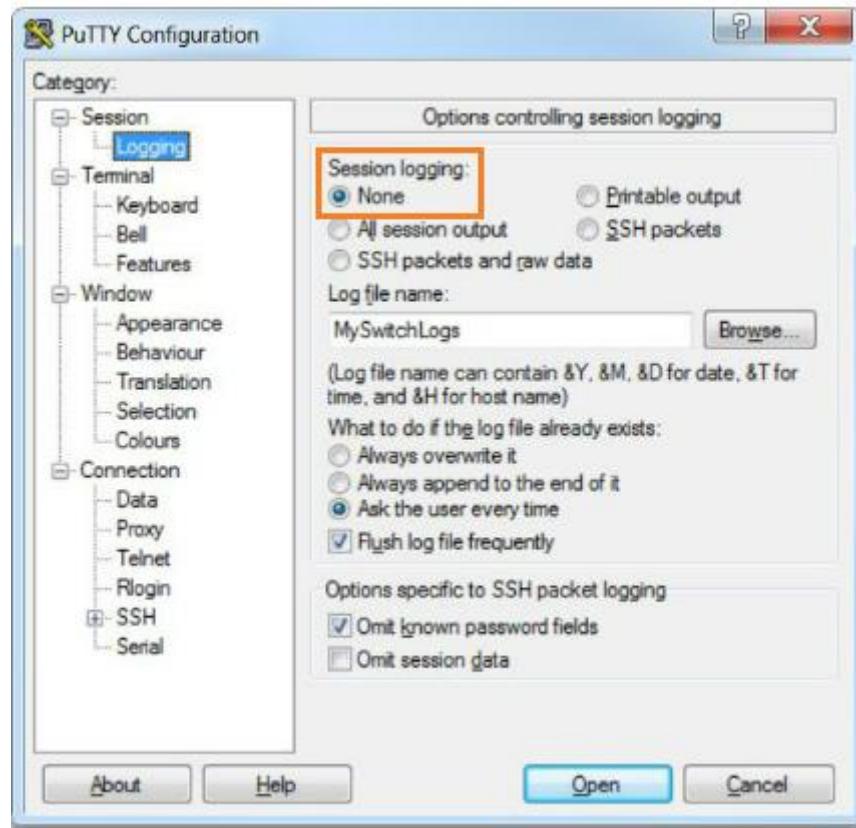
File teks yang dibuat dapat digunakan sebagai catatan bagaimana perangkat saat ini diterapkan. File bisa memerlukan pengeditan sebelum digunakan untuk mengembalikan konfigurasi tersimpan ke perangkat.

Untuk mengembalikan file konfigurasi ke perangkat:

- ✓ Masuki mode konfigurasi global pada perangkat
- ✓ Copy dan paste file teks ke jendela terminal yang terhubung ke switch.

Teks dalam file akan diterapkan sebagai perintah di CLI dan menjadi konfigurasi yang berjalan pada perangkat. Ini adalah metode yang mudah digunakan untuk mengkonfigurasi perangkat secara manual.





❖ SKEMA PENGALAMATAN

• IP ADDRESS

Penggunaan alamat IP adalah sarana utama untuk memungkinkan perangkat menemukan satu sama lain dan membuat komunikasi end-to-end di Internet. Setiap perangkat akhir pada jaringan harus dikonfigurasi dengan alamat IP.

Devices Requiring IP Addresses

- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- Security cameras
- Smart phones
- Mobile handheld devices (such as wireless barcode scanners)

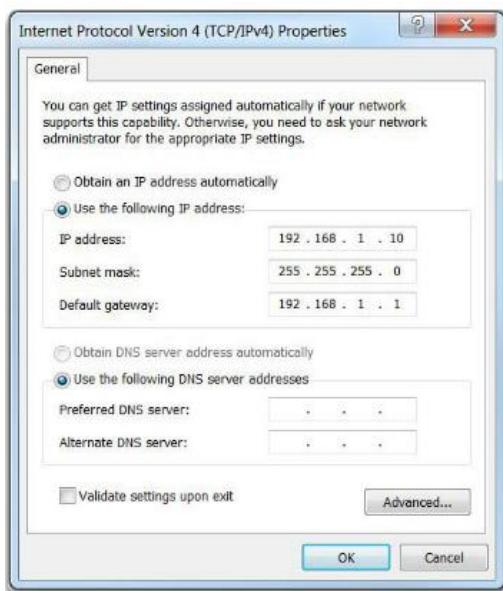
Struktur alamat IPv4 disebut notasi desimal bertitik dan diwakili oleh empat angka desimal antara 0 dan 255. Alamat IPv4 ditugaskan ke masing-masing perangkat yang terhubung ke jaringan.

Dengan alamat IPv4, subnet mask juga diperlukan. Subnet mask adalah tipe khusus dari

alamat IPv4. Ditambah dengan alamat IPv4, subnet mask menentukan subnet tertentu dari perangkat yang menjadi anggota.

Contoh pada alamat IPv4 (192.168.1.10), subnet mask (255.255.255.0), dan gateway default (192.168.1.1) yang ditugaskan ke host. Alamat gateway default adalah alamat IP dari router yang akan digunakan host untuk mengakses jaringan jarak jauh, termasuk Internet.

Alamat IP dapat diberikan ke port fisik dan antarmuka virtual pada perangkat. Antarmuka virtual berarti tidak ada perangkat keras fisik pada perangkat yang terkait dengannya.



- **TAMPILAN DAN PORTS**

Komunikasi jaringan bergantung pada antarmuka perangkat pengguna akhir, antarmuka perangkat jaringan, dan kabel yang menghubungkannya. Setiap antarmuka fisik memiliki spesifikasi, atau standar, yang menentukannya. Sambungan kabel ke antarmuka harus dirancang agar sesuai dengan standar fisik antarmuka. Jenis media jaringan meliputi kabel tembaga twisted-pair, kabel serat optik, kabel koaksial, atau nirkabel seperti yang ditunjukkan pada gambar.

Berbagai jenis media jaringan memiliki fitur dan manfaat yang berbeda. Tidak semua media jaringan memiliki karakteristik yang sama dan sesuai untuk tujuan yang sama. Beberapa perbedaan antara berbagai jenis media meliputi:

- ✓ Jarak media bisa berhasil membawa sinyal
- ✓ Lingkungan tempat media dipasang
- ✓ Jumlah data dan kecepatan yang harus ditransmisikan
- ✓ Biaya media dan instalasi

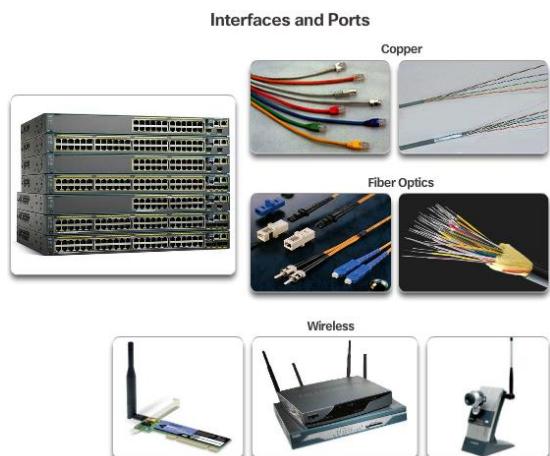
Tidak hanya setiap link di Internet memerlukan jenis media jaringan tertentu, namun setiap link juga memerlukan teknologi jaringan tertentu. Sebagai contoh, Ethernet adalah teknologi

jaringan area lokal (LAN) yang paling umum digunakan saat ini. Port Ethernet ditemukan pada perangkat pengguna akhir, perangkat peralihan, dan perangkat jaringan lainnya yang dapat terhubung secara fisik ke jaringan menggunakan kabel.

Cisco IOS Layer 2 switch memiliki port fisik untuk perangkat untuk terhubung. Port ini tidak mendukung alamat IP Layer 3. Oleh karena itu, switch memiliki satu atau lebih antarmuka virtual switch (SVI). Ini adalah antarmuka virtual karena tidak ada perangkat keras fisik pada perangkat yang terkait dengannya. SVI dibuat dalam perangkat lunak.

Antarmuka virtual menyediakan sarana untuk mengatur jarak jauh dari sebuah switch melalui jaringan menggunakan IPv4. Setiap saklar hadir dengan satu SVI yang muncul dalam konfigurasi default "out-of-the-box." SVI default adalah antarmuka VLAN1.

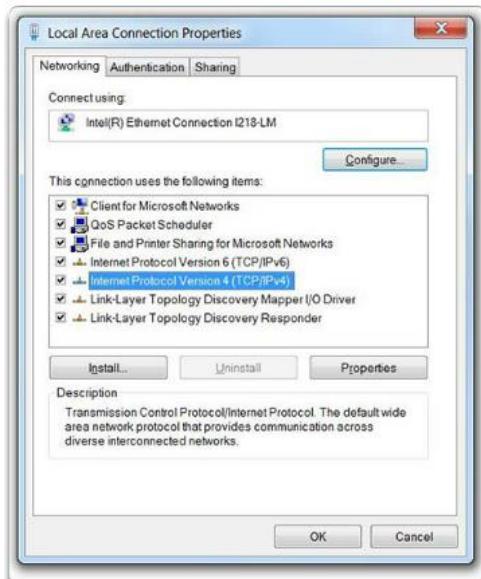
Catatan: Switch Layer 2 tidak memerlukan alamat IP. Alamat IP yang ditugaskan ke SVI digunakan untuk mengakses saklar jarak jauh. Alamat IP tidak diperlukan bagi peralihan untuk menjalankan operasinya.



- **KONFIGURASI MANUAL ALAMAT IP UNTUK PERANGKAT**

Agar perangkat akhir berkomunikasi melalui jaringan, harus dikonfigurasi dengan alamat IP dan subnet mask yang unik. Informasi alamat IP dapat dimasukkan ke dalam perangkat akhir secara manual, atau secara otomatis menggunakan Dynamic Host Configuration Protocol (DHCP).

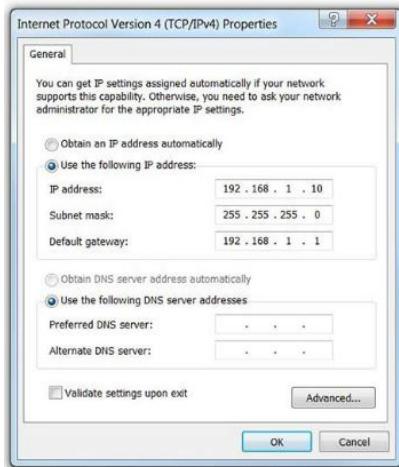
Untuk mengkonfigurasi alamat IP pada host Windows secara manual, buka Control Panel → Network Sharing Center → Ubah pengaturan adaptor dan pilih adaptornya. Selanjutnya klik kanan dan pilih Properties untuk menampilkan Local Area Connection Properties



Ethernet Adapter Properties

Sorot Internet Protocol Version 4 (TCP / IPv4) dan klik Properties untuk membuka jendela Properties Internet Protocol Version 4 (TCP / IPv4) yang ditunjukkan pada Gambar . Mengkonfigurasi alamat IPv4 dan informasi subnet mask, dan gateway default.

Catatan: Alamat server DNS adalah alamat IP dari server Sistem Nama Domain (DNS), yang digunakan untuk menerjemahkan alamat IP ke nama domain.

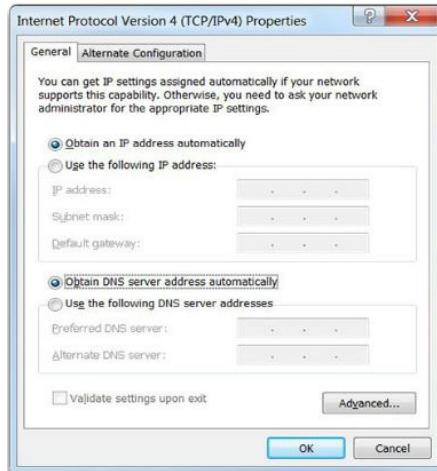


• KONFIGURASI ALAMAT IP OTOMATIS UNTUK PERANGKAT

PC biasanya default menggunakan DHCP untuk konfigurasi alamat IP otomatis. DHCP adalah teknologi yang digunakan di hampir setiap jaringan. Cara terbaik untuk memahami mengapa DHCP sangat populer adalah dengan mempertimbangkan semua pekerjaan ekstra yang harus dilakukan tanpa itu.

Dalam sebuah jaringan, DHCP memungkinkan konfigurasi alamat IPv4 otomatis untuk setiap perangkat akhir yang mengaktifkan DHCP. Bayangkan jumlah waktu yang akan dikonsumsi jika setiap kali Anda terhubung ke jaringan, Anda harus memasukkan alamat IP secara manual, subnet mask, gateway default, dan server DNS. Kalikan itu oleh setiap pengguna dan setiap

perangkat dalam sebuah organisasi dan Anda melihat masalahnya. Konfigurasi manual juga meningkatkan kemungkinan kesalahan konfigurasi dengan menduplikat alamat IP perangkat lain.



Assign Dynamic Address

untuk mengkonfigurasi DHCP pada PC Windows, Anda hanya perlu memilih "Mendapatkan alamat IP secara otomatis" dan "Mendapatkan alamat server DNS secara otomatis". PC Anda akan mencari server DHCP dan diberi pengaturan alamat yang diperlukan untuk berkomunikasi di jaringan.

Hal ini dimungkinkan untuk menampilkan pengaturan konfigurasi IP pada PC Windows dengan menggunakan perintah ipconfig pada command prompt. Outputnya akan menampilkan alamat IP, subnet mask, dan informasi gateway yang diterima dari server DHCP.

```
Enter the command to display the IP configuration on a Windows PC.

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : cisco.com
Link-local IPv6 Address . . . . . : fe80::b0ef:ca42:af2c:c6c7%16
IPv4 Address . . . . . : 10.82.240.197
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.82.240.198

-----
You successfully displayed the IP configuration on a Windows PC.
```

Verifying Windows PC IP Config

- **SWITCH VIRTUAL INTERFACE CONFIGURATION**

Untuk mengakses Switch jarak jauh, alamat IP dan subnet mask harus dikonfigurasi pada SVI. Untuk mengkonfigurasi SVI di switch, gunakan perintah konfigurasi global `vlan 1 interface`. Vlan 1 bukan *physical interface* yang sebenarnya tapi yang virtual. Selanjutnya tetapkan alamat IPv4 menggunakan alamat `ip ip-address subnet-mask interface configuration command`. Akhirnya, aktifkan *virtual interface* menggunakan perintah `no shutdown interface configuration command`.

Setelah perintah ini dikonfigurasi, switch memiliki semua elemen IPv4 yang siap untuk komunikasi melalui jaringan.

- **SYNTAX CHECKER - CONFIGURING A SWITCH VIRTUAL INTERFACE**

```
Configure a Switch Virtual Interface
  • Enter interface configuration mode for VLAN 1.
  • Configure the IPv4 address as 192.168.10.2 and the subnet mask as 255.255.255.0.
  • Enable the interface.
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.10.2 255.255.255.0
Switch(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
Switch(config-if)#
You have successfully configured the switch virtual interface for VLAN 1.
```

- **INTERFACE ADDRESSING VERIFICATION**

Dengan cara yang sama seperti Anda menggunakan perintah dan utilitas seperti ipconfig untuk memverifikasi konfigurasi jaringan host PC, Anda juga menggunakan perintah untuk memverifikasi pengaturan antarmuka dan alamat perangkat perantara seperti switch dan router.

LATIHAN SOAL 2

1. Apa itu OPerating system dalam Networking
2. Jelaskan tujuan dari Operating system Networking
3. Sebutkan perbedaan metode akses antara console, SSH, Telnet
4. Sebutkan dan jelaskan program / aplikasi untuk emulasi terminal
5. Jelaskan yang dimaksud dengan command mode: User Exec Mode dan Priviledge Exec Mode
6. Tuliskan struktur dasar command IOS
7. Tuliskan syntax untuk konfigurasi Name device & Hostname
8. Tuliskan syntax untuk konfigurasi password dan enkripsi pada switch
9. Jelaskan perbedaan konfigurasi ip secara manual dengan otomatis
10. Jelaskan perbedaan antara startup-config dan running-config

BAB 3 PROTOKOL JARINGAN DAN KOMUNIKASI

3.1 PENGANTAR

Semakin banyak jaringan yang menghubungkan kita. Orang berkomunikasi secara online dari mana-mana. Percakapan di ruang kelas berpindah ke sesi obrolan pesan instan, dan perdebatan online berlanjut di sekolah. Layanan baru sedang dikembangkan setiap hari untuk memanfaatkan jaringan.

Daripada mengembangkan sistem yang unik dan terpisah untuk pengiriman setiap layanan baru, industri jaringan secara keseluruhan telah mengadopsi kerangka perkembangan yang memungkinkan perancang memahami platform jaringan saat ini, dan merawatnya. Pada saat yang sama, kerangka kerja ini digunakan untuk memfasilitasi pengembangan teknologi baru guna mendukung kebutuhan komunikasi dan penyempurnaan teknologi masa depan.

Inti dari kerangka perkembangan ini, adalah penggunaan model yang diterima secara umum yang menggambarkan peraturan dan fungsi jaringan.

Dalam bab ini, Anda akan belajar tentang model ini, serta standar yang membuat jaringan bekerja, dan bagaimana komunikasi terjadi melalui jaringan.

❖ ATURAN DALAM BERKOMUNIKASI

• DASAR-DASAR BERKOMUNIKASI

Jaringan bisa serumit perangkat yang terhubung di Internet, atau sesederhana dua komputer yang terhubung langsung satu sama lain dengan satu kabel, dan apapun yang ada di antaranya. Jaringan dapat bervariasi dalam ukuran, bentuk, dan fungsi. Namun, hanya memiliki koneksi fisik kabel atau nirkabel antara perangkat akhir tidak cukup untuk memungkinkan komunikasi. Agar komunikasi terjadi, perangkat harus tahu "bagaimana" berkomunikasi.

Orang bertukar ide menggunakan banyak metode komunikasi yang berbeda. Namun, terlepas dari metode yang dipilih, semua metode komunikasi memiliki tiga elemen yang sama. Yang pertama dari elemen ini adalah, atau pengirim. Sumber pesan adalah orang, atau perangkat elektronik, yang perlu mengirim pesan ke orang lain atau perangkat. Elemen kedua komunikasi adalah tujuan, atau penerima, dari pesan. Tujuannya menerima pesan dan menafsirkannya. Unsur ketiga, disebut saluran, terdiri dari media yang menyediakan jalur dimana pesan berpindah dari sumber ke tujuan.

Komunikasi dimulai dengan pesan, atau informasi, yang harus dikirim dari sumber ke tujuan. Pengiriman pesan, baik dengan komunikasi tatap muka atau melalui jaringan, diatur oleh peraturan yang disebut **protokol**. Protokol ini khusus untuk jenis metode komunikasi yang tertentu. Dalam komunikasi pribadi sehari-hari, peraturan yang kita gunakan untuk berkomunikasi melalui satu media, seperti panggilan telepon, tidak harus sama dengan protokol untuk menggunakan media lain, seperti mengirim surat.

Misalnya, perhatikan dua orang yang berkomunikasi tatap muka, Sebelum berkomunikasi, mereka harus menyetujui bagaimana berkomunikasi. Jika komunikasi menggunakan suara, mereka harus terlebih dahulu menyetujui bahasa tersebut. Selanjutnya, saat mereka memiliki

pesan untuk dibagikan, mereka harus bisa memformat pesan itu dengan cara yang bisa dimengerti. Misalnya, jika seseorang menggunakan bahasa Inggris, tapi struktur kalimatnya buruk, pesannya bisa dengan mudah disalahpahami. Masing-masing tugas ini menggambarkan protokol yang ada untuk menyelesaikan komunikasi. Hal ini juga berlaku untuk komunikasi komputer.

Banyak aturan atau protokol yang berbeda mengatur semua metode komunikasi yang ada di dunia saat ini.

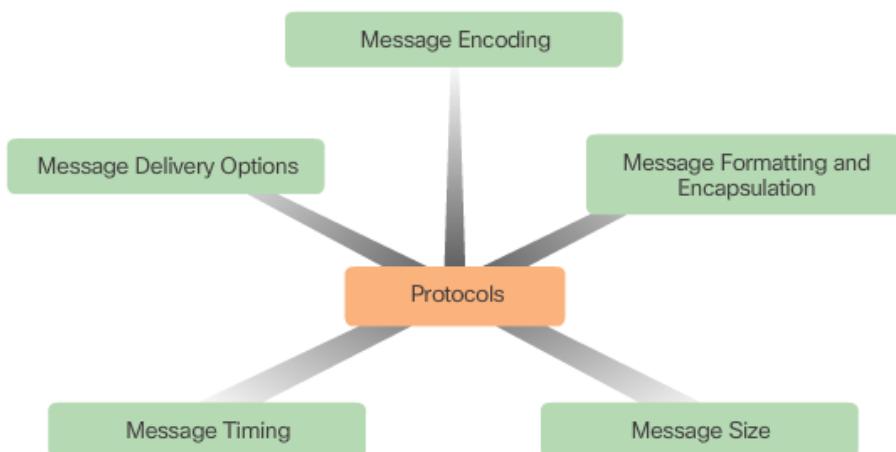


● ATURAN PEMBENTUKAN

Sebelum berkomunikasi satu sama lain, individu harus menggunakan peraturan atau kesepakatan yang telah ditetapkan untuk mengatur pembicaraan. Protokol diperlukan untuk komunikasi yang efektif. Aturan atau protokol, harus diikuti agar pesan berhasil disampaikan dan dipahami. Protokol harus memperhitungkan persyaratan berikut:

- ✓ Identitas Pengirim dan Penerima
- ✓ Bahasa dan tatabahasa yang umum
- ✓ Kecepatan dan waktu pengiriman
- ✓ Konfirmasi atau persyaratan.

Protokol yang digunakan dalam komunikasi jaringan berbagi banyak sifat mendasar. Selain mengidentifikasi sumber dan tujuan, protokol komputer dan jaringan menentukan rincian tentang bagaimana sebuah pesan dikirim melalui jaringan. Protokol komputer yang umum mencakup persyaratan yang ditunjukkan pada Gambar.



● ENCODING PESAN

Salah satu langkah pertama untuk mengirim pesan adalah pengkodean. **Encoding** adalah proses mengubah informasi menjadi bentuk lain yang dapat diterima, untuk transmisi. **Decoding** membalik proses ini untuk menafsirkan informasi.

Bayangkan seseorang merencanakan perjalanan liburan bersama seorang teman, dan memanggil teman untuk mendiskusikan rincian dari mana mereka ingin pergi. Untuk mengkomunikasikan pesannya, dia mengubah pemikirannya menjadi bahasa yang disepakati. Dia kemudian mengucapkan kata-kata yang menggunakan suara dan infleksi bahasa lisan yang menyampaikan pesannya. Temannya mendengarkan deskripsi dan menerjemahkan suara untuk memahami pesan yang diterimanya.

Encoding juga terjadi dalam komunikasi komputer. Pengkodean antar host harus dalam format yang sesuai untuk medium. Pesan yang dikirim melalui jaringan pertama-tama diubah menjadi bit oleh host pengirim. Setiap bit dikodekan menjadi pola suara, gelombang cahaya, atau impuls listrik tergantung pada media jaringan tempat bit ditransmisikan. Host tujuan menerima dan menerjemahkan sinyal untuk menafsirkan pesan.

● FORMAT PESAN DAN ENKAPSULASI

Bila pesan dikirim dari sumber ke tujuan, maka pesan tersebut harus menggunakan format atau struktur tertentu. Format pesan tergantung pada jenis pesan dan saluran yang digunakan untuk menyampaikan pesan.

Menulis surat adalah salah satu bentuk komunikasi manusia tertulis yang paling umum. Selama berabad-abad, format yang disepakati untuk surat pribadi tidak berubah. Dalam banyak budaya, sebuah surat pribadi mengandung unsur-unsur berikut:

- ✓ Identitas Penerima
- ✓ Sapa & Salam
- ✓ Isi Pesan
- ✓ Pesan Penutup
- ✓ Identitas Pengirim

Selain memiliki format yang benar, kebanyakan surat pribadi juga harus disertakan dalam amplop untuk pengiriman. Amplop ini memiliki alamat pengirim dan penerima, masing-masing diletakkan di tempat yang tepat pada amplop. Jika alamat dan format tujuan tidak benar, surat tersebut tidak terkirim. Proses menempatkan satu format pesan (huruf) di dalam format pesan lain (amplop) disebut **enkapsulasi**. **De-enkapsulasi** terjadi saat proses dibalik oleh penerima dan surat tersebut dikeluarkan dari amplop.



Recipient (destination) Location address	Sender (source) Location address	Salutation (start of message indicator)	Recipient (destination) identifier	Content of Letter (encapsulated data)	Sender (source) identifier	End of Frame (End of message indicator)
Envelope Addressing		Encapsulated Letter				
1400 Main Street Canton, Ohio 44203	4085 SE Pine Street Ocala, Florida 34471	Dear	Jane	I just returned from my trip. I thought you might like to see my pictures.	John	

Pesan yang dikirim melalui jaringan komputer mengikuti peraturan format spesifik agar dikirim dan diproses. Sama seperti sebuah surat yang dienkapsulasi dalam amplop untuk pengiriman, demikian juga pesan komputer. Setiap pesan komputer dienkapsulasi dalam format tertentu, disebut bingkai, sebelum dikirim melalui jaringan. Bingkai seperti sebuah amplop; Ini menyediakan alamat tujuan dan alamat host sumber. Perhatikan bahwa frame memiliki sumber dan tujuan di bagian pengalaman bingkai dan dalam pesan yang dienkapsulasi.

Format dan isi bingkai ditentukan oleh jenis pesan yang dikirim dan saluran yang dikomunikasikan. Pesan yang tidak diformat dengan benar tidak berhasil dikirim ke atau diproses oleh host tujuan.

Destination (physical / hardware address)	Source (physical / hardware address)	Start Flag (start of message indicator)	Recipient (destination identifier)	Sender (source identifier)	Encapsulated Data (bits)	End of Frame (end of message indicator)
Frame Addressing		Encapsulated Message				

● UKURAN PESAN

Aturan komunikasi lainnya adalah ukuran. Ketika orang berkomunikasi satu sama lain, pesan yang mereka kirim biasanya dipecah menjadi beberapa bagian atau kalimat yang lebih kecil. Kalimat ini terbatas pada ukuran yang dapat diproses oleh seseorang pada satu waktu. Percakapan individual dapat terdiri dari banyak kalimat yang lebih kecil untuk memastikan bahwa setiap bagian dari pesan diterima dan dipahami. Bayangkan bagaimana rasanya membaca buku ini jika semuanya muncul sebagai satu kalimat panjang; Tidak mudah untuk membaca dan memahami.

Demikian juga, ketika sebuah pesan panjang dikirim dari satu host ke host lain melalui jaringan, perlu untuk memecahkan pesan menjadi beberapa bagian yang lebih kecil. Aturan yang mengatur ukuran potongan, atau bingkai, yang dikomunikasikan di seluruh jaringan sangat ketat. Mereka juga bisa berbeda, tergantung dari saluran yang digunakan. Bingkai yang terlalu panjang atau terlalu pendek tidak terkirim.

Pembatasan ukuran frame mengharuskan host sumber untuk memecahkan pesan panjang menjadi potongan individual yang memenuhi persyaratan minimum dan ukuran maksimal. Pesan panjang akan dikirim dalam bingkai terpisah, dengan setiap bingkai berisi sepotong pesan asli. Setiap frame juga akan memiliki informasi pengalaman tersendiri. Di host penerima, masing-masing potongan pesan direkonstruksi menjadi pesan asli.

● WAKTU PESAN

Ada beberapa aturan dalam waktu pengiriman pesan:

- ✓ Metode Akses

Metode akses menentukan kapan seseorang bisa mengirim pesan. Jika dua orang berbicara pada saat bersamaan, terjadi tabrakan informasi dan perlu bagi keduanya untuk mundur dan memulai lagi. Demikian juga, komputer perlu menentukan metode akses. Host pada jaringan memerlukan metode akses untuk mengetahui kapan harus mulai mengirim pesan dan bagaimana merespons saat terjadi kesalahan.

- ✓ *Flow Control*

Waktu juga mempengaruhi berapa banyak informasi yang bisa dikirim dan kecepatan pengirimannya. Jika seseorang berbicara terlalu cepat, sulit bagi orang lain untuk mendengar dan memahami pesannya. Dalam komunikasi jaringan, sumber dan host tujuan menggunakan metode pengendalian arus untuk menegosiasikan waktu yang tepat untuk komunikasi yang berhasil.

- ✓ *Response Timeout*

Jika seseorang mengajukan pertanyaan dan tidak mendengar tanggapan dalam jumlah waktu yang dapat diterima, orang tersebut beranggapan bahwa tidak ada jawaban yang masuk dan bereaksi sesuai. Orang tersebut dapat mengulangi pertanyaan tersebut, atau mungkin terus melanjutkan percakapan. Host di jaringan juga memiliki aturan yang menentukan berapa lama menunggu tanggapan dan tindakan apa yang harus diambil jika timeout respon terjadi.

- **PILIHAN PENGIRIMAN PESAN**

Sebuah pesan dapat disampaikan dengan cara yang berbeda. Kadang-kadang, seseorang ingin mengkomunikasikan informasi kepada satu individu. Di lain waktu, orang tersebut mungkin perlu mengirimkan informasi kepada sekelompok orang pada saat bersamaan, atau bahkan untuk semua orang di wilayah yang sama.

Ada juga saat pengirim pesan perlu memastikan bahwa pesan berhasil dikirim ke tempat tujuan. Dalam kasus ini, penerima harus mengembalikan pengakuan kepada pengirim. Jika tidak ada pengakuan, opsi pengiriman disebut tidak diakui.

Host di jaringan menggunakan opsi pengiriman serupa untuk berkomunikasi.

Pilihan pengiriman satu-ke-satu disebut sebagai ***unicast***, yang berarti hanya ada satu tujuan untuk pesan tersebut.

Bila sebuah host perlu mengirim pesan menggunakan opsi pengiriman satu-ke-banyak, ini disebut sebagai ***multicast***. ***Multicasting*** adalah pengiriman pesan yang sama ke sekelompok tujuan host secara bersamaan.

Jika semua host di jaringan perlu menerima pesan pada saat bersamaan dimakan dengan ***Broadcast***. *Broadcast* mewakili opsi pengiriman pesan satu-ke-semua. Beberapa protokol menggunakan pesan *multicast* khusus yang dikirim ke semua perangkat, sehingga pada dasarnya sama dengan *Broadcast*. Selain itu, host mungkin diminta untuk mengakui penerimaan beberapa pesan sambil tidak perlu mengakui orang lain.

- ❖ **PROTOKOL JARINGAN DAN STANDARD**

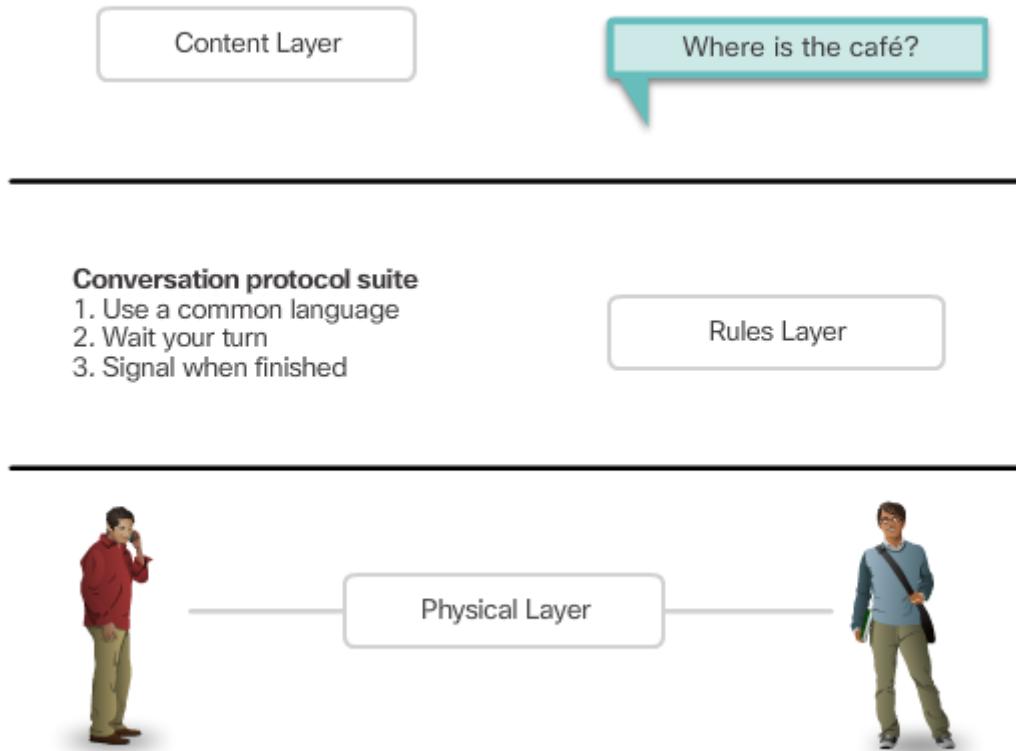
- **ATURAN YANG MENGATUR KOMUNIKASI**

Sekelompok protokol yang saling terkait yang diperlukan untuk melakukan fungsi komunikasi disebut ***protocol suite***. *Protocol suite* diimplementasikan oleh *host* dan perangkat jaringan di perangkat lunak, perangkat keras atau keduanya.

Salah satu cara terbaik untuk memvisualisasikan bagaimana protokol dalam sebuah suite berinteraksi adalah dengan melihat interaksi sebagai tumpukan. Tumpukan protokol menunjukkan bagaimana masing-masing protokol dalam sebuah suite diimplementasikan. Protokol dilihat dari segi lapisan, dengan masing-masing layanan tingkat lebih tinggi tergantung pada fungsionalitas yang ditentukan oleh protokol yang ditunjukkan pada tingkat yang lebih rendah. Lapisan bawah tumpukan berkaitan dengan pemindahan data melalui jaringan dan memberikan layanan ke lapisan atas, yang difokuskan pada isi pesan yang sedang dikirim.

Seperti yang ditunjukkan oleh gambar, kita dapat menggunakan lapisan untuk menggambarkan aktivitas yang terjadi dalam contoh komunikasi tatap muka. Di bagian bawah, lapisan fisik, kita memiliki dua orang, masing-masing dengan suara yang bisa mengucapkan kata-kata dengan lantang. Di tengah, lapisan aturan, kita memiliki kesepakatan untuk berbicara dalam bahasa yang sama. Di bagian atas, lapisan konten, ada kata-kata yang benar-benar diucapkan. Ini adalah isi dari komunikasi

Protocol Suite



Protocol suites are sets of rules that work together to help solve a problem.

• PROTOKOL JARINGAN

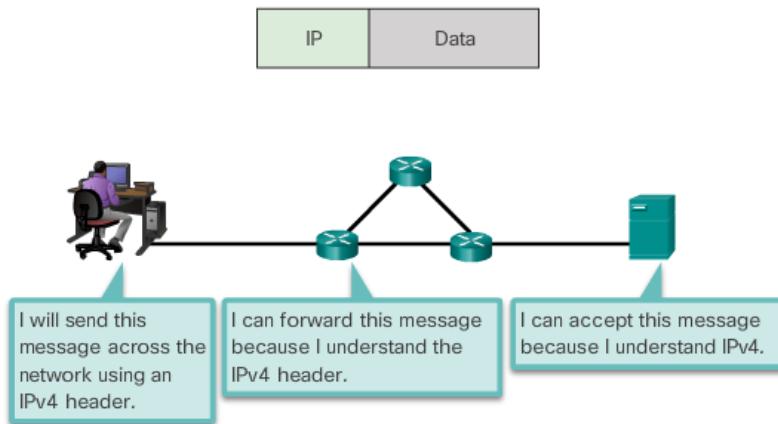
Pada tingkat manusia, beberapa peraturan komunikasi bersifat formal dan yang lainnya hanya dipahami berdasarkan kebiasaan dan praktik. Agar perangkat berhasil berkomunikasi, suite protokol jaringan harus menjelaskan persyaratan dan interaksi yang tepat. Protokol jaringan mendefinisikan format umum dan serangkaian aturan untuk bertukar pesan antar perangkat. Beberapa protokol jaringan yang umum adalah Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP), dan Internet Protocol (IP).

Catatan: IP dalam kursus ini mengacu pada protokol IPv4 dan IPv6. IPv6 adalah versi IP terbaru dan pengganti untuk IPv4 yang lebih umum.

protokol jaringan yang menggambarkan proses berikut:

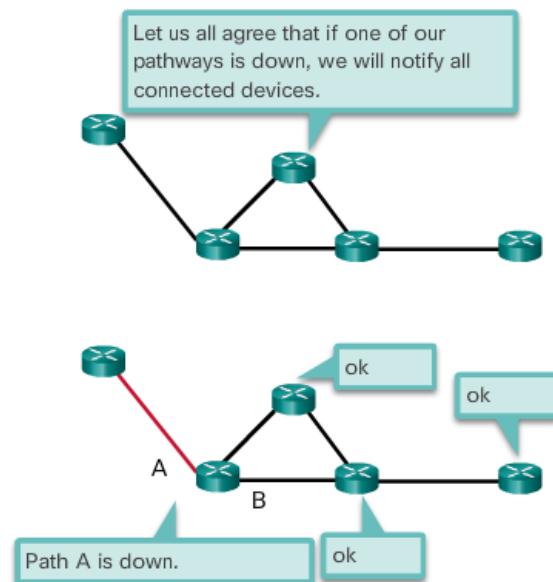
- ✓ Bagaimana pesan diformat atau terstruktur

The Role of Protocols



- ✓ Proses dimana perangkat jaringan berbagi informasi dan jalur dengan jaringan lain

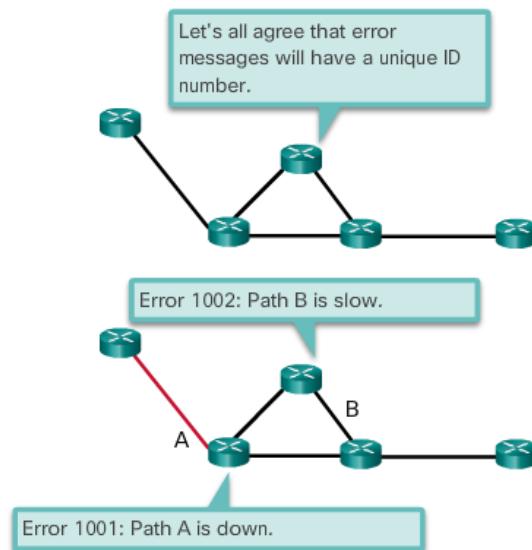
The Role of Protocols



The process by which networking devices share information about pathways to other networks

- ✓ Bagaimana dan kapan pesan kesalahan dan sistem dilewati antar perangkat

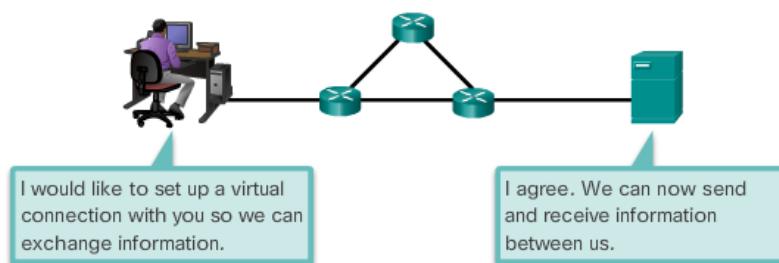
The Role of Protocols



How and when error and system messages are passed between devices

- ✓ Pengaturan dan penghentian sesi transfer data

The Role of Protocols



• INTERAKSI PROTOKOL

Komunikasi antara web server dan web client adalah contoh interaksi antara beberapa protokol. Protokol tersebut meliputi

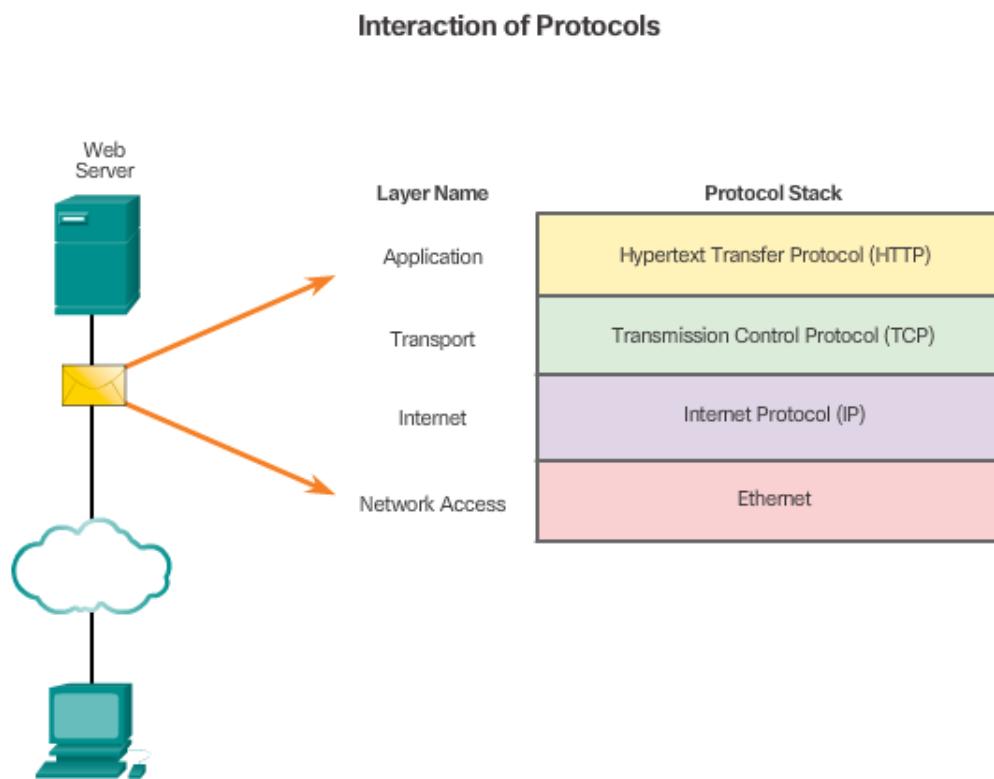
HTTP - adalah protokol aplikasi yang mengatur cara server web dan klien web berinteraksi. HTTP mendefinisikan konten dan format permintaan dan tanggapan yang dipertukarkan antara klien dan server. Baik klien dan perangkat lunak server web menerapkan HTTP sebagai bagian dari aplikasi. HTTP bergantung pada protokol lain untuk mengatur bagaimana pesan dikirim antara klien dan server.

TCP - adalah protokol transport yang mengelola percakapan individual. TCP membagi pesan HTTP menjadi beberapa bagian kecil, disebut segmen. Segmen ini dikirim antara server web

dan proses klien yang berjalan di host tujuan. TCP juga bertanggung jawab untuk mengendalikan ukuran dan tingkat di mana pesan dipertukarkan antara server dan klien.

IP - bertanggung jawab untuk mengambil segmen yang diformat dari TCP, mengenkapsulasi mereka ke dalam paket, menugaskan mereka alamat yang sesuai, dan mengantarkannya ke host tujuan.

Ethernet - adalah protokol akses jaringan yang menjelaskan dua fungsi utama: komunikasi melalui link data dan transmisi fisik data pada media jaringan. Protokol akses jaringan bertanggung jawab untuk mengambil paket dari IP dan memformatnya agar dikirim melalui media.



- **STANDART PROTOKOL DAN STANDART INDUSTRI**

Suite protokol adalah seperangkat protokol yang bekerja sama untuk menyediakan layanan komunikasi jaringan yang komprehensif. Sebuah suite protokol dapat ditentukan oleh organisasi standar atau dikembangkan oleh vendor. Protokol suite pada gambar, dapat sedikit berlebihan. Namun, buku ini hanya akan mencakup protokol dari paket protokol TCP / IP.

Protokol TCP / IP adalah standar terbuka, yang berarti protokol ini tersedia secara bebas untuk umum, dan setiap vendor dapat menerapkan protokol ini pada perangkat keras atau perangkat lunak mereka.

Protokol berbasis standar adalah proses yang telah disahkan oleh industri jaringan dan disetujui oleh organisasi standar. Penggunaan standar dalam mengembangkan dan menerapkan protokol memastikan bahwa produk dari berbagai produsen dapat saling

beroperasi dengan sukses. Jika sebuah protokol tidak diawasi secara ketat oleh produsen tertentu, peralatan atau perangkat lunak mereka mungkin tidak dapat berhasil berkomunikasi dengan produk yang dibuat oleh produsen lain.

Beberapa protokol bersifat proprietary yang berarti satu perusahaan atau vendor mengendalikan definisi protokol dan fungsinya. Contoh protokol proprietary adalah AppleTalk dan Novell Netware, yang merupakan suite protokol lawas. Hal ini tidak biasa bagi vendor (atau kelompok vendor) untuk mengembangkan protokol berpemilik untuk memenuhi kebutuhan pelanggannya dan kemudian membantu membuat protokol berpemilik itu menjadi standar terbuka.

Protocol Suites and Industry Standards

Layer Name	TCP/IP	ISO	AppleTalk	Novell Netware
Application	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transport	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Network Access	Ethernet PPP Frame Relay		ATM WLAN	

- **PERKEMBANGAN TCP/IP**

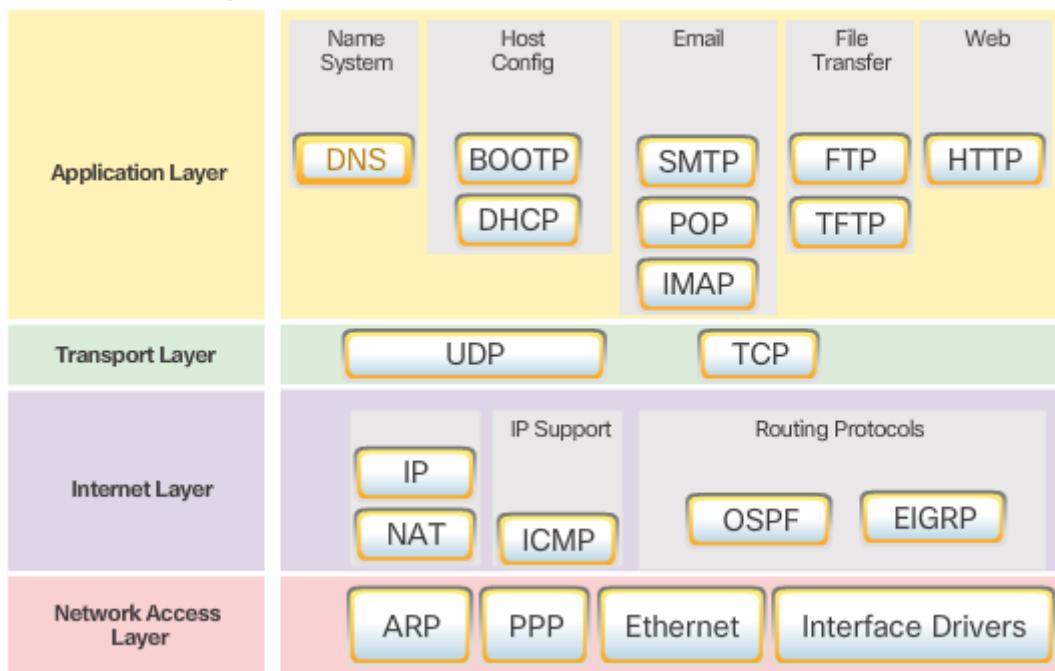
Jaringan peralihan paket pertama dan pendahulunya ke Internet saat ini adalah Advanced Research Projects Agency Network (ARPANET), yang mulai hidup pada tahun 1969 dengan menghubungkan komputer mainframe di empat lokasi. ARPANET didanai oleh Departemen Pertahanan A.S. untuk digunakan oleh universitas dan laboratorium penelitian.

- **TCP/ IP PROTOKOL SUITE**

paket protokol TCP / IP mencakup banyak protokol. Protokol individu diatur secara berlapis dengan menggunakan model protokol TCP / IP: Lapisan Aplikasi, Transport, Internet, dan Network Access. Protokol TCP / IP khusus untuk lapisan Aplikasi, Transportasi, dan Internet. Protokol lapisan akses jaringan bertanggung jawab untuk mengirimkan paket IP melalui medium fisik. Protokol lapisan bawah ini dikembangkan oleh berbagai standar organisasi.

Protokol TCP / IP diimplementasikan sebagai tumpukan TCP / IP pada host pengirim dan penerima untuk menyediakan pengiriman aplikasi melalui jaringan secara end-to-end. Protokol Ethernet digunakan untuk mentransmisikan paket IP melalui medium fisik yang digunakan oleh LAN.

TCP/IP Protocol Suite and Communication Process



- ✓ **DNS** (Domain Name System / Service); menerjemahkan nama domain, seperti cisco.com, ke alamat IP
- ✓ **BOOTP** (Bootstrap Protocol); Memungkinkan workstation diskless untuk menemukan alamat IP-nya sendiri, alamat IP dari server BOOTP di jaringan, dan file yang akan dimasukkan ke memori untuk booting mesin.
- ✓ **DHCP** (Dynamic Host Configuration Protocol); Dinamis menugaskan alamat IP ke stasiun klien saat start-up , Memungkinkan alamat digunakan kembali bila tidak lagi dibutuhkan
- ✓ **SMTP** (Simple Mail Transfer Protocol); Memungkinkan klien untuk mengirim email ke server surat, Mengaktifkan server untuk mengirim email ke server lain.
- ✓ **POP** (Post Office Protocol version 3 /POP 3); Memungkinkan klien untuk mengambil email dari server surat, Download email dari server surat ke desktop
- ✓ **IMAP** (Internet Message Access Protocol); Memungkinkan klien mengakses email yang tersimpan di server surat, Menjaga email di server.
- ✓ **FTP**(File Transfer Protocol); Menetapkan aturan yang memungkinkan pengguna di satu host mengakses dan mentransfer file ke dan dari host lain melalui jaringan, Protokol pengiriman file yang andal, berorientasi koneksi, dan diakui

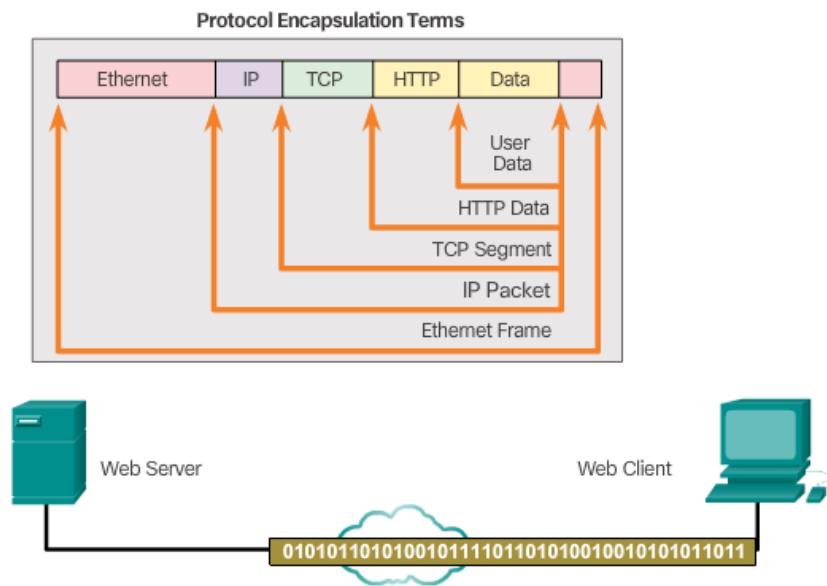
- ✓ **TFTP** (Trivial File Transfer Protocol); Sebuah protokol transfer file tanpa koneksi yang sederhana, Protokol pengiriman file best-effort, tidak diakui, Menggunakan lebih sedikit overhead daripada FTP
- ✓ **HTTP** (Hypertext Transfer Protocol); Kumpulan aturan untuk bertukar teks, gambar grafis, suara, video, dan file multimedia lainnya di World Wide Web
- ✓ **UDP** (User Diagram Protocol); Mengaktifkan proses yang berjalan pada satu host untuk mengirim paket ke sebuah proses yang berjalan pada host lain, Tidak mengkonfirmasi transmisi datagram yang berhasil
- ✓ **TCP** (Transmission Control Protocol); Mengaktifkan komunikasi yang handal antara proses yang berjalan pada host yang terpisah, Transmisi yang andal dan diakui yang mengkonfirmasi pengiriman yang berhasil
- ✓ **IP** (Internet Protocol); Menerima segmen pesan dari lapisan transport, Paket pesan ke dalam paket, Alamat paket untuk pengiriman end-to-end melalui Internetwork
- ✓ **NAT** (Network Address Translation); Menerjemahkan alamat IP dari jaringan pribadi ke dalam alamat IP publik global yang unik
- ✓ **ICMP** (Internet Control Message Protocol); Menyediakan umpan balik dari host tujuan ke host sumber tentang kesalahan dalam pengiriman paket
- ✓ **OSPF** (Open Shortest Path First); Link-state routing protocol, Desain hierarkis berdasarkan daerah, Buka protokol routing interior standar
- ✓ **EIGRP** (Enhanced Interior Gateway Routing Protocol); Protokol routing berpemilik Cisco, Menggunakan metrik komposit berdasarkan bandwidth, delay, load dan reliability
- ✓ **ARP** (Address Resolution Protocol); Menyediakan pemetaan alamat dinamis antara alamat IP dan alamat perangkat keras
- ✓ **PPP** (Point – to- point Protocol); Menyediakan sarana mengenkapsulasi paket untuk transmisi melalui tautan serial
- ✓ **Ethernet**; Mendefinisikan aturan untuk pengkabelan dan standar pemberian sinyal pada lapisan akses jaringan
- ✓ **Interface Driver**; Memberikan instruksi pada mesin untuk mengendalikan antarmuka tertentu pada perangkat jaringan

- **TCP/ IP PROSES KOMUNIKASI**

proses komunikasi yang lengkap dengan menggunakan contoh server web yang mengirimkan data ke klien.

1. Pengiriman dimulai dengan server web yang menyiapkan halaman Hypertext Markup Language (HTML) sebagai data yang akan dikirim.
2. Protokol HTTP header aplikasi ditambahkan ke bagian depan data HTML. Header berisi berbagai informasi, termasuk versi HTTP yang digunakan server dan kode status yang menunjukkan bahwa ia memiliki informasi untuk klien web.
3. Protokol lapisan aplikasi HTTP mengirimkan data halaman HTML berformat HTML ke lapisan transport. Protokol lapisan transport TCP digunakan untuk mengelola percakapan individual, dalam contoh ini antara web server dan web client.

4. Selanjutnya, informasi IP ditambahkan ke bagian depan informasi TCP. IP menetapkan alamat IP sumber dan tujuan yang sesuai. Informasi ini dikenal sebagai paket IP.
5. Protokol Ethernet menambahkan informasi ke kedua ujung paket IP, yang dikenal sebagai bingkai data link. Frame ini dikirim ke router terdekat sepanjang jalan menuju web client. Router ini menghapus informasi Ethernet, menganalisis paket IP, menentukan jalur terbaik untuk paket, memasukkan paket ke dalam bingkai baru, dan mengirimkannya ke router tetangga berikutnya menuju tujuan. Setiap router menghapus dan menambahkan informasi link data baru sebelum meneruskan paket.
6. Data ini sekarang diangkut melalui internetwork, yang terdiri dari media dan perangkat perantara.
7. Penerima dimulai dengan klien menerima frame data link yang berisi data. Setiap header protokol diproses dan kemudian dihapus dengan urutan berlawanan yang ditambahkan. Informasi Ethernet diproses dan dihapus, diikuti oleh informasi protokol IP, informasi TCP, dan akhirnya informasi HTTP.
8. Informasi halaman web kemudian diteruskan ke perangkat lunak browser web klien.



• STANDART TERBUKA

Standar terbuka mendorong interoperabilitas, persaingan, dan inovasi. Mereka juga menjamin bahwa tidak ada produk satu perusahaan yang dapat memonopoli pasar, atau memiliki keuntungan yang tidak adil atas persaingannya.

Contoh bagusnya adalah saat membeli router nirkabel untuk rumah. Ada banyak pilihan berbeda yang tersedia dari berbagai vendor, yang semuanya menggabungkan protokol standar seperti IPv4, DHCP, 802.3 (Ethernet), dan 802.11 (LAN Nirkabel). Standar terbuka ini juga memungkinkan klien menjalankan sistem operasi Apple OS X untuk mendownload halaman web dari server web yang menjalankan sistem operasi Linux. Ini karena kedua sistem operasi menerapkan protokol standar terbuka, seperti protokol TCP / IP.

Organisasi standar penting dalam menjaga Internet terbuka dengan spesifikasi dan protokol yang dapat diakses secara bebas yang dapat diterapkan oleh vendor manapun. Organisasi standar mungkin merancang seperangkat peraturan sepenuhnya sendiri atau dalam kasus lain dapat memilih protokol berpemilik sebagai dasar standar. Jika protokol berpemilik digunakan, biasanya melibatkan vendor yang membuat protokol.

Organisasi standar biasanya merupakan organisasi netral dan non-profit vendor yang dibentuk untuk mengembangkan dan mempromosikan konsep standar terbuka.

- **STANDART INTERNET**

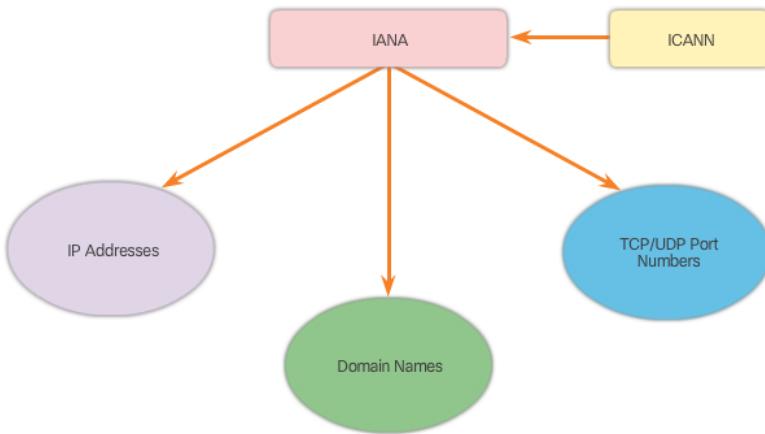
Organisasi standar biasanya adalah institusi netral dan non-profit vendor yang dibentuk untuk mengembangkan dan mempromosikan konsep standar terbuka. Berbagai organisasi memiliki tanggung jawab yang berbeda untuk mempromosikan dan menciptakan standar untuk protokol TCP / IP.

Organisasi standar meliputi:

- ✓ Internet Society (ISOC) - Bertanggung jawab untuk mempromosikan pengembangan terbuka dan evolusi penggunaan Internet di seluruh dunia.
- ✓ Internet Architecture Board (IAB) - Bertanggung jawab atas keseluruhan pengelolaan dan pengembangan standar Internet.
- ✓ Internet Engineering Task Force (IETF) - Mengembangkan, memperbarui, dan memelihara teknologi Internet dan TCP / IP. Ini termasuk proses dan dokumen untuk mengembangkan protokol baru dan memperbarui protokol yang ada yang dikenal sebagai dokumen Permintaan untuk Komentar (RFC).
- ✓ Internet Research Task Force (IRTF) - Berfokus pada penelitian jangka panjang yang berkaitan dengan protokol Internet dan TCP / IP seperti Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), dan Peer-to-Peer Research Group (P2PRG).

Organisasi standar meliputi:

- ✓ Internet Corporation untuk Ditugaskan Nama dan Nomor (ICANN) - Berbasis di Amerika Serikat, koordinat alokasi alamat IP, pengelolaan nama domain, dan penugasan informasi lainnya menggunakan protokol TCP / IP.
- ✓ Internet Assigned Numbers Authority (IANA) - Bertanggung jawab untuk mengawasi dan mengelola alokasi alamat IP, pengelolaan nama domain, dan pengidentifikasi protokol untuk ICANN.



- **STANDART ORGANISASI KOMUNIKASI DAN ELEKTRONIK**

Organisasi standar lainnya memiliki tanggung jawab untuk mempromosikan dan menciptakan standar elektronik dan komunikasi yang digunakan untuk menyampaikan paket IP sebagai sinyal elektronik melalui media kabel atau nirkabel.

Institute of Electrical and Electronics Engineers (IEEE, diucapkan "I-triple-E") - Organisasi teknik elektro dan elektronika yang didedikasikan untuk memajukan inovasi teknologi dan menciptakan standar di berbagai bidang industri termasuk energi dan energi, kesehatan, telekomunikasi, dan jaringan.

Electronic Industries Alliance (EIA) - Paling terkenal dengan standar yang berkaitan dengan kabel listrik, konektor, dan rak 19 inci yang digunakan untuk memasang peralatan jaringan.

Asosiasi Industri Telekomunikasi (TIA) - Bertanggung jawab untuk mengembangkan standar komunikasi di berbagai bidang termasuk peralatan radio, menara seluler, perangkat Voice over IP (VoIP), komunikasi satelit, dan banyak lagi.

Sektor Standardisasi Telekomunikasi-Telekomunikasi Internasional (ITU-T) - Salah satu organisasi standar komunikasi tertua dan tertua. ITU-T mendefinisikan standar untuk kompresi video, Internet Protocol Television (IPTV), dan komunikasi broadband, seperti jalur pelanggan digital (DSL).

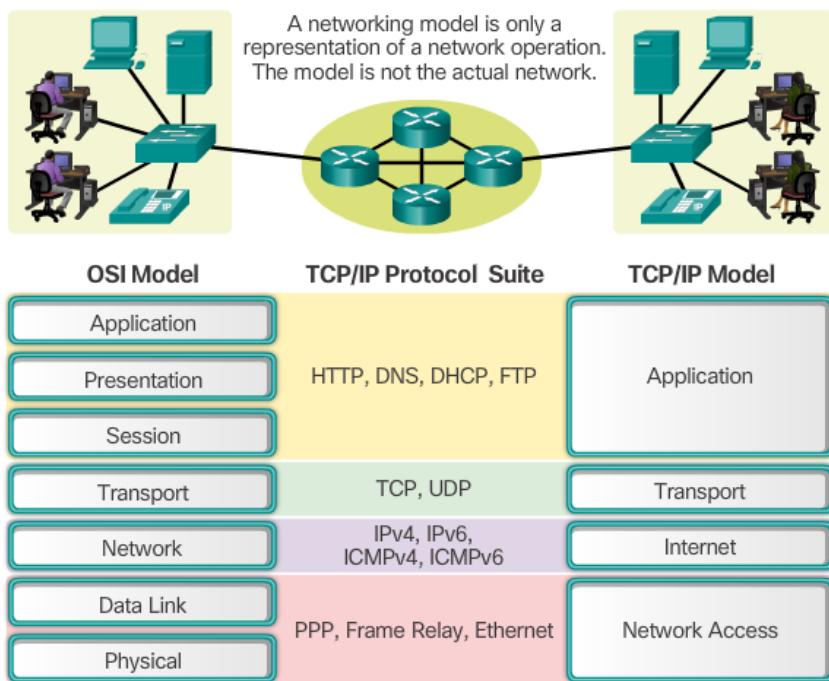
- **KEUNTUNGAN MENGGUNAKAN LAYERED MODEL**

Manfaat menggunakan model berlapis untuk menggambarkan protokol jaringan dan operasi meliputi:

- ✓ Membantu dalam desain protokol karena protokol yang beroperasi pada lapisan tertentu telah menentukan informasi yang mereka lakukan dan antarmuka yang didefinisikan ke lapisan di atas dan di bawahnya.
- ✓ Membina persaingan karena produk dari vendor yang berbeda dapat bekerja sama.
- ✓ Mencegah perubahan teknologi atau kemampuan dalam satu lapisan mempengaruhi lapisan lainnya di atas dan di bawahnya.
- ✓ Menyediakan bahasa yang umum untuk menggambarkan fungsi dan kemampuan jaringan.

Model TCP / IP dan model Open System Interconnection (OSI) adalah model utama yang digunakan saat membahas fungsionalitas jaringan. Masing-masing mewakili tipe dasar dari model jaringan berlapis:

- ✓ **Model Protokol** - Jenis model ini sangat sesuai dengan struktur dari paket protokol tertentu. Model TCP / IP adalah model protokol karena menggambarkan fungsi yang terjadi pada setiap lapisan protokol di dalam paket TCP / IP. TCP / IP juga digunakan sebagai model referensi.
- ✓ **Model referensi** - Jenis model ini memberikan konsistensi dalam semua jenis protokol dan layanan jaringan dengan menjelaskan apa yang harus dilakukan pada lapisan tertentu, namun tidak memberikan resep bagaimana hal itu harus dilakukan. Model OSI adalah model referensi internetwork yang banyak dikenal, namun juga merupakan model protokol untuk suite protokol OSI.



• MODEL REFERENSI OSI

Model OSI menyediakan daftar fungsi dan layanan yang ekstensif yang dapat terjadi pada setiap lapisan. Ini juga menggambarkan interaksi setiap lapisan dengan lapisan tepat di atas dan di bawahnya. Protokol TCP / IP disusun di seputar model OSI dan TCP / IP.

Catatan: lapisan model TCP / IP hanya mengacu pada nama, tujuh lapisan model OSI lebih sering disebut dengan nomor dan bukan berdasarkan nama. Misalnya, lapisan fisik disebut sebagai Layer 1 dari model OSI.

OSI MODEL;

7. **APPLICATION**; Lapisan aplikasi berisi protokol yang digunakan untuk komunikasi proses-ke-proses.

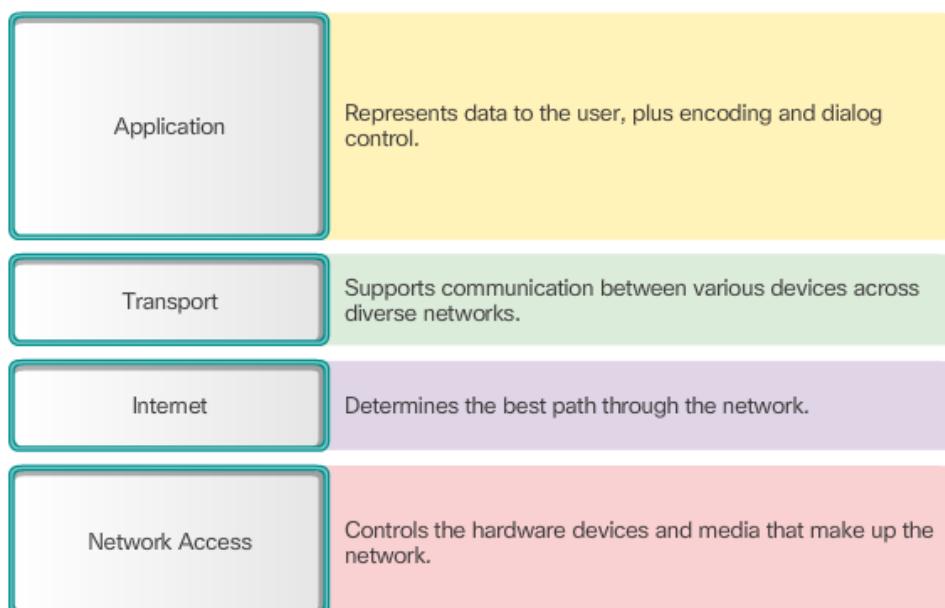
6. **Presentation**; Lapisan presentasi menyediakan representasi umum dari data yang ditransfer antara layanan lapisan aplikasi.
5. **SESSION**; Lapisan sesi memberikan layanan ke lapisan presentasi untuk mengatur dialognya dan mengelola pertukaran data.
4. **TRANSPORT**; Lapisan transport mendefinisikan layanan untuk mengelompokkan, mentransfer, dan memasang kembali data untuk komunikasi individual di antara perangkat akhir.
3. **NETWORK**; Lapisan jaringan menyediakan layanan untuk menukar potongan data individual melalui jaringan antara perangkat akhir yang teridentifikasi.
2. **DATA LINK**; Protokol lapisan data link menjelaskan metode untuk menukar frame data antar perangkat melalui media umum.
1. **PHYSICAL**; Protokol lapisan fisik menggambarkan sarana mekanis, elektrikal, fungsional, dan prosedural untuk mengaktifkan, memelihara, dan menonaktifkan koneksi fisik untuk transmisi bit ke dan dari perangkat jaringan.

- **TCP/IP PROTOCOL MODEL**

Model protokol TCP / IP untuk komunikasi internetwork dibuat pada awal tahun 1970an dan kadang-kadang disebut sebagai model Internet. Seperti yang ditunjukkan pada gambar, ia mendefinisikan empat kategori fungsi yang harus terjadi agar komunikasi menjadi sukses. Arsitektur dari paket protokol TCP / IP mengikuti struktur model ini. Karena itu, model internet biasa disebut sebagai **model TCP / IP**.

Sebagian besar model protokol menggambarkan tumpukan protokol khusus vendor. Suite protokol lawas, seperti Novell Netware dan AppleTalk, adalah contoh tumpukan protokol khusus vendor. Karena model TCP / IP adalah standar terbuka, satu perusahaan tidak mengendalikan definisi model. Definisi standar dan protokol TCP / IP dibahas dalam forum publik dan didefinisikan dalam rangkaian RFC yang tersedia untuk umum.

TCP/IP Model



- **PERBANDINGAN OSI MODEL DAN TCP / IP MODEL**

Protokol yang membentuk paket protokol TCP / IP juga dapat dijelaskan berdasarkan model referensi OSI. Dalam model OSI, lapisan akses jaringan dan lapisan aplikasi dari model TCP / IP dibagi lagi untuk menggambarkan fungsi diskrit yang harus terjadi pada lapisan ini.

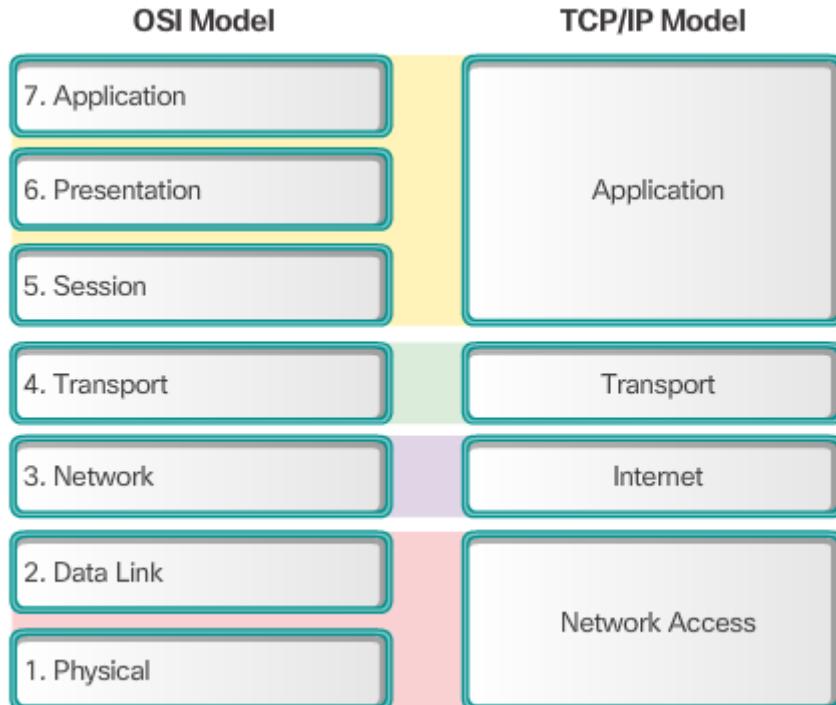
Pada lapisan akses jaringan, suite protokol TCP / IP tidak menentukan protokol mana yang akan digunakan saat mentransmisikan media fisik; itu hanya menggambarkan handoff dari lapisan internet ke protokol jaringan fisik. Lapisan OSI 1 dan 2 membahas prosedur yang diperlukan untuk mengakses media dan sarana fisik untuk mengirim data melalui jaringan.

OSI Layer 3, lapisan jaringan, memetakan langsung ke lapisan Internet TCP / IP. Lapisan ini digunakan untuk menggambarkan protokol yang menangani dan mengarahkan pesan melalui internetwork.

OSI Layer 4, lapisan transport, memetakan langsung ke lapisan Transport TCP / IP. Lapisan ini menjelaskan layanan umum dan fungsi yang menyediakan pengiriman data yang teratur dan dapat diandalkan antara sumber dan host tujuan.

Lapisan aplikasi TCP / IP mencakup sejumlah protokol yang menyediakan fungsionalitas spesifik untuk berbagai aplikasi pengguna akhir. Model OSI Layers 5, 6, dan 7 digunakan sebagai referensi bagi pengembang perangkat lunak aplikasi dan vendor untuk menghasilkan produk yang beroperasi pada jaringan.

Kedua model TCP / IP dan OSI biasa digunakan saat mengacu pada protokol pada berbagai lapisan. Karena model OSI memisahkan lapisan data link dari lapisan fisik, biasanya digunakan saat mengacu pada lapisan bawah ini.



❖ PENGIRIMAN DATA DIDALAM JARINGAN

• SEGMENTASI PESAN

Secara teori, satu komunikasi, seperti video musik atau pesan email, dapat dikirim melalui jaringan dari sumber ke tujuan sebagai satu arus bit yang tidak terputus. Jika pesan benar-benar dikirim dengan cara ini, itu berarti tidak ada perangkat lain yang dapat mengirim atau menerima pesan di jaringan yang sama saat pengiriman data ini berlangsung. Aliran data yang besar ini akan mengakibatkan penundaan yang signifikan. Selanjutnya, jika link di infrastruktur jaringan yang saling berhubungan gagal selama pengiriman, pesan lengkap akan hilang dan harus dipancarkan ulang secara penuh.

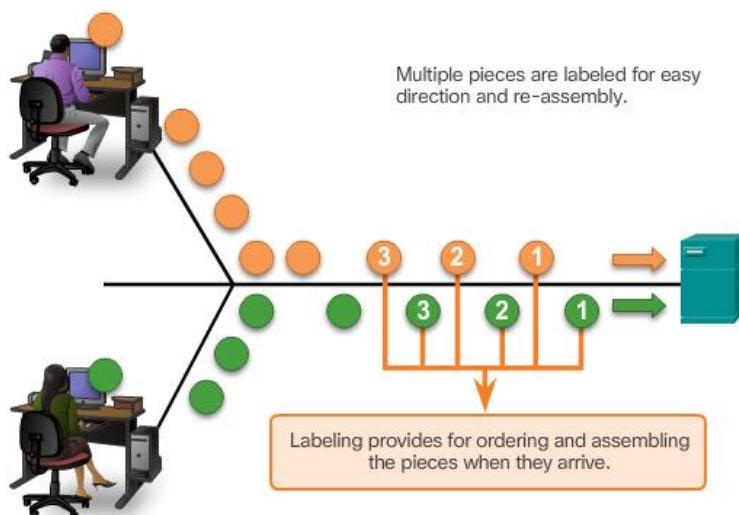
Pendekatan yang lebih baik adalah membagi data menjadi potongan yang lebih kecil dan mudah diatur untuk dikirim melalui jaringan. Pembagian arus data ini menjadi potongan yang lebih kecil disebut **segmentasi**. Menyegmentasikan pesan memiliki dua manfaat utama:

- ✓ Dengan mengirimkan potongan individu yang lebih kecil dari sumber ke tujuan, banyak percakapan yang berbeda dapat disisipkan pada jaringan, yang disebut **multiplexing**.
- ✓ Segmentasi dapat meningkatkan efisiensi komunikasi jaringan. Jika bagian dari pesan gagal sampai ke tujuan, karena kegagalan jaringan atau kemacetan jaringan, hanya bagian yang hilang yang perlu dipancarkan ulang.

Tantangan untuk menggunakan segmentasi dan multiplexing untuk mentransmisikan pesan ke jaringan adalah tingkat kerumitan yang ditambahkan ke prosesnya. Bayangkan jika Anda harus mengirim surat setebal 100 halaman, namun masing-masing amplop hanya akan menyimpan satu halaman. Proses pengalamatan, pelabelan, pengiriman, penerimaan, dan pembukaan keseluruhan 100 amplop akan menyita waktu bagi pengirim dan penerima.

Dalam komunikasi jaringan, setiap segmen pesan harus melalui proses yang serupa untuk memastikannya mencapai tujuan yang benar dan dapat disusun kembali ke isi pesan asli.

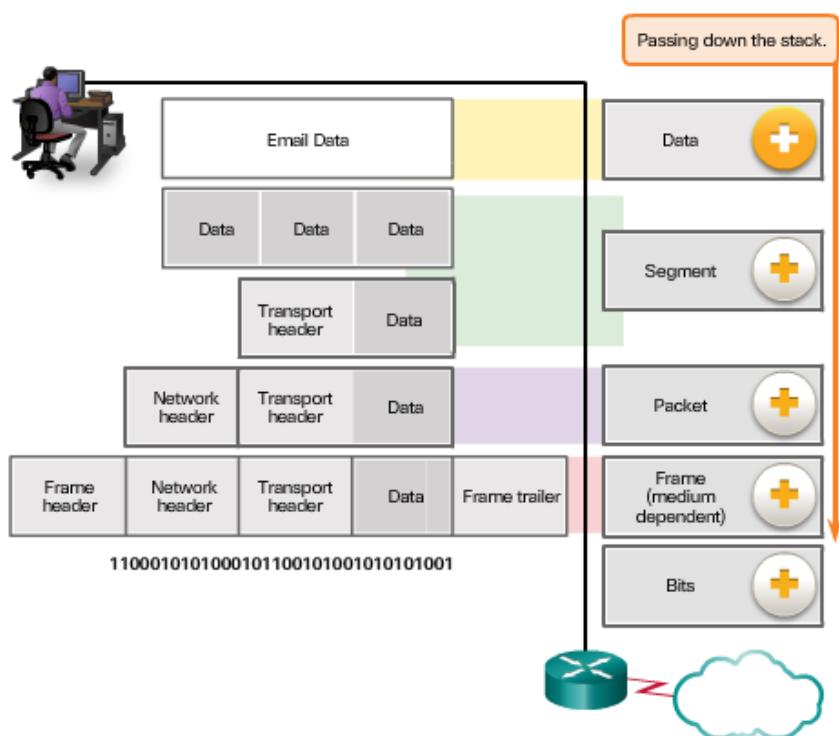
Communicating the Message



- **PROTOCOL DATA UNIT**

Sebagai data aplikasi diturunkan stack protokol pada cara untuk dikirim melalui media jaringan, berbagai informasi protokol ditambahkan pada setiap tingkat. Ini dikenal sebagai proses **enkapsulasi**.

Bentuk yang sepotong data mengambil pada lapisan apapun disebut unit data protokol (PDU). Selama enkapsulasi, masing-masing lapisan berhasil mengenkapsulasi PDU yang diterimanya dari lapisan di atas sesuai dengan protokol yang digunakan. Pada setiap tahap proses, PDU memiliki nama yang berbeda untuk mencerminkan fungsinya yang baru. Meskipun tidak ada konvensi penamaan universal untuk PDU, dalam kursus ini, PDU diberi nama sesuai dengan protokol dari paket TCP / IP, seperti yang ditunjukkan pada gambar. Klik setiap PDU di gambar untuk informasi lebih lanjut



- ✓ **Data**; Istilah umum untuk PDU yang digunakan pada lapisan aplikasi
- ✓ **Segment**; Transport layer PDU
- ✓ **Packet**; Network layer PDU
- ✓ **Frame**; Data Link layer PDU
- ✓ **Bits**; Lapisan fisik PDU digunakan saat mentransmisikan data secara fisik melalui medium

- **CONTOH ENKAPSULASI**

Saat mengirim pesan di jaringan, proses enkapsulasi bekerja dari atas ke bawah. Pada setiap lapisan, informasi lapisan atas dianggap data dalam protokol yang dienkapsulasi. Misalnya, segmen TCP dianggap data dalam paket IP.

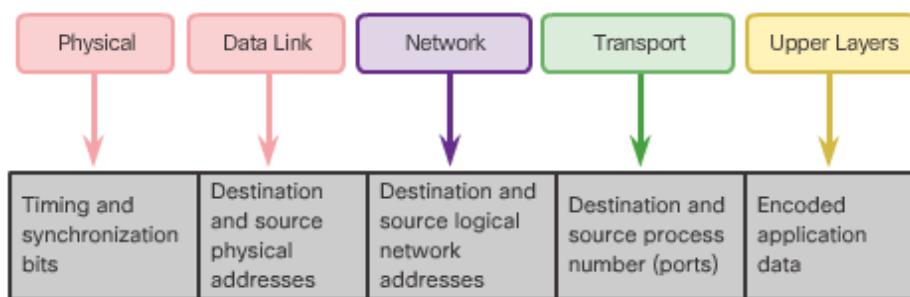
- **DE-ENKAPSULASI**

Proses ini dibalik pada host penerima, dan dikenal sebagai de-enkapsulasi. De-enkapsulasi adalah proses yang digunakan oleh perangkat penerima untuk menghapus satu atau lebih dari tajuk protokol. Data dienkapsulasi karena menggerakkan tumpukan ke arah aplikasi pengguna akhir.

- **ALAMAT JARINGAN**

Lapisan jaringan dan data link bertanggung jawab untuk mengirimkan data dari perangkat sumber ke perangkat tujuan. Protokol pada kedua lapisan berisi alamat sumber dan tujuan, namun alamat mereka memiliki tujuan yang berbeda.

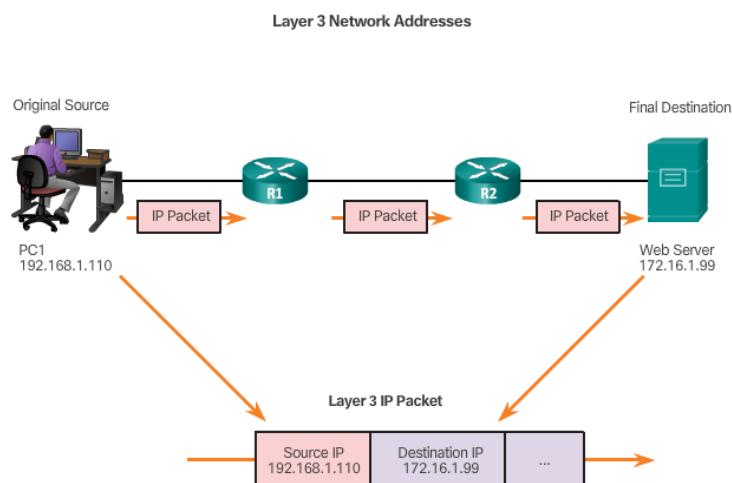
- ✓ **Network layer source and destination addresses** - Bertanggung jawab untuk mengirimkan paket IP dari sumber asli ke tujuan akhir, baik pada jaringan yang sama atau ke jaringan jarak jauh.
- ✓ **Data link layer source and destination addresses** - Bertanggung jawab untuk mengirimkan frame data dari satu kartu antarmuka jaringan (NIC) ke NIC lain pada jaringan yang sama.



Alamat IP adalah lapisan jaringan, atau Layer 3, alamat logis yang digunakan untuk mengirimkan paket IP dari sumber asli ke tujuan akhir.

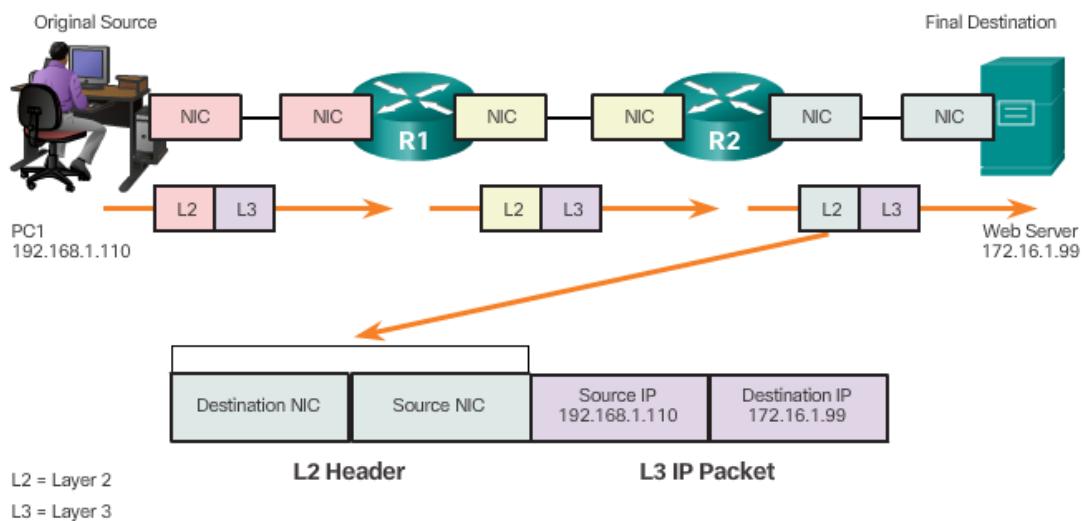
Paket IP berisi dua alamat IP:

- ✓ **Source IP address** - Alamat IP perangkat pengirim, sumber asli paket.
- ✓ **Destination IP address** - Alamat IP perangkat penerima, tujuan akhir paket.



- **ALAMAT DATALINK**

Data link, atau Layer 2, alamat fisik memiliki peran yang berbeda. Tujuan dari data link address adalah untuk memberikan data link frame dari satu interface jaringan ke interface jaringan lain pada jaringan yang sama.



Sebelum paket IP dapat dikirim melalui jaringan kabel atau nirkabel, paket tersebut harus dienkapsulasi dalam bingkai data sehingga dapat dikirim melalui medium fisik.

Karena paket IP berjalan dari host-to-router, router-to-router, dan akhirnya router-to-host, pada setiap titik di sepanjang paket IP dienkapsulasi dalam bingkai data link baru. Setiap frame data link berisi alamat link data sumber dari kartu NIC yang mengirimkan frame, dan alamat link data tujuan dari kartu NIC yang menerima frame.

Layer 2, protokol data link hanya digunakan untuk mengirimkan paket dari NIC-to-NIC ke jaringan yang sama. Router menghapus informasi Layer 2 seperti yang diterima pada satu NIC dan menambahkan informasi link data baru sebelum meneruskan keluarnya NIC dalam perjalanan menuju tujuan akhir.

Paket IP dienkapsulasi dalam bingkai data link yang berisi informasi link data, termasuk:

- ✓ **Source data link address** - Alamat fisik perangkat NIC yang mengirim bingkai data link.
- ✓ **Destination data link address** - Alamat fisik NIC yang menerima frame data link. Alamat ini adalah router hop berikutnya atau perangkat tujuan akhir.

- **PERANGKAT PADA JARINGAN YANG SAMA**

Untuk memahami bagaimana perangkat berkomunikasi dalam jaringan, penting untuk memahami peran kedua alamat lapisan jaringan dan alamat link data.

Peran dari Network Layer Addresses

Lapisan jaringan alamat, atau alamat IP, menunjukkan sumber asli dan tujuan akhir. Alamat IP berisi dua bagian:

- ✓ **Network portion** - Bagian paling kiri dari alamat yang menunjukkan jaringan mana alamat IP adalah anggota. Semua perangkat pada jaringan yang sama akan memiliki bagian alamat yang sama.
- ✓ **Host portion** - Sisa bagian dari alamat yang mengidentifikasi perangkat tertentu pada jaringan. Bagian host unik untuk setiap perangkat di jaringan

Catatan: Subnet mask digunakan untuk mengidentifikasi bagian jaringan dari sebuah alamat dari bagian host. Subnet mask dibahas di bab selanjutnya.

Dalam contoh ini kita memiliki komputer klien, PC1, berkomunikasi dengan server FTP pada jaringan IP yang sama.

- ✓ Source IP address - Alamat IP perangkat pengirim, komputer klien PC1: 192.168.1.110.
- ✓ Destination IP address - Alamat IP perangkat penerima, server FTP: 192.168.1.9.

Perhatikan pada gambar bahwa bagian jaringan dari kedua alamat IP sumber dan alamat tujuan IP berada pada jaringan yang sama

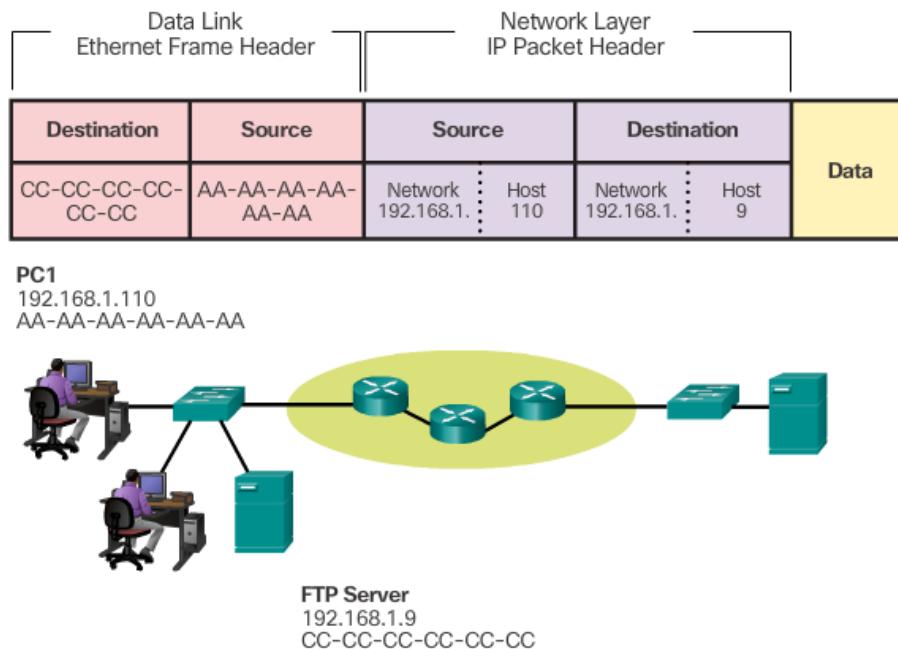
Peran Alamat Lapisan Data Link

Bila pengirim dan penerima paket IP berada pada jaringan yang sama, frame data link dikirim langsung ke perangkat penerima. Pada jaringan Ethernet, alamat data link dikenal sebagai alamat Ethernet (Media Access Control). Alamat MAC secara fisik tertanam pada NIC Ethernet.

- ✓ **Source MAC address** - Ini adalah alamat data link, atau alamat MAC Ethernet, dari perangkat yang mengirimkan bingkai data link dengan paket IP yang dienkapsulasi. Alamat MAC dari NIC Ethernet PC1 adalah AA-AA-AA-AA-AA-AA, yang ditulis dalam notasi heksadesimal.
- ✓ **Destination MAC address** - Bila perangkat penerima berada pada jaringan yang sama dengan perangkat pengirim, ini adalah alamat data dari perangkat penerima. Dalam contoh ini, alamat MAC tujuan adalah alamat MAC dari server FTP: CC-CC-CC-CC-CC-CC, ditulis dalam notasi heksadesimal.

Bingkai dengan paket IP yang dienkapsulasi sekarang dapat dikirim dari PC1 langsung ke server FTP.

Communicating with a Device on the Same Network



• PERANGKAT DI JARINGAN JARAK JAUH

Peran dari Network Layer Addresses

Ketika pengirim paket berada pada jaringan yang berbeda dari penerima, alamat IP sumber dan tujuan akan mewakili host pada jaringan yang berbeda. Ini akan ditunjukkan oleh bagian jaringan dari alamat IP host tujuan.

- ✓ Source IP address - Alamat IP perangkat pengirim, komputer klien PC1: 192.168.1.110.
- ✓ Destination IP address - Alamat IP perangkat penerima, server, Web Server: 172.16.1.99.

Peran Alamat Lapisan Data Link

Bila pengirim dan penerima paket IP berada pada jaringan yang berbeda, frame data link Ethernet tidak dapat dikirim langsung ke host tujuan karena host tidak dapat dijangkau secara langsung di jaringan pengirim. Frame Ethernet harus dikirim ke perangkat lain yang dikenal sebagai router atau gateway default. Dalam contoh kita, gateway default adalah R1. R1 memiliki link data Ethernet yang berada pada jaringan yang sama dengan PC1. Hal ini memungkinkan PC1 untuk mencapai router secara langsung.

- ✓ **Source MAC address** - Alamat MAC Ethernet dari perangkat pengirim, PC1. Alamat MAC dari antarmuka Ethernet PC1 adalah AA-AA-AA-AA-AA-AA
- ✓ **Destination MAC address** - Bila perangkat penerima, alamat IP tujuan, berada pada jaringan yang berbeda dari perangkat pengirim, perangkat pengirim menggunakan alamat MAC Ethernet dari gateway default atau router. Dalam contoh ini, alamat MAC tujuan adalah

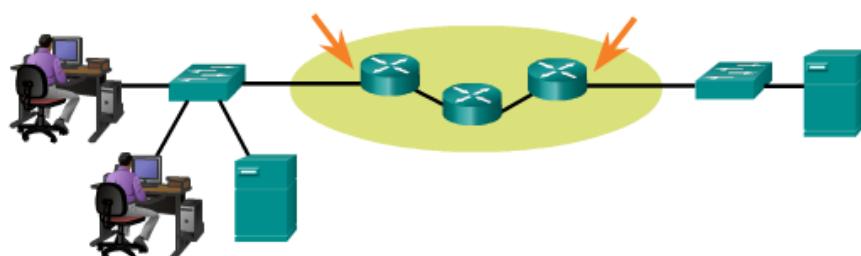
alamat MAC dari antarmuka Ethernet R1, 11-11-11-11-11-11. Ini adalah antarmuka yang terhubung ke jaringan yang sama dengan PC1.

Bingkai Ethernet dengan paket IP yang dienkapsulasi sekarang dapat dikirim ke R1. R1 meneruskan paket ke tujuan, Web Server. Ini mungkin berarti bahwa R1 meneruskan paket ke router lain atau langsung ke Web Server jika tujuan berada pada jaringan yang terhubung ke R1.

Adalah penting bahwa alamat IP dari gateway default dikonfigurasi pada setiap host di jaringan lokal. Semua paket ke tujuan pada jaringan jarak jauh dikirim ke gateway default. Alamat MAC Ethernet dan gateway default dibahas di bab selanjutnya.

Communicating with a Device on a Remote Network

Data Link Ethernet Frame Header		Network Layer IP Packet Header		
Destination	Source	Source	Destination	Data
11-11-11-11-11-11	AA-AA-AA-AA-AA-AA	Network 192.168.1.110	Device 110	Network 172.16.1.99
PC1 192.168.1.110 AA-AA-AA-AA-AA-AA	R1 192.168.1.1 11-11-11-11-11-11	R2 172.16.1.1 22-22-22-22-22-22	Device 99	Web Server 172.16.1.99 AB-CD-EF-12-34-56



LATIHAN SOAL 3

- 1) Sebutkan elemen komunikasi
- 2) Jelaskan yang dimaksud dengan PROTOKOL
- 3) apa Manfaat protokol
- 4) Sebutkan aturan-aturan komunikasi
- 5) Apa itu encoding dan decoding, encapsulasi dan decapsulasi
- 6) Jelaskan apa itu, unicast, multicast, broadcast
- 6) apa itu Protokol suite
- 7) Jelaskan yg dimaksud dengan HTTP, TCP, IP, Ethernet
- 8) sebutkan Layer dan protocols jaringan
- 9) Jelaskan yang dimaksud dengan DNS dan DHCP
- 10) jelaskan proses pengiriman email secara detail

BAB 4 AKSES JARINGAN

4.1 PENGANTAR

Untuk mendukung komunikasi kita, model OSI membagi fungsi jaringan data menjadi beberapa lapisan. Setiap lapisan bekerja dengan lapisan di atas dan di bawah untuk mentransmisikan data. Dua lapisan model OSI sangat terkait erat, bahwa menurut model TCP / IP mereka pada dasarnya adalah satu lapisan. Kedua layer tersebut adalah layer data link dan physical layer.

Pada perangkat pengirim, ini adalah peran lapisan data link untuk menyiapkan data transmisi dan kontrol bagaimana data tersebut mengakses media fisik. Namun, lapisan fisik mengontrol bagaimana data dikirimkan ke media fisik dengan mengkodekan digit biner yang mewakili data menjadi sinyal.

Pada sisi penerimaan, lapisan fisik menerima sinyal melintasi media penghubung. Setelah decoding sinyal kembali ke data, lapisan fisik melewati frame ke lapisan data link untuk penerimaan dan pemrosesan.

Bab ini dimulai dengan fungsi umum lapisan fisik dan standar dan protokol yang mengelola transmisi data di media lokal. Ini juga mengenalkan fungsi lapisan data link dan protokol yang terkait dengannya.

4.2 PROTOKOL LAYER FISIK

❖ KONEKSI LAYER FISIK

• TIPE KONEKSI

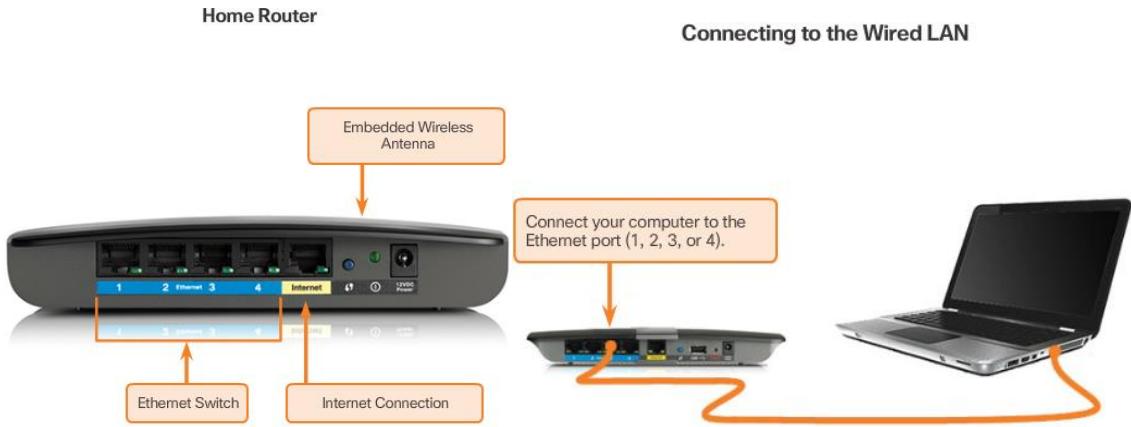
Sebelum komunikasi jaringan dapat terjadi, koneksi fisik ke jaringan lokal harus ditetapkan. Sambungan fisik bisa berupa sambungan kabel menggunakan kabel atau koneksi nirkabel menggunakan gelombang radio.

Jenis koneksi fisik yang digunakan tergantung pada pengaturan jaringan. Misalnya, di banyak kantor perusahaan, karyawan memiliki komputer desktop atau laptop yang terhubung secara fisik, melalui kabel, ke saklar bersama. Jenis pengaturan ini adalah jaringan kabel. Data ditransmisikan melalui kabel fisik.

Selain koneksi kabel, beberapa bisnis mungkin juga menawarkan koneksi nirkabel untuk laptop, tablet, dan smartphone. Dengan perangkat nirkabel, data ditransmisikan menggunakan gelombang radio. Penggunaan konektivitas nirkabel menjadi lebih umum seperti individu, dan bisnis sama, menemukan keuntungan dari menawarkan jenis layanan ini. Untuk menawarkan kemampuan nirkabel, perangkat pada jaringan nirkabel harus terhubung ke titik akses nirkabel (AP).

Beralih perangkat dan titik akses nirkabel sering kali merupakan dua perangkat khusus terpisah dalam implementasi jaringan. Namun, ada juga perangkat yang menawarkan konektivitas kabel dan nirkabel. Di banyak rumah, misalnya, individu menerapkan router layanan terpadu (ISR). ISR menawarkan komponen switching dengan beberapa port, yang memungkinkan beberapa perangkat terhubung ke jaringan area lokal (LAN) menggunakan

kabel. Selain itu, banyak ISR juga menyertakan AP, yang memungkinkan perangkat nirkabel terhubung juga.



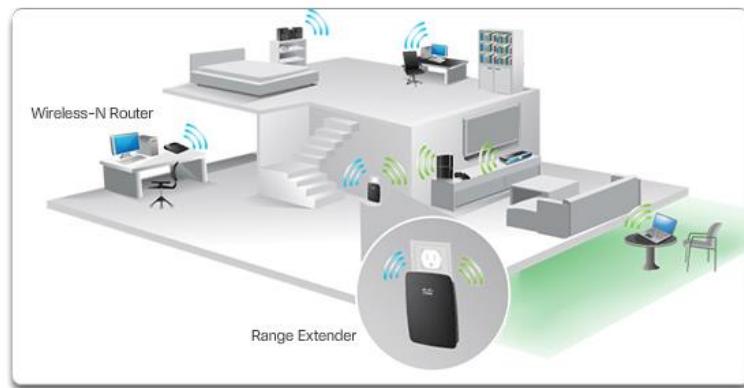
• NETWORK INTERFACE CARD

Network Interface Cards (NIC) menghubungkan perangkat ke jaringan. NIC Ethernet digunakan untuk koneksi kabel, sedangkan WLAN (Wireless Local Area Network) NIC digunakan untuk nirkabel. Perangkat pengguna akhir mungkin termasuk satu atau dua jenis NIC. Printer jaringan, misalnya, mungkin hanya memiliki NIC Ethernet, dan karena itu, harus terhubung ke jaringan menggunakan kabel Ethernet. Perangkat lain, seperti tablet dan smartphone, mungkin hanya berisi WLAN NIC dan harus menggunakan koneksi nirkabel.

Tidak semua koneksi fisik sama, dalam hal tingkat kinerja, saat terhubung ke jaringan. Misalnya, perangkat nirkabel akan mengalami penurunan kinerja berdasarkan jaraknya dari titik akses nirkabel. Semakin jauh perangkat dari jalur akses, semakin lemah sinyal nirkabel yang diterimanya. Ini bisa berarti bandwidth kurang atau tidak ada koneksi nirkabel sama sekali. Gambar menunjukkan bahwa extender jangkauan nirkabel dapat digunakan untuk meregenerasi sinyal nirkabel ke bagian lain rumah yang terlalu jauh dari titik akses nirkabel. Sebagai alternatif, koneksi kabel tidak akan menurunkan kinerja.

Semua perangkat nirkabel harus berbagi akses ke gelombang udara yang terhubung ke jalur akses nirkabel. Ini berarti kinerja jaringan yang lebih lambat dapat terjadi karena lebih banyak perangkat nirkabel yang mengakses jaringan secara bersamaan. Perangkat berkabel tidak perlu berbagi akses ke jaringan dengan perangkat lain. Setiap perangkat kabel memiliki saluran komunikasi terpisah di atas kabel Ethernet-nya. Hal ini penting saat mempertimbangkan beberapa aplikasi, seperti game online, video streaming, dan konferensi video, yang membutuhkan bandwidth lebih dedicated daripada aplikasi lainnya.

Selama beberapa topik berikutnya, Anda akan belajar lebih banyak tentang koneksi lapisan fisik yang terjadi dan bagaimana koneksi tersebut mempengaruhi pengangkutan data.



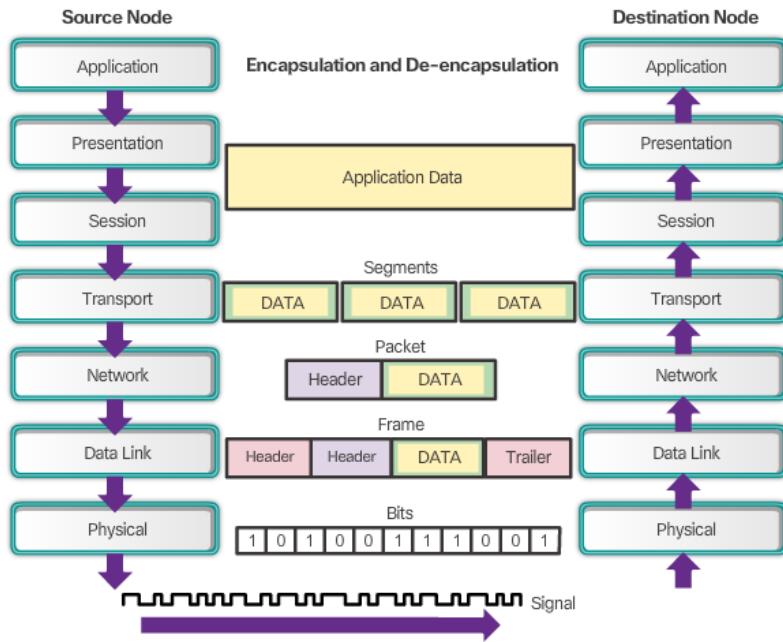
❖ TUJUAN PROTOKOL LAYER FISIK

- **LAYER FISIK**

Lapisan fisik OSI menyediakan sarana untuk mengangkut bit yang membentuk bingkai lapisan data link di media jaringan. Lapisan ini menerima bingkai lengkap dari lapisan data link dan mengkodekannya sebagai rangkaian sinyal yang dikirim ke media lokal. Bit yang dikodekan yang terdiri dari bingkai diterima oleh perangkat akhir atau perangkat perantara.

Proses yang dialami data dari node sumber ke simpul tujuan adalah:

- ✓ Data pengguna tersegmentasi oleh lapisan transport, ditempatkan ke dalam paket oleh lapisan jaringan, dan selanjutnya dienkapsulasi ke dalam frame oleh lapisan data link.
- ✓ Lapisan fisik mengkodekan frame dan menciptakan sinyal gelombang elektrik, optik, atau radio yang mewakili bit pada setiap frame.
- ✓ Sinyal kemudian dikirim ke media, satu per satu.
- ✓ Lapisan fisik simpul tujuan mengambil sinyal individual ini dari media, mengembalikannya ke representasi bit mereka, dan meneruskan bit ke lapisan data link sebagai bingkai yang lengkap.



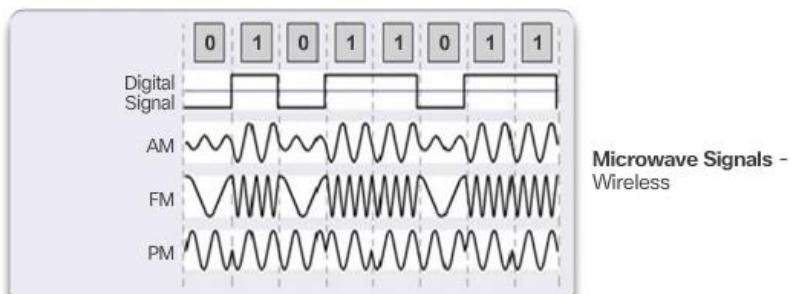
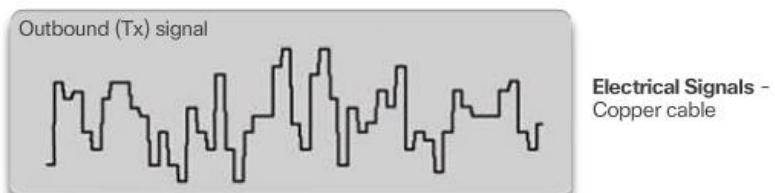
• MEDIA LAYER FISIK

Ada tiga bentuk dasar media jaringan. Lapisan fisik menghasilkan representasi dan pengelompokan bit untuk setiap jenis media sebagai:

- ✓ Copper cable (Kabel tembaga): Sinyal adalah pola pulsa elektrik
- ✓ Fiber-optic cable (Kabel serat optik): Sinyal adalah pola cahaya.
- ✓ Wireless (Nirkabel) : Sinyal adalah pola transmisi gelombang mikro.

contoh pensinyalan untuk tembaga, serat optik, dan nirkabel.

Untuk mengaktifkan interoperabilitas lapisan fisik, semua aspek fungsi ini diatur oleh organisasi standar.



• STANDART LAYER FISIK

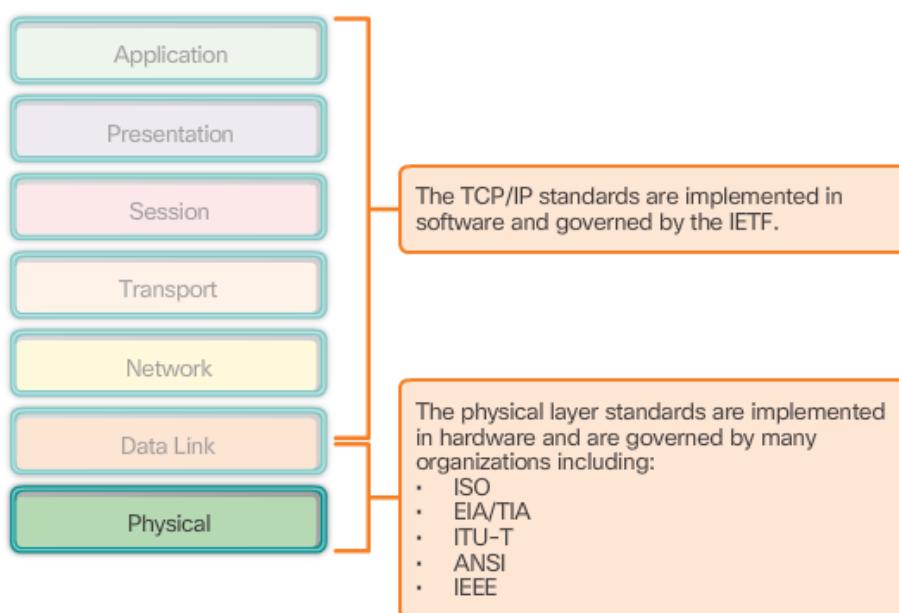
Protokol dan operasi lapisan OSI atas dilakukan dalam perangkat lunak yang dirancang oleh insinyur perangkat lunak dan ilmuwan komputer. Layanan dan protokol di suite TCP / IP didefinisikan oleh Internet Engineering Task Force (IETF).

Lapisan fisik terdiri dari sirkuit elektronik, media, dan konektor yang dikembangkan oleh para insinyur. Oleh karena itu, adalah tepat bahwa standar yang mengatur perangkat keras ini ditentukan oleh organisasi teknik elektro dan komunikasi yang relevan.

Ada banyak organisasi internasional dan nasional yang berbeda, organisasi pemerintah yang mengatur peraturan, dan perusahaan swasta yang terlibat dalam membangun dan memelihara standar lapisan fisik. Misalnya, lapisan fisik perangkat keras, media, pengkodean, dan standar pemberian sinyal didefinisikan dan diatur oleh:

- ✓ Organisasi Internasional untuk Standardisasi (ISO)
- ✓ Asosiasi Industri Telekomunikasi / Asosiasi Industri Elektronika (TIA / EIA)
- ✓ International Telecommunication Union (ITU)
- ✓ Institut Teknik Elektro dan Elektronika (IEEE)
- ✓ Badan pengawas telekomunikasi nasional termasuk Komisi Komunikasi Federal (FCC) di Amerika Serikat dan European Telecommunications Standards Institute (ETSI)

Selain itu, sering ada kelompok pengkabelan regional seperti CSA (Canadian Standards Association), CENELEC (Komite Eropa untuk Standardisasi Elektroteknik), dan JSA / JIS (Asosiasi Standar Jepang), mengembangkan spesifikasi lokal.



❖ KARAKTERISTIK LAYER FISIK

- FUNCTION

Standar lapisan fisik menangani tiga area fungsional:

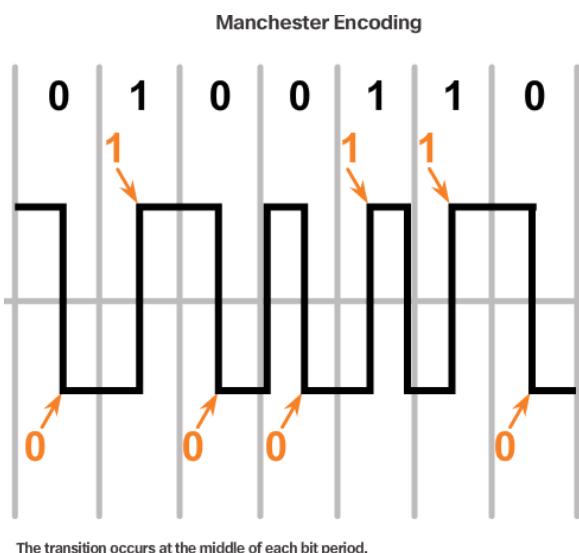
- ✓ **Physical Components**

Komponennya adalah perangkat perangkat elektronik, media, dan konektor lain yang mentransmisikan dan membawa sinyal untuk mewakili bit. Komponen perangkat keras seperti NIC, antarmuka dan konektor, bahan kabel, dan desain kabel semuanya ditentukan dalam standar yang terkait dengan lapisan fisik. Berbagai port dan interface pada router Cisco 1941 juga merupakan contoh komponen fisik dengan konektor dan pinouts spesifik yang dihasilkan dari standar.

- ✓ **Encoding**

Encoding atau line encoding adalah metode untuk mengubah aliran bit data menjadi "kode" yang telah ditentukan. Kode adalah pengelompokan bit yang digunakan untuk menyediakan pola yang dapat diprediksi yang dapat dikenali oleh pengirim dan penerima. Dalam kasus jaringan, pengkodean adalah pola tegangan atau arus yang digunakan untuk mewakili bit; 0s dan 1s.

Sebagai contoh, pengkodean Manchester mewakili 0 bit dengan transisi tegangan tinggi ke tegangan rendah, dan bit 1 diwakili sebagai transisi tegangan rendah ke tinggi. Contoh pengkodean Manchester diilustrasikan pada Gambar 1. Transisi terjadi pada pertengahan setiap periode bit. Jenis pengkodean ini digunakan dalam 10 b / s Ethernet. Kecepatan data yang lebih cepat memerlukan pengkodean yang lebih kompleks.



- ✓ **Signaling**

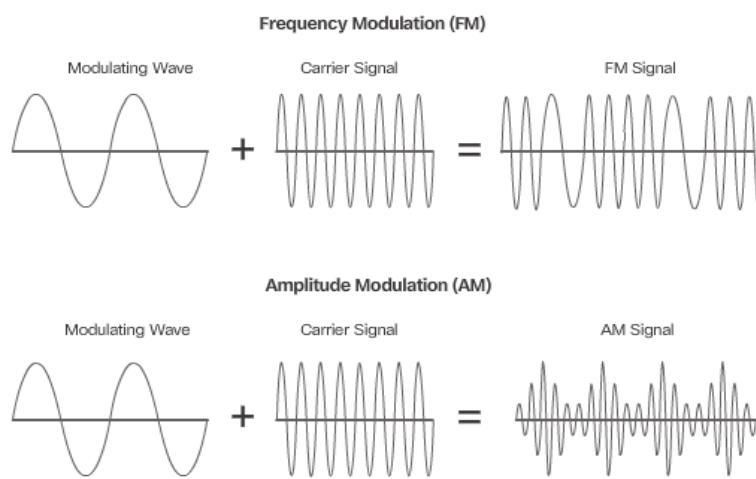
Lapisan fisik harus menghasilkan sinyal listrik, optik, atau nirkabel yang mewakili "1" dan "0" pada media. Metode untuk mewakili bit disebut metode pensinyalan. Standar lapisan fisik harus menentukan jenis sinyal yang mewakili "1" dan jenis sinyal yang mewakili "0". Ini bisa

sesederhana perubahan pada tingkat sinyal listrik atau pulsa optik. Misalnya, pulsa panjang mungkin mewakili 1 sedangkan pulsa pendek mewakili angka 0.

Ini mirip dengan bagaimana kode Morse digunakan untuk komunikasi. Kode Morse adalah metode pensinyalan lain yang menggunakan serangkaian nada, lampu, atau klik on-off untuk mengirim teks melalui kabel telepon atau antar kapal di laut.

Ada banyak cara untuk mentransmisikan sinyal. Metode umum untuk mengirim data menggunakan teknik modulasi. Modulasi adalah proses dimana karakteristik satu gelombang (sinyal) memodifikasi gelombang lain (pembawa).

Sifat dari sinyal aktual yang mewakili bit pada media akan bergantung pada metode pensinyalan yang digunakan.



• BANDWIDTH

Media fisik yang berbeda mendukung transfer bit pada tingkat yang berbeda. Transfer data biasanya didiskusikan dalam hal bandwidth dan throughput.

Bandwidth adalah kapasitas medium untuk membawa data. Bandwidth digital mengukur jumlah data yang dapat mengalir dari satu tempat ke tempat lain dalam jumlah waktu tertentu. Bandwidth biasanya diukur dalam kilobit per detik (kb / s), megabit per detik (Mb / s), atau gigabit per detik (Gb / s). Bandwidth kadang-kadang dianggap sebagai kecepatan yang bit perjalanan, namun hal ini tidak akurat. Misalnya, di Ethernet 10Mb / s dan 100Mb / s, bit dikirim pada kecepatan listrik. Perbedaannya adalah jumlah bit yang ditransmisikan per detik.

Kombinasi faktor menentukan bandwidth praktis dari sebuah jaringan:

- ✓ The properties of the physical media
- ✓ Teknologi yang dipilih untuk sinyal dan mendeteksi sinyal jaringan

Sifat media fisik, teknologi terkini, dan hukum fisika semuanya berperan dalam menentukan bandwidth yang ada.

Tabel menunjukkan ukuran pengukuran bandwidth yang umum digunakan.

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	b/s	1 b/s = fundamental unit of bandwidth
Kilobits per second	kb/s	1 kb/s = 1,000 bps = 10^3 bps
Megabits per second	Mb/s	1 Mb/s = 1,000,000 bps = 10^6 bps
Gigabits per second	Gb/s	1 Gb/s = 1,000,000,000 bps = 10^9 bps
Terabits per second	Tb/s	1 Tb/s = 1,000,000,000,000 bps = 10^{12} bps

- **THROUGHPUT**

Throughput adalah ukuran transfer bit melintasi media selama periode waktu tertentu. Karena sejumlah faktor, throughput biasanya tidak sesuai dengan bandwidth yang ditentukan dalam implementasi lapisan fisik. Banyak faktor yang mempengaruhi throughput, diantaranya:

- ✓ Jumlah lalu lintas / TRAFFIC
- ✓ Jenis lalu lintas
- ✓ Latency yang diciptakan oleh jumlah perangkat jaringan yang ditemui antara sumber dan tujuan

Latency mengacu pada jumlah waktu, termasuk penundaan, data untuk melakukan perjalanan dari satu titik ke titik lainnya.

Dalam jaringan atau jaringan dengan banyak segmen, throughput tidak bisa lebih cepat daripada link paling lambat di jalur dari sumber ke tujuan. Bahkan jika semua atau sebagian besar segmen memiliki bandwidth tinggi, hanya dibutuhkan satu segmen di jalur dengan throughput rendah untuk menciptakan kemacetan pada throughput keseluruhan jaringan.

Ada banyak tes kecepatan online yang bisa mengungkap throughput koneksi internet. Angka tersebut memberikan hasil sampel dari tes kecepatan.

Ada pengukuran ketiga untuk menilai transfer data yang bisa digunakan yang dikenal dengan goodput. Goodput adalah ukuran data yang dapat digunakan yang ditransfer selama periode waktu tertentu. Goodput adalah throughput dikurangi overhead lalu lintas untuk membangun sesi, ucapan terima kasih, dan enkapsulasi.

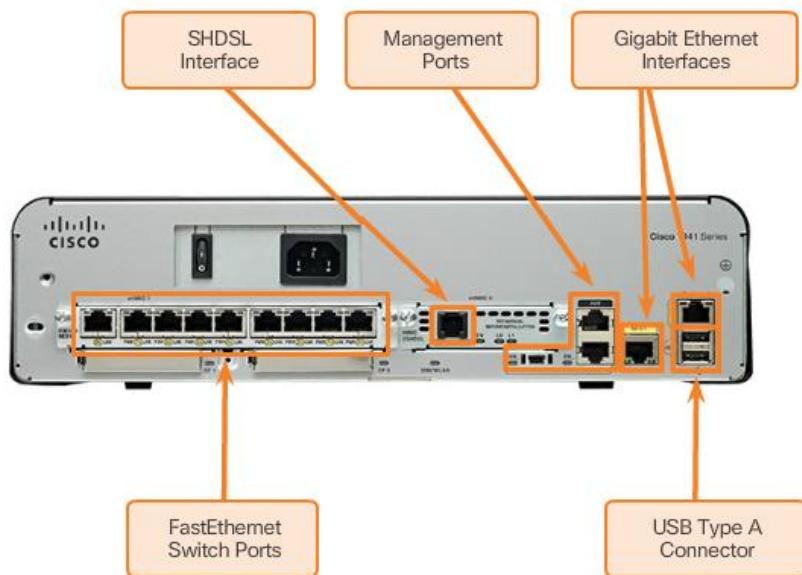
- **TIPE MEDIA FISIK**

Lapisan fisik menghasilkan representasi dan pengelompokan bit sebagai tegangan, frekuensi radio, atau pulsa ringan. Berbagai standar organisasi telah berkontribusi pada definisi sifat fisik, listrik, dan mekanik dari media yang tersedia untuk komunikasi data yang berbeda. Spesifikasi ini menjamin bahwa kabel dan konektor akan berfungsi seperti yang diantisipasi dengan implementasi lapisan data link yang berbeda.

Sebagai contoh, standar untuk media tembaga ditetapkan untuk:

- ✓ Jenis kabel tembaga yang digunakan

- ✓ Bandwidth dari komunikasi
- ✓ Jenis konektor yang digunakan
- ✓ Pinout dan kode warna koneksi ke media
- ✓ Jarak maksimal media



4.3 MEDIA JARINGAN

- ❖ **COPPER CABLING**
- **KARAKTERISTIK KABEL COPER**

Jaringan menggunakan media tembaga karena harganya murah, mudah dipasang dan memiliki daya tahan rendah terhadap arus listrik. Namun, media tembaga dibatasi oleh jarak dan gangguan sinyal.

Data ditransmisikan pada kabel tembaga sebagai pulsa elektrik. Detektor pada antarmuka jaringan perangkat tujuan harus menerima sinyal yang dapat berhasil diterjemahkan agar sesuai dengan sinyal yang dikirim. Namun, semakin lama sinyal bergerak, semakin memburuk. Ini disebut sebagai redaman sinyal. Untuk alasan ini, semua media tembaga harus mengikuti batasan jarak yang ketat seperti yang ditentukan oleh standar panduan.

Nilai waktu dan voltase pulsa listrik juga rentan terhadap gangguan dari dua sumber:

- ✓ **Electromagnetic interference (EMI)** atau gangguan frekuensi radio (RFI) - Sinyal EMI dan RFI dapat mendistorsi dan merusak sinyal data yang dibawa oleh media tembaga. Sumber potensial EMI dan RFI meliputi gelombang radio dan perangkat elektromagnetik, seperti lampu neon atau motor listrik seperti yang ditunjukkan pada gambar.
- ✓ **Crosstalk** - Crosstalk adalah gangguan yang disebabkan oleh medan listrik atau medan magnet dari sebuah sinyal pada satu kawat ke sinyal di kawat yang berdekatan. Di sirkuit telepon, crosstalk dapat menyebabkan pendengaran dari percakapan suara lain

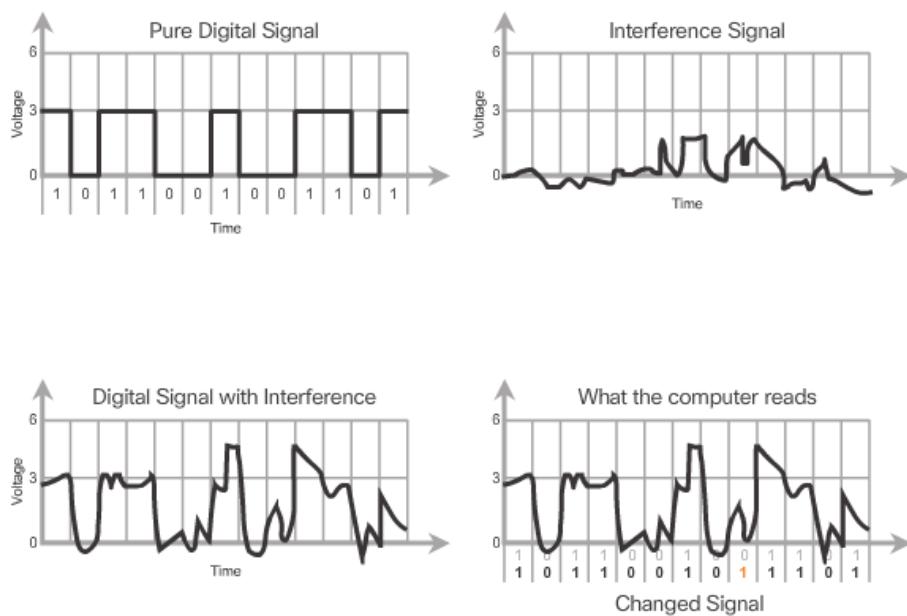
dari sirkuit yang berdekatan. Secara khusus, ketika arus listrik mengalir melalui kawat, ia menciptakan medan magnet melingkar kecil di sekitar kawat, yang dapat diambil oleh kawat yang berdekatan.

Untuk mengatasi efek negatif EMI dan RFI, beberapa jenis kabel tembaga dibungkus dengan pelindung logam dan memerlukan koneksi grounding yang tepat.

Untuk mengatasi efek negatif dari crosstalk, beberapa jenis kabel tembaga memiliki sepasang pasang kawat yang saling berlawanan, yang secara efektif membantalkan crosstalk.

Kerentanan kabel tembaga terhadap kebisingan elektronik juga dapat dibatasi oleh:

- ✓ Memilih jenis kabel atau kategori yang paling cocok untuk lingkungan jaringan tertentu.
- ✓ Merancang infrastruktur kabel untuk menghindari sumber gangguan yang diketahui dan potensial dalam struktur bangunan.
- ✓ Menggunakan teknik pemasangan kabel yang mencakup penanganan dan penghentian kabel yang tepat.



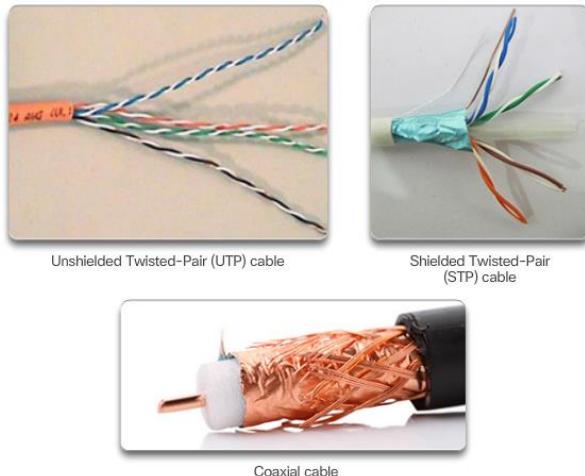
• MEDIA KABEL COPER

Ada tiga jenis utama media tembaga yang digunakan dalam jaringan:

- ✓ Unshielded Twisted-Pair (UTP)
- ✓ Shielded Twisted-Pair (STP)
- ✓ Koaksial

Kabel ini digunakan untuk menghubungkan node pada perangkat LAN dan infrastruktur seperti switch, router, dan titik akses nirkabel. Setiap jenis koneksi dan perangkat yang menyertainya memiliki persyaratan pemasangan kabel yang ditetapkan oleh standar lapisan fisik.

Standar lapisan fisik yang berbeda menentukan penggunaan berbagai konektor. Standar ini menentukan dimensi mekanis dari konektor dan sifat listrik yang dapat diterima dari masing-masing jenis. Media jaringan menggunakan jack modular dan colokan untuk memudahkan koneksi dan pemutusan hubungan. Juga, satu jenis konektor fisik dapat digunakan untuk beberapa jenis koneksi. Misalnya, konektor RJ-45 banyak digunakan di LAN dengan satu jenis media dan pada beberapa WAN dengan jenis media lainnya.

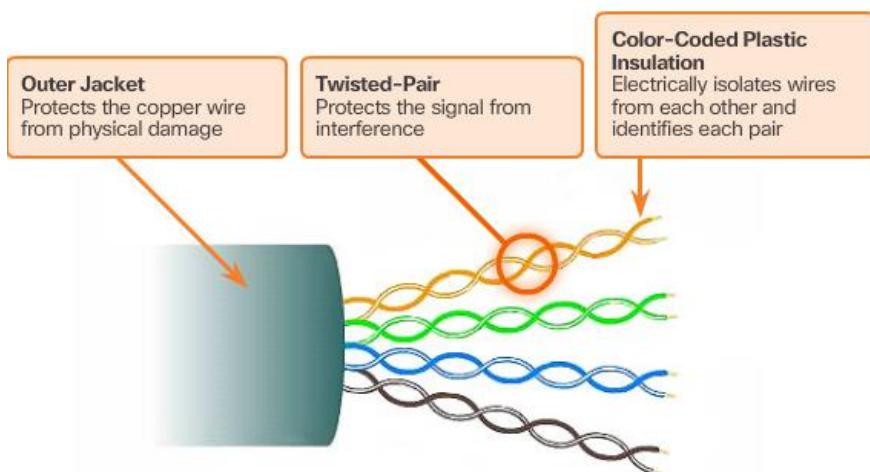


- **KABEL TWISTED-PAIR UNSHIELDED**

Pemasangan kabel twisted-pair (UTP) unshielded adalah media jaringan yang paling umum. Kabel UTP, diakhiri dengan konektor RJ-45, digunakan untuk host jaringan interkoneksi dengan perangkat jaringan menengah, seperti switch dan router.

Di LAN, kabel UTP terdiri dari empat pasang kabel berkoda warna yang telah dipelintir bersama dan kemudian terbungkus dalam selubung plastik fleksibel yang melindungi dari kerusakan fisik ringan. Memutar kabel membantu melindungi dari gangguan sinyal dari kabel lain.

Seperti yang terlihat pada gambar, kode warna mengidentifikasi pasangan dan kabel masing-masing dan membantu penghentian kabel.

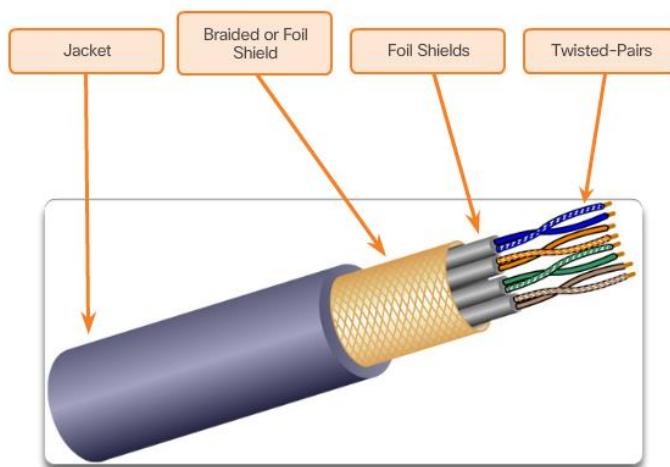


• KABEL SHIELDED TWISTED-PAIR

Shielded twisted-pair (STP) memberikan perlindungan noise yang lebih baik daripada pemasangan kabel UTP. Namun, dibandingkan dengan kabel UTP, kabel STP secara signifikan lebih mahal dan sulit dipasang. Seperti kabel UTP, STP menggunakan konektor RJ-45.

Kabel STP menggabungkan teknik perisai untuk melawan EMI dan RFI, dan kawat memutar untuk melawan crosstalk. Untuk mendapatkan keuntungan penuh dari perisai, kabel STP diakhiri dengan konektor data STP terlindung khusus. Jika kabel tidak dilapisi dengan benar, perisai dapat bertindak sebagai antena dan mengambil sinyal yang tidak diinginkan.

Kabel STP yang ditampilkan menggunakan empat pasang kabel, masing-masing dibungkus perisai foil, yang kemudian dibungkus dengan kain utuh secara keseluruhan atau foil.



• KABEL COAXIAL

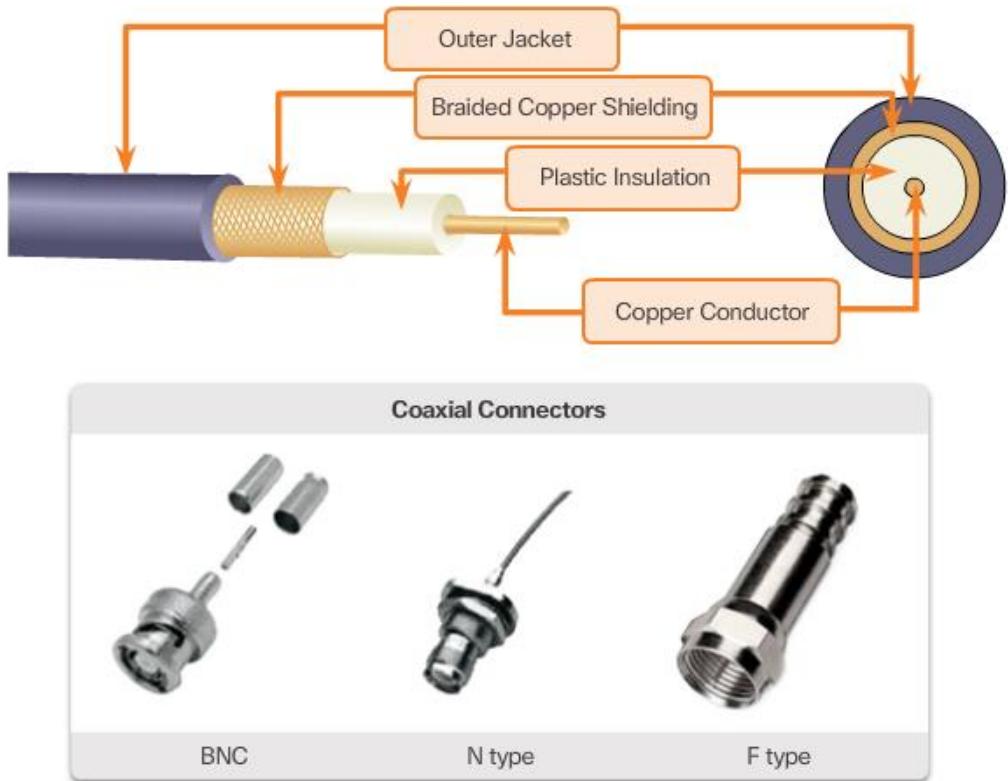
Kabel coaxial, atau coax for short, mendapat namanya dari kenyataan bahwa ada dua konduktor yang memiliki sumbu yang sama. Seperti yang ditunjukkan pada gambar, kabel koaksial terdiri dari:

- ✓ Sebuah konduktor tembaga digunakan untuk mentransmisikan sinyal elektronik.
- ✓ Lapisan isolasi plastik fleksibel yang mengelilingi konduktor tembaga.
- ✓ Bahan isolasi dikelilingi oleh jalinan tembaga anyaman, atau lembaran logam, yang berfungsi sebagai kawat kedua di sirkuit dan sebagai pelindung konduktor dalam. Lapisan kedua ini, atau perisai, juga mengurangi jumlah gangguan elektromagnetik luar.
- ✓ Seluruh kabel ditutupi dengan jaket kabel untuk mencegah kerusakan fisik ringan

Ada berbagai jenis konektor yang digunakan dengan kabel coax.

Meskipun kabel UTP pada dasarnya telah menggantikan kabel koaksial pada instalasi Ethernet modern, desain kabel koaksial digunakan pada:

- ✓ Instalasi nirkabel: Kabel koaksial memasang antena ke perangkat nirkabel. Kabel koaksial membawa energi frekuensi radio (RF) antara antena dan peralatan radio.
- ✓ Instalasi Internet Kabel: Penyedia layanan kabel menyediakan koneksi Internet kepada pelanggan mereka dengan mengganti bagian kabel koaksial dan elemen penguat pendukung dengan kabel serat optik. Namun, pemasangan kabel di dalam tempat pelanggan masih menggunakan coax kabel.



• KEAMANAN KABEL COPPER / TEMBAGA

Ketiga jenis media tembaga ini rentan terhadap bahaya kebakaran dan listrik.

Bahaya kebakaran ada karena isolasi kabel dan selubung mungkin mudah terbakar, atau menghasilkan asap beracun bila dipanaskan atau dibakar. Otoritas atau organisasi bangunan dapat menetapkan standar keselamatan terkait untuk pemasangan kabel dan perangkat keras.

Bahaya listrik adalah masalah potensial karena kabel tembaga dapat mengalirkan listrik dengan cara yang tidak diinginkan. Hal ini dapat menyebabkan personil dan peralatan untuk berbagai bahaya listrik. Misalnya, perangkat jaringan yang rusak bisa melakukan arus ke sasis perangkat jaringan lain. Selain itu, pemasangan kabel jaringan dapat menghadirkan tingkat voltase yang tidak diinginkan saat digunakan untuk menghubungkan perangkat yang memiliki sumber daya dengan potensi tanah yang berbeda. Situasi seperti itu dimungkinkan saat pemasangan kabel tembaga digunakan untuk menghubungkan jaringan di berbagai bangunan atau di lantai terpisah yang menggunakan fasilitas tenaga yang berbeda. Akhirnya, kabel tembaga dapat melakukan voltase yang disebabkan oleh sambaran petir ke perangkat jaringan.

Hasil dari voltase dan arus yang tidak diinginkan dapat mencakup kerusakan pada perangkat jaringan dan komputer yang terhubung, atau cedera pada personil. Adalah penting bahwa

pemasangan kabel tembaga dipasang dengan benar, dan sesuai dengan spesifikasi dan kode bangunan yang relevan, untuk menghindari situasi yang berpotensi membahayakan dan merusak.

- ❖ **UTP Cabling**

- **PROPERTI KABEL UTP**

Saat digunakan sebagai media jaringan, kabel unshielded twisted-pair (UTP) terdiri dari empat pasang kabel tembaga berkode warna yang telah dipelintir bersama dan kemudian terbungkus dalam selubung plastik fleksibel. Ukurannya yang kecil bisa menguntungkan saat pemasangan.

Kabel UTP tidak menggunakan pelindung untuk melawan efek EMI dan RFI. Sebagai gantinya, perancang kabel telah menemukan bahwa mereka dapat membatasi efek negatif dari crosstalk dengan:

- ✓ Pembatalan: Desainer sekarang memasangkan kabel di sirkuit. Bila dua kabel di sirkuit listrik ditempatkan berdekatan, medan magnetnya saling berlawanan satu sama lain. Oleh karena itu, dua medan magnet saling membantalkan dan juga membantalkan sinyal EMI dan RFI di luar.
- ✓ Memvariasikan jumlah tikungan per pasang kawat: Untuk lebih meningkatkan efek pembatalan kabel sirkuit pasangan, perancang memvariasikan jumlah tikungan masing-masing pasangan kawat di kabel. Kabel UTP harus mengikuti spesifikasi yang tepat yang mengatur berapa banyak tikungan atau jalinan yang diijinkan per meter (3,28 kaki) kabel. Perhatikan pada gambar bahwa pasangan putih oranye / oranye dipelintir kurang dari pasangan biru / biru putih. Setiap pasangan berwarna dipelintir beberapa kali.

Kabel UTP hanya mengandalkan efek pembatalan yang dihasilkan oleh pasangan kawat yang dipilin untuk membatasi degradasi sinyal dan secara efektif melindungi diri dari pasangan kawat di media jaringan



- **STANDART KABEL UTP**

Pemasangan kabel UTP sesuai dengan standar yang ditetapkan bersama oleh TIA / AMDAL. Secara khusus, TIA / EIA-568 menetapkan standar pengkabelan komersial untuk instalasi LAN dan merupakan standar yang paling umum digunakan di lingkungan pemasangan kabel LAN. Beberapa elemen yang didefinisikan adalah:

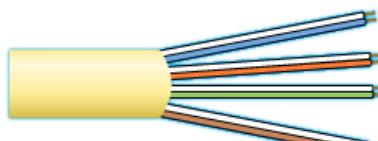
- ✓ Tipe kabel
- ✓ Panjang kabel
- ✓ Konektor
- ✓ Penghentian kabel / Termination
- ✓ Metode pengujian kabel

Karakteristik listrik dari kabel tembaga didefinisikan oleh Institute of Electrical and Electronics Engineers (IEEE). Tarif IEEE kabel UTP sesuai kinerjanya. Kabel ditempatkan ke dalam kategori berdasarkan kemampuan mereka untuk membawa tingkat bandwidth yang lebih tinggi. Misalnya, kabel Kategori 5 (Cat5) biasanya digunakan pada instalasi Fast Ethernet 100BASE-TX. Kategori lainnya termasuk kabel Enhanced Category 5 (Cat5e), Kategori 6 (Cat6), dan Kategori 6a.

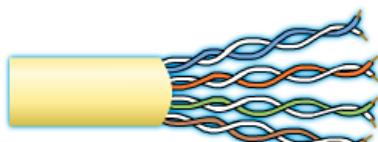
Kabel dalam kategori yang lebih tinggi dirancang dan dibangun untuk mendukung kecepatan data yang lebih tinggi. Sebagai teknologi Ethernet kecepatan gigabit baru sedang dikembangkan dan diadopsi, Cat5e sekarang merupakan jenis kabel yang dapat diterima minimal, dengan Cat6 menjadi tipe yang direkomendasikan untuk instalasi bangunan baru.

Beberapa produsen membuat kabel melebihi spesifikasi TIA / EIA Category 6a dan merujuk pada Kategori 7 ini

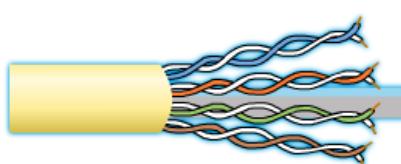
- ✓ **Kategori 3 Kabel UTP;** Digunakan untuk komunikasi suara, Paling sering digunakan untuk saluran telepon
- ✓ **Kategori 5 Kabel UTP dan 5e UTP;** Digunakan untuk transmisi data, Cat5 mendukung 100 Mb / s dan bisa mendukung 1000 Mb / s, tapi tidak disarankan, Cat5e mendukung 1000 Mb / s
- ✓ **Kategori 6 Kabel UTP;** Digunakan untuk transmisi data, Pemisah tambahan ada di antara masing-masing pasang kabel yang memungkinkannya berfungsi pada kecepatan yang lebih tinggi, Mendukung 1000 Mb / s - 10 Gb / s, meski 10 Gb / s tidak disarankan



Category 3 Cable (UTP)



Category 5 and 5e Cable (UTP)



Category 6 Cable (UTP)

• KONEKTOR KABEL UTP

Kabel UTP biasanya diakhiri dengan konektor RJ-45. Konektor ini digunakan untuk berbagai spesifikasi lapisan fisik, salah satunya adalah Ethernet. Standar TIA / EIA-568 menggambarkan kode warna kawat ke pin assignments (pinouts) untuk kabel Ethernet.

Seperti ditunjukkan pada Gambar, **konektor RJ-45** adalah komponen laki-laki, dikerutkan di ujung kabel. **Soket** adalah komponen wanita dari perangkat jaringan, dinding, partisi bilik, atau panel tempel.

Setiap kali kabel tembaga dihentikan; ada kemungkinan kehilangan sinyal dan pengenalan noise ke dalam rangkaian komunikasi. Bila diakhiri dengan tidak semestinya, setiap kabel merupakan sumber potensial penurunan kinerja lapisan fisik. Adalah penting bahwa semua penghentian media tembaga berkualitas tinggi untuk memastikan kinerja optimal dengan teknologi jaringan saat ini dan masa depan.

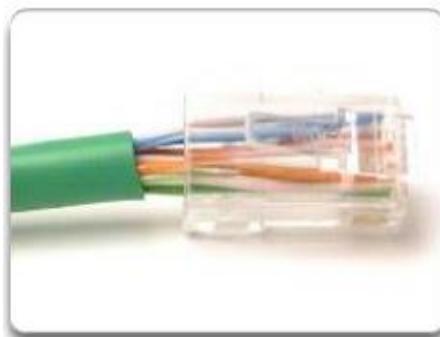
RJ-45 UTP Plugs



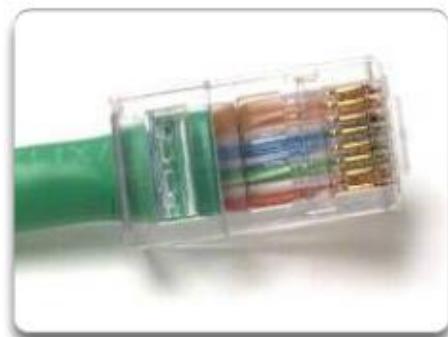
RJ-45 UTP Socket



Contoh kabel UTP yang dihentikan dengan buruk dan kabel UTP yang dihentikan dengan baik.



Bad connector - Wires are exposed, untwisted, and not entirely covered by the sheath.



Good connector - Wires are untwisted to the extent necessary to attach the connector.

• TIPE KABEL UTP

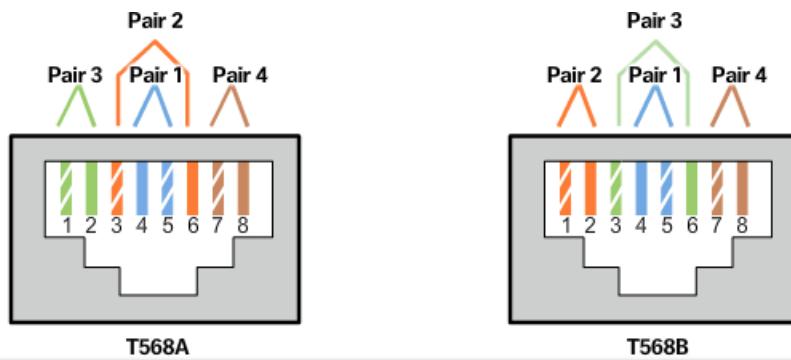
Situasi yang berbeda mungkin memerlukan kabel UTP untuk dihubungkan sesuai dengan konvensi pengkabelan yang berbeda. Ini berarti kabel individu di kabel harus dihubungkan dalam berbagai tatanan ke berbagai pin pada konektor RJ-45.

Berikut adalah jenis kabel utama yang diperoleh dengan menggunakan konvensi pengkabelan yang spesifik:

- ✓ **Ethernet Straight-through:** Jenis kabel jaringan yang paling umum. Hal ini biasanya digunakan untuk menghubungkan host ke switch dan sebuah switch ke router.

- ✓ **Ethernet Crossover:** Kabel yang digunakan untuk menghubungkan perangkat serupa. Misalnya untuk menghubungkan switch ke switch, host ke host, atau router ke router.
- ✓ **Rollover:** Kabel berpemilik Cisco yang digunakan untuk menghubungkan workstation ke port konsol router atau switch.

Menggunakan kabel crossover atau straight-through secara tidak benar antar perangkat mungkin tidak merusak perangkat, namun koneksi dan komunikasi antar perangkat tidak akan berlangsung. Ini adalah kesalahan umum di lab dan memerlukan pemeriksaan apakah koneksi perangkat benar harus menjadi tindakan pemecahan masalah pertama jika koneksi tidak tercapai.



Cable Type	Standard	Application
Ethernet Straight-through	Both ends T568A or both ends T568B	Connects a network host to a network device such as a switch or hub.
Ethernet Crossover	One end T568A, other end T568B	<ul style="list-style-type: none"> Connects two network hosts Connects two network intermediary devices (switch to switch, or router to router)
Rollover	Cisco proprietary	Connects a workstation serial port to a router console port, using an adapter.

• TESTING KABEL UTP

Setelah pemasangan, tester kabel UTP, seperti yang ditunjukkan pada gambar, harus digunakan untuk menguji parameter berikut:

- ✓ Wire map
- ✓ Panjang kabel
- ✓ Signal loss due to attenuation
- ✓ Crosstalk

Dianjurkan untuk memeriksa secara menyeluruh bahwa semua persyaratan pemasangan UTP telah terpenuhi.

❖ FIBER-OPTIC CABLING

• PROPERTI FIBER-OPTIC KABEL

Kabel serat optik mentransmisikan data jarak jauh dan bandwidth yang lebih tinggi daripada media jaringan lainnya. Tidak seperti kabel tembaga, kabel serat optik dapat mengirimkan

sinyal dengan atenuasi kurang dan benar-benar kebal terhadap EMI dan RFI. Serat optik biasanya digunakan untuk interkoneksi perangkat jaringan.

Serat optik adalah, fleksibel tapi sangat tipis, transparan untai gelas sangat murni, tidak jauh lebih besar dari rambut manusia. Bit dikodekan pada serat sebagai impuls ringan. Kabel serat optik bertindak sebagai waveguide, atau "light pipe", untuk mentransmisikan cahaya di antara kedua ujungnya dengan sedikit kehilangan sinyal.

Sebagai analogi, perhatikan gulungan handuk kertas kosong dengan bagian dalamnya dilapisi seperti cermin. Panjangnya seribu meter, dan sebuah laser pointer kecil digunakan untuk mengirim sinyal kode Morse dengan kecepatan cahaya. Intinya begitulah cara kerja kabel serat optik, kecuali yang berdiameter lebih kecil dan menggunakan teknologi cahaya yang canggih.

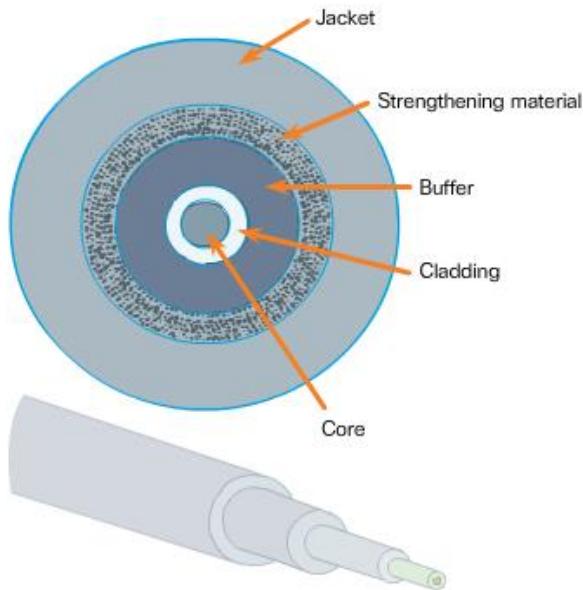
Serat optik kabel sekarang digunakan dalam empat jenis industri:

- ✓ Jaringan Enterprise: Digunakan untuk pemasangan kabel backbone dan perangkat infrastruktur yang saling terkait.
- ✓ Fiber-to-the-Home (FTTH): Digunakan untuk selalu menyediakan layanan broadband ke rumah dan usaha kecil.
- ✓ Long-Haul Networks: Digunakan oleh penyedia layanan untuk menghubungkan negara dan kota.
- ✓ Jaringan Submarine: Digunakan untuk menyediakan solusi berkecepatan tinggi dan berkapasitas tinggi yang andal yang mampu bertahan di lingkungan bawah laut yang keras hingga jarak lintas samudra. Klik di sini untuk melihat peta telegeografi yang menggambarkan lokasi kabel kapal selam.

• DESAIN KABEL MEDIA FIBER

Serat optik terdiri dari dua jenis kaca (inti dan kelongsong) dan pelindung pelindung luar (jaket). Klik setiap komponen pada gambar untuk mempelajari lebih banyak informasi.

Meski serat optiknya sangat tipis dan rentan terhadap tikungan tajam, sifat inti dan kelongsong membuatnya sangat kuat. Serat optik tahan lama dan dikerahkan dalam kondisi lingkungan yang keras di jaringan di seluruh dunia.



- **TIPE MEDIA FIBER**

Pulsa ringan yang mewakili data yang dipancarkan sebagai bit pada media dihasilkan oleh:

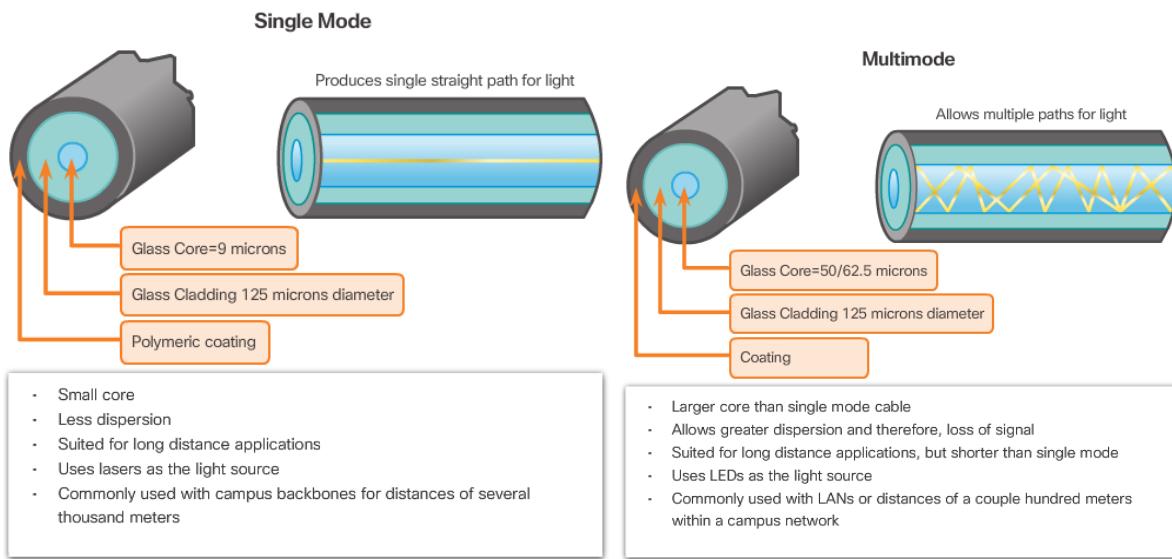
- ✓ LASER
- ✓ Dioda pemancar cahaya (LED)

Perangkat semikonduktor elektronik disebut fotodioda mendeteksi pulsa cahaya dan mengkonversikannya ke voltase. Cahaya laser yang ditransmisikan melalui kabel serat optik dapat merusak mata manusia. Perhatian harus diberikan untuk menghindari melihat ke ujung serat optik aktif.

Kabel serat optik diklasifikasikan secara luas menjadi dua jenis:

- ✓ **Single-mode fiber (SMF):** Terdiri dari inti yang sangat kecil dan menggunakan teknologi laser mahal untuk mengirim secercah sinar cahaya, seperti yang ditunjukkan pada Gambar 1. Populer dalam situasi jarak jauh yang mencakup ratusan kilometer, seperti yang dibutuhkan dalam waktu lama. aplikasi tangkapan telephony dan kabel TV.
- ✓ **Serat multimode (MMF):** Terdiri dari inti yang lebih besar dan menggunakan pemanca LED untuk mengirim pulsa cahaya. Secara khusus, cahaya dari LED memasuki serat multimode pada sudut yang berbeda, seperti yang ditunjukkan pada Gambar 2. Populer di LAN karena dapat didukung oleh LED berbiaya rendah. Ini menyediakan bandwidth hingga 10 Gb / s di atas panjang tautan hingga 550 meter.

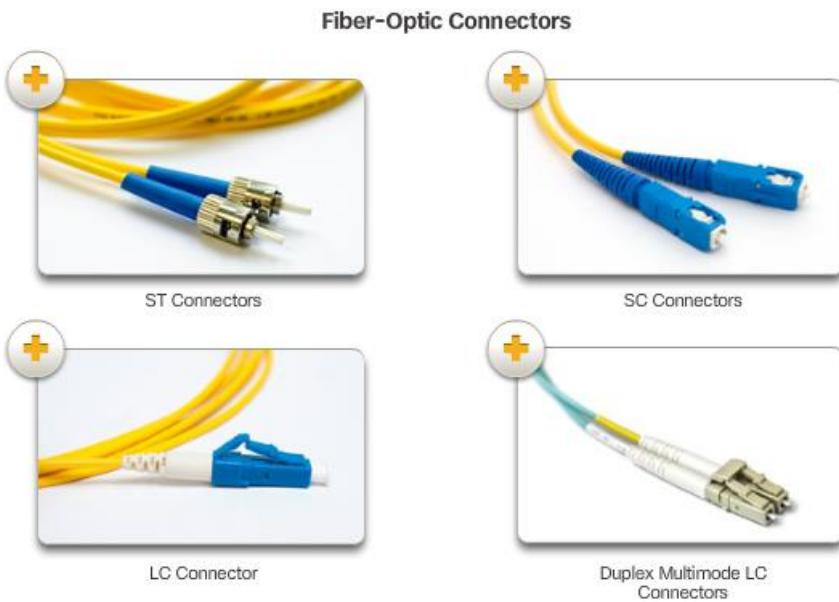
Salah satu perbedaan yang disorot antara serat multimode dan single-mode adalah jumlah dispersi. Dispersi mengacu pada penyebaran pulsa cahaya dari waktu ke waktu. Semakin banyak dispersi yang ada, semakin besar pula kehilangan kekuatan sinyal.



• FIBER OPTIC KONEKTOR

Konektor serat optik mengakhiri ujung serat optik. Berbagai konektor serat optik tersedia. Perbedaan utama antara jenis konektor adalah dimensi dan metode penggandengan. Bisnis memutuskan jenis konektor yang akan digunakan, berdasarkan peralatan mereka.

Karena cahaya hanya bisa berjalan dalam satu arah di atas serat optik, dua serat dibutuhkan untuk mendukung operasi dupleks penuh. Oleh karena itu, kabel patch serat optik menggabungkan dua kabel serat optik dan menghentikannya dengan sepasang konektor serat tunggal standar. Beberapa konektor serat menerima baik serat pemancar dan penerima dalam satu konektor yang dikenal sebagai konektor dupleks.



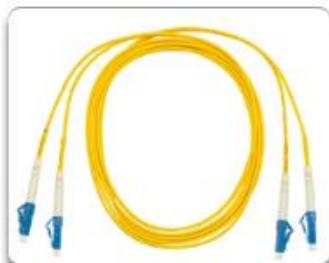
- ✓ **Straight Tip / ST Connectors;** Salah satu jenis konektor pertama yang digunakan. Konektor terkunci dengan aman dengan mekanisme gaya bayonet "twist-on / twist-off".
- ✓ **Subscriber / SC Connector;** Terkadang disebut sebagai konektor persegi atau konektor standar. Ini adalah konektor LAN dan WAN yang banyak digunakan yang menggunakan mekanisme push-pull untuk memastikan penyisipan positif. Tipe konektor ini digunakan dengan multimode dan single-mode fiber.
- ✓ **Lucent Connector / LC Connector;** Versi yang lebih kecil dari konektor SC serat optik. Terkadang disebut konektor kecil atau lokal dan dengan cepat semakin populer karena ukurannya yang lebih kecil
- ✓ **Duplex Multimode LC Connector;** Serupa dengan konektor simpleks LC, namun menggunakan konektor dupleks.

Kabel kabel serat diperlukan untuk menghubungkan perangkat infrastruktur. Gambar bawah menampilkan berbagai kabel patch yang umum. Penggunaan warna membedakan antara single-mode dan multimode patch cords. Jaket kuning adalah untuk kabel serat single-mode dan oranye (atau aqua) untuk kabel serat multimode.

Kabel serat harus dilindungi dengan tutup plastik kecil bila tidak digunakan.



SC-SC Multimode Patch Cord



LC-LC Single-mode Patch Cord



ST-LC Multimode Patch Cord



SC-ST Single-mode Patch Cord

• TESTING FIBER KABEL

Pemutusan dan penyambungan kabel serat optik membutuhkan pelatihan dan peralatan khusus. Pemutusan yang salah media serat optik akan mengakibatkan jarak sinyal berkurang atau kegagalan transmisi.

Tiga jenis pemutusan serat optik dan kesalahan splicing adalah:

- ✓ Misalignment: Media serat optik tidak sejajar satu sama lain saat digabungkan
- ✓ End GAP: Media tidak sepenuhnya menyentuh sambutan atau koneksi.
- ✓ End Finish: Media berakhir tidak dipoles dengan baik, atau kotoran hadir saat penghentian

Uji lapangan yang cepat dan mudah dapat dilakukan dengan menyinari senter terang ke salah satu ujung serat sambil mengamati ujung yang lain. Jika cahaya terlihat, seratnya mampu menerangi cahaya. Meskipun ini tidak menjamin kinerja, namun cara ini cepat dan murah untuk menemukan serat yang rusak.

Optical Time Domain Reflectometer (OTDR) dapat digunakan untuk menguji setiap segmen kabel serat optik. Perangkat ini menyuntikkan pulsa uji cahaya ke kabel dan mengukur backscatter dan pantulan cahaya yang terdeteksi sebagai fungsi waktu. OTDR akan menghitung perkiraan jarak di mana kesalahan ini terdeteksi sepanjang kabel.

- **FIBER VS TEMBAGA**

Ada banyak keuntungan menggunakan kabel fiber optic dibanding kabel tembaga. Angka tersebut menyoroti beberapa perbedaan ini.

Mengingat bahwa serat yang digunakan dalam media serat optik bukanlah konduktor listrik, media kebal terhadap gangguan elektromagnetik dan tidak akan melakukan arus listrik yang tidak diinginkan karena masalah grounding. Serat optik tipis dan memiliki kehilangan sinyal yang relatif rendah dan dapat dioperasikan pada jarak yang jauh lebih besar daripada media tembaga. Beberapa spesifikasi lapisan serat optik fisik memungkinkan panjang yang bisa mencapai beberapa kilometer.

Saat ini, di sebagian besar lingkungan perusahaan, serat optik terutama digunakan sebagai kabel backbone untuk koneksi point-to-point dengan lalu lintas tinggi antara fasilitas distribusi data dan untuk interkoneksi bangunan di kampus multi-bangunan. Karena serat optik tidak melakukan listrik dan memiliki kehilangan sinyal rendah, ini sangat sesuai untuk penggunaan ini.

Implementation Issues	UTP Cabling	Fiber-optic Cabling
Bandwidth supported	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Distance	Relatively short (1 - 100 meters)	Relatively high (1 - 100,000 meters)
Immunity to EMI and RFI	Low	High (Completely immune)
Immunity to electrical hazards	Low	High (Completely immune)
Media and connector costs	Lowest	Highest
Installation skills required	Lowest	Highest
Safety precautions	Lowest	Highest

- ❖ **MEDIA WIRELESS**

- **PROPERTI MEDIA WIRELESS**

Media *wireless* / nirkabel membawa sinyal elektromagnetik yang mewakili digit biner komunikasi data dengan menggunakan frekuensi radio atau gelombang mikro.

Media nirkabel menyediakan pilihan mobilitas terbesar dari semua media, dan jumlah perangkat berkemampuan nirkabel terus meningkat. Seiring meningkatnya pilihan bandwidth jaringan, nirkabel cepat mulai populer di jaringan perusahaan.

Angka tersebut menyoroti berbagai simbol yang berhubungan dengan nirkabel.

Nirkabel memang memiliki beberapa area yang menjadi perhatian, termasuk:

- ✓ **Area cakupan:** Teknologi komunikasi data nirkabel bekerja dengan baik di lingkungan yang terbuka. Namun, bahan konstruksi tertentu yang digunakan pada bangunan dan bangunan, dan medan lokal, akan membatasi cakupan efektif.

- ✓ **Gangguan / Interference** : Nirkabel rentan terhadap gangguan dan dapat terganggu oleh perangkat umum seperti telepon nirkabel tanpa rumah, beberapa jenis lampu fluorescent, oven microwave, dan komunikasi nirkabel lainnya.
- ✓ **Keamanan**: Cakupan komunikasi nirkabel tidak memerlukan akses ke media fisik. Oleh karena itu, perangkat dan pengguna, tidak berwenang untuk akses ke jaringan, bisa mendapatkan akses ke transmisi. Keamanan jaringan merupakan komponen utama administrasi jaringan nirkabel.
- ✓ **Shared Media** : WLAN beroperasi dalam half-duplex, yang berarti hanya satu perangkat yang dapat mengirim atau menerima sekaligus. Media nirkabel dibagi di antara semua pengguna nirkabel. Semakin banyak pengguna yang perlu mengakses WLAN secara bersamaan, menghasilkan bandwidth yang kurang untuk setiap pengguna.

Meskipun nirkabel semakin populer untuk konektivitas desktop, tembaga dan serat adalah media lapisan fisik yang paling populer untuk penyebaran jaringan.

- **TIPE MEDIA WIRELESS**

Standar industri IEEE dan telekomunikasi untuk komunikasi data nirkabel mencakup data link dan lapisan fisik. Klik pada setiap standar dalam gambar untuk informasi lebih lanjut.

Catatan: Teknologi nirkabel lainnya seperti komunikasi seluler dan satelit juga dapat menyediakan konektivitas jaringan data. Namun, teknologi nirkabel ini tidak tersedia untuk bab ini.

Dalam masing-masing standar ini, spesifikasi Layer fisik diterapkan pada area yang meliputi:

- ✓ Data to radio signal encoding
- ✓ Frekuensi dan kekuatan transmisi
- ✓ Penerimaan sinyal dan persyaratan decoding
- ✓ Desain dan konstruksi antena

Wi-Fi adalah merek dagang dari Aliansi Wi-Fi. Wi-Fi digunakan dengan produk bersertifikasi yang termasuk perangkat WLAN yang didasarkan pada standar IEEE 802.11.

- ✓ Wi-Fi Standard IEEE 802.11; Teknologi Wireless LAN (WLAN), biasa disebut Wi-Fi. WLAN menggunakan protokol berbasis contention yang dikenal dengan Carrier Sense Multiple Access / Collision Avoidance (CSMA / CA). NIC nirkabel pertama-tama harus mendengarkan sebelum mentransmisikan untuk menentukan apakah saluran radio sudah jelas. Jika perangkat nirkabel lain mentransmisikan, maka NIC harus menunggu sampai salurannya bersih. CSMA / CA dibahas nanti di bab ini.
- ✓ Standart IEEE 802.15: Bluetooth; Standar Wireless Personal Area Network (WPAN), yang biasa dikenal dengan "Bluetooth", menggunakan proses pairing perangkat untuk berkomunikasi jarak jauh dari 1 sampai 100 meter.
- ✓ Standart IEEE 802.16: WiMAX; Umumnya dikenal sebagai Worldwide Interoperability for Microwave Access (WiMAX), menggunakan topologi point-to-multipoint untuk menyediakan akses broadband nirkabel.

- **WIRELESS LAN**

Implementasi data nirkabel yang umum memungkinkan perangkat terhubung secara nirkabel melalui LAN. Secara umum, LAN nirkabel memerlukan perangkat jaringan berikut:

- ✓ Wireless Access Point (AP): Mengkonsentrasi sinyal nirkabel dari pengguna dan terhubung ke infrastruktur jaringan berbasis tembaga yang ada, seperti Ethernet. Rumah dan router nirkabel bisnis kecil mengintegrasikan fungsi router, switch, dan access point ke dalam satu perangkat
- ✓ Wireless Adaptor NIC: Menyediakan kemampuan komunikasi nirkabel ke setiap host jaringan.

Seiring perkembangan teknologi, sejumlah standar berbasis Ethernet WLAN telah muncul. Perhatian perlu dilakukan dalam membeli perangkat nirkabel untuk memastikan kompatibilitas dan interoperabilitas.

Manfaat teknologi komunikasi data nirkabel terbukti, terutama penghematan pada pemasangan kabel mahal dan kenyamanan mobilitas host. Administrator jaringan perlu mengembangkan dan menerapkan kebijakan dan proses keamanan yang ketat untuk melindungi LAN nirkabel dari akses dan kerusakan yang tidak sah.

4.4 DATA LINK LAYER PROTOCOL

- ❖ **TUJUAN DATA LINK LAYER**

- **DATA LINK LAYER**

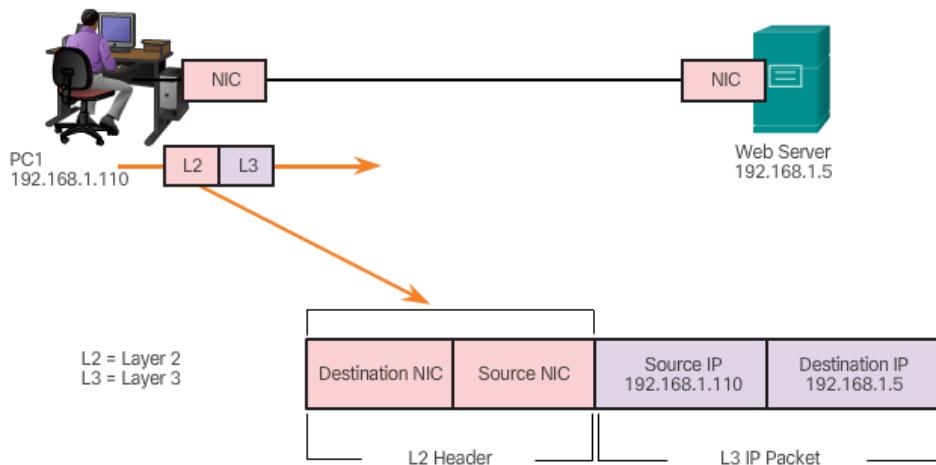
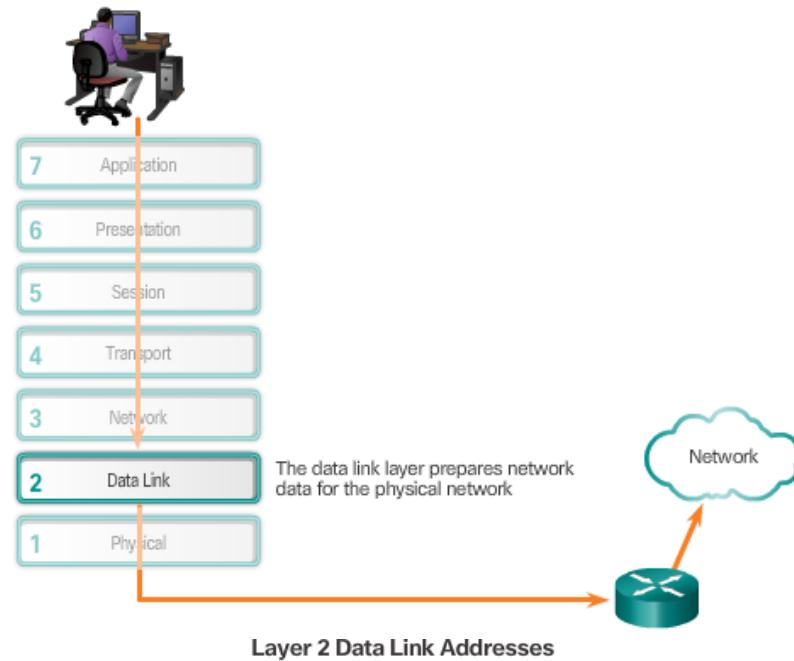
Lapisan data link dari model OSI (Layer 2), bertanggung jawab untuk:

- ✓ Mengizinkan lapisan atas mengakses media
- ✓ Menerima paket Layer 3 dan mengemasnya ke dalam bingkai
- ✓ Menyiapkan data jaringan untuk jaringan fisik
- ✓ Mengontrol bagaimana data ditempatkan dan diterima di media
- ✓ Saling menukar frame antar node melalui media jaringan fisik, seperti UTP atau fiber optic
- ✓ Menerima dan mengarahkan paket ke protokol lapisan atas
- ✓ Melakukan deteksi kesalahan

Notasi Layer 2 untuk perangkat jaringan yang terhubung ke media umum disebut node. Node membangun dan meneruskan frame. lapisan data link OSI bertanggung jawab atas pertukaran frame Ethernet antara node sumber dan tujuan melalui media jaringan fisik.

Lapisan data link secara efektif memisahkan transisi media yang terjadi saat paket diteruskan dari proses komunikasi lapisan yang lebih tinggi. Lapisan data link menerima paket dari dan mengarahkan paket ke protokol lapisan atas, dalam hal ini IPv4 atau IPv6. Protokol lapisan atas ini tidak perlu disadari media mana yang akan digunakan komunikasi.

Data Link Layer

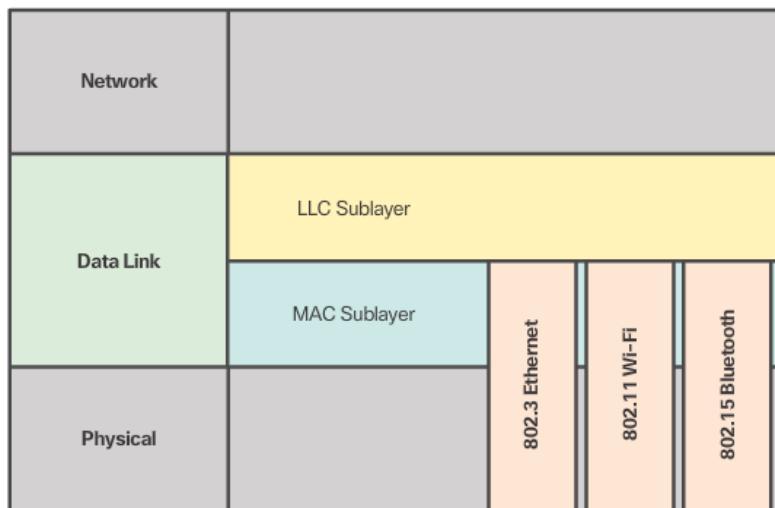


- **DATA LINK SUBLAYER**

Lapisan data link dibagi menjadi dua sublayer

- ✓ **Logical Link Control (LLC)** - Sublayer atas ini berkomunikasi dengan lapisan jaringan. Ini menempatkan informasi dalam bingkai yang mengidentifikasi protokol lapisan jaringan yang digunakan untuk frame tersebut. Informasi ini memungkinkan beberapa protokol Layer 3, seperti IPv4 dan IPv6, untuk memanfaatkan antarmuka jaringan dan media yang sama.
- ✓ **Media Access Control (MAC)** - Sublayer bawah ini mendefinisikan proses akses media yang dilakukan oleh perangkat keras. Ini menyediakan pengalaman lapisan data link dan akses ke berbagai teknologi jaringan.

bagaimana data link layer dipisahkan menjadi sublayer LLC dan MAC. LLC berkomunikasi dengan lapisan jaringan sementara sublayer MAC memungkinkan berbagai teknologi akses jaringan. Misalnya, sublayer MAC berkomunikasi dengan teknologi Ethernet LAN untuk mengirim dan menerima frame melalui kabel tembaga atau serat optik. Sublayer MAC juga berkomunikasi dengan teknologi nirkabel seperti Wi-Fi dan Bluetooth untuk mengirim dan menerima frame tanpa kabel.



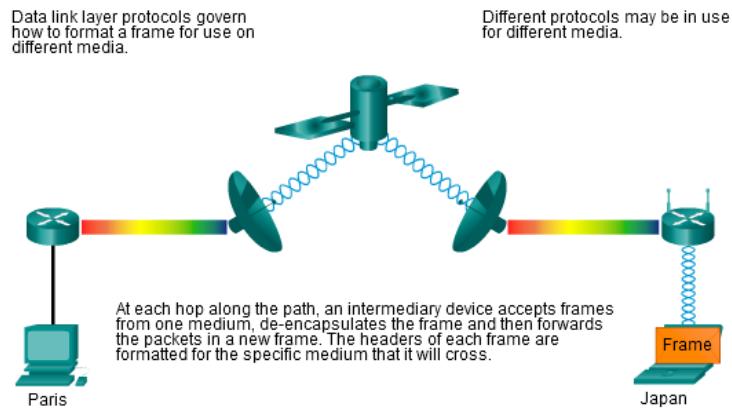
- **MEDIA AKSES CONTROL**

Protokol Layer 2 menentukan enkapsulasi paket ke dalam bingkai dan teknik untuk mendapatkan paket yang dienkapsulasi dan nonaktifkan setiap media. Teknik yang digunakan untuk mendapatkan frame dan mematikan media disebut metode kontrol akses media.

Selama perjalanan dari host sumber ke host tujuan, mereka biasanya melintasi jaringan fisik yang berbeda. Jaringan fisik ini dapat terdiri dari berbagai jenis media fisik seperti kabel tembaga, serat optik, dan nirkabel yang terdiri dari sinyal elektromagnetik, frekuensi radio dan gelombang mikro, dan tautan satelit.

Tanpa lapisan data link, protokol lapisan jaringan seperti IP, harus membuat ketentuan untuk terhubung ke setiap jenis media yang bisa ada di sepanjang jalur pengiriman. Apalagi IP harus beradaptasi setiap saat teknologi atau media jaringan baru dikembangkan. Proses ini akan menghambat inovasi dan pengembangan media protokol dan jaringan. Ini adalah alasan utama untuk menggunakan pendekatan berlapis untuk berjejaring.

The Data Link Layer



• PENYEDIAAN AKSES KE MEDIA

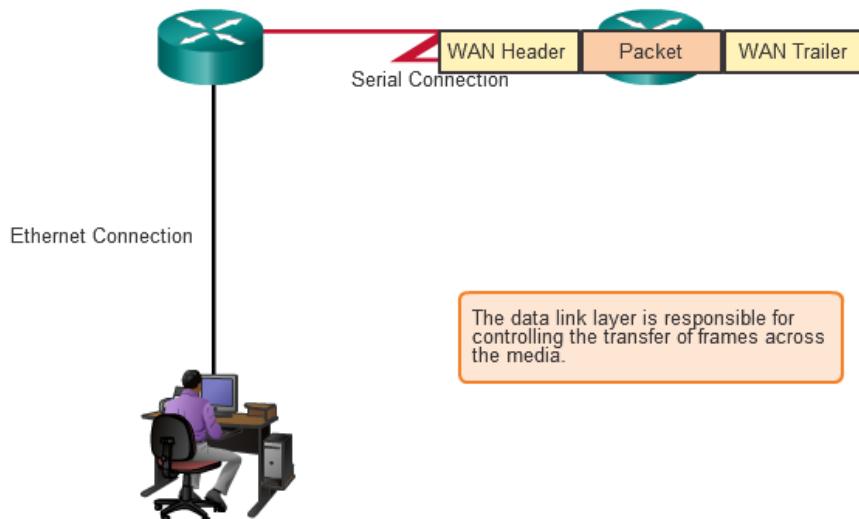
Metode kontrol akses media yang berbeda mungkin diperlukan selama satu komunikasi. Setiap lingkungan jaringan yang dihadapi paket saat mereka melakukan perjalanan dari host lokal ke host jarak jauh dapat memiliki karakteristik yang berbeda. Misalnya, LAN Ethernet terdiri dari banyak host yang bersaing untuk mengakses media jaringan. Tutan serial terdiri dari koneksi langsung antara hanya dua perangkat.

Antarmuka router mengenkapsulasi paket ke frame yang sesuai, dan metode kontrol akses media yang sesuai digunakan untuk mengakses setiap tautan. Dalam setiap pertukaran paket lapisan jaringan, mungkin ada banyak lapisan data link dan media transisi.

Pada setiap hop di sepanjang jalan, sebuah router:

- ✓ Accepts a frame from a medium
- ✓ De-encapsulates the frame
- ✓ Re-encapsulates the packet into a new frame
- ✓ Forwards the new frame appropriate to the medium of that segment of the physical network

Transfer of Frames



Router pada gambar memiliki antarmuka Ethernet untuk terhubung ke LAN dan sebuah antarmuka serial untuk terhubung ke WAN. Sebagai frame proses router, akan menggunakan layanan lapisan data link untuk menerima frame dari satu medium, de-encapsulate ke Layer 3 PDU, mengenkapsulasi kembali PDU ke dalam bingkai baru, dan letakkan bingkai pada medium dari link jaringan berikutnya.

- **STANDARISASI DATA LINK LAYER**

Berbeda dengan protokol lapisan atas dari paket TCP / IP, protokol lapisan data link umumnya tidak ditentukan oleh Request for Comments (RFC). Meskipun Internet Engineering Task Force (IETF) mempertahankan protokol dan layanan fungsional untuk suite protokol TCP / IP di lapisan atas, IETF tidak menentukan fungsi dan pengoperasian lapisan akses jaringan model tersebut.

Organisasi teknik yang mendefinisikan standar terbuka dan protokol yang berlaku untuk lapisan akses jaringan meliputi:

- ✓ Institute of Electrical and Electronics Engineers (IEEE)
- ✓ International Telecommunication Union (ITU)
- ✓ International Organization for Standardization (ISO)
- ✓ American National Standards Institute (ANSI)

4.5 KENDALI AKSES MEDIA

- ❖ **TOPOLOGIES**

- **PENGENDALIAN AKSES KE MEDIA**

Mengatur penempatan frame data ke media dikendalikan oleh media access control sublayer. Kontrol akses media sama dengan peraturan lalu lintas yang mengatur masuknya kendaraan bermotor ke jalan raya. Tidak adanya kontrol akses media akan sama dengan kendaraan yang mengabaikan semua lalu lintas lainnya dan memasuki jalan tanpa memperhatikan kendaraan lain. Namun, tidak semua jalan dan pintu masuk sama saja. Lalu lintas bisa masuk jalan dengan penggabungan, dengan menunggu giliran pada tanda berhenti, atau dengan mematuhi lampu sinyal. Sopir mengikuti peraturan yang berbeda untuk setiap jenis pintu masuk.

Dengan cara yang sama, ada beberapa metode yang berbeda untuk mengatur penempatan frame ke media. Protokol pada lapisan data link menentukan aturan untuk akses ke media yang berbeda. Teknik kontrol akses media ini menentukan apakah dan bagaimana node berbagi media.

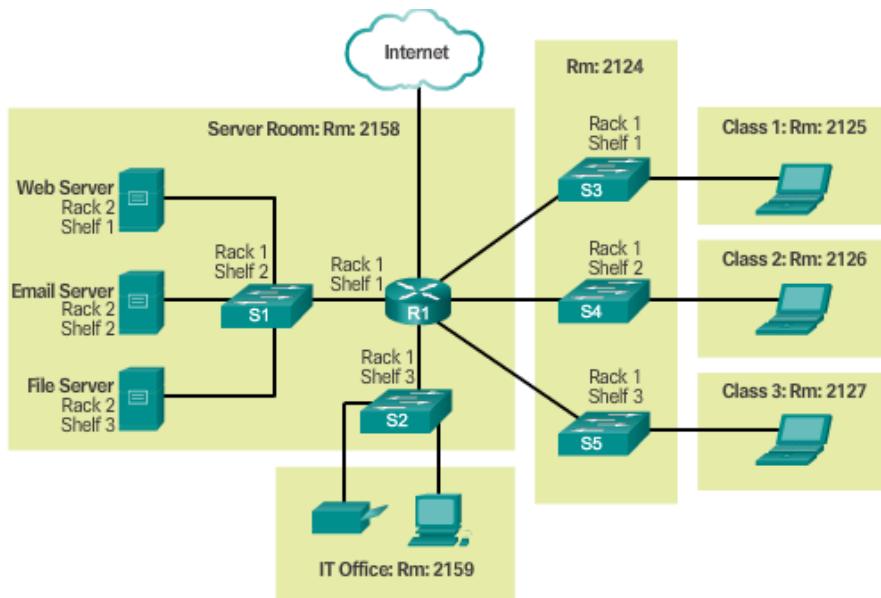
Metode kontrol akses media yang sebenarnya digunakan bergantung pada:

- ✓ **Topologi** - Bagaimana hubungan antara node muncul ke lapisan data link.
- ✓ **Sharing media** - Bagaimana node berbagi media. Sharing media bisa saling point-to-point, seperti koneksi WAN, atau shared seperti di jaringan LAN.

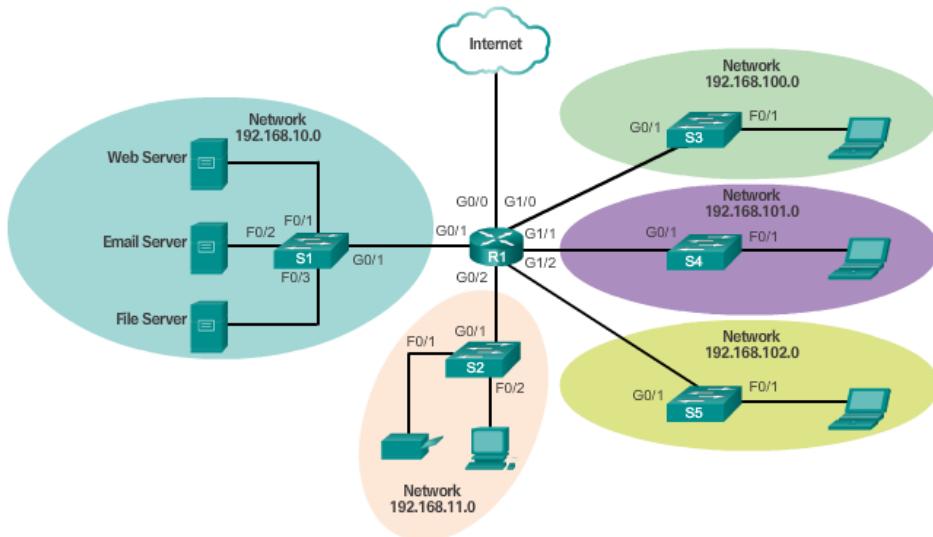
• TOPOLOGI FISIK DAN LOGIKA

Topologi jaringan adalah pengaturan atau hubungan perangkat jaringan dan interkoneksi di antara keduanya. Topologi LAN dan WAN dapat dilihat dengan dua cara:

- ✓ **Topologi fisik** - Mengacu pada koneksi fisik dan mengidentifikasi bagaimana perangkat akhir dan perangkat infrastruktur seperti router, switch, dan titik akses nirkabel saling terkait. Topologi fisik biasanya mengarah ke titik atau bintang.



- ✓ **Topologi logis** - Mengacu pada cara jaringan mentransfer frame dari satu node ke node berikutnya. Pengaturan ini terdiri dari koneksi virtual antara node jaringan. Jalur sinyal logis ini didefinisikan oleh protokol lapisan data link. Topologi logis dari link point-to-point relatif sederhana sementara media berbagi menawarkan metode kontrol akses yang berbeda.

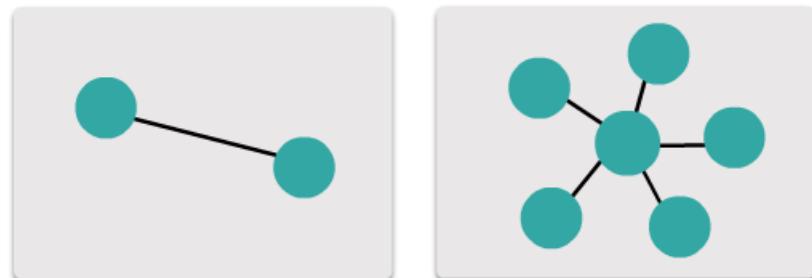


❖ WAN TOPOLOGIES

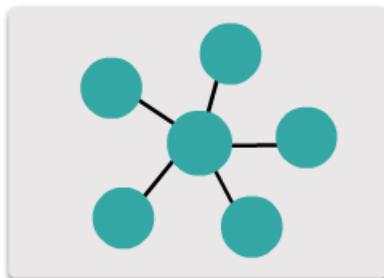
- TOPOLOGI FISIK WAN SECARA UMUM

WAN biasanya saling berhubungan menggunakan topologi fisik berikut:

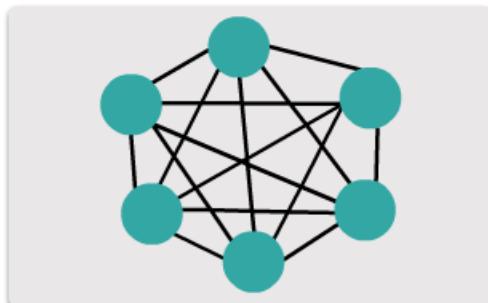
- ✓ **Point-to-Point** - Ini adalah topologi paling sederhana yang terdiri dari hubungan permanen antara dua titik akhir. Untuk alasan ini, ini adalah topologi WAN yang sangat populer.
- ✓ **Hub and Spoke** - Versi WAN dari topologi bintang di mana situs utama menghubungkan situs cabang menggunakan tautan point-to-point.
- ✓ **Mesh** - Topologi ini menyediakan ketersediaan tinggi, namun mengharuskan setiap sistem akhir saling terhubung ke setiap sistem lainnya. Oleh karena itu biaya administrasi dan fisik bisa jadi signifikan. Setiap link pada dasarnya adalah link point-to-point ke node lainnya. Variasi topologi ini termasuk mesh parsial dimana beberapa tapi tidak semua perangkat akhir saling berhubungan.



Point-to-point topology



Hub and spoke topology

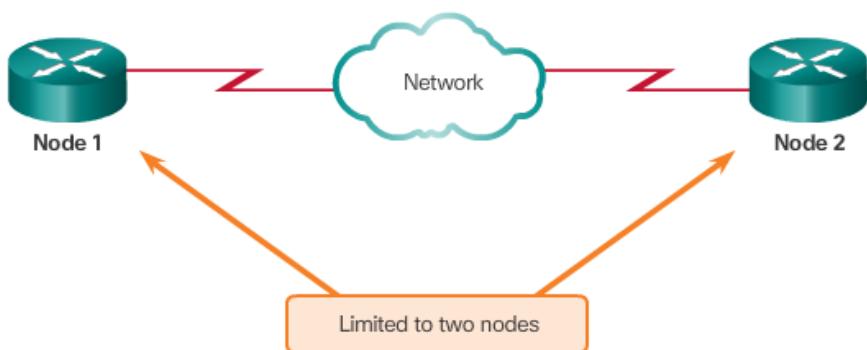


Full mesh topology

- **TOPOLOGI POINT – TO – POINT FISIK**

Topologi point-to-point fisik secara langsung menghubungkan dua simpul.

Dalam pengaturan ini, dua node tidak harus berbagi media dengan host lain. Selain itu, sebuah simpul tidak harus membuat keputusan apakah frame yang masuk ditakdirkan untuk itu atau simpul lainnya. Oleh karena itu, protokol data link logis bisa sangat sederhana, karena semua frame di media hanya bisa melakukan perjalanan ke atau dari dua node. Bingkai ditempatkan pada media oleh simpul di salah satu ujung dan diambil dari media oleh simpul di ujung sirkuit point-to-point.

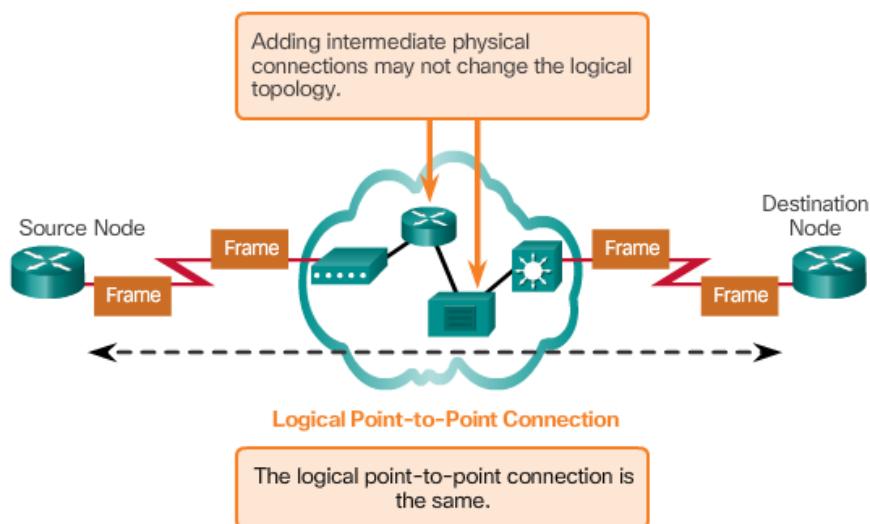


- **TOPOLOGI POINT – TO – POINT LOGIS**

Titik akhir yang berkomunikasi dalam jaringan point-to-point dapat dihubungkan secara fisik melalui sejumlah perangkat perantara. Namun, penggunaan perangkat fisik dalam jaringan tidak mempengaruhi topologi logis.

Simpul sumber dan tujuan dapat dihubungkan secara tidak langsung satu sama lain melalui beberapa jarak geografis. Dalam beberapa kasus, koneksi logis antara node membentuk apa yang disebut rangkaian virtual. Rangkaian virtual adalah koneksi logis yang dibuat di dalam jaringan di antara dua perangkat jaringan. Dua simpul di kedua ujung sirkuit virtual saling menukar bingkai satu sama lain. Hal ini terjadi bahkan jika frame diarahkan melalui perangkat perantara.

Sirkuit virtual adalah komunikasi logis penting yang digunakan oleh beberapa teknologi Layer 2. Metode akses media yang digunakan oleh protokol data link ditentukan oleh topologi logical point-to-point, bukan topologi fisik. Ini berarti bahwa koneksi point-to-point logis antara dua node mungkin tidak harus berada di antara dua node fisik di setiap akhir dari satu tautan fisik.



❖ LAN TOPOLOGIES

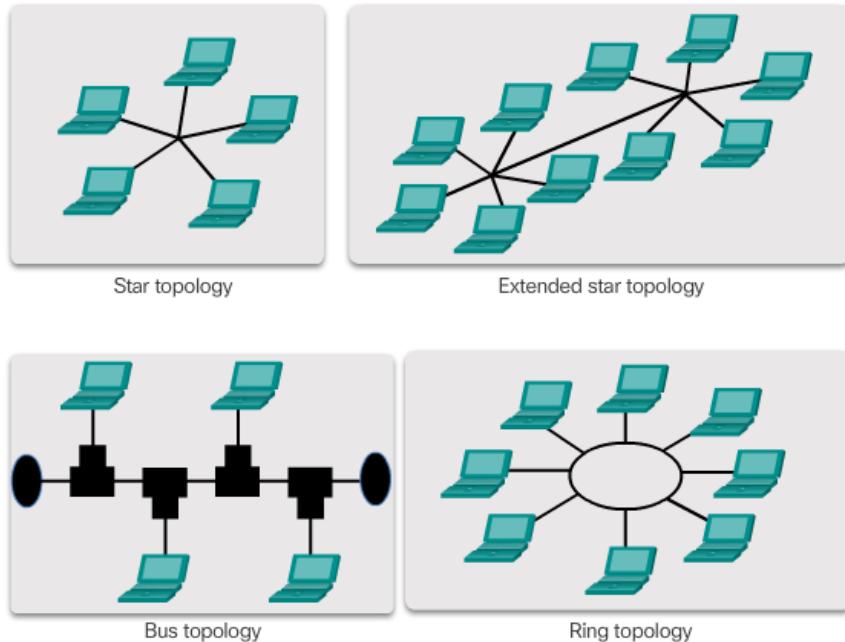
• TOPOLOGI FISIK LAN SECARA UMUM

Topologi fisik menentukan bagaimana sistem akhir saling berhubungan secara fisik. Dalam LAN media bersama, perangkat akhir dapat saling berhubungan menggunakan topologi fisik berikut:

- ✓ **Star** - Perangkat akhir terhubung ke perangkat perantara pusat. Topologi bintang awal menghubungkan perangkat akhir menggunakan hub Ethernet. Namun, topologi star sekarang menggunakan switch Ethernet. Topologi star mudah dipasang, sangat skalabel (mudah untuk menambahkan dan menghapus perangkat akhir), dan mudah untuk memecahkan masalah.
- ✓ **Extended Star** - Dalam topologi bintang yang diperluas, switch Ethernet tambahan menghubungkan topologi bintang lainnya.
- ✓ **Bus** - Semua sistem akhir dirantai satu sama lain dan diakhiri dalam beberapa bentuk pada setiap akhir. Perangkat infrastruktur seperti switch tidak diharuskan untuk

menghubungkan perangkat akhir. Topologi bus yang menggunakan kabel coax digunakan di jaringan Ethernet warisan karena harganya murah dan mudah dipasang.

- ✓ **Sistem Ring** - End terhubung ke tetangga masing-masing membentuk sebuah cincin. Berbeda dengan topologi bus, ring tidak perlu diakhiri. Topologi ring digunakan dalam jaringan Fiber Distributed Data Interface (FDDI) dan jaringan Token Ring yang terdepribusi.



- **HALF DAN FULL DUPLEX**

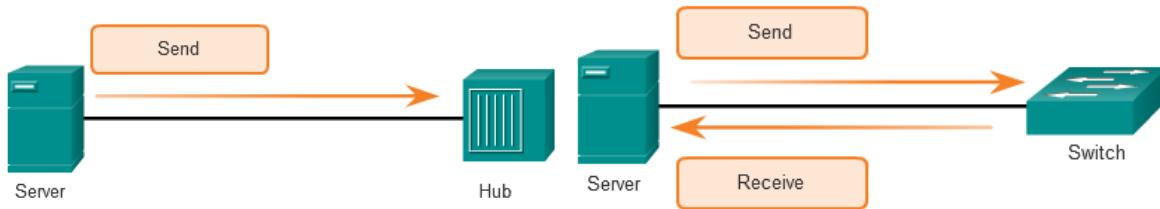
Komunikasi dupleks mengacu pada arah transmisi data antara dua perangkat. Komunikasi half-duplex membatasi pertukaran data ke satu arah pada satu waktu sementara full-duplex memungkinkan pengiriman dan penerimaan data terjadi secara bersamaan.

- ✓ **Komunikasi half-duplex** - Kedua perangkat dapat mentransmisikan dan menerima di media namun tidak dapat melakukannya secara bersamaan. Mode half-duplex digunakan dalam topologi bus lama dan dengan hub Ethernet. WLAN juga beroperasi dalam half-duplex. Half-duplex hanya mengizinkan satu perangkat untuk mengirim atau menerima sekaligus pada media bersama dan digunakan dengan metode akses berbasis contention.
- ✓ **Komunikasi full-duplex** - Kedua perangkat dapat mentransmisikan dan menerima pada media secara bersamaan. Lapisan tautan data mengasumsikan bahwa media tersedia untuk transmisi untuk kedua nodus kapan saja. Switch Ethernet beroperasi dalam mode full-duplex secara default, namun dapat beroperasi dalam half-duplex jika terhubung ke perangkat seperti hub Ethernet.

Penting bahwa dua antarmuka yang saling berhubungan, seperti NIC host dan sebuah antarmuka pada switch Ethernet beroperasi menggunakan mode dupleks yang sama. Jika tidak, akan ada ketidakcocokan dupleks yang menciptakan inefisiensi dan latensi pada tautan.

Half-Duplex Communication

Full-Duplex Communication



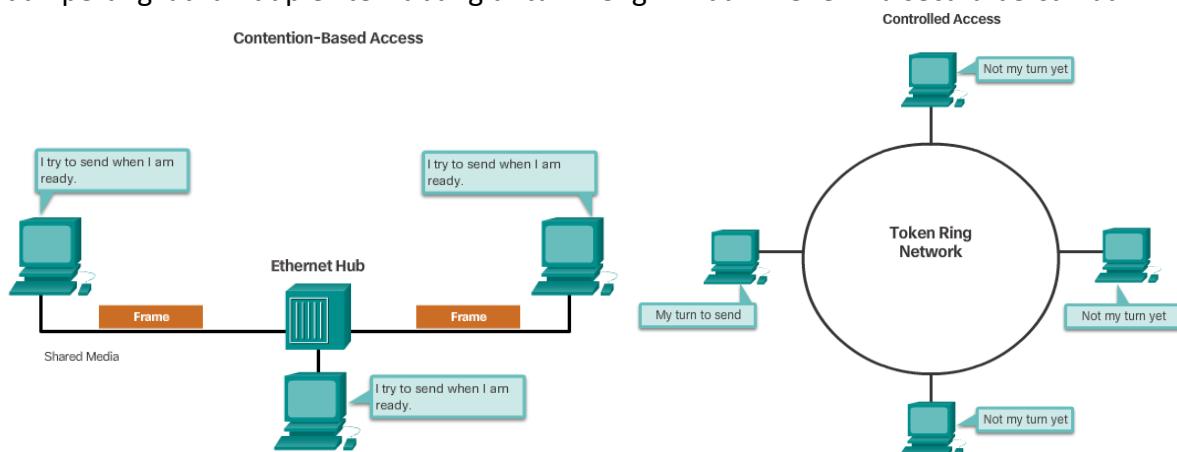
• METODE AKSES KONTROL MEDIA

Beberapa topologi jaringan berbagi media umum dengan banyak node. Ini disebut jaringan multi-akses. LAN Ethernet dan WLAN adalah contoh jaringan multi-akses. Pada satu waktu, mungkin ada sejumlah perangkat yang mencoba mengirim dan menerima data menggunakan media jaringan yang sama.

Beberapa jaringan multi-akses memerlukan aturan untuk mengatur bagaimana perangkat berbagi media fisik. Ada dua metode kontrol akses dasar untuk media bersama:

- ✓ **Contention Based access** - Semua node yang beroperasi dalam half-duplex bersaing untuk penggunaan media, namun hanya satu perangkat yang bisa mengirim sekaligus. Namun, ada proses jika lebih dari satu perangkat mentransmisikan pada saat bersamaan. LAN Ethernet yang menggunakan hub dan WLAN adalah contoh dari jenis kontrol akses ini.
- ✓ **Controlled Access** - Setiap node memiliki waktu sendiri untuk menggunakan medium. Jenis jaringan deterministik ini tidak efisien karena perangkat harus menunggu giliran untuk mengakses media. Warisan Token Ring LAN adalah contoh dari jenis kontrol akses ini.

Secara default, switch Ethernet beroperasi dalam mode full-duplex. Ini memungkinkan switch dan perangkat full-duplex terhubung untuk mengirim dan menerima secara bersamaan.



❖ DATA LINK FRAME

• FRAME

Lapisan data link menyiapkan paket untuk transportasi melintasi media lokal dengan mengenkapsulasinya dengan sebuah header dan sebuah trailer untuk membuat bingkai. Deskripsi frame adalah elemen kunci dari setiap protokol layer data link. Meskipun ada banyak protokol lapisan data link yang menggambarkan frame layer data link, setiap tipe frame memiliki tiga bagian dasar:

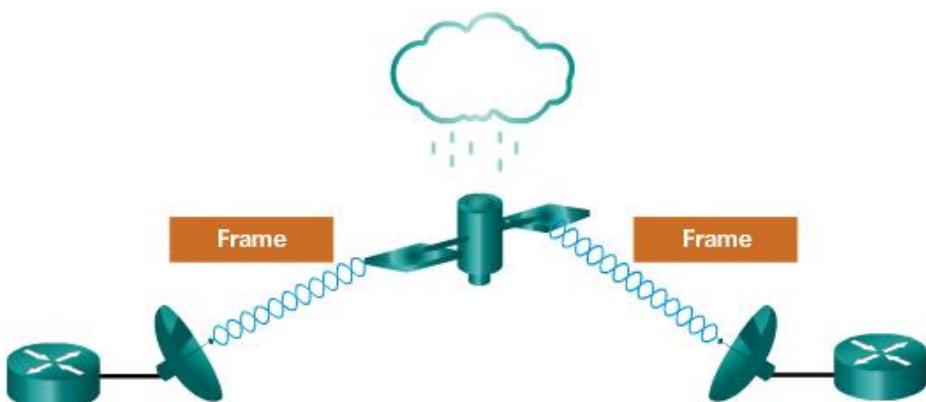
- ✓ Header
- ✓ Data
- ✓ Trailer

Semua protokol lapisan data link merangkum Layer 3 PDU di dalam bidang data frame. Namun, struktur frame dan field yang terdapat pada header dan trailer bervariasi sesuai dengan protokol.

Tidak ada satu struktur rangka yang memenuhi kebutuhan semua data transportasi di semua jenis media. Bergantung pada lingkungan, jumlah informasi kontrol yang dibutuhkan dalam bingkai bervariasi sesuai dengan persyaratan kontrol akses media dan topologi logis.

Fragile Environment

Greater effort needed to ensure delivery = higher overhead = slower transmission rates



• FRAME FIELDS

Pembingkaian memecah arus menjadi pengelompokan yang dapat diuraikan, dengan informasi kontrol dimasukkan ke dalam header dan trailer sebagai nilai di berbagai bidang. Format ini memberi sinyal fisik suatu struktur yang bisa diterima oleh node dan diterjemahkan ke dalam paket di tempat tujuan.

Seperi ditunjukkan pada gambar, jenis bidang bingkai generik meliputi:

- ✓ **Frame start and stop indicator flags** - Digunakan untuk mengidentifikasi batasan awal dan akhir frame.
- ✓ **Addressing** - Mengindikasikan node sumber dan tujuan pada media.
- ✓ **Type** - Mengidentifikasi protokol Layer 3 di bidang data.

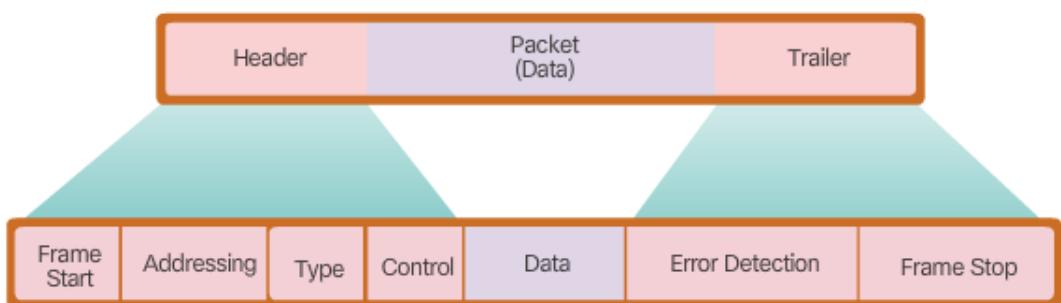
- ✓ **Control** - Mengidentifikasi layanan kontrol aliran khusus seperti kualitas layanan (QoS). QoS digunakan untuk memberi prioritas penerusan pada jenis pesan tertentu. Bingkai data link yang membawa paket voice over IP (VoIP) biasanya mendapat prioritas karena sensitif terhadap penundaan.
- ✓ **Data** - Berisi muatan payload (yaitu header paket, header segmen, dan data).
- ✓ **Deteksi Kesalahan** - Bidang bingkai ini digunakan untuk mendeteksi kesalahan dan disertakan setelah data dimasukkan ke dalam trailer.

Tidak semua protokol mencakup semua bidang ini. Standar untuk protokol link data tertentu menentukan format frame yang sebenarnya.

Protokol lapisan data link menambahkan trailer ke akhir setiap frame. Trailer digunakan untuk menentukan apakah frame tersebut tiba tanpa kesalahan. Proses ini disebut deteksi kesalahan dan dilakukan dengan menempatkan ringkasan logis atau matematis dari bit-bit yang membentuk bingkai di trailer. Deteksi kesalahan ditambahkan pada lapisan data link karena sinyal pada media dapat terganggu, distorsi, atau kehilangan yang secara substansial akan mengubah nilai bit yang ditunjukkan oleh sinyal tersebut.

Sebuah node transmisi menciptakan ringkasan logis dari isi frame, yang dikenal sebagai nilai cek redundansi siklik (CRC). Nilai ini ditempatkan di bidang Frame Check Sequence (FCS) untuk mewakili isi frame. Di trailer Ethernet, FCS menyediakan metode untuk node penerima untuk menentukan apakah frame mengalami kesalahan transmisi.

Frame Fields



LATIHAN SOAL 4

1. Jelaskan yang dimaksud dengan NIC
2. Apa yang dimaksud dengan layer fisik
3. Sebutkan media layer fisik
4. Jelaskan karakteristik layer fisik
5. Jelaskan yang dimaksud dengan throughput
6. sebutkan jenis-jenis kabel coper
7. Jelaskan perbedaan antara kabel Unshielded Twisted Pair (UTP), Shielded Twisted Pair (STP) & Kabel Coaxial,
8. Jelaskan tipe-tipe kabel UTP
9. Sebutkan jenis-jenis serat optik
10. Sebutkan area / hal yang mempengaruhi kinerja wireless
11. Jelaskan yang dimaksud dengan Data link layer
12. Jelaskan perbedaan antara Topologi Fisik dan Topologgi Logik suatu Jaringan
13. Sebutkan jenis topologik fisik sebuah LAN
14. Jelaskan perbedaan antara Half dan full DUPlex
15. Jelaskan yang dimaksud dengan Frame datalink

BAB 5 ETHERNET

5.1 PENGANTAR

Lapisan fisik OSI menyediakan sarana untuk mengangkut bit yang membentuk bingkai lapisan data link di media jaringan.

Ethernet sekarang merupakan teknologi LAN yang dominan di dunia. Ethernet beroperasi di lapisan data link dan lapisan fisik. Standar protokol Ethernet menentukan banyak aspek komunikasi jaringan termasuk format frame, ukuran frame, timing, dan encoding. Bila pesan dikirim antara host pada jaringan Ethernet, host akan memformat pesan ke dalam susunan bingkai yang ditentukan oleh standar.

Karena Ethernet terdiri dari standar pada lapisan bawah ini, paling baik dipahami mengacu pada model OSI. Model OSI memisahkan fungsionalitas lapisan link data untuk menangani, membungkai, dan mengakses media dari standar lapisan fisik media. Standar Ethernet menentukan protokol Layer 2 dan teknologi Layer 1. Meskipun spesifikasi Ethernet mendukung media, bandwidth, dan variasi Layer 1 dan 2 yang berbeda, format frame dasar dan skema alamatnya sama untuk semua jenis Ethernet.

Bab ini membahas karakteristik dan pengoperasian Ethernet karena telah berevolusi dari media bersama, teknologi komunikasi data berbasis contention hingga bandwidth tinggi saat ini, teknologi full-duplex.

5.2 ETHERNET PROTOCOL

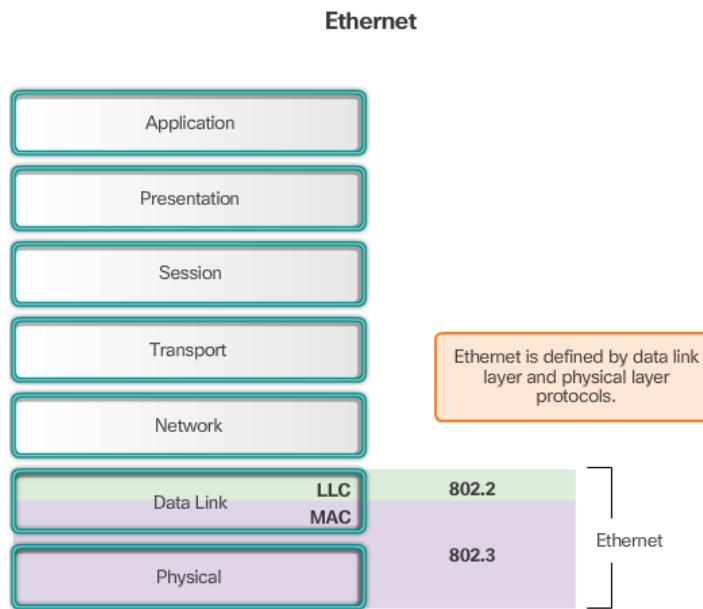
- ❖ **ETHERNET FRAME**
- **ETHERNET ENCAPSULATION**

Ethernet adalah teknologi LAN yang paling banyak digunakan saat ini.

Ethernet beroperasi di lapisan data link dan lapisan fisik. Ini adalah keluarga teknologi jaringan yang didefinisikan dalam standar IEEE 802.2 dan 802.3. Ethernet mendukung bandwidth data dari:

- ✓ 10 Mb / s
- ✓ 100 Mb / s
- ✓ 1000 Mb / s (1 Gb / s)
- ✓ 10.000 Mb / s (10 Gb / s)
- ✓ 40.000 Mb / s (40 Gb / s)
- ✓ 100.000 Mb / s (100 Gb / s)

Standar Ethernet menentukan protokol Layer 2 dan teknologi Layer 1. Untuk protokol Layer 2, seperti pada semua standar 802 IEEE, Ethernet mengandalkan dua sublayer lapisan data link yang terpisah untuk beroperasi, Logical Link Control (LLC) dan sublayer MAC.



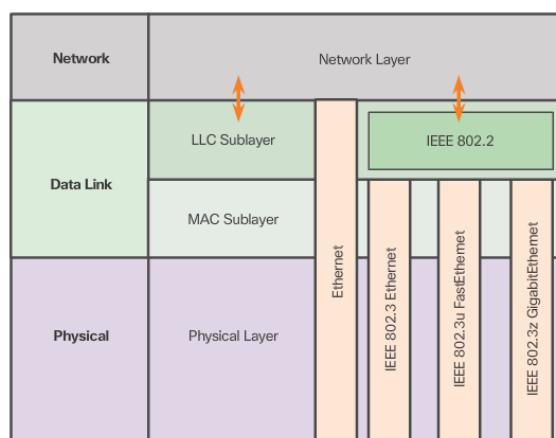
Sublayer LLC

Sublayer Ethernet LLC menangani komunikasi antara lapisan atas dan lapisan bawah. Ini biasanya antara perangkat lunak jaringan dan perangkat keras perangkat. Sublayer LLC mengambil data protokol jaringan, yang biasanya merupakan paket IPv4, dan menambahkan informasi kontrol untuk membantu mengirimkan paket ke simpul tujuan. LLC digunakan untuk berkomunikasi dengan lapisan atas aplikasi, dan mentransmisikan paket ke lapisan bawah untuk pengiriman.

LLC diimplementasikan dalam perangkat lunak, dan implementasinya tidak tergantung pada perangkat kerasnya. Di komputer, LLC bisa dianggap sebagai perangkat lunak driver untuk NIC. Driver NIC adalah program yang berinteraksi langsung dengan perangkat keras pada NIC untuk melewatkannya data antara sublayer MAC dan media fisik.

Sublayer MAC

MAC merupakan lapisan bawah lapisan data link. MAC diimplementasikan oleh perangkat keras, biasanya di komputer NIC. Spesifikasinya tercantum dalam standar IEEE 802.3.



- **MAC SUBLAYER**

Sublayer MAC Ethernet memiliki dua tanggung jawab utama:

- ✓ Enkapsulasi data
- ✓ Kontrol akses media

Enkapsulasi data

Proses enkapsulasi data mencakup perakitan bingkai sebelum transmisi, dan pembongkaran bingkai pada saat penerimaan bingkai. Dalam membentuk frame, lapisan MAC menambahkan header dan trailer ke lapisan jaringan PDU.

Enkapsulasi data menyediakan tiga fungsi utama:

- ✓ **Frame delimiting** - Proses pembingkaian memberikan pembatas penting yang digunakan untuk mengidentifikasi sekelompok bit yang membentuk bingkai. Bit delimiting ini menyediakan sinkronisasi antara node pemancar dan penerima.
- ✓ **Addressing** - Proses enkapsulasi berisi Layer 3 PDU dan juga menyediakan pengalamanan lapisan data link.
- ✓ **Error detection** - Setiap bingkai berisi cuplikan yang digunakan untuk mendeteksi kesalahan dalam transmisi.

Penggunaan frame membantu transmisi bit saat ditempatkan pada media dan dalam pengelompokan bit pada node penerima.

Media Access Control

Tanggung jawab kedua dari sublayer MAC adalah kontrol akses media. Kontrol akses media bertanggung jawab atas penempatan frame pada media dan penghapusan frame dari media. Sesuai namanya, ia mengendalikan akses ke media. Sublayer ini berkomunikasi langsung dengan layer fisik.

Topologi logis Ethernet yang mendasarinya adalah bus multi-akses; Oleh karena itu, semua node (perangkat) pada satu segmen jaringan berbagi media. Ethernet adalah metode pertarungan berbasis networking. Metode berbasis contention berarti bahwa setiap perangkat dapat mencoba mentransmisikan data ke media bersama setiap kali data dikirim. Proses Carrier Sense Multiple Access / Collision Detection (CSMA / CD) digunakan di LAN Ethernet setengah-dupleks untuk mendeteksi dan menyelesaikan tabrakan. Ethernet LAN hari ini menggunakan switch full-duplex, yang memungkinkan beberapa perangkat untuk mengirim dan menerima bersamaan tanpa benturan.

- **ETHERNET EVOLUTION**

Sejak penciptaan Ethernet pada tahun 1973, standar telah berkembang untuk menentukan versi teknologi yang lebih cepat dan lebih fleksibel. Kemampuan Ethernet ini untuk memperbaiki seiring berjalannya waktu adalah salah satu alasan utama mengapa menjadi sangat populer. Versi awal Ethernet relatif lambat pada 10 Mbps. Versi terbaru dari Ethernet beroperasi pada 10 Gigabit per detik dan lebih cepat.

Pada layer data link, struktur frame hampir identik untuk semua kecepatan Ethernet. Struktur bingkai Ethernet menambahkan header dan trailer di sekitar Layer 3 PDU untuk merangkum pesan yang sedang dikirim,

Ethernet II adalah format frame Ethernet yang digunakan pada jaringan TCP / IP.

- **ETHERNET FRAME FIELDS**

Ukuran frame Ethernet minimum adalah 64 byte dan maksimumnya adalah 1518 byte. Ini mencakup semua byte dari field Destination MAC Address melalui bidang Frame Check Sequence (FCS). Bidang Mukadimah tidak disertakan saat menjelaskan ukuran bingkai.

Setiap frame berdurasi kurang dari 64 byte dianggap sebagai "fragmen tabrakan" atau "kerangka keruntuhan" dan secara otomatis dibuang oleh stasiun penerima. Bingkai dengan lebih dari 1500 byte data dianggap "jumbo" atau "bingkai raksasa bayi".

Jika ukuran frame yang ditransmisikan kurang dari minimum atau lebih besar dari maksimum, perangkat penerima akan menjatuhkan frame. Jari yang terjatuh kemungkinan besar merupakan hasil tabrakan atau sinyal yang tidak diinginkan lainnya dan oleh karena itu dianggap tidak valid.

- **ETHERNET MAC ADDRESSES**

Alamat MAC Ethernet adalah nilai biner 48 bit yang dinyatakan sebagai 12 digit heksadesimal (4 bit per digit heksadesimal).

Sama seperti desimal adalah sistem bilangan dasar sepuluh, heksadesimal adalah sistem enam belas basis. Sistem bilangan enam belas dasar menggunakan angka 0 sampai 9 dan huruf A sampai F. Gambar 1 menunjukkan nilai desimal dan heksadesimal yang setara untuk biner 0000 sampai 1111. Lebih mudah untuk mengekspresikan nilai sebagai digit heksadesimal tunggal daripada empat bit biner .

Mengingat 8 bit (satu byte) adalah pengelompokan biner yang umum, biner 00000000 sampai 11111111 dapat direpresentasikan dalam heksadesimal sebagai rentang 00 ke FF, seperti yang ditunjukkan pada Gambar 2. Angka nol yang menonjol selalu ditampilkan untuk melengkapi representasi 8-bit. Sebagai contoh, nilai biner 0000 1010 ditampilkan dalam heksadesimal sebagai 0A.

Catatan: Penting untuk membedakan nilai heksadesimal dari nilai desimal berkenaan dengan karakter 0 sampai 9

Representing Nilai Hexadecimal

Heksadesimal biasanya diwakili dalam teks dengan nilai yang didahului oleh 0x (misalnya 0x73) atau subskrip 16. Kurang umum, hal itu mungkin diikuti oleh H (misalnya 73H). Namun, karena teks subscript tidak dikenali pada lingkungan perintah atau pemrograman, representasi teknis heksadesimal didahului dengan "0x" (nol X).

Heksadesimal digunakan untuk mewakili alamat MAC Ethernet dan alamat IP Version 6.

Konversi Heksadesimal

Jumlah konversi antara nilai desimal dan nilai heksadesimal sangat mudah, namun dengan cepat membagi atau mengalikan dengan 16 tidak selalu mudah. Jika konversi semacam itu diperlukan, biasanya lebih mudah untuk mengubah nilai desimal atau heksadesimal menjadi biner, dan kemudian mengubah nilai biner menjadi desimal atau heksadesimal yang sesuai.

Hexadecimal Numbering		
Selected Decimal, Binary, and Hexadecimal equivalents		
Decimal	Binary	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

• MAC ADDRESSES : IDENTITAS ETHERNET

Di Ethernet, setiap perangkat jaringan terhubung ke media bersama yang sama. Ethernet pernah didominasi oleh topologi half-duplex menggunakan bus multi-access atau hub Ethernet yang lebih baru. Ini berarti semua node akan menerima setiap frame yang ditransmisikan. Untuk mencegah overhead yang berlebihan yang terlibat dalam pemrosesan setiap frame, alamat MAC dibuat untuk mengidentifikasi sumber dan tujuan yang sebenarnya. MAC addressing menyediakan metode untuk identifikasi perangkat pada tingkat yang lebih rendah dari model OSI. Meskipun Ethernet sekarang telah beralih ke NIC full-duplex dan switch, masih mungkin perangkat yang bukan tujuan yang dimaksud akan menerima frame Ethernet.

MAC Address Structure

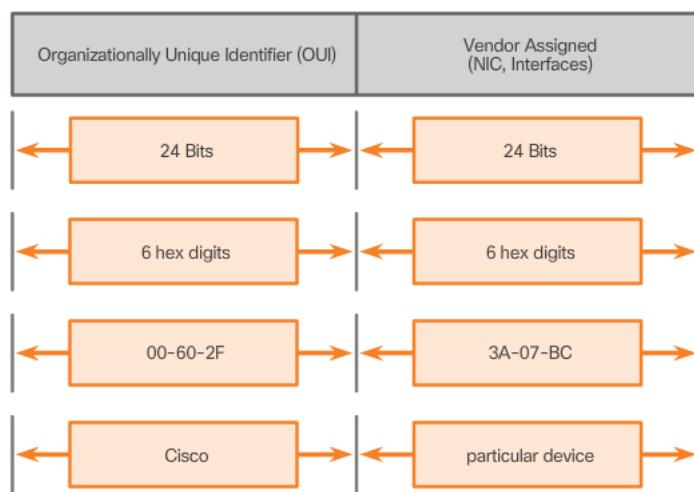
Nilai alamat MAC adalah akibat langsung dari aturan yang diberlakukan IEEE bagi vendor untuk memastikan alamat unik global untuk setiap perangkat Ethernet. Aturan yang ditetapkan oleh IEEE memerlukan vendor yang menjual perangkat Ethernet untuk mendaftar ke IEEE. IEEE menugaskan vendor kode 3-byte (24-bit), yang disebut Organizationally Unique Identifier (OUI).

IEEE membutuhkan vendor untuk mengikuti dua aturan sederhana:

- ✓ Semua alamat MAC yang ditugaskan ke NIC atau perangkat Ethernet lainnya harus menggunakan OUI yang diberikan vendor tersebut sebagai 3 byte pertama.
- ✓ Semua alamat MAC dengan OUI yang sama harus diberi nilai unik dalam 3 byte terakhir.

Catatan: Ada kemungkinan alamat duplikat MAC ada karena kesalahan selama pembuatan atau beberapa metode penerapan mesin virtual. Dalam kedua kasus tersebut, perlu memodifikasi alamat MAC dengan NIC baru atau perangkat lunak.

The Ethernet MAC Address Structure



• FRAME PROCESSING

Alamat MAC sering disebut sebagai alamat yang dibakar (BIA) karena, secara historis, alamat ini dibakar ke ROM (Read-Only Memory) pada NIC. Ini berarti alamat tersebut dikodekan ke dalam chip ROM secara permanen.

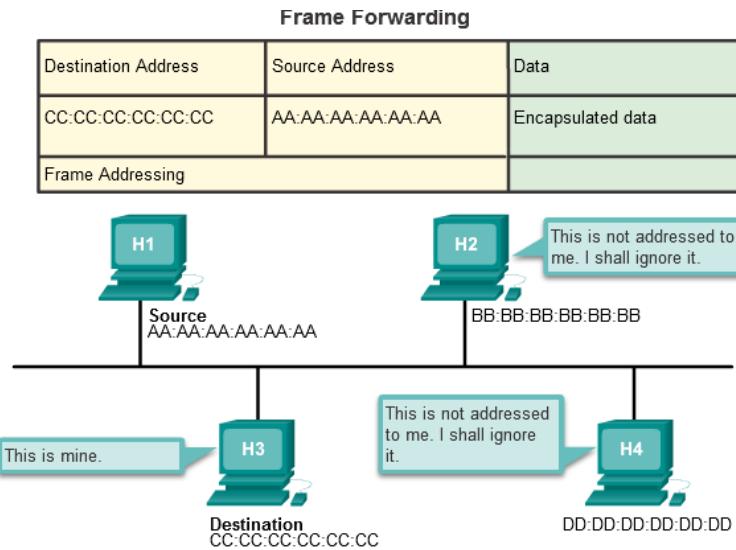
Catatan: Pada sistem operasi PC modern dan NIC, adalah mungkin untuk mengubah alamat MAC dalam perangkat lunak. Ini berguna saat mencoba mengakses jaringan yang memfilter berdasarkan BIA. Akibatnya, memfilter atau mengendalikan lalu lintas berdasarkan alamat MAC tidak lagi seaman.

Saat komputer dinyalakan, hal pertama yang dilakukan NIC adalah menyalin alamat MAC dari ROM ke RAM. Saat perangkat meneruskan pesan ke jaringan Ethernet, perangkat akan memasukkan informasi header ke paket. Informasi header berisi alamat MAC sumber dan tujuan.

Bila NIC menerima frame Ethernet, ia akan memeriksa alamat MAC tujuan untuk mengetahui apakah itu sesuai dengan alamat MAC fisik perangkat yang tersimpan dalam RAM. Jika tidak ada yang cocok, perangkat akan membuang frame. Jika ada kecocokan, ia melewati bingkai di atas lapisan OSI, di mana proses de-enkapsulasi berlangsung.

Catatan: NIC Ethernet juga akan menerima frame jika alamat MAC tujuan disiarkan atau grup multicast dimana host adalah anggota.

Setiap perangkat yang bisa menjadi sumber atau tujuan dari sebuah frame Ethernet harus diberi alamat MAC. Ini termasuk workstation, server, printer, perangkat mobile, dan router.



- **MAC ADDRESS REPRESENTATIONS**

Pembuat perangkat keras dan perangkat lunak yang berbeda mungkin mewakili alamat MAC dalam format heksadesimal yang berbeda, seperti yang ditunjukkan di bawah ini:

- 00-05-9A-3C-78-00
- 00:05:9A:3C:78:00
- 0005.9A3C.7800

Pada host Windows, perintah ipconfig / all dapat digunakan untuk mengidentifikasi alamat MAC dari adaptor Ethernet. Pada Gambar 1, perhatikan tampilan menunjukkan Alamat Fisik (MAC) komputer menjadi 00-18-DE-DD-A7-B2. Jika Anda memiliki akses, Anda mungkin ingin mencobanya di komputer Anda sendiri. Pada host MAC atau Linux, perintah ifconfig digunakan.

Bergantung pada perangkat dan sistem operasi, Anda akan melihat berbagai representasi alamat MAC

```
C:\> ipconfig/all

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : example.com
Description . . . . . : Intel(R) Gigabit Network Connection
Physical Address . . . . . : 00-18-DE-DD-A7-B2
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::449f:c2:de06:ebad%10 (Preferred)
IPv4 Address. . . . . : 10.10.10.2 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, June 01, 2015 11:19:48 AM
Lease Expires . . . . . : Thursday, June 04, 2015 11:19:49 PM
Default Gateway . . . . . : 10.10.10.1
DHCP Server . . . . . : 10.10.10.1
DNS Servers . . . . . : 10.10.10.1
```

- **UNICAST MAC ADDRESS**

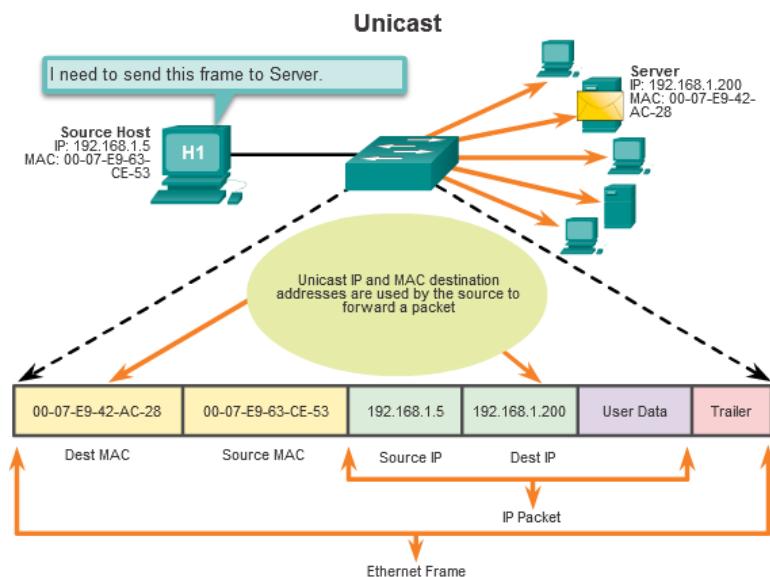
Di Ethernet, alamat MAC yang berbeda digunakan untuk komunikasi Layer 2 unicast, broadcast, dan multicast.

Alamat MAC unicast adalah alamat unik yang digunakan saat bingkai dikirim dari satu perangkat transmisi ke perangkat tujuan tunggal.

host dengan alamat IPv4 192.168.1.5 (sumber) meminta halaman web dari server di alamat unicast IPv4 192.168.1.200. Untuk paket unicast yang akan dikirim dan diterima, alamat IP tujuan harus berada dalam header paket IP. Alamat MAC tujuan yang sesuai juga harus ada dalam header bingkai Ethernet. Alamat IP dan alamat MAC digabungkan untuk mengirimkan data ke satu host tujuan tertentu.

Proses yang digunakan host sumber untuk menentukan alamat MAC tujuan dikenal sebagai Address Resolution Protocol (ARP). ARP dibahas nanti di bab ini.

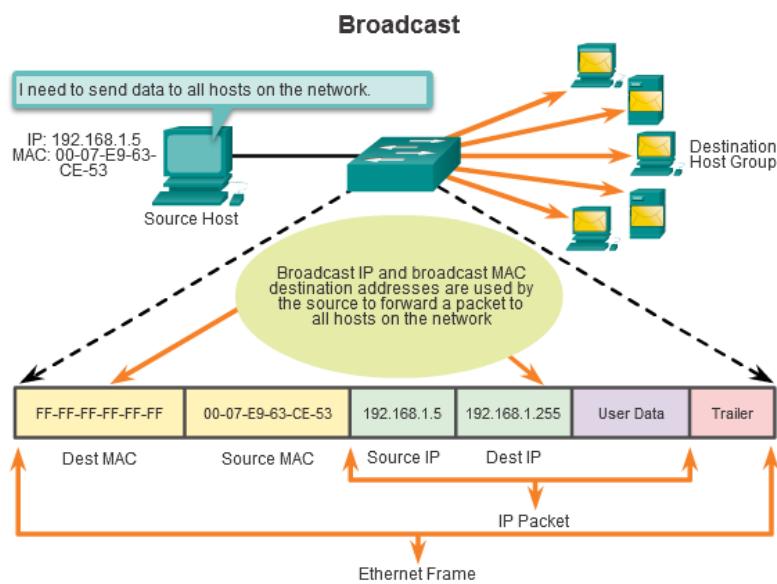
Meskipun alamat MAC tujuan bisa menjadi alamat unicast, broadcast, atau multicast, alamat MAC sumber harus selalu unicast.



- **BROADCAST MAC ADDRESS**

Paket broadcast berisi alamat IPv4 tujuan yang memiliki semua (1s) di bagian host. Penomoran di alamat ini berarti bahwa semua host pada jaringan lokal tersebut (broadcast domain) akan menerima dan memproses paket. Banyak protokol jaringan, seperti DHCP dan ARP, menggunakan siaran.

host sumber mengirimkan paket siaran IPv4 ke semua perangkat di jaringannya. Alamat tujuan IPv4 adalah alamat broadcast, 192.168.1.255. Ketika paket siaran IPv4 dienkapsulasi dalam bingkai Ethernet, alamat MAC tujuan adalah alamat MAC broadcast dari FF-FF-FF-FF-FF-FF dalam heksadesimal (48 di biner).



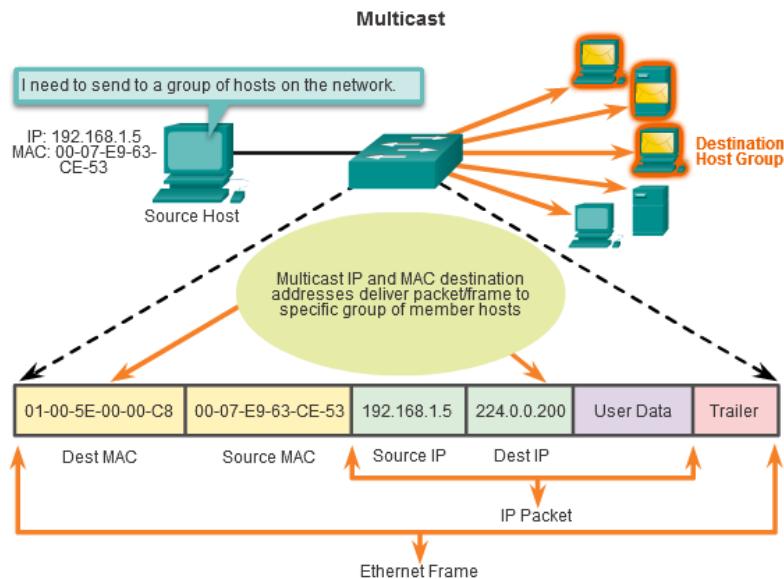
- **MULTICAST MAC ADDRESS**

Alamat multicast memungkinkan perangkat sumber mengirim paket ke sekelompok perangkat. Perangkat yang termasuk dalam grup multicast diberi alamat IP grup multicast. Kisaran alamat multicast IPv4 adalah 224.0.0.0 sampai 239.255.255.255. Karena alamat multicast mewakili sekelompok alamat (kadang-kadang disebut grup host), karena alamat hanya bisa digunakan sebagai tujuan paket. Sumber akan selalu menjadi alamat unicast.

Alamat multicast akan digunakan di game jarak jauh, di mana banyak pemain terhubung dari jarak jauh namun bermain game yang sama. Penggunaan alamat multicast lainnya adalah pembelajaran jarak jauh melalui konferensi video, di mana banyak siswa terhubung ke kelas yang sama.

Seperti alamat unicast dan broadcast, alamat IP multicast memerlukan alamat MAC multicast yang sesuai untuk benar-benar mengirimkan frame pada jaringan lokal. Alamat MAC multicast adalah nilai khusus yang dimulai dengan 01-00-5E dalam heksadesimal. Sisa bagian dari alamat MAC multicast dibuat dengan mengubah 23 bit yang lebih rendah dari alamat grup multicast IP menjadi 6 karakter heksadesimal.

Contohnya, seperti yang ditunjukkan pada animasi, adalah alamat heksadesimal multicast 01-00-5E-00-00-C8. Byte terakhir, atau delapan bit, dari alamat IP 224.0.0.200, adalah nilai desimal 200. Cara termudah untuk melihat persamaan heksadesimal adalah mengkonversikannya menjadi biner dengan spasi di antara masing-masing empat bit, 200 (desimal) = 1100 1000 (biner). Dengan menggunakan biner ke grafik konversi heksadesimal yang ditunjukkan sebelumnya, 1100 1000 (biner) = 0xC8.



5.3 LAN SWITCHES

- ❖ **MAC ADDRESS TABLE**
- **FUNDAMENTAL SWITCH**

Switch Ethernet adalah perangkat Layer 2, yang berarti menggunakan alamat MAC untuk membuat keputusan penerusan. Ini sama sekali tidak mengetahui protokol yang dibawa dalam bagian data frame, seperti paket IPv4. *Switching* membuat keputusan penerusannya hanya didasarkan pada alamat MAC Layer 2 Ethernet.

Tidak seperti hub Ethernet yang mengulangi bit out semua port kecuali port yang masuk, sebuah switch Ethernet berkonsultasi dengan tabel alamat MAC untuk membuat keputusan forwarding untuk setiap frame. Pada gambar, Switch empat port baru saja dinyalakan. Ini belum mempelajari alamat MAC untuk keempat PC yang terpasang.

Catatan: Tabel alamat MAC kadang-kadang disebut tabel memori beralamat alamat (CAM). Sedangkan istilah tabel CAM cukup umum, untuk keperluan kursus ini, kita akan menyebutnya sebagai tabel alamat MAC

- **BELAJAR ALAMAT MAC**

Switch secara dinamis membangun tabel alamat MAC dengan memeriksa alamat MAC sumber dari frame yang diterima pada port. Switch meneruskan frame dengan mencari kecocokan antara alamat MAC tujuan di frame dan entri di tabel alamat MAC.

Proses berikut dilakukan pada setiap frame Ethernet yang masuk ke switch.

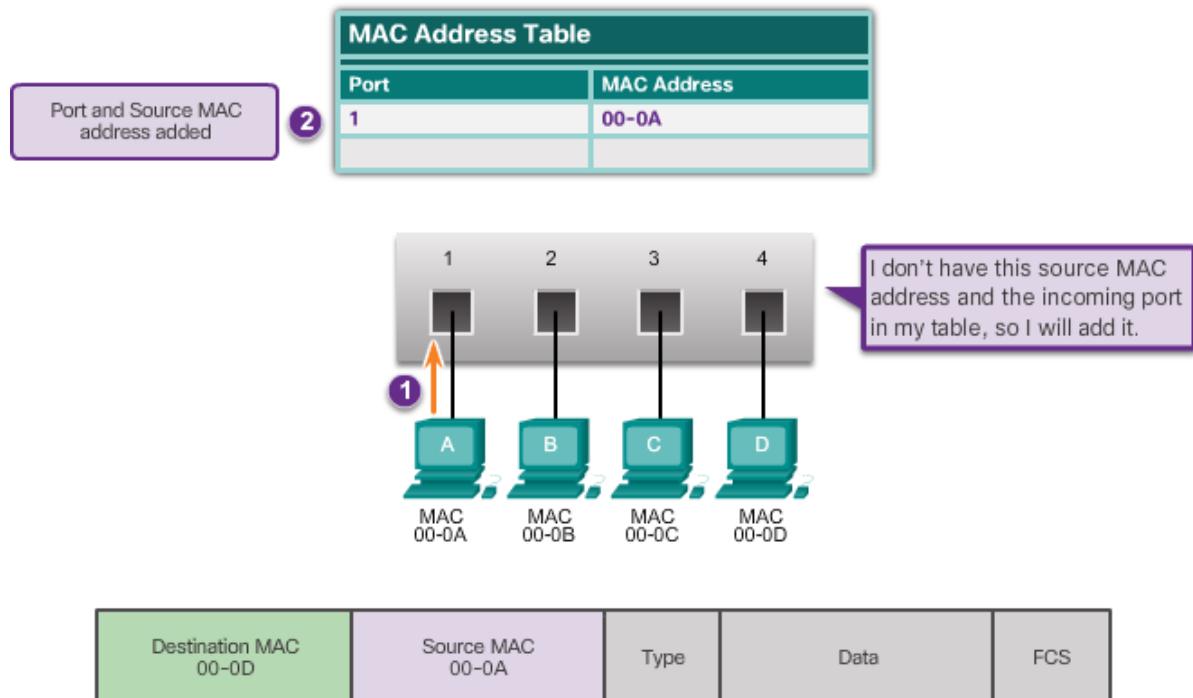
Pelajari - Memeriksa Alamat MAC Sumber

Setiap frame yang masuk *switch* dicentang untuk mendapatkan informasi baru. Hal ini dilakukan dengan memeriksa sumber frame alamat MAC dan nomor port dimana frame masuk *switch*

- ✓ Jika alamat MAC sumber tidak ada, maka akan ditambahkan ke tabel beserta nomor port yang masuk. Pada Gambar, PC-A mengirim frame Ethernet ke PC-D. Switch menambahkan alamat MAC untuk PC-A ke tabel.
- ✓ Jika alamat MAC sumber tidak ada, *Switch* memperbarui timer refresh untuk entri itu. Secara default, sebagian besar switch Ethernet menyimpan entri di tabel selama 5 menit.

Catatan: Jika alamat MAC sumber tidak ada di tabel tapi di port yang berbeda, switch memperlakukan ini sebagai entri baru. Entri diganti menggunakan alamat MAC yang sama namun dengan nomor port yang lebih baru.

Learn: Examine Source MAC Address



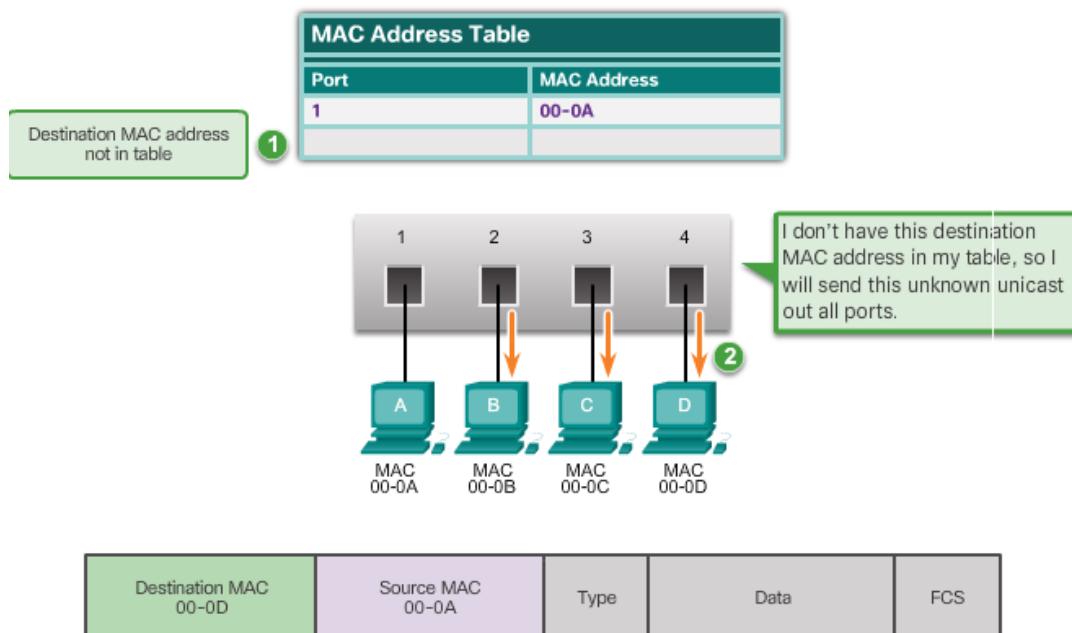
Meneliti Destination MAC Address

Selanjutnya, jika alamat MAC tujuan adalah alamat unicast, switch akan mencari kecocokan antara alamat MAC tujuan dari frame dan entri di tabel alamat MAC-nya.

- ✓ Jika alamat MAC tujuan ada di tabel, maka akan meneruskan frame dari port yang ditentukan.
- ✓ Jika alamat MAC tujuan tidak ada dalam tabel, switch akan meneruskan frame out semua port kecuali port yang masuk. Ini dikenal sebagai unicast yang tidak diketahui. Seperti ditunjukkan pada Gambar, switch tidak memiliki alamat MAC tujuan di tabelnya untuk PC-D, sehingga akan mengirim frame keluar semua port kecuali port 1.

Catatan: Jika alamat MAC tujuan adalah broadcast atau multicast, frame juga membanjiri semua port kecuali port yang masuk.

Forward: Examine Destination MAC Address



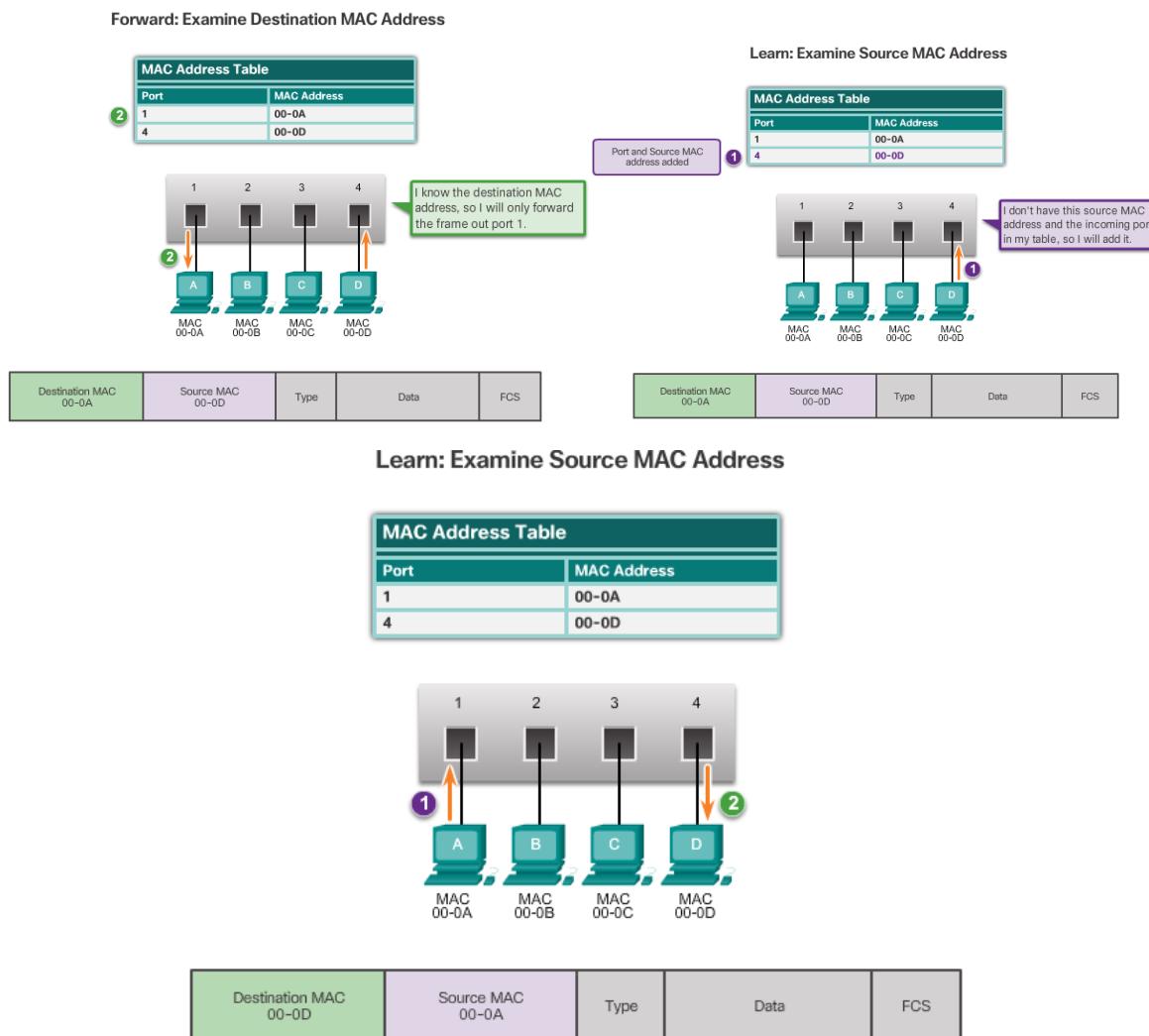
MAC addresses are shortened for demonstration purposes.

- **MEMFILTER FRAME**

Sebagai *Switch* menerima frame dari perangkat yang berbeda, ia mampu mengisi tabel alamat MAC-nya dengan memeriksa alamat MAC sumber dari setiap frame. Bila tabel alamat MAC switch berisi alamat MAC tujuan, ia dapat memfilter frame dan meneruskan satu port tunggal.

Angka 1 dan 2 menunjukkan PC-D mengirim bingkai kembali ke PC-A. *Switching* pertama akan belajar alamat MAC PC-D. Selanjutnya, karena *switch* memiliki alamat MAC PC-A di tabelnya, ia akan mengirim frame hanya keluar port 1.

Gambar menunjukkan PC-A mengirim frame lain ke PC-D. Tabel alamat MAC sudah berisi alamat MAC PC-A, jadi timer penyegaran lima menit untuk entri tersebut akan disetel ulang. Selanjutnya, karena tabel switch berisi alamat MAC PC-D, ia mengirimkan frame hanya di luar port 4.



❖ SWITCH FORWARDING METHODS

• METODE FRAME FORWARDING PADA CISCO SWITCHES

Switch menggunakan salah satu metode penerusan berikut untuk mengalihkan data antar port jaringan:

- ✓ *Store-and-forward switching*
- ✓ *Cut-through switching*

Catatan: *Cut-through switching* adalah metode switching utama yang digunakan pada switch Cisco

Dalam *switching store and forward*, ketika switch menerima frame, ia menyimpan data di buffer sampai frame yang lengkap telah diterima. Selama proses penyimpanan, switch menganalisa frame untuk mendapatkan informasi tentang tujuannya. Dalam proses ini, switch juga melakukan pengecekan error dengan menggunakan bagian trailer Cyclic Redundancy Check (CRC) dari frame Ethernet.

Dalam *switching cut-through* dilakukan sebaliknya, sebelum seluruhnya diterima, alamat tujuan harus dibaca sebelum bisa dikirimkan.

CRC menggunakan rumus matematika, berdasarkan jumlah bit (1s) pada frame, untuk menentukan apakah frame yang diterima memiliki kesalahan. Setelah mengkonfirmasikan integritas frame, frame tersebut diteruskan keluar port yang sesuai, menuju tujuannya. Bila kesalahan terdeteksi dalam bingkai, saklar akan membuang frame. Buang frame dengan kesalahan mengurangi jumlah bandwidth yang dikonsumsi oleh data korup. Penyandian toko dan forward diperlukan untuk analisis Quality of Service (QoS) pada jaringan yang terkonvergensi dimana klasifikasi rangka untuk prioritas lalu lintas diperlukan. Misalnya, voice over IP data stream perlu diprioritaskan daripada lalu lintas web-browsing.

• CUT – THROUGH SWITCHING

Dalam *cut-through switching*, switch bertindak sesuai data segera setelah diterima, meski transmisinya tidak lengkap. *Switch buffer frame* cukup membaca alamat MAC tujuan sehingga bisa menentukan ke port mana yang akan meneruskan data. Alamat MAC tujuan terletak di 6 byte pertama frame setelah pembukaan. *Switch* mencari alamat MAC tujuan di *switching table*, menentukan port antarmuka keluar, dan meneruskan frame ke tujuannya melalui port *switch* yang ditunjuk. *Switching* tidak melakukan pengecekan kesalahan pada frame.

• MEMORY BUFFERING ON SWITCHES

Switch Ethernet dapat menggunakan teknik *buffering* untuk menyimpan *frame* sebelum meneruskannya. *Buffering* juga bisa digunakan saat port tujuan sibuk karena kemacetan dan switch menyimpan frame sampai bisa ditransmisikan.

✓ Port-based Memory Buffering

Dalam buffering memori berbasis port, frame disimpan dalam antrian yang terhubung ke port masuk dan keluar tertentu. Sebuah frame ditransmisikan ke port keluar hanya jika semua frame di depannya dalam antrian telah berhasil dikirim. Ada kemungkinan satu frame untuk menunda transmisi semua frame di memori karena adanya port

tujuan yang sibuk. Penundaan ini terjadi bahkan jika frame lainnya bisa ditransmisikan ke port tujuan terbuka.

✓ **Shared Memory Buffering**

Shared Memory buffering membagi semua frame ke buffer memori umum bahwa semua port pada *switch share*. Jumlah memori penyanga yang dibutuhkan oleh port dialokasikan secara dinamis. frame di buffer dihubungkan secara dinamis ke port tujuan. Hal ini memungkinkan paket yang akan diterima pada satu port dan kemudian ditransmisikan pada port lain, tanpa memindahkannya ke antrian yang berbeda.

Switch menyimpan peta *frame* ke *link-port* yang menunjukkan tempat paket perlu ditransmisikan. *Map Link* akan dihapus setelah frame berhasil dikirim. Jumlah frame yang tersimpan dalam buffer dibatasi oleh ukuran buffer memori keseluruhan dan tidak terbatas pada buffer port tunggal. Ini memungkinkan frame yang lebih besar ditransmisikan dengan frame yang lebih sedikit. Hal ini sangat penting untuk *switch* asimetris. **Asymmetric switching** memungkinkan kecepatan data berbeda pada port yang berbeda. Hal ini memungkinkan lebih banyak *bandwidth* untuk didedikasikan ke port tertentu, seperti port yang terhubung ke server.

❖ **SETTING PORT SWITCH**

• **DUPLEX AND SPEED SETTINGS**

Dua pengaturan paling mendasar pada peralihan adalah pengaturan bandwidth dan dupleks untuk setiap port switch individual. Sangat penting bahwa pengaturan dupleks dan bandwidth cocok antara port switch dan perangkat yang terhubung, seperti komputer atau switch lain.

Ada dua jenis pengaturan dupleks yang digunakan untuk komunikasi pada jaringan Ethernet: half duplex dan full duplex.

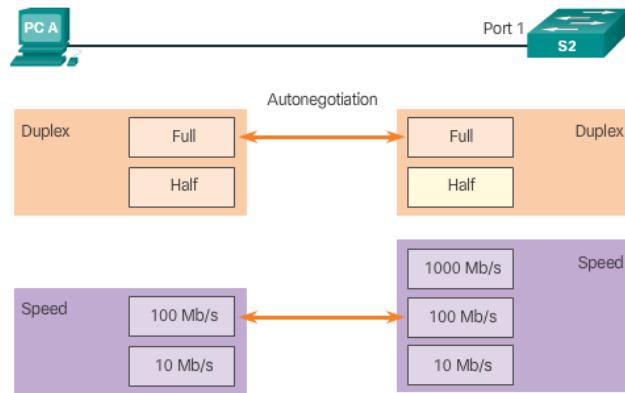
- ✓ **FULL DUPLEX** : Kedua ujung koneksi bisa mengirim dan menerima secara bersamaan.
- ✓ **HALF DUPLEX** : Hanya satu ujung sambungan yang bisa dikirim sekaligus.

Autonegotiation adalah fungsi opsional yang ditemukan pada kebanyakan switch Ethernet dan NIC. Autonegotiation memungkinkan dua perangkat untuk secara otomatis bertukar informasi tentang kemampuan kecepatan dan dupleks. Peralihan dan perangkat yang terhubung akan memilih mode kinerja tertinggi. Full-duplex dipilih jika kedua perangkat memiliki kemampuan bersama dengan bandwidth umum tertinggi mereka.

Sebagai contoh, pada Gambar PC-A's Ethernet NIC dapat beroperasi dalam full-duplex atau half-duplex, dan dalam 10 Mb / s atau 100 Mb / s. PC-A terhubung untuk beralih S1 pada port 1, yang dapat beroperasi dalam full-duplex atau half-duplex, dan dalam 10 Mb / s, 100 Mb / s atau 1000 Mb / s (1 Gb / s). Jika kedua perangkat menggunakan autonegotiation, mode operasi akan full-duplex dan 100 Mb / s.

Catatan: Sebagian besar switch Cisco dan NIC Ethernet default untuk autonegotiation untuk kecepatan dan dupleks. Port Gigabit Ethernet hanya beroperasi dalam full-duplex.

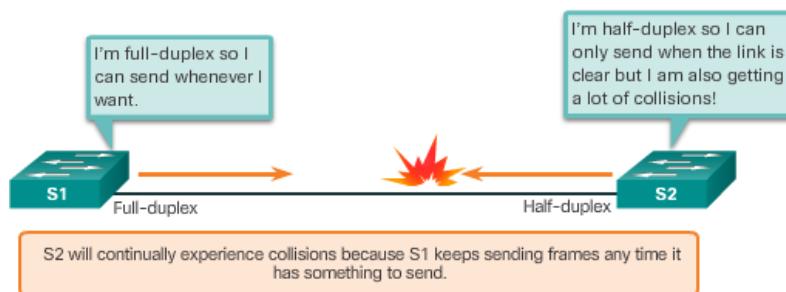
Duplex and Speed Settings



Duplex Mismatch

Salah satu penyebab masalah kinerja paling umum pada jaringan Ethernet 10/100 Mb / s terjadi ketika satu port pada link beroperasi pada half-duplex sementara port lainnya beroperasi pada full-duplex, seperti yang ditunjukkan pada Gambar. Hal ini terjadi ketika seseorang atau kedua port pada link di-reset, dan proses autonegotiation tidak menghasilkan kedua mitra link yang memiliki konfigurasi yang sama. Hal ini juga dapat terjadi ketika pengguna mengkonfigurasi ulang satu sisi link dan lupa untuk mengkonfigurasi ulang yang lain. Kedua sisi link harus memiliki autonegotiation pada, atau kedua belah pihak harus memiliki.

Duplex Mismatch



- **AUTO – MDIX**

Selain memiliki pengaturan dupleks yang benar, Anda juga perlu mengetikkan jenis kabel yang benar untuk setiap port. Koneksi antara perangkat tertentu, seperti switch-to-switch, switch-to-router, switch-to-host, dan perangkat router-to-host, sekali mengharuskan penggunaan jenis kabel tertentu (crossover atau straight-through). Sebagian besar perangkat switch sekarang mendukung perintah konfigurasi antarmuka mdix auto di CLI untuk mengaktifkan fitur crossover interface crossover otomatis (auto-MDIX).

Saat fitur auto-MDIX diaktifkan, switch mendeteksi jenis kabel yang terpasang pada port, dan mengkonfigurasi antarmuka yang sesuai. Oleh karena itu, Anda dapat menggunakan crossover atau kabel straight-through untuk koneksi ke port tembaga 10/100/1000 pada peralihan, terlepas dari jenis perangkat di ujung lain dari koneksi.

Catatan: Fitur auto-MDIX diaktifkan secara default pada switch yang menjalankan Cisco IOS Release 12.2 (18) SE atau yang lebih baru. Untuk rilis antara Cisco IOS Release 12.1 (14) EA1 dan 12.2 (18) SE, fitur auto-MDIX dinonaktifkan secara default.

5.4 ADDRESS RESOLUTION PROTOCOL

- ❖ **MAC AND IP**

- **TUJUAN PADA JARINGAN YANG SAMA**

Ada dua alamat utama yang ditetapkan ke perangkat di LAN Ethernet:

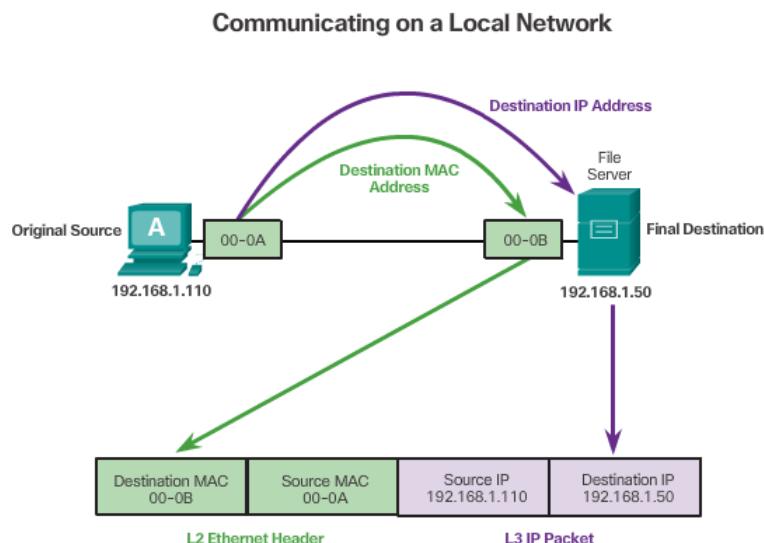
- ✓ **Alamat fisik (alamat MAC)** - Digunakan untuk Ethernet NIC ke komunikasi Ethernet NIC pada jaringan yang sama.
- ✓ **Alamat logis (alamat IP)** - Digunakan untuk mengirim paket dari sumber asli ke tujuan akhir.

Alamat IP digunakan untuk mengidentifikasi alamat sumber asli dan tujuan akhir. Alamat IP tujuan mungkin berada pada jaringan IP yang sama dengan sumbernya atau mungkin berada pada jaringan jarak jauh.

Catatan: Sebagian besar aplikasi menggunakan DNS (Domain Name System) untuk menentukan alamat IP saat diberi nama domain seperti www.cisco.com. DNS dibahas di bab selanjutnya.

Layer 2 atau alamat fisik, seperti alamat MAC Ethernet, memiliki tujuan yang berbeda. Alamat ini digunakan untuk mengirimkan frame data frame dengan paket IP yang dienkapsulasi dari satu NIC ke NIC lain pada jaringan yang sama. Jika alamat IP tujuan berada pada jaringan yang sama, alamat MAC tujuan adalah perangkat tujuan.

Pada gambar menunjukkan alamat MAC Ethernet dan alamat IP untuk PC-A mengirimkan paket IP ke server file pada jaringan yang sama.



Frame Ethernet Layer 2 berisi:

- ✓ Destination MAC address - Ini adalah alamat MAC dari file server Ethernet NIC.
- ✓ Alamat MAC sumber - Ini adalah alamat MAC dari PC-A's Ethernet NIC.

Paket IP Layer 3 berisi:

- ✓ Alamat IP sumber - Ini adalah alamat IP sumber asli, PC-A.
- ✓ Destination IP address - Ini adalah alamat IP tujuan akhir, file server.

❖ ARP

• PENGENALAN ARP

Ingat bahwa setiap perangkat dengan alamat IP pada jaringan Ethernet juga memiliki alamat MAC Ethernet. Saat perangkat mengirim bingkai Ethernet, ini berisi kedua alamat ini:

- ✓ **Destination MAC address** - Alamat MAC dari NIC Ethernet, yang akan berupa alamat MAC dari perangkat tujuan akhir atau router.
- ✓ **Source MAC address** - Alamat MAC dari NIC Ethernet pengirim.

Untuk menentukan alamat MAC tujuan, perangkat menggunakan ARP. ARP menyediakan dua fungsi dasar:

- ✓ Menyelesaikan alamat IPv4 ke alamat MAC
- ✓ Mempertahankan tabel pemetaan

- **FUNGSI ARP**

Resolving IPv4 Addresses to MAC Addresses

Ketika sebuah paket dikirim ke lapisan data link yang akan dienkapsulasi ke dalam bingkai Ethernet, perangkat merujuk ke sebuah tabel dalam ingatannya untuk menemukan alamat MAC yang dipetakan ke alamat IPv4. Tabel ini disebut tabel ARP atau cache ARP. Tabel ARP disimpan dalam RAM perangkat.

Perangkat pengirim akan mencari tabel ARP-nya untuk alamat IPv4 tujuan dan alamat MAC yang sesuai.

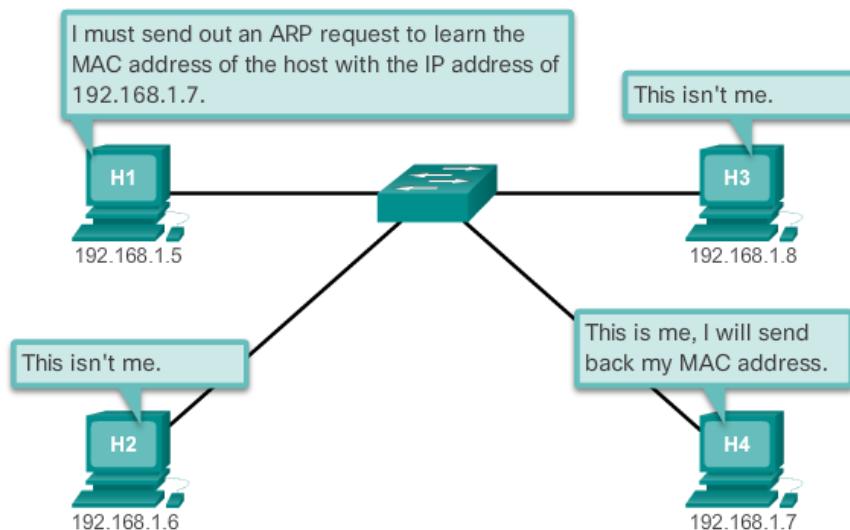
- ✓ Jika alamat tujuan paket IPv4 berada pada jaringan yang sama dengan alamat IPv4 sumber, perangkat akan mencari tabel ARP untuk alamat IPv4 tujuan.
- ✓ Jika alamat IPv4 tujuan berada pada jaringan yang berbeda dari alamat IPv4 sumber, perangkat akan mencari tabel ARP untuk alamat IPv4 dari gateway default

Dalam kedua kasus tersebut, pencarian adalah untuk alamat IPv4 dan alamat MAC yang sesuai untuk perangkat.

Setiap entri, atau baris, tabel ARP mengikat alamat IPv4 dengan alamat MAC. Kami memanggil hubungan antara dua nilai peta - ini berarti Anda dapat menemukan alamat IPv4 di tabel dan menemukan alamat MAC yang sesuai. Tabel ARP menyimpan sementara (cache) pemetaan untuk perangkat di LAN.

Jika perangkat menempatkan alamat IPv4, alamat MAC yang sesuai digunakan sebagai alamat MAC tujuan pada frame. Jika tidak ada entri yang ditemukan, maka perangkat akan mengirimkan permintaan ARP.

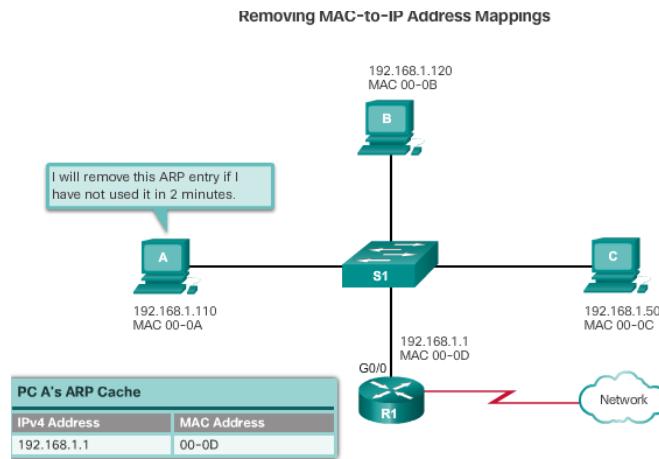
The ARP Process



- **MENGHAPUS ENTRI DARI TABEL ARP**

Untuk setiap perangkat, timer cache ARP akan menghapus entri ARP yang belum pernah digunakan untuk jangka waktu tertentu. Waktu berbeda tergantung pada sistem operasi perangkat. Sebagai contoh, beberapa sistem operasi Windows menyimpan entri cache ARP selama 2 menit, seperti yang ditunjukkan pada gambar.

Perintah juga dapat digunakan untuk secara manual menghapus semua atau beberapa entri dalam tabel ARP. Setelah entri dihapus, proses pengiriman permintaan ARP dan menerima balasan ARP harus terjadi lagi untuk masuk ke peta di tabel ARP.



• ARP TABEL

Pada router Cisco, perintah show ip arp digunakan untuk menampilkan tabel ARP, seperti yang ditunjukkan pada Gambar .

Router ARP Table

Router# show ip arp					
Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	172.16.233.229	-	0000.0c59.f892	ARPA	Ethernet0/0
Internet	172.16.233.218	-	0000.0c07.ac00	ARPA	Ethernet0/0
Internet	172.16.168.11	-	0000.0c63.1300	ARPA	Ethernet0/0
Internet	172.16.168.254	9	0000.0c36.6965	ARPA	Ethernet0/0

Pada PC Windows 7, perintah arp -a digunakan untuk menampilkan tabel ARP, seperti yang ditunjukkan pada Gambar .

Host ARP Table

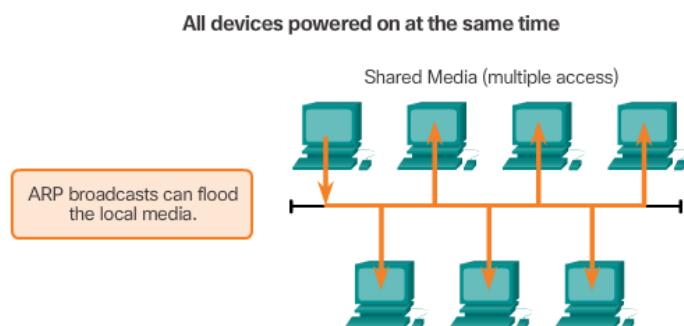
C:\> arp -a			
Interface:	192.168.1.67 --- 0xa		
Internet Address	Physical Address	Type	
192.168.1.254	64-0a-49-0d-3e-21	dynamic	
192.168.1.255	ff-ff-ff-ff-ff-ff	static	
224.0.0.22	01-00-5e-00-00-16	static	
224.0.0.251	01-00-5e-00-00-fb	static	
224.0.0.252	01-00-5e-00-00-fc	static	
255.255.255.255	ff-ff-ff-ff-ff-ff	static	
Interface:	10.82.253.91 --- 0x10		
Internet Address	Physical Address	Type	
10.82.253.252	64-0a-49-0d-3e-21	dynamic	
224.0.0.22	01-00-5e-00-00-16	static	
224.0.0.251	01-00-5e-00-00-fb	static	
224.0.0.252	01-00-5e-00-00-fc	static	
255.255.255.255	ff-ff-ff-ff-ff-ff	static	

❖ MASALAH ARP

• ARP BROADCAST

Sebagai *broadcast frame*, permintaan ARP diterima dan diproses oleh setiap perangkat di jaringan lokal. Pada jaringan bisnis yang khas, *broadcast* ini mungkin akan berdampak minimal pada kinerja jaringan. Namun, jika sejumlah besar perangkat diaktifkan dan semua mulai mengakses layanan jaringan secara bersamaan, mungkin ada beberapa penurunan kinerja untuk waktu yang singkat, seperti yang ditunjukkan pada gambar. Setelah perangkat mengirimkan siaran ARP awal dan telah mempelajari alamat MAC yang diperlukan, dampak pada jaringan akan diminimalkan

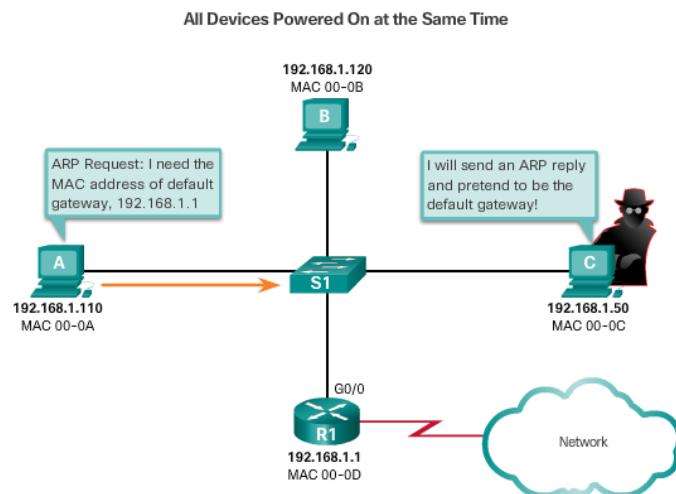
ARP Broadcasts and Security



• ARP SPOOFING

Dalam beberapa kasus, penggunaan ARP dapat menyebabkan risiko keamanan potensial yang dikenal dengan ARP spoofing atau ARP poisoning. Ini adalah teknik yang digunakan oleh penyerang untuk membalas permintaan ARP untuk alamat IPv4 milik perangkat lain, seperti gateway default, seperti yang ditunjukkan pada gambar. Penyerang mengirim balasan ARP dengan alamat MAC-nya sendiri. Penerima balasan ARP akan menambahkan alamat MAC yang salah ke tabel ARP-nya dan mengirimkan paket ini ke penyerang.

Switch tingkat enterprise mencakup teknik mitigasi yang dikenal dengan dynamic ARP inspection (DAI).



LATIHAN SOAL 5

1. Jelaskan yang dimaksud dengan Ethernet
2. Jelaskan fungsi utama dari Enkapsulasi data
3. Jelaskan yang dimaksud dengan MAC address
4. Jelaskan perbedaan antara MAC address dengan IP address
5. Jelaskan perbedaan antara Unicast, multicast dan Broadcast
6. Sebutkan metode forwading pada switch
7. Jelaskan yang dimaksud dengan ARP
8. Sebutkan fungsi dari ARP
9. Sebutkan Isue atau masalah yang sering timbul pada ARP
10. Jelaskan process suatu ARP

BAB 6 NETWORK LAYER

6.1 PENGANTAR

Aplikasi dan layanan jaringan pada satu perangkat akhir dapat berkomunikasi dengan aplikasi dan layanan yang berjalan pada perangkat akhir yang lain. Bagaimana data ini dikomunikasikan melalui jaringan dengan cara yang efisien?

Protokol lapisan jaringan model OSI menentukan pengalaman dan proses yang memungkinkan data lapisan transport dikemas dan diangkut. Enkapsulasi lapisan jaringan memungkinkan data dikirimkan ke tujuan dalam jaringan (atau di jaringan lain) dengan overhead minimum.

Bab ini berfokus pada peran lapisan jaringan. Ini mengkaji bagaimana membagi jaringan menjadi beberapa kelompok host untuk mengelola arus paket data dalam jaringan. Ini juga mencakup bagaimana komunikasi antar jaringan difasilitasi. Komunikasi antar jaringan disebut routing.

6.2 PROTOKOL LAPISAN JARINGAN

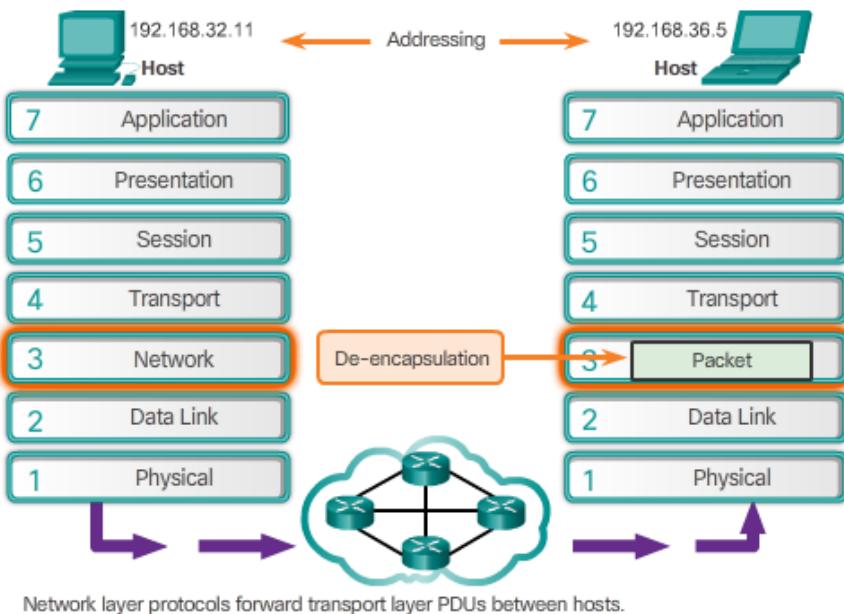
- ❖ **KOMUNIKASI LAPISAN JARINGAN**
- **LAPISAN JARINGAN**

Lapisan jaringan, atau OSI Layer 3, menyediakan layanan untuk mengizinkan perangkat akhir bertukar data di seluruh jaringan. Untuk mencapai transportasi end-to-end ini, lapisan jaringan menggunakan empat proses dasar:

- ✓ **Addressing end devices** - Perangkat akhir harus dikonfigurasi dengan alamat IP unik untuk identifikasi pada jaringan.
- ✓ **Enkapsulasi** - Lapisan jaringan mengenkapsulasi unit data protokol (PDU) dari lapisan transport ke dalam paket. Proses enkapsulasi menambahkan informasi header IP, seperti alamat IP dari host sumber (pengiriman) dan tujuan (penerima).
- ✓ **Routing** - Lapisan jaringan menyediakan layanan untuk mengarahkan paket ke host tujuan di jaringan lain. Untuk melakukan perjalanan ke jaringan lain, paket tersebut harus diproses oleh router. Peranan router adalah memilih jalur terbaik dan paket langsung menuju host tujuan dalam sebuah proses yang dikenal sebagai routing. Sebuah paket dapat melewati banyak perangkat perantara sebelum mencapai host tujuan. Setiap router sebuah paket melintasi untuk mencapai host tujuan disebut hop.
- ✓ **De-enkapsulasi** - Ketika paket tiba di lapisan jaringan host tujuan, host akan memeriksa header IP dari paket. Jika alamat IP tujuan dalam header cocok dengan alamat IP-nya sendiri, header IP akan dihapus dari paket. Setelah paket di-enkapsulasi oleh lapisan jaringan, Layer 4 PDU yang dihasilkan dilewatkan ke layanan yang sesuai pada lapisan transport.

Tidak seperti lapisan transport (OSI Layer 4), yang mengelola transport data antara proses yang berjalan pada masing-masing host, protokol lapisan jaringan menentukan struktur paket dan pengolahan yang digunakan untuk membawa data dari satu host ke host lain. Beroperasi tanpa memperhatikan data yang dibawa dalam setiap paket memungkinkan lapisan jaringan membawa paket untuk beberapa jenis komunikasi antara beberapa host.

The Exchange of Data



• PROTOKOL LIPISAN JARINGAN

Ada beberapa protokol lapisan jaringan yang ada. Namun, hanya dua berikut yang umum diterapkan:

- ✓ Protokol Internet versi 4 (IPv4)
- ✓ Protokol Internet versi 6 (IPv6)

Catatan: Protokol lapisan jaringan lawas tidak ditunjukkan pada gambar dan tidak dibahas dalam kursus ini.

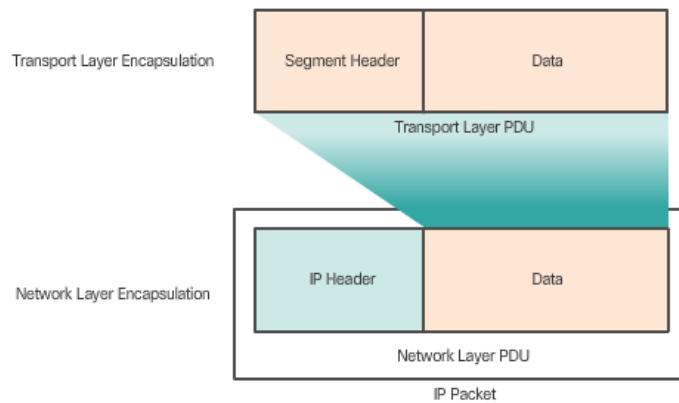
❖ KARAKTERISTIK IP PROTOKOL

• ENKAPSULASI IP

IP mengenkapsulasi segmen lapisan transport dengan menambahkan header IP. Header ini digunakan untuk mengirimkan paket ke host tujuan. Header IP tetap di tempat sejak paket meninggalkan host sumber sampai tiba di host tujuan.

Gambar menunjukkan proses pembuatan lapisan transport PDU dan mengilustrasikan bagaimana lapisan transport PDU tersebut kemudian dienkapsulasi oleh lapisan jaringan PDU untuk membuat paket IP.

Network Layer PDU = IP Packet



Proses encapsulating data layer by layer memungkinkan layanan pada lapisan yang berbeda berkembang dan berskala tanpa mempengaruhi lapisan lainnya. Ini berarti segmen lapisan transport dapat dengan mudah dikemas oleh IPv4 atau IPv6 atau oleh protokol baru yang mungkin dikembangkan di masa depan.

Router dapat menerapkan protokol lapisan jaringan yang berbeda ini untuk beroperasi secara bersamaan melalui jaringan. Perutean yang dilakukan oleh perangkat perantara ini hanya mempertimbangkan isi header paket lapisan jaringan. Dalam semua kasus, bagian data dari paket, yaitu, lapisan transport yang dienkapsulasi PDU, tetap tidak berubah selama proses lapisan jaringan.

• KARAKTERISTIK IP

IP didesain sebagai protokol dengan overhead rendah. Ini hanya menyediakan fungsi yang diperlukan untuk mengirimkan paket dari sumber ke tujuan melalui sistem jaringan yang saling terkait. Protokol ini tidak dirancang untuk melacak dan mengelola aliran paket. Fungsi ini, jika diperlukan, dilakukan oleh protokol lain di lapisan lain.

Characteristics of the IP Protocol

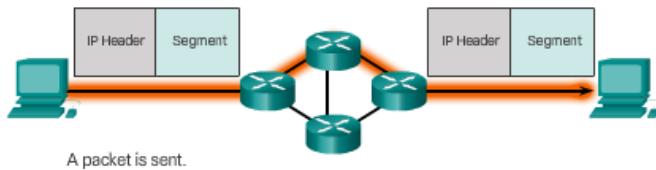


- **IP TANPA KONEKSI**

IP tidak terhubung, artinya tidak ada sambungan end-to-end khusus yang dibuat sebelum data dikirim. Seperti ditunjukkan pada Gambar, komunikasi tanpa koneksi secara konseptual serupa dengan mengirim surat kepada seseorang tanpa memberi tahu penerima sebelumnya.

Komunikasi data tanpa koneksi bekerja dengan prinsip yang sama. Seperti ditunjukkan pada Gambar, IP tidak memerlukan pertukaran informasi kontrol awal untuk membuat koneksi end-to-end sebelum paket diteruskan. IP juga tidak memerlukan field tambahan di header untuk menjaga koneksi yang mapan. Proses ini sangat mengurangi biaya overhead IP. Namun, tanpa koneksi end-to-end yang sudah ada sebelumnya, pengirim tidak sadar apakah perangkat tujuan ada dan berfungsi saat mengirim paket, atau mereka tidak sadar jika tujuannya menerima paket, atau apakah mereka dapat mengakses dan membaca paket .

Connectionless Communication



The sender doesn't know:

- If the receiver is present
- If the packet arrived
- If the receiver can read the packet

The receiver doesn't know:

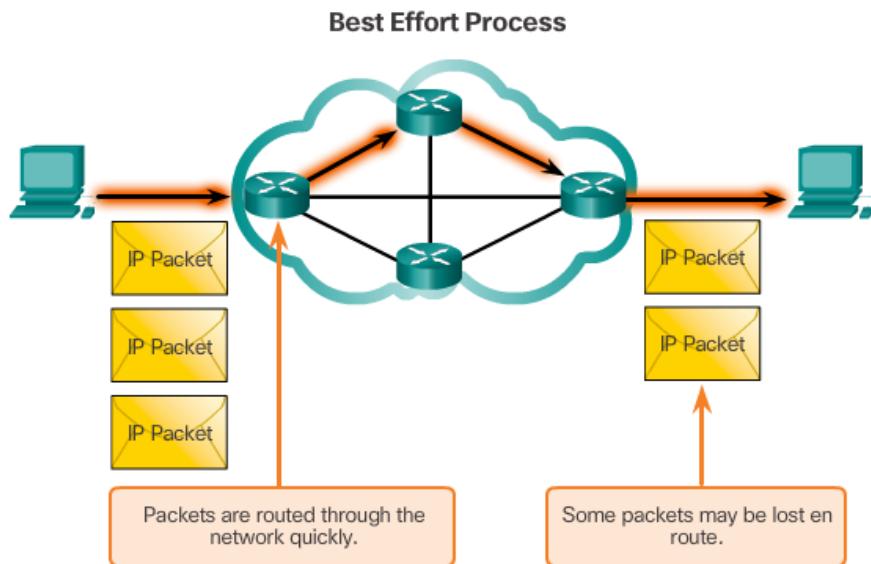
- When it is coming

- **IP BEST EFFORT DELIVERY**

karakteristik pengiriman IP yang tidak dapat diandalkan atau best-effort. Protokol IP tidak menjamin bahwa semua paket yang dikirimkan sebenarnya diterima.

Tidak dapat diandalkan berarti IP tidak memiliki kemampuan untuk mengelola dan memulihkan dari paket yang tidak terkirim atau rusak. Ini karena sementara paket IP dikirim dengan informasi tentang lokasi pengiriman, tidak mengandung informasi yang dapat diproses untuk memberi tahu pengirim apakah pengiriman berhasil. Paket mungkin sampai pada tujuan yang rusak, tidak beraturan, atau tidak sama sekali. IP tidak memberikan kemampuan untuk pengiriman ulang paket jika terjadi kesalahan.

Jika paket out-of-order dikirim, atau paket hilang, maka aplikasi yang menggunakan data, atau layanan lapisan atas, harus menyelesaikan masalah ini. Hal ini memungkinkan IP berfungsi dengan sangat efisien. Dalam paket protokol TCP / IP, keandalan adalah peran lapisan transport.



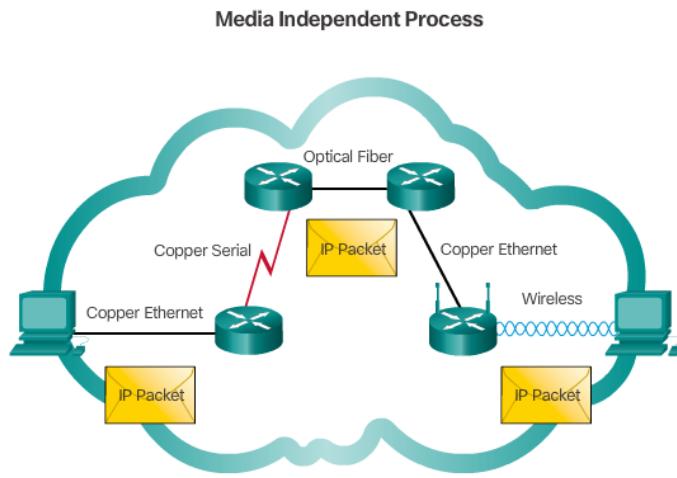
- **IP MEDIA INDEPENDENT**

IP beroperasi secara independen dari media yang membawa data pada lapisan bawah tumpukan protokol. Seperti yang ditunjukkan pada gambar, paket IP dapat dikomunikasikan sebagai sinyal elektronik melalui kabel tembaga, seperti sinyal optik melalui serat, atau tanpa kabel sebagai sinyal radio.

Ini adalah tanggung jawab lapisan data link OSI untuk mengambil paket IP dan mempersiapkannya untuk transmisi melalui media komunikasi. Ini berarti bahwa pengangkutan paket IP tidak terbatas pada media tertentu.

Namun, ada satu karakteristik utama media yang dipertimbangkan oleh lapisan jaringan: ukuran maksimum PDU yang dapat diangkut oleh masing-masing media. Karakteristik ini disebut sebagai unit transmisi maksimum (MTU). Bagian dari komunikasi kontrol antara lapisan data link dan lapisan jaringan adalah pembentukan ukuran maksimum untuk paket. Lapisan data link melewati nilai MTU sampai ke lapisan jaringan. Lapisan jaringan kemudian menentukan seberapa besar paketnya.

Dalam beberapa kasus, perangkat perantara, biasanya router, harus memecah paket saat meneruskannya dari satu media ke medium lain dengan MTU yang lebih kecil. Proses ini disebut fragmentasi paket atau fragmentasi.



❖ IPv4 PAKET

- **IPV4 PACKET HEADER**

Header paket IPv4 terdiri dari field-field yang berisi informasi penting tentang paket. Bidang ini berisi bilangan biner yang diperiksa oleh proses Layer 3. Nilai biner dari masing-masing field mengidentifikasi berbagai setting dari paket IP. Diagram header protokol, seperti yang ditunjukkan pada gambar, dibaca dari kiri ke kanan, dan bagian atas ke bawah.

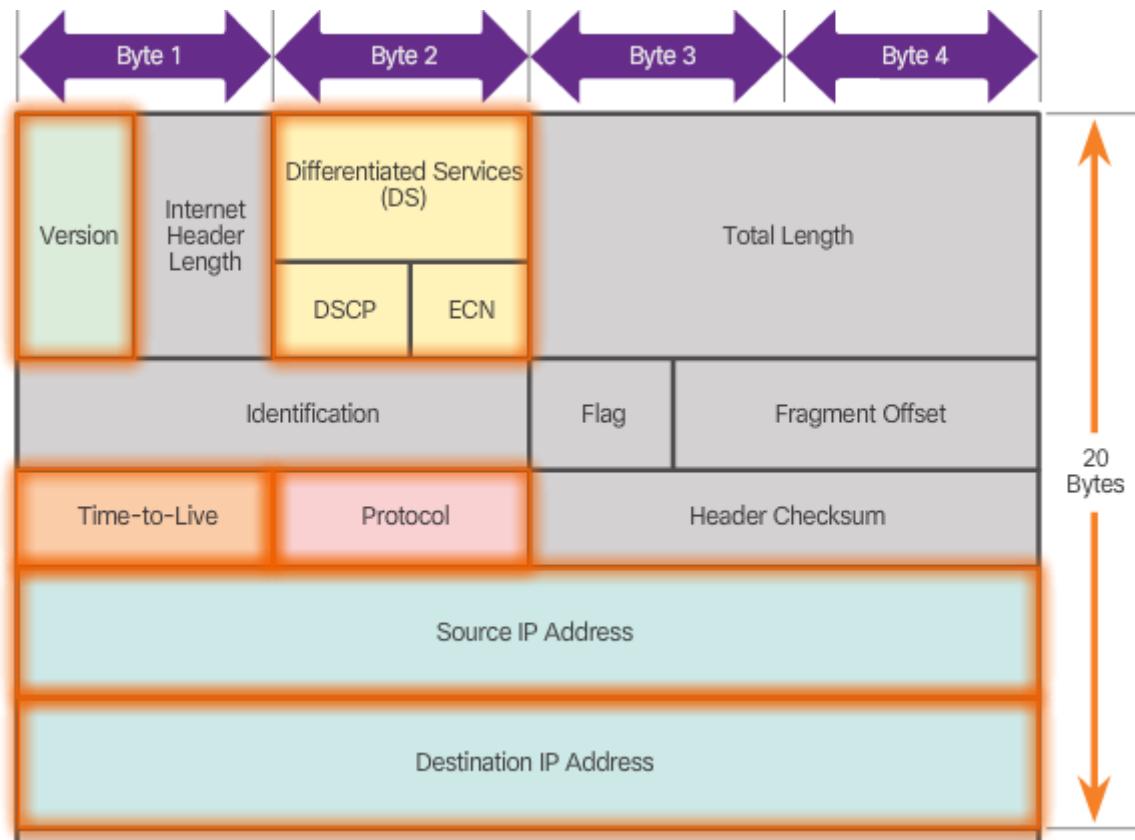
Bidang penting di header IPv4 meliputi:

- ✓ **Versi** - Berisi nilai biner 4 bit yang diatur ke 0100 yang mengidentifikasi ini sebagai paket versi IP 4.
- ✓ **Differentiated Services (DS)** - Dahulu disebut bidang Type of Service (ToS), field DS adalah bidang 8-bit yang digunakan untuk menentukan prioritas masing-masing paket.
- ✓ **Time-to-Live (TTL)** - Berisi nilai biner 8 bit yang digunakan untuk membatasi masa pakai paket. Pengirim paket menetapkan nilai TTL awal, dan itu akan berkurang satu kali setiap paket diproses oleh router. Jika bidang TTL beregenerasi nol, router membuang paket dan mengirim pesan Message Control Protocol (ICMP) Time Exceeded ke alamat IP sumber.
- ✓ **Protokol** - Nilai biner 8 bit ini menunjukkan jenis muatan data yang dibawa oleh paket, yang memungkinkan lapisan jaringan meneruskan data ke protokol lapisan atas yang sesuai. Nilai umum meliputi ICMP (1), TCP (6), dan UDP (17).
- ✓ **Source IP Address** - Berisi nilai biner 32-bit yang mewakili alamat IP sumber dari paket.
- ✓ **Destination IP Address** - Berisi nilai biner 32-bit yang mewakili alamat IP tujuan dari paket.

Dua bidang yang paling sering direferensikan adalah **source and destination IP addresses**. Bidang ini mengidentifikasi dari mana paket itu berasal dan kemana arahnya. Biasanya alamat ini tidak berubah saat bepergian dari sumber ke tujuan.

Field Header Panjang Internet (Panjang), Panjang Total, dan **Header Checksum** digunakan untuk mengidentifikasi dan memvalidasi paket.

Bidang lainnya digunakan untuk menyusun ulang paket terfragmentasi. Secara khusus, paket IPv4 menggunakan *field Identification, Flags, dan Fragment Offset* untuk melacak fragment tersebut. Router mungkin harus memecah paket saat meneruskannya dari satu media ke media lainnya dengan MTU yang lebih kecil.



❖ IPv6 PAKET

• KETERBATASAN IPv4

Selama bertahun-tahun, IPv4 telah diperbarui untuk menjawab tantangan baru. Namun, meski dengan perubahan, IPv4 masih memiliki tiga masalah utama:

- ✓ **Penipisan alamat IP** - IPv4 memiliki sejumlah alamat IPv4 publik yang unik yang tersedia. Meskipun ada sekitar 4 miliar alamat IPv4, semakin banyak perangkat IP-enabled yang baru, selalu terhubung, dan potensi pertumbuhan daerah yang kurang berkembang telah meningkatkan kebutuhan akan lebih banyak alamat.
- ✓ **Internet routing table expansion** - Tabel routing digunakan oleh router untuk membuat penentuan jalur terbaik. Karena jumlah server yang terhubung ke Internet meningkat, demikian juga jumlah rute jaringan. Rute IPv4 ini menghabiskan banyak sumber daya memori dan prosesor di router Internet.
- ✓ **Lack of end-to-end connectivity** - **Network Address Translation (NAT)** adalah teknologi yang umumnya diterapkan dalam jaringan IPv4. NAT menyediakan cara bagi beberapa perangkat untuk berbagi alamat IPv4 publik tunggal. Namun, karena alamat IPv4 publik dibagi, alamat IPv4 dari host jaringan internal tersembunyi. Ini bisa menjadi masalah bagi teknologi yang membutuhkan konektivitas end-to-end.

- **PERKENALAN IPv6**

Pada awal 1990an, **Internet Engineering Task Force (IETF)** mulai khawatir dengan isu-isu dengan IPv4 dan mulai mencari penggantinya. Kegiatan ini berujung pada pengembangan IP versi 6 (IPv6). IPv6 mengatasi keterbatasan IPv4 dan merupakan peningkatan yang kuat dengan fitur yang sesuai dengan tuntutan jaringan terkini dan yang diperkirakan.

Perbaikan yang disediakan oleh IPv6 meliputi:

- ✓ **Increased address space** - Alamat IPv6 didasarkan pada pengalamatan hirarkis 128 bit yang bertentangan dengan IPv4 dengan 32 bit.
- ✓ **Penanganan paket yang lebih baik** - Header IPv6 telah disederhanakan dengan lebih sedikit bidang.
- ✓ **Menghilangkan kebutuhan akan NAT** - Dengan sejumlah besar alamat IPv6 publik, NAT antara alamat IPv4 pribadi dan IPv4 publik tidak diperlukan. Hal ini untuk menghindari beberapa masalah aplikasi yang disebabkan oleh NAT yang dialami oleh aplikasi yang memerlukan koneksi end-to-end.

The 32-bit IPv4 address space provides approximately 4,294,967,296 unique addresses. IPv6 address space provides 340,282,366,920,938,463,463,374,607,431,768,211,456, or 340 undecillion addresses, which is roughly equivalent to every grain of sand on Earth

- **ENCAPSULASI IPv6**

Salah satu penyempurnaan desain utama IPv6 melalui IPv4 adalah header IPv6 yang disederhanakan.

Misalnya, header IPv4 yang ditunjukkan pada Gambar terdiri dari 20 oktet (sampai 60 byte jika field Pilihan digunakan) dan 12 bidang header dasar, tidak termasuk bidang Pilihan dan bidang Padding. Seperti yang disoroti pada gambar, untuk IPv6, beberapa bidang tetap sama, beberapa bidang telah mengubah nama dan posisi, dan beberapa bidang IPv4 tidak lagi diperlukan.

IPv4 Header

Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
Time-to-Live	Protocol	Header Checksum		
Source Address				
Destination Address				
Options			Padding	

- [Yellow Box] - Field names kept from IPv4 to IPv6
- [Green Box] - Name and position changed in IPv6
- [Grey Box] - Fields not kept in IPv6

Sebaliknya, header IPv6 yang disederhanakan yang ditunjukkan pada Gambar terdiri dari 40 oktet (sebagian besar disebabkan oleh panjang alamat sumber dan alamat IPv6 tujuan) dan 8 bidang header (3 kolom header IPv4 dan 5 kolom header tambahan). Seperti yang disoroti dalam gambar ini, beberapa bidang menyimpan nama yang sama dengan IPv4, beberapa bidang telah mengubah nama atau posisi, dan bidang baru telah ditambahkan.

IPv6 Header

Version	Traffic Class	Flow Label	
		Payload Length	Next Header
Source IP Address			Hop Limit
Destination IP Address			

Legend

- [Yellow Box] - Field names kept from IPv4 to IPv6
- [Green Box] - Name and position changed in IPv6
- [New Green Box] - New field in IPv6

Header IPv6 disederhanakan menawarkan beberapa keunggulan dibanding IPv4 seperti yang tercantum dibawah:

- ✓ Penyederhanaan *format header* untuk efisiensi *packet handling*
- ✓ lapisan *payload* untuk peningkatan *throughput* dan efisiensi transportasi
- ✓ Hirarki arsitektur jaringan untuk efisiensi routing
- ✓ Auto konfigurasi untuk pengalaman
- ✓ Pengurangan kebutuhan NAT antara *private* dan *public addresses*

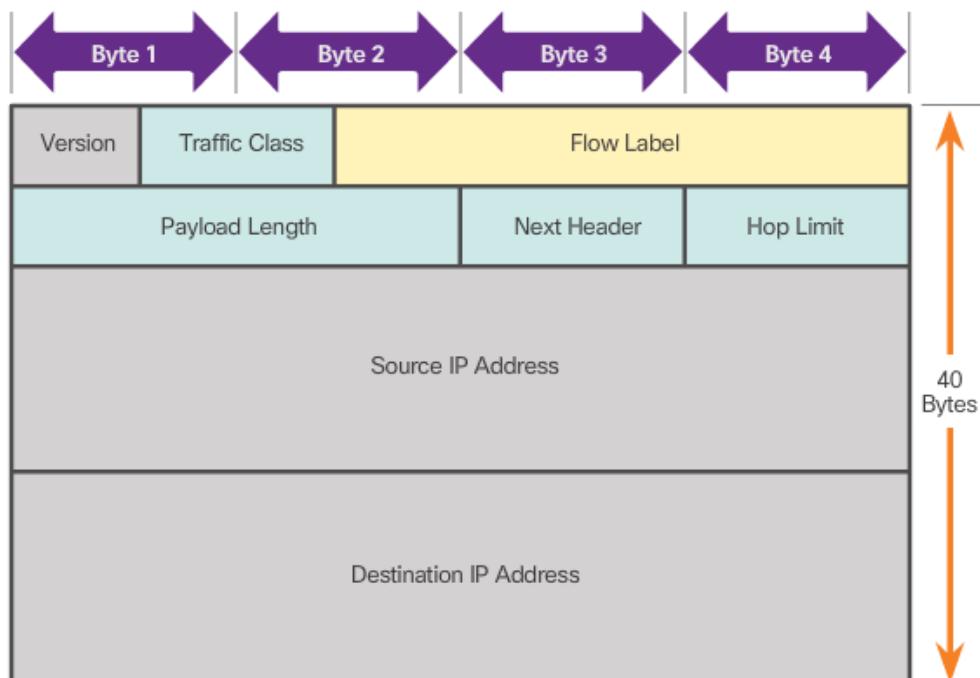
- **IPv6 PACKET HEADER**

Kolom pada *header packet* IPv6 meliputi:

- ✓ **Version** - Bidang ini berisi nilai biner 4-bit yang diatur ke 0110 yang mengidentifikasi ini sebagai paket versi IP 6.
- ✓ **Traffic Class** - Bidang 8-bit ini setara dengan bidang IPv4 Differentiated Services (DS).
- ✓ **Flow Label** - Bidang 20-bit ini menunjukkan bahwa semua paket dengan label aliran yang sama menerima jenis penanganan yang sama oleh router.
- ✓ **Payload Length** - Bidang 16-bit ini menunjukkan panjang bagian data atau muatan paket IPv6.
- ✓ **Next Header** - Bidang 8-bit ini setara dengan bidang Protokol IPv4. Ini menunjukkan jenis payload data yang dibawa oleh paket, memungkinkan lapisan jaringan meneruskan data ke protokol lapisan atas yang sesuai.
- ✓ **Hop Limit** - Field 8-bit ini menggantikan field TTL IPv4. Nilai ini dikurangi dengan nilai 1 oleh setiap router yang meneruskan paket. Saat counter mencapai 0, paket akan dibuang, dan pesan ICMPv6 Time Exceeded diteruskan ke host pengirim, menunjukkan bahwa paket tersebut tidak mencapai tujuannya karena batas hop terlampaui.
- ✓ **Source Address** - Bidang 128-bit ini mengidentifikasi alamat IPv6 dari host pengirim
- ✓ **Destination Address** - Bidang 128-bit ini mengidentifikasi alamat IPv6 dari host penerima.

Paket IPv6 juga berisi header ekstensi (EH), yang menyediakan informasi lapisan jaringan opsional. Header ekstensi bersifat opsional dan ditempatkan di antara header IPv6 dan payload. EH digunakan untuk fragmentasi, keamanan, untuk mendukung mobilitas dan banyak lagi.

Fields in the IPv6 Packet Header



6.3 ROUTING

- ❖ **HOW a HOST ROUTES**
- **HOST FORWARDING DECISION**

Peran lain dari lapisan jaringan adalah mengarahkan paket antar host. Host dapat mengirim paket ke:

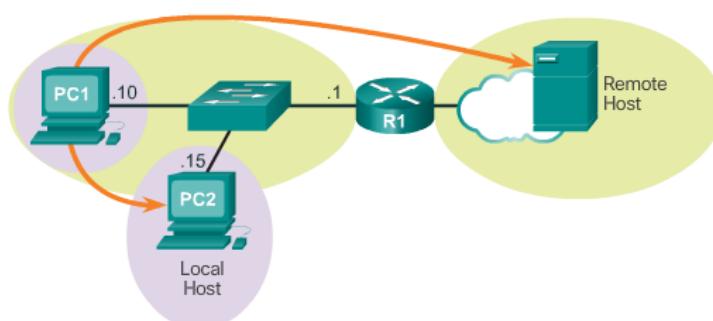
- ✓ **Itself** - Host dapat melakukan ping sendiri dengan mengirimkan paket ke alamat IPv4 khusus 127.0.0.1, yang disebut sebagai antarmuka loopback. Ping antarmuka loopback menguji tumpukan protokol TCP / IP di host.
- ✓ **Host lokal** - Ini adalah host pada jaringan lokal yang sama dengan host pengirim. Host berbagi alamat jaringan yang sama.
- ✓ **Remote host** - Ini adalah host pada jaringan jarak jauh. Host tidak berbagi alamat jaringan yang sama.

Apakah sebuah paket ditujukan untuk host lokal atau host jarak jauh ditentukan oleh kombinasi alamat IPv4 dan subnet mask dari perangkat sumber (atau pengiriman) dibandingkan dengan alamat IPv4 dan subnet mask dari perangkat tujuan.

Di jaringan rumah atau bisnis, Anda mungkin memiliki beberapa perangkat kabel dan nirkabel yang saling berhubungan bersama menggunakan perangkat perantara, seperti sakelar LAN dan / atau jalur akses nirkabel (WAP). Perangkat perantara ini menyediakan interkoneksi antara host lokal pada jaringan lokal. Host lokal dapat saling menghubungi dan berbagi informasi tanpa memerlukan perangkat tambahan. Jika sebuah host mengirimkan sebuah paket ke perangkat yang dikonfigurasi dengan jaringan IP yang sama dengan perangkat host, paket tersebut diteruskan keluar dari antarmuka host, melalui perangkat perantara, dan ke perangkat tujuan secara langsung.

Tentu saja, dalam kebanyakan situasi, kami ingin perangkat kami dapat terhubung melampaui segmen jaringan lokal, seperti ke rumah lain, bisnis, dan Internet. Perangkat yang berada di luar segmen jaringan lokal dikenal sebagai host jarak jauh. Bila perangkat sumber mengirimkan paket ke perangkat tujuan jauh, maka bantuan router dan perutean diperlukan. Routing adalah proses mengidentifikasi jalur terbaik menuju tujuan. Router yang terhubung ke segmen jaringan lokal disebut sebagai default gateway.

Three Types of Destinations



- **DEFAULT GATEWAY**

Gateway default adalah perangkat jaringan yang dapat mengarahkan lalu lintas ke jaringan lain. Ini adalah router yang bisa mengarahkan lalu lintas keluar dari jaringan lokal.

Jika Anda menggunakan analogi bahwa jaringan itu seperti sebuah ruangan, maka gateway defaultnya seperti pintu. Jika Anda ingin pergi ke ruangan lain atau jaringan Anda perlu menemukan pintu.

Sebagai alternatif, PC atau komputer yang tidak mengetahui alamat IP dari gateway default adalah seperti seseorang dalam sebuah ruangan, yang tidak tahu di mana letak pintu. Mereka bisa berbicara dengan orang lain di ruangan atau jaringan, tapi kalau mereka tidak tahu alamat gateway defaultnya, atau tidak ada gateway default, maka tidak ada jalan keluarnya.

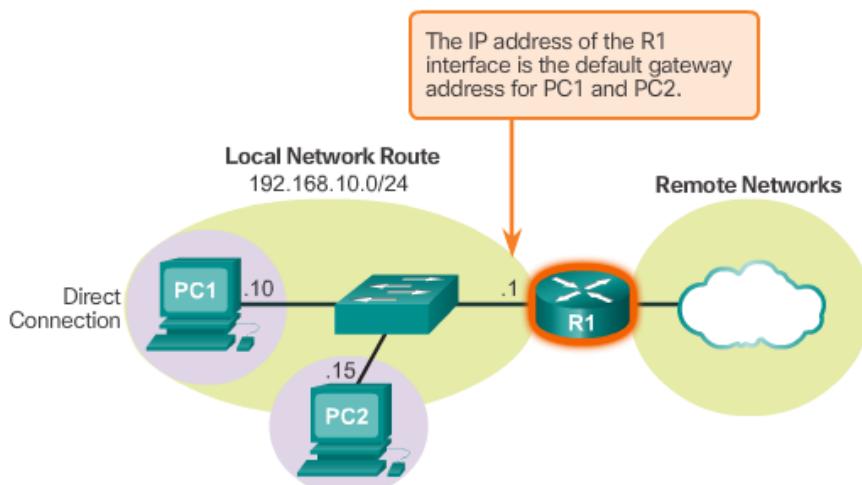
- ✓ Mengatur lintasan ke jaringan lain
- ✓ Dapat mengambil *data in* dan *forward data out*
- ✓ Memiliki *Local Ip addresses* didalam rentang alamat yang sama sebagai host lain didalam jaringan

- **MENGGUNAKAN DEFAULT GATEWAY**

Tabel routing host biasanya akan menyertakan gateway default. Host menerima alamat IPv4 dari gateway default baik secara dinamis dari Dynamic Host Configuration Protocol (DHCP) atau dikonfigurasi secara manual. Pada gambar, PC1 dan PC2 dikonfigurasikan dengan alamat IPv4 default gateway 192.168.10.1. Memiliki gateway default yang dikonfigurasi membuat rute default di tabel routing PC. Rute default adalah rute atau jalur yang akan ditempuh komputer saat mencoba menghubungi jaringan jarak jauh.

Rute default berasal dari konfigurasi gateway default dan ditempatkan di tabel routing komputer host. PC1 dan PC2 akan memiliki rute default untuk mengirim semua lalu lintas yang ditujukan ke jaringan jarak jauh ke R1.

Host Default Gateway



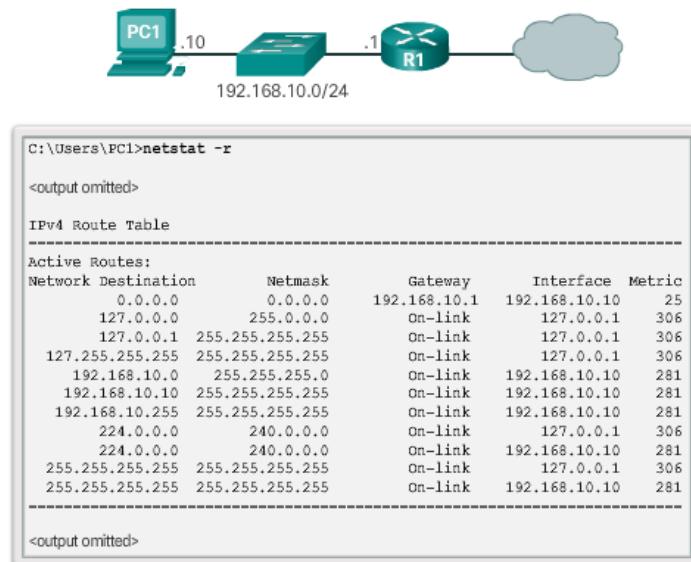
- **HOST ROUTING TABLE**

Pada host Windows, perintah print atau netstat -r rute dapat digunakan untuk menampilkan tabel routing host. Kedua perintah menghasilkan output yang sama. Keluarnya mungkin tampak luar biasa pada awalnya, tapi cukup mudah dimengerti.

Memasukkan perintah netstat -r atau perintah cetak rute setara, menampilkan tiga bagian yang terkait dengan koneksi jaringan TCP / IP saat ini:

- ✓ **Interface List** - Mencantumkan alamat Kontrol Akses Media (MAC) dan nomor antarmuka yang ditetapkan dari setiap antarmuka berkemampuan jaringan pada host, termasuk Ethernet, Wi-Fi, dan adaptor Bluetooth
- ✓ **IPv4 Route Table** - Menampilkan semua rute IPv4 yang diketahui, termasuk koneksi langsung, jaringan lokal, dan rute default lokal.
- ✓ **IPv6 Route Table** - Menampilkan semua rute IPv6 yang diketahui, termasuk koneksi langsung, jaringan lokal, dan rute default lokal.

IPv4 Routing Table for PC1



- ❖ **ROUTER ROUTING TABLE**

- **ROUTER PACKET FORWARDING DECISION**

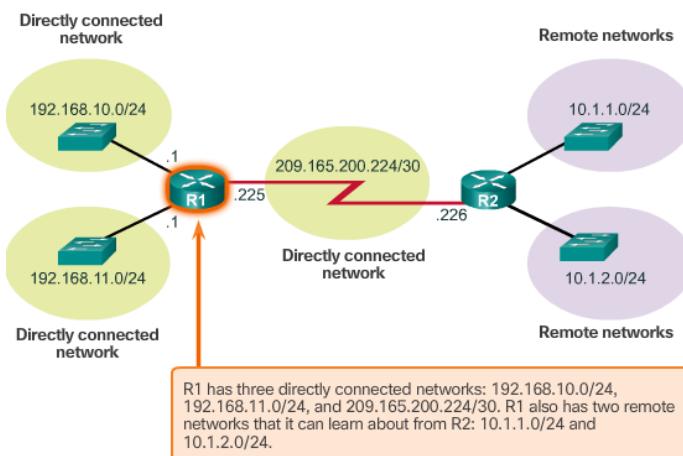
Ketika sebuah host mengirimkan sebuah paket ke host lain, ia akan menggunakan tabel routing untuk menentukan kemana harus mengirim paket. Jika host tujuan berada pada jaringan jarak jauh, paket diteruskan ke *gateway default*.

Apa yang terjadi ketika sebuah paket tiba di *gateway default*, yang biasanya merupakan router? Router melihat tabel routing-nya untuk menentukan kemana harus meneruskan paket.

Tabel routing router dapat menyimpan informasi tentang:

- ✓ **Directly-connected routes** - Rute ini berasal dari antarmuka router aktif. Router menambahkan rute yang terhubung langsung saat sebuah antarmuka dikonfigurasi dengan alamat IP dan diaktifkan. Masing-masing interface router terhubung ke segmen jaringan yang berbeda.
- ✓ **Remote routes** - Rute ini berasal dari jaringan jarak jauh yang terhubung ke router lain. Rute ke jaringan ini dapat dikonfigurasi secara manual di router lokal oleh administrator jaringan atau dikonfigurasi secara dinamis dengan memungkinkan router lokal menukar informasi routing dengan router lain menggunakan protokol perutean dinamis.
- ✓ **Default route** - Seperti host, router juga menggunakan rute default sebagai upaya terakhir jika tidak ada rute lain ke jaringan yang diinginkan di tabel routing.

Directly Connected and Remote Network Routes

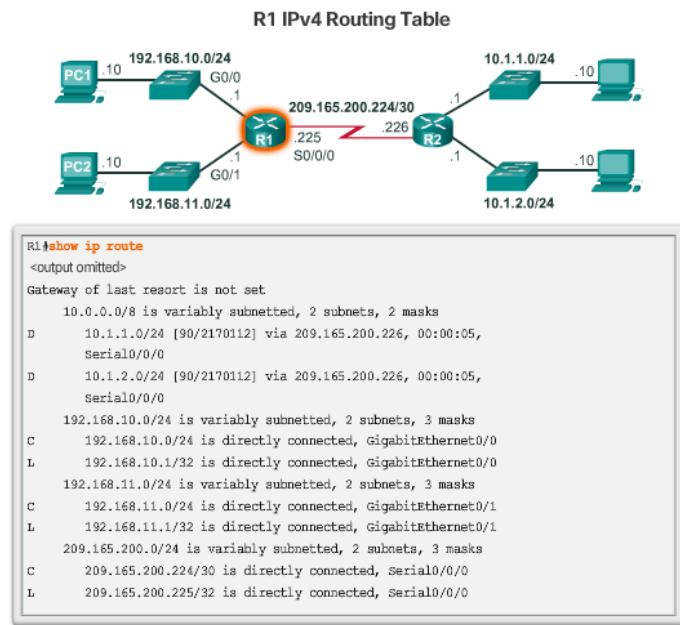


• IPv4 ROUTER ROUTING TABLE

Pada router Cisco IOS, perintah show ip route dapat digunakan untuk menampilkan tabel routing router, seperti yang ditunjukkan pada gambar.

Selain menyediakan informasi routing untuk jaringan dan jaringan jarak jauh yang terhubung langsung, tabel routing juga memiliki informasi tentang bagaimana rute dipelajari, tingkat kepercayaan dan penilaian rute, saat rute terakhir diperbarui, dan antarmuka mana yang akan digunakan untuk menjangkau tujuan yang diminta

Ketika sebuah paket tiba di antarmuka router, router memeriksa header paket untuk menentukan jaringan tujuan. Jika jaringan tujuan sesuai dengan rute di tabel routing, router meneruskan paket menggunakan informasi yang ditentukan dalam tabel routing. Jika ada dua atau lebih rute yang mungkin ke tujuan yang sama, metrik tersebut digunakan untuk menentukan rute mana yang muncul di tabel routing.



- DIRECTLY CONNECTED ROUTING TABLE ENTRIES**

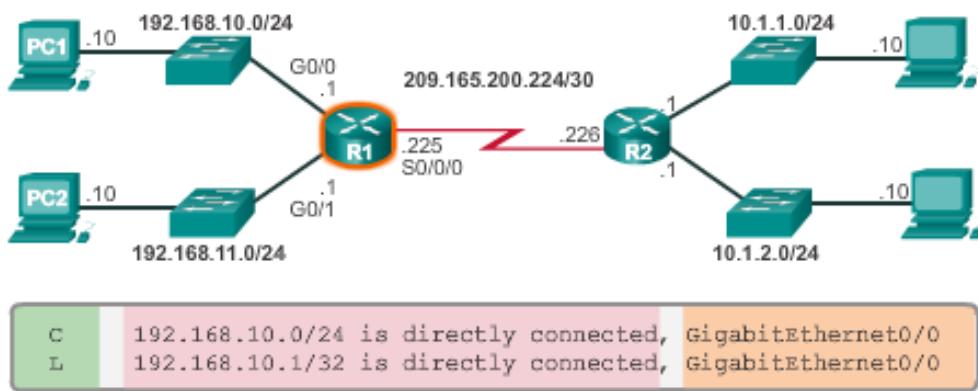
Ketika sebuah antarmuka router dikonfigurasi dengan alamat IPv4, subnet mask, dan diaktifkan, dua tabel routing berikut secara otomatis dibuat:

- ✓ C - Mengidentifikasi jaringan yang terhubung langsung. Jaringan terhubung langsung dibuat secara otomatis saat sebuah antarmuka dikonfigurasi dengan alamat IP dan diaktifkan.
- ✓ L - Mengidentifikasi bahwa ini adalah antarmuka lokal. Ini adalah alamat IPv4 dari antarmuka pada router.

entri tabel routing pada R1 untuk jaringan yang terhubung langsung 192.168.10.0. Entri ini secara otomatis ditambahkan ke tabel routing saat antarmuka GigabitEthernet 0/0 dikonfigurasi dan diaktifkan.

Catatan: Entri antarmuka lokal tidak muncul dalam tabel routing sebelum IOS Release

Understanding Local Route Entries

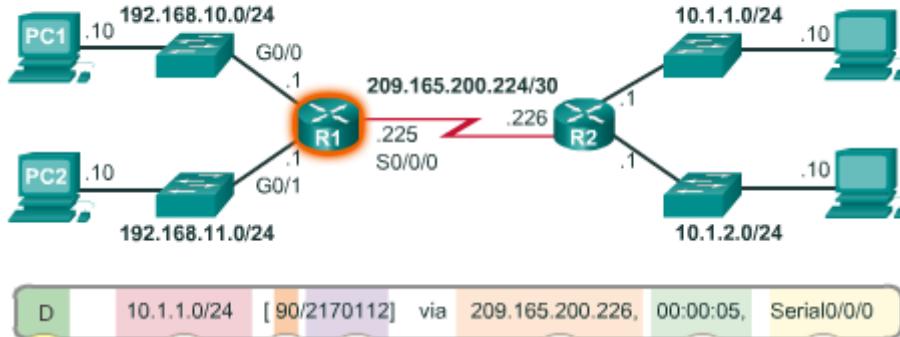


- REMOTE CONNECTED ROUTING TABLE ENTRIES

Router biasanya memiliki banyak antarmuka yang dikonfigurasi. Tabel routing menyimpan informasi tentang jaringan yang terhubung langsung dan jaringan jarak jauh.

rute R1 ke jaringan jarak jauh 10.1.1.0.

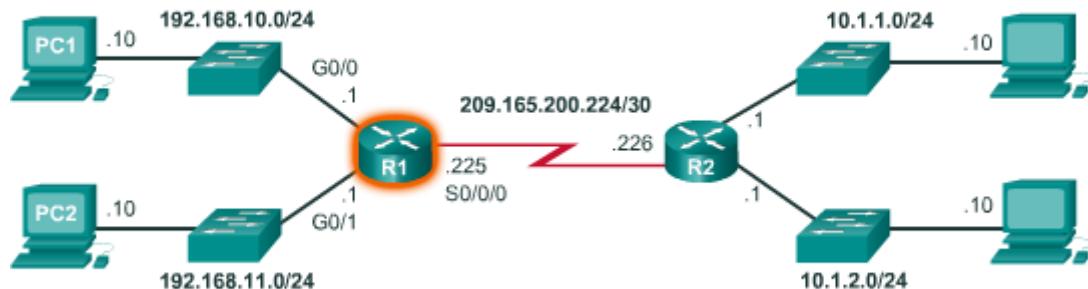
Understanding Remote Route Entries



- NEXT HOP ADDRESS

Ketika sebuah paket yang ditujukan untuk jaringan jarak jauh tiba di router, router sesuai dengan jaringan tujuan ke rute di tabel routing. Jika ada kecocokan, router meneruskan paket ke alamat hop berikutnya dari antarmuka yang teridentifikasi.

Lihat contoh topologi jaringan pada Gambar . Asumsikan bahwa PC1 atau PC2 telah mengirim paket yang ditujukan untuk jaringan 10.1.1.0 atau 10.1.2.0. Saat paket tiba di antarmuka R1 Gigabit, R1 akan membandingkan alamat tujuan IPv4 paket dengan entri dalam tabel routingnya. Tabel routing ditampilkan pada Gambar . Berdasarkan isi peruteannya, R1 akan meneruskan paket dari antarmuka Serial 0/0/0 ke alamat hop berikutnya 209.165.200.226.



Perhatikan bagaimana jaringan yang terhubung langsung dengan sumber rute C dan L tidak memiliki alamat next-hop. Ini karena router dapat meneruskan paket langsung ke host pada jaringan ini menggunakan antarmuka yang ditunjuk.

Penting juga untuk memahami bahwa paket tidak dapat diteruskan oleh router tanpa rute untuk jaringan tujuan di tabel routing. Jika rute yang mewakili jaringan tujuan tidak berada dalam tabel routing, paket tersebut akan terjatuh (artinya tidak diteruskan). Namun, seperti

host dapat menggunakan *gateway default* untuk meneruskan paket ke tujuan yang tidak diketahui, router juga dapat dikonfigurasi untuk menggunakan rute statis default untuk membuat *Gateway of Last Resort*.

R1 Routing Table

```
R1# show ip route
<output omitted>
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D        10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
          Serial0/0/0
D        10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
          Serial0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C          192.168.10.0/24 is directly connected, GigabitEthernet0/0
L          192.168.10.1/32 is directly connected, GigabitEthernet0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C          192.168.11.0/24 is directly connected, GigabitEthernet0/1
L          192.168.11.1/32 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C          209.165.200.224/30 is directly connected, Serial0/0/0
L          209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

6.4 ROUTERS

❖ ANATOMI ROUTER

• ROUTER ADALAH KOMPUTER

Ada banyak jenis router infrastruktur yang tersedia. Sebenarnya, router Cisco dirancang untuk memenuhi kebutuhan berbagai jenis bisnis dan jaringan:

- ✓ **Branch** - Teleworkers, usaha kecil, dan situs cabang berukuran sedang. Termasuk Cisco Integrated Services Routers (ISR) G2 (generasi ke-2).
- ✓ **WAN** - Bisnis besar, organisasi, dan perusahaan. Meliputi Cisco Catalyst Series Switches dan Cisco Aggregation Services Routers (ASR).
- ✓ **Service Provider** - Penyedia layanan besar. Termasuk Cisco ASR, Cisco CRS-3 Carrier Routing System, dan router Seri 7600.

Fokus sertifikasi CCNA ada pada keluarga cabang router. Angka tersebut menampilkan Router Terpadu Cisco 1900, 2900, dan 3900 G2.

Terlepas dari fungsi, ukuran atau kompleksitasnya, semua model router pada dasarnya adalah komputer. Sama seperti komputer, tablet, dan perangkat pintar, router juga memerlukan:

- ✓ Central processing units (CPU)
- ✓ Operating systems (OS)
- ✓ Memory consisting of random-access memory (RAM), read-only memory (ROM), nonvolatile random-access memory (NVRAM), and flash

- **ROUTER CPU DAN OS**

Seperti semua komputer, tablet, konsol game, dan perangkat cerdas, perangkat Cisco memerlukan CPU untuk menjalankan perintah OS, seperti inisialisasi sistem, fungsi perutean, dan fungsi peralihan.

Komponen yang disorot pada gambar adalah CPU router Cisco 1941 dengan heatsink terpasang. Heatsink membantu menghilangkan panas yang dihasilkan oleh CPU.

CPU membutuhkan sebuah OS untuk menyediakan routing dan fungsi switching. Cisco Internetwork Operating System (IOS) adalah perangkat lunak sistem yang digunakan untuk sebagian besar perangkat Cisco terlepas dari ukuran dan jenis perangkatnya. Ini digunakan untuk router, switch LAN, titik akses nirkabel kecil, router besar dengan puluhan antarmuka, dan banyak perangkat lainnya.



- **ROUTER MEMORY**

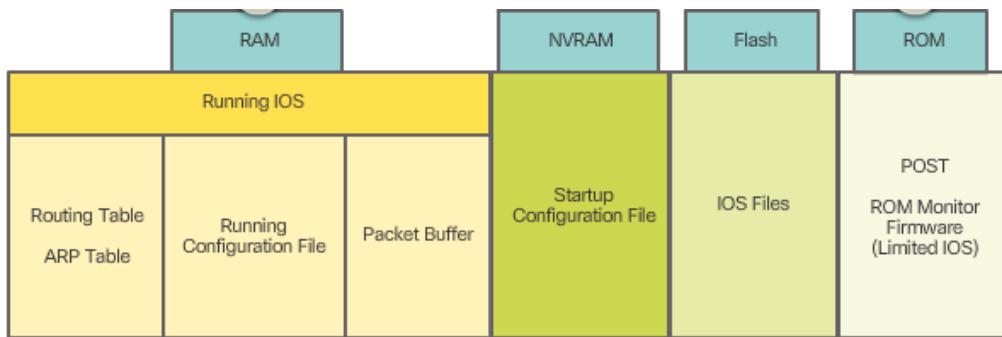
Router memiliki akses ke penyimpanan memori yang mudah menguap atau tidak mudah menguap. Memori volatil membutuhkan kekuatan terus menerus untuk menjaga informasinya. Saat router dimatikan atau dihidupkan ulang, konten akan terhapus dan hilang. Memori non-volatile menyimpan informasinya meskipun perangkat di-reboot.

Secara khusus, router Cisco menggunakan empat jenis memori:

- ✓ **RAM** - Ini adalah memori volatile yang digunakan pada router Cisco untuk menyimpan aplikasi, proses, dan data yang dibutuhkan untuk dieksekusi oleh CPU. Router Cisco menggunakan tipe RAM cepat yang disebut synchronous dynamic random access memory (SDRAM).
- ✓ **ROM** - Memori non-volatile ini digunakan untuk menyimpan instruksi operasional penting dan IOS terbatas. Secara khusus, ROM adalah firmware yang disematkan di sirkuit terpadu di dalam router yang hanya bisa diubah oleh Cisco.
- ✓ **NVRAM** - Memori ini digunakan sebagai tempat penyimpanan permanen untuk file konfigurasi startup (*startup-config*).
- ✓ **Flash** - *memori Flash* adalah memori komputer non-volatile yang digunakan sebagai penyimpanan permanen untuk iOS dan file terkait sistem lainnya seperti file log, file konfigurasi suara, file HTML, konfigurasi cadangan, dan lainnya. Saat router di-reboot, iOS disalin dari flash ke RAM

Semua platform router memiliki pengaturan dan komponen default. Sebagai contoh, Cisco 1941 hadir dengan SDRAM 512 MB namun diupgrade sampai 2,0 GB. Router Cisco 1941 juga dilengkapi dengan 256 MB flash namun diupgrade menggunakan dua slot Compact Flash

eksternal. Setiap slot dapat mendukung kartu penyimpanan berkecepatan tinggi yang dapat diupgrade sampai 4GB.



• DIDALAM SEBUAH ROUTER

Meskipun ada beberapa tipe dan model router yang berbeda, setiap router memiliki komponen perangkat keras umum yang sama.

Angka tersebut menunjukkan bagian dalam generasi pertama Cisco 1841 ISR. gambar komponen lain yang ditemukan di router, seperti power supply, kipas pendingin, perisai panas, dan modul integrasi lanjutan (AIM).

Catatan: Seorang profesional jaringan harus mengenal dan memahami fungsi komponen internal utama router, bukan lokasi yang tepat dari komponen di dalam router tertentu. Bergantung pada model, komponen tersebut berada di tempat yang berbeda di dalam router.



- **KONEKSI KE ROUTER**

Perangkat Cisco, router, dan switch biasanya menghubungkan banyak perangkat. Untuk alasan ini, perangkat ini memiliki beberapa jenis port dan interface yang digunakan untuk terhubung ke perangkat. Sebagai contoh, sebuah backplane router Cisco 1941 mencakup koneksi dan port yang dijelaskan pada gambar.

Seperti banyak perangkat jaringan, perangkat Cisco menggunakan indikator light emitting diode (LED) untuk memberikan informasi status. LED antarmuka menunjukkan aktivitas antarmuka yang sesuai. Jika LED mati saat antarmuka aktif, dan antarmuka terhubung dengan benar, ini mungkin merupakan indikasi adanya masalah pada antarmuka tersebut. Jika sebuah antarmuka sangat sibuk, LED-nya selalu menyala.

- **LAN & WAN INTERFACE**

Sambungan pada router Cisco dapat dikelompokkan menjadi dua kategori: Antarmuka router dan port pengelolaan In-band.

Mirip dengan switch Cisco, ada beberapa cara untuk mengakses mode EXEC pengguna di lingkungan CLI di router Cisco. Ini adalah yang paling umum:

- ✓ **Console** - Ini adalah port manajemen fisik yang menyediakan akses out-of-band ke perangkat Cisco. Akses out-of-band mengacu pada akses melalui saluran pengelolaan khusus yang hanya digunakan untuk tujuan perawatan perangkat.
- ✓ **Secure Shell (SSH)** - SSH adalah metode untuk jarak jauh membuat koneksi CLI yang aman melalui antarmuka virtual, melalui jaringan. Tidak seperti koneksi konsol, koneksi SSH memerlukan layanan jaringan aktif pada perangkat termasuk antarmuka aktif yang dikonfigurasi dengan sebuah alamat.
- ✓ **Telnet** - Telnet adalah metode yang tidak aman untuk membangun sesi CLI dari jarak jauh melalui antarmuka virtual, melalui jaringan. Tidak seperti SSH, Telnet tidak menyediakan koneksi yang terenkripsi dengan aman. Otentikasi pengguna, kata sandi, dan perintah dikirim melalui jaringan di plaintext.

Catatan: Beberapa perangkat, seperti router, mungkin juga mendukung port pelengkap warisan yang digunakan untuk membuat sesi CLI dari jarak jauh menggunakan modem. Serupa dengan koneksi konsol, port AUX tidak beroperasi dan tidak memerlukan layanan jaringan untuk dikonfigurasi atau tersedia.

Telnet dan SSH memerlukan koneksi jaringan inband yang berarti bahwa administrator harus mengakses router melalui salah satu antarmuka WAN atau LAN.

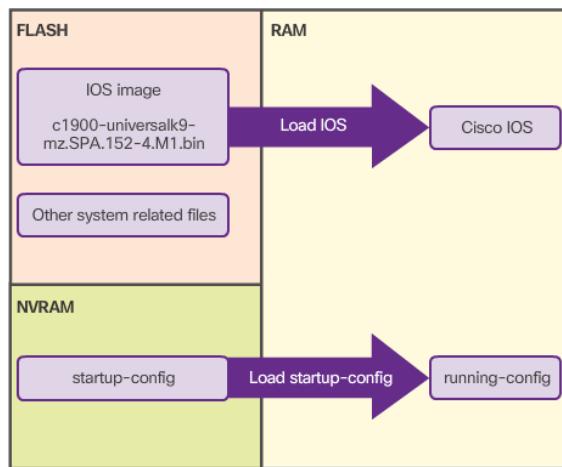
Inband interface menerima dan meneruskan paket IP. Setiap antarmuka yang dikonfigurasi dan aktif di router adalah anggota atau host pada jaringan IP yang berbeda. Setiap antarmuka harus dikonfigurasi dengan alamat IPv4 dan subnet mask dari jaringan yang berbeda. Cisco IOS tidak mengizinkan dua antarmuka aktif pada router yang sama termasuk dalam jaringan yang sama.

❖ ROUTER BOOT-UP

• BOOTSET FILES

Konfigurasi berjalan dimodifikasi saat administrator jaringan melakukan konfigurasi perangkat. Perubahan yang dilakukan pada file *running-config* harus disimpan ke file konfigurasi startup di NVRAM, jika router di-restart atau kehilangan daya.

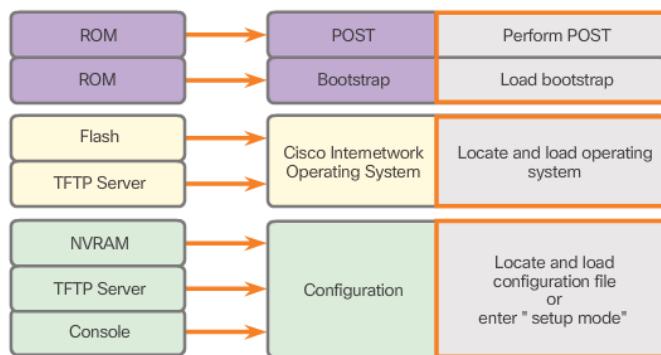
Files Copied to RAM During Bootup



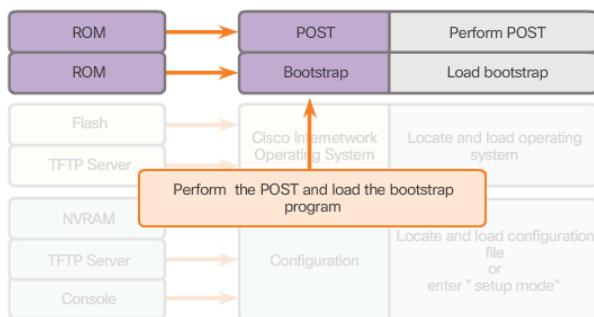
• ROUTER BOOTUP PROCESS

Ada tiga fase utama untuk proses bootup. Seperti ditunjukkan pada Gambar , mereka adalah:

1. Lakukan POST dan muat program bootstrap.
2. Cari dan muat perangkat lunak Cisco IOS.
3. Cari dan muat file konfigurasi startup atau masuk ke mode setup.



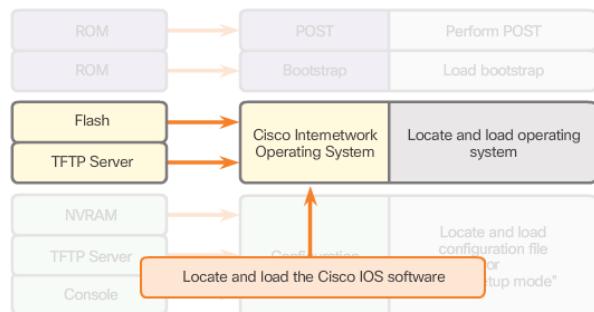
1. Melakukan Program Bootstrap POST dan Load



Selama Power-On Self-Test (POST), router mengeksekusi diagnostik dari ROM pada beberapa komponen perangkat keras, termasuk CPU, RAM, dan NVRAM. Setelah POST, program bootstrap disalin dari ROM ke RAM. Tugas utama program bootstrap adalah mencari Cisco IOS dan memasukkannya ke RAM.

Catatan: Pada titik ini, jika Anda memiliki koneksi konsol ke router, Anda akan mulai melihat output di layar.

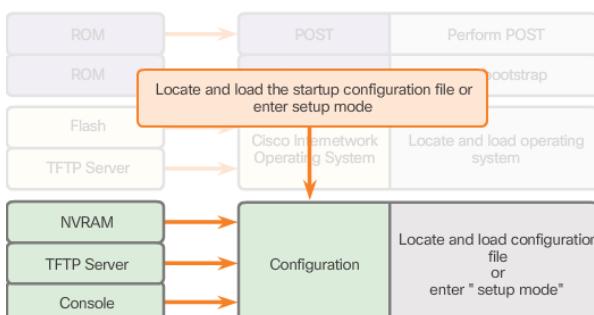
2. Menemukan dan Mengunggah Cisco IOS



IOS biasanya tersimpan dalam memori flash dan disalin ke RAM untuk dieksekusi oleh CPU. Jika gambar iOS tidak terletak di flashdisk, maka router mungkin mencarinya menggunakan server Trivial File Transfer Protocol (TFTP). Jika gambar IOS penuh tidak dapat ditemukan, IOS terbatas akan disalin ke RAM, yang dapat digunakan untuk mendiagnosis masalah dan mentransfer IOS penuh ke memori Flash.

3. Menemukan dan Memuat File Konfigurasi

How a Router Boots Up



Program bootstrap kemudian menyalin file konfigurasi startup dari NVRAM ke RAM. Ini menjadi konfigurasi yang berjalan. Jika file konfigurasi startup tidak ada di NVRAM, router dapat dikonfigurasi untuk mencari server TFTP. Jika server TFTP tidak ditemukan, router akan menampilkan prompt mode setup.

Catatan: Mode pengaturan tidak digunakan dalam kursus ini untuk mengkonfigurasi router. Saat diminta masuk ke mode setup, selalu jawab no. Jika Anda menjawab ya dan masuk ke mode setup, tekan Ctrl + C kapan saja untuk menghentikan proses penyiapan.

6.5 CONFIGURE ROUTERS

❖ CONFIGURE INITIAL SETTINGS

• BASIC SWITCH CONFIGURATION STEPS

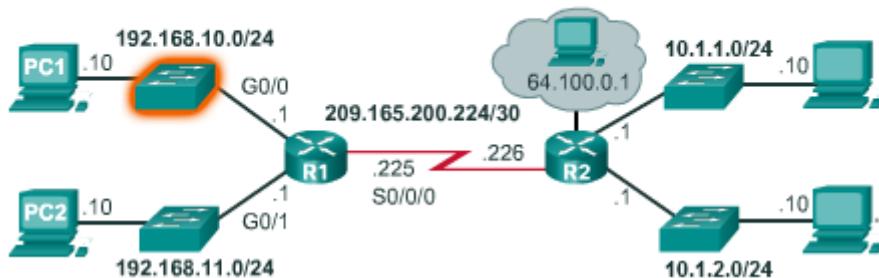
Router Cisco dan switch Cisco memiliki banyak kesamaan. Mereka mendukung sistem operasi yang sama, mendukung struktur perintah yang serupa dan mendukung banyak perintah yang sama. Selain itu, kedua perangkat memiliki langkah konfigurasi awal yang identik saat diimplementasikan dalam jaringan.

Sebelum kita mulai mengkonfigurasi router, tinjau kembali tugas-tugas konfigurasi switch.

- Configure the device name
 - `hostname name`
- Secure user EXEC mode
 - `line console 0`
 - `password password`
 - `login`
- Secure remote Telnet / SSH access
 - `line vty 0 15`
 - `password password`
 - `login`
- Secure privileged EXEC mode
 - `enable secret password`
- Secure all passwords in the config file
 - `service password-encryption`
- Provide legal notification
 - `banner motd delimiter message delimiter`
- Configure the management SVI
 - `interface vlan 1`
 - `ip address ip-address subnet-mask`
 - `no shutdown`
- Save the configuration
 - `copy running-config startup-config`

CONTOH CONFIGURASI

Sample Switch Configuration



```
Switch>enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# enable secret class
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)# service password-encryption
S1(config)# banner motd #No unauthorized access allowed!#
S1(config)# interface vlan1
S1(config-if)# ip address 192.168.10.50 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

- **BASIC ROUTER CONFIGURATION STEPS**

Mirip dengan mengkonfigurasi switch, tugas yang tercantum pada Gambar harus selesai saat mengkonfigurasi pengaturan awal pada router.

```

Configure the device name
  • hostname name

Secure user EXEC mode
  • line console 0
  • password password
  • login

Secure remote Telnet / SSH access
  • line vty 0 15
  • password password
  • login

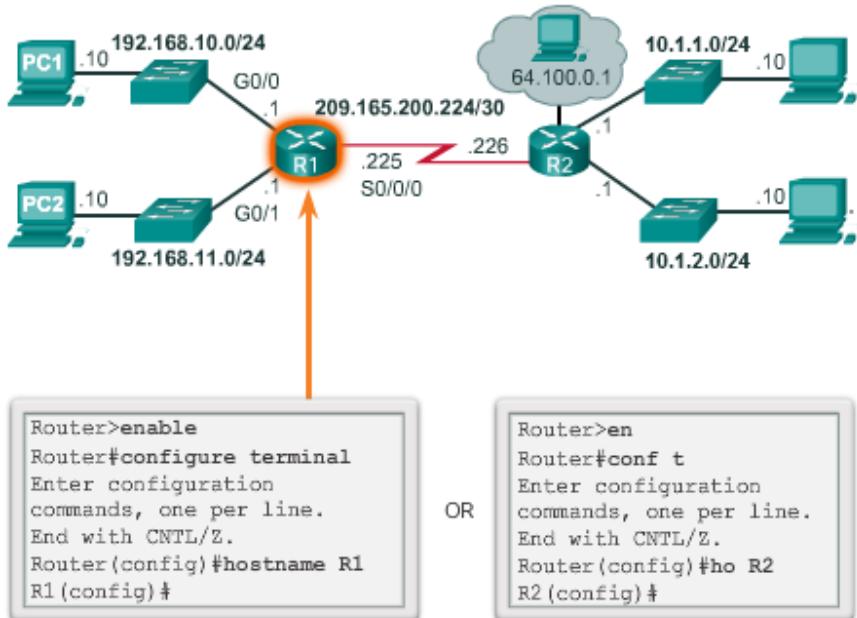
Secure privileged EXEC mode
  • enable secret password

Secure all passwords in the config file
  • service password-encryption

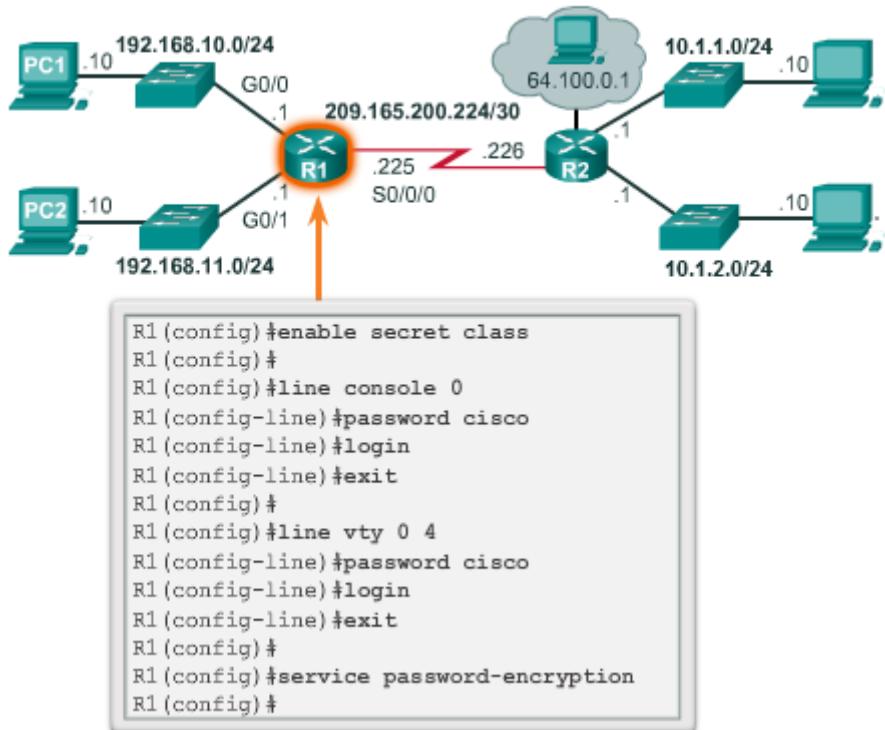
Provide legal notification
  • banner motd delimiter message delimiter

Save the configuration
  • copy running-config startup-config
  
```

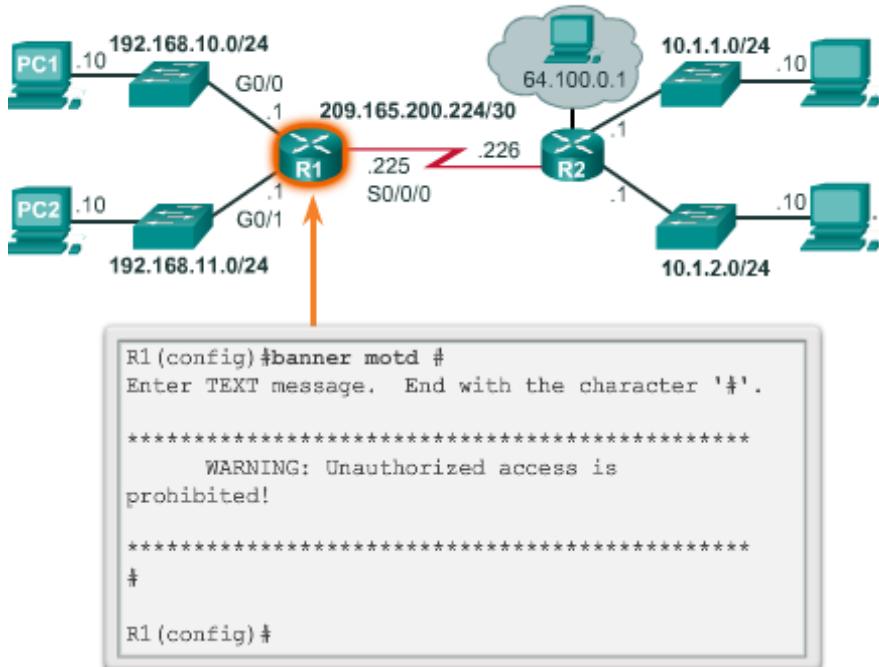
Configuring Hostname



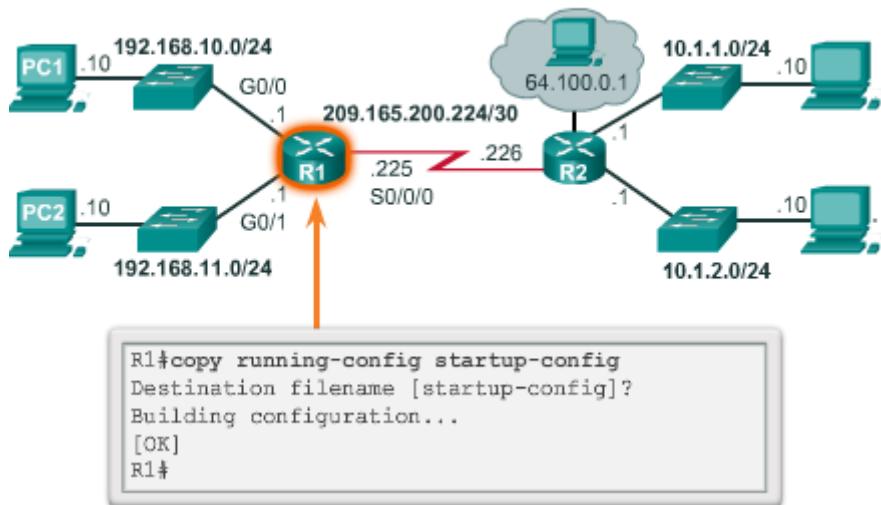
Securing Management Access



Providing Legal Notification



Saving the Configuration



- ❖ **CONFIGURE INTERFACE**
 - **CONFIGURE ROUTER INTERFACE**

Agar router dapat dijangkau, antarmuka router in-band harus dikonfigurasi. Ada banyak jenis antarmuka yang tersedia di router Cisco. Dalam contoh ini, router Cisco 1941 dilengkapi dengan:

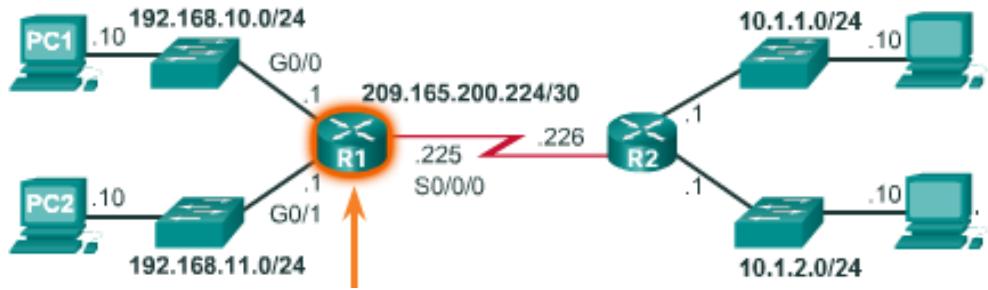
- ✓ **Two Gigabit Ethernet interfaces** - GigabitEthernet 0/0 (G0/0) and GigabitEthernet 0/1 (G0/1)
- ✓ **A serial WAN interface card (WIC) consisting of two interfaces** - Serial 0/0/0 (S0/0/0) and Serial 0/0/1 (S0/0/1)

Tugas untuk mengkonfigurasi antarmuka router tercantum pada Gambar. Perhatikan bagaimana mereka sangat mirip dengan konfigurasi manajemen SVI pada sebuah switch.

Configure the interface

- **interface type-and-number**
- **description description-text**
- **ip address ipv4-address subnet-mask**
- **no shutdown**

CONTOH CONFIGURASI



```
R1#conf t
Enter configuration commands, one per line.
End with CNTL/Z.

R1(config)#
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#description Link to LAN-10
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#
R1(config)#int g0/1
R1(config-if)#ip add 192.168.11.1 255.255.255.0
R1(config-if)#des Link to LAN-11
R1(config-if)#no shut
%LINK-5-CHANGED: Interface GigabitEthernet0/1,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)#exit
R1(config)#

```

Meski tidak diperlukan, ada baiknya untuk mengkonfigurasi deskripsi pada setiap *interface* untuk membantu mendokumentasikan informasi jaringan. Teks deskripsi dibatasi hingga 240 karakter. Pada jaringan produksi, deskripsi dapat membantu dalam pemecahan masalah dengan memberikan informasi tentang jenis jaringan yang terhubung dengan *interface* dan jika ada router lain di jaringan itu. Jika *interface* terhubung ke ISP atau operator layanan, ada baiknya untuk memasukkan koneksi pihak ketiga dan informasi kontak. Menggunakan perintah *shutdown* tidak mengaktifkan *interface* dan mirip dengan menyalakan *interface*. *interface* juga harus terhubung ke perangkat lain (hub, switch, atau router lain) agar lapisan fisik dapat aktif.

- **VERIFIKASI INTERFACE CONFIGURE**

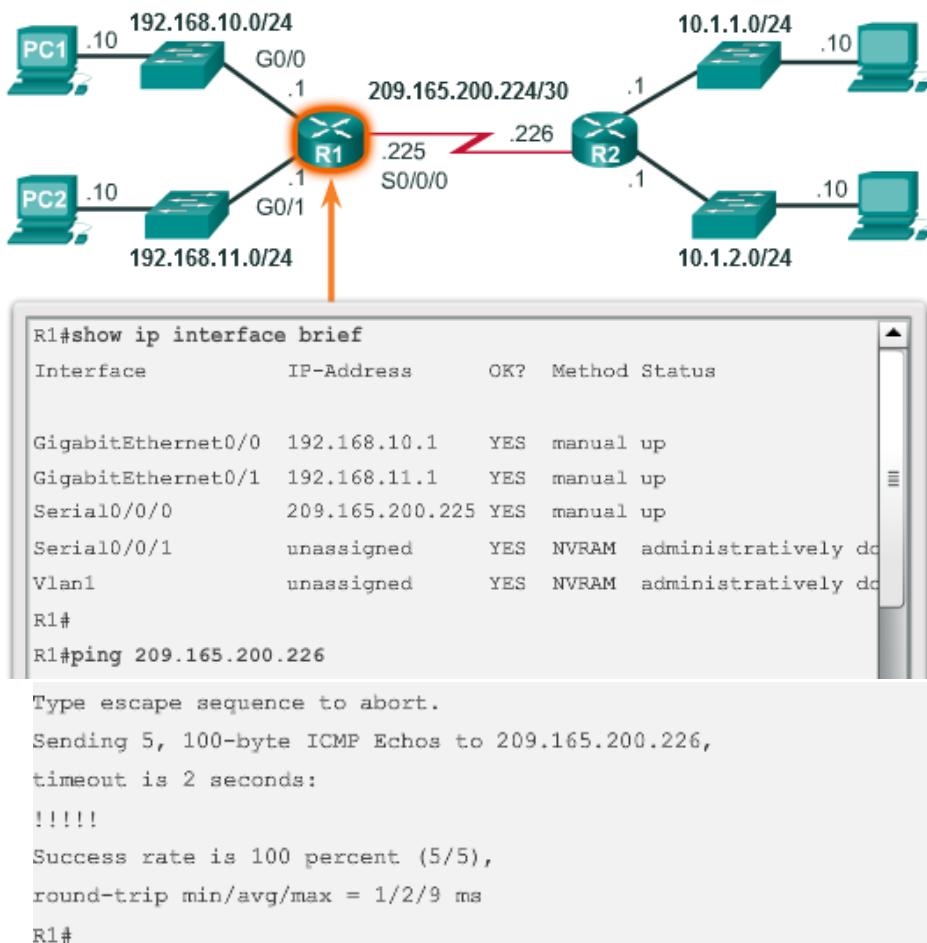
Ada beberapa perintah yang bisa digunakan untuk memverifikasi konfigurasi *interface*. Yang paling berguna adalah perintah *show ip interface brief*. Output yang dihasilkan menampilkan semua antarmuka, alamat IPv4 mereka, dan status mereka saat ini. *Interface* yang dikonfigurasi dan terhubung harus menampilkan Status "naik" dan Protokol "naik". Ada lagi yang mengindikasikan masalah dengan konfigurasi atau pemasangan kabel.

Anda dapat memverifikasi konektivitas dari *interface* menggunakan perintah ping. Router Cisco mengirim lima buah ping berturut-turut dan mengukur waktu rabat minimal, rata-rata, dan maksimum. Tanda seru memverifikasi konektivitas.

Gambar menampilkan output dari perintah *show ip interface brief*, yang menunjukkan bahwa antarmuka LAN dan link WAN semuanya diaktifkan dan beroperasi. Perhatikan bahwa perintah ping menghasilkan lima tanda seru yang memverifikasi konektivitas ke R2.

Perintah verifikasi antarmuka lainnya meliputi:

- ✓ **show ip route** - Menampilkan isi tabel routing IPv4 yang tersimpan dalam RAM.
- ✓ **show interfaces** - Menampilkan statistik untuk semua antarmuka pada perangkat.
- ✓ **show ip interface** - Menampilkan statistik IPv4 untuk semua interface pada router.



Gambar menampilkan output perintah ip show route. Perhatikan tiga entri jaringan terhubung langsung dengan alamat IPv4 antarmuka lokal mereka.

Ingatlah untuk menyimpan konfigurasi menggunakan perintah **running-config startup-config**.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP,
       M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
           IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
           i - IS-IS, L1 - IS-IS level-1,
           L2 - IS-IS level-2, ia - IS-IS inter area
           * - candidate default, U - per-user static route, o - ODR
           P - periodic downloaded static route

Gateway of last resort is not set

      192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C        209.165.200.224/30 is directly connected, Serial0/0/0
L        209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

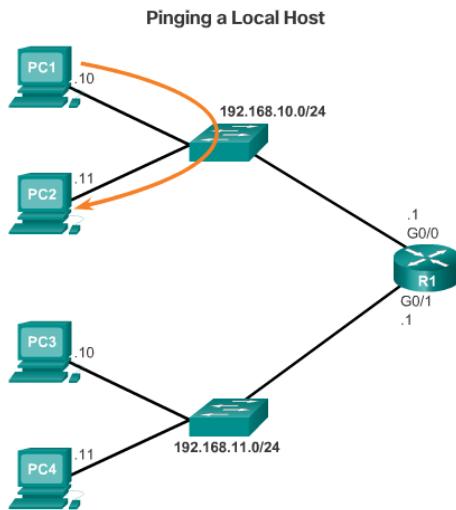
❖ CONFIGURE THE DEFAULT GATEWAY

• DEFAULT GATEWAY FOR A HOST

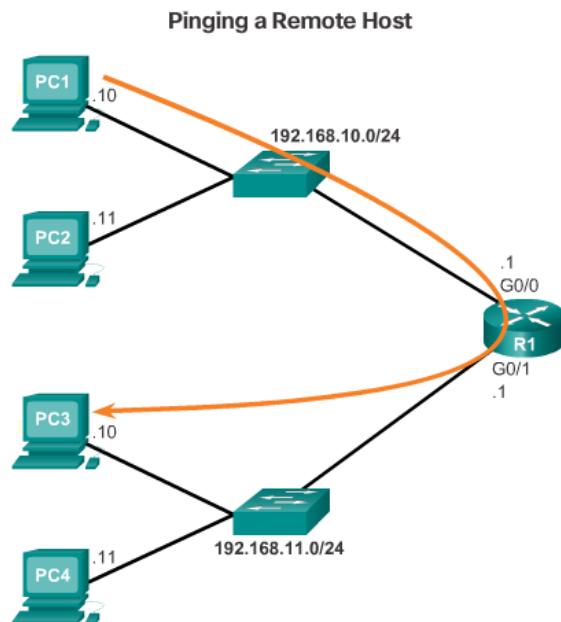
Untuk perangkat akhir untuk berkomunikasi melalui jaringan, perangkat harus dikonfigurasi dengan informasi alamat IP yang benar, termasuk alamat gateway default. Gateway default hanya digunakan saat host ingin mengirim paket ke perangkat di jaringan lain. Alamat gateway default umumnya adalah alamat antarmuka router yang terhubung ke jaringan lokal host. Alamat IP perangkat host dan alamat antarmuka router harus berada dalam jaringan yang sama.

Angka tersebut menampilkan topologi router dengan dua antarmuka terpisah. Setiap antarmuka terhubung ke jaringan yang terpisah. G0 / 0 terhubung ke jaringan 192.168.10.0, sementara G0 / 1 terhubung ke jaringan 192.168.11.0. Setiap perangkat host dikonfigurasi dengan alamat gateway default yang sesuai.

Pada Gambar, PC1 mengirimkan sebuah paket ke PC2. Dalam contoh ini, gateway default tidak digunakan; Sebaliknya, PC1 alamat paket dengan alamat IP PC2 dan meneruskan paket langsung ke PC2 melalui switch



Pada Gambar, PC1 mengirimkan sebuah paket ke PC3. Dalam contoh ini, PC1 menangani paket dengan alamat IP PC3, namun kemudian meneruskan paket ke router. Router menerima paket, mengakses tabel routing untuk menentukan antarmuka keluar yang sesuai berdasarkan alamat tujuan, dan kemudian meneruskan paket dari antarmuka yang sesuai untuk mencapai PC3.



- **DEFAULT GATEWAY FOR SWITCH**

Biasanya switch workgroup yang menghubungkan komputer client adalah perangkat Layer 2. Dengan demikian, switch Layer 2 tidak memerlukan alamat IP agar berfungsi dengan baik. Namun, jika Anda ingin terhubung ke switch dan mengurnya secara administratif melalui beberapa jaringan, Anda perlu mengkonfigurasi SVI dengan alamat IPv4, subnet mask, dan alamat gateway default.

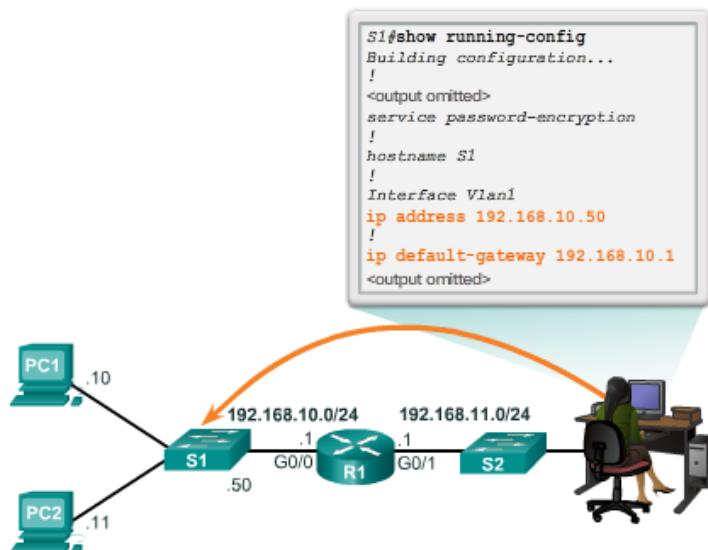
Alamat gateway default biasanya dikonfigurasi pada semua perangkat yang ingin berkomunikasi lebih dari sekedar jaringan lokal mereka. Dengan kata lain, untuk mengakses switch dari jaringan lain menggunakan SSH atau Telnet, peralihan harus memiliki SVI dengan

alamat IPv4, subnet mask, dan alamat gateway default yang dikonfigurasi. Jika switch diakses dari host dalam jaringan lokal, maka alamat gateway default IPv4 tidak diperlukan.

Untuk mengkonfigurasi gateway default pada switch gunakan perintah konfigurasi global ip gateway default. Alamat IP yang dikonfigurasi adalah interface router dari switch yang terhubung.

Gambar menunjukkan administrator yang terhubung ke switch pada jaringan jarak jauh. Agar peralihan ke forward response packets ke administrator, gateway default harus dikonfigurasi.

Kesalahpahaman yang umum adalah bahwa switch menggunakan alamat gateway default yang dikonfigurasi untuk menentukan kemana harus meneruskan paket yang berasal dari host yang terhubung ke switch dan ditujukan untuk host pada jaringan jarak jauh. Sebenarnya alamat IP dan informasi gateway default hanya digunakan untuk paket yang berasal dari switch. Paket yang berasal dari komputer host yang terhubung ke peralihan harus sudah memiliki alamat gateway default yang dikonfigurasi pada sistem operasi komputer induk mereka.



If the default gateway was not configured on S1, response packets from S1 would not be able to reach the administrator at 192.168.11.10. The administrator would not be able to manage the device remotely.

LATIHAN SOAL 6

1. Jelaskan yang dimaksud dengan Network Layer
2. Sebutkan proses-proses dasar pada network layer
3. Jelaskan yang dimaksud dengan enkapsulasi IP
4. Jelaskan yang dimaksud dengan IP Connectionless / IP tanpa koneksi
5. Sebutkan header yang ada pada IPv4
6. Sebutkan keterbatasan IPv4
7. Sebutkan kelebihan IPv6 dibandingkan dengan IPv4
8. Jelaskan perbedaan antara header IPv4 dengan header IPv6
9. Jelaskan yang dimaksud dengan Gateway default
10. Jelaskan apa itu Router dan fungsinya
11. Jelaskan cara proses bootup router
12. Jelaskan cara konfigurasi sebuah router

BAB 7 IP ADDRESSING

7.1 PENGANTAR

Addressing adalah fungsi penting dari protokol lapisan jaringan. Pengalamatan memungkinkan komunikasi data antar host, terlepas dari apakah host berada pada jaringan yang sama, atau pada jaringan yang berbeda. Baik Protokol Internet versi 4 (IPv4) dan Protokol Internet versi 6 (IPv6) memberikan pengalamatan hirarkis untuk paket yang membawa data.

Merancang, menerapkan dan mengelola rencana pengalamatan IP yang efektif memastikan bahwa jaringan dapat beroperasi secara efektif dan efisien.

Bab ini membahas secara rinci struktur alamat IP dan aplikasinya pada konstruksi dan pengujian jaringan dan subnetwork IP.

7.2 IPv4 NETWORK ADDRESSES

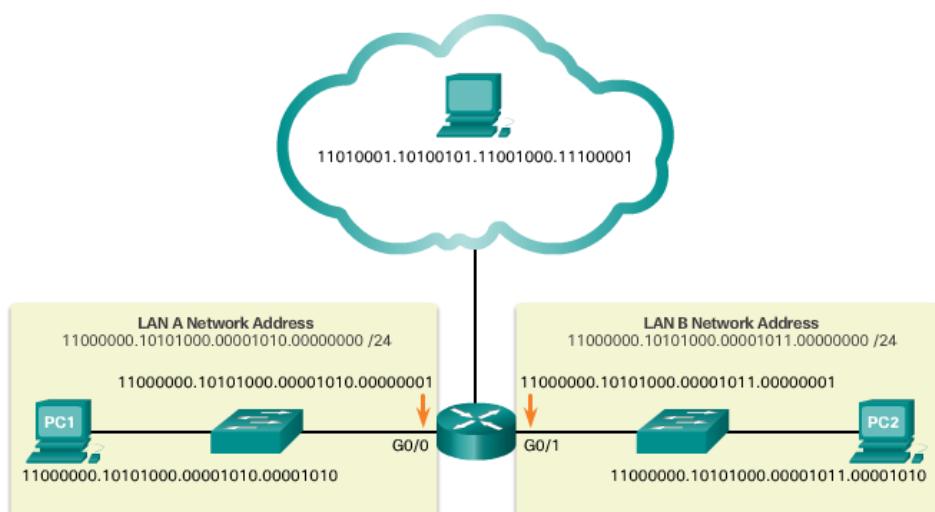
- ❖ **BINARY & DESIMAL CONVERSION**
- **IPV4 ADDRESSES**

Biner adalah sistem penomoran yang terdiri dari angka 0 dan 1 yang disebut bit. Sebaliknya, sistem penomoran desimal terdiri dari 10 digit yang terdiri dari angka 0 - 9.

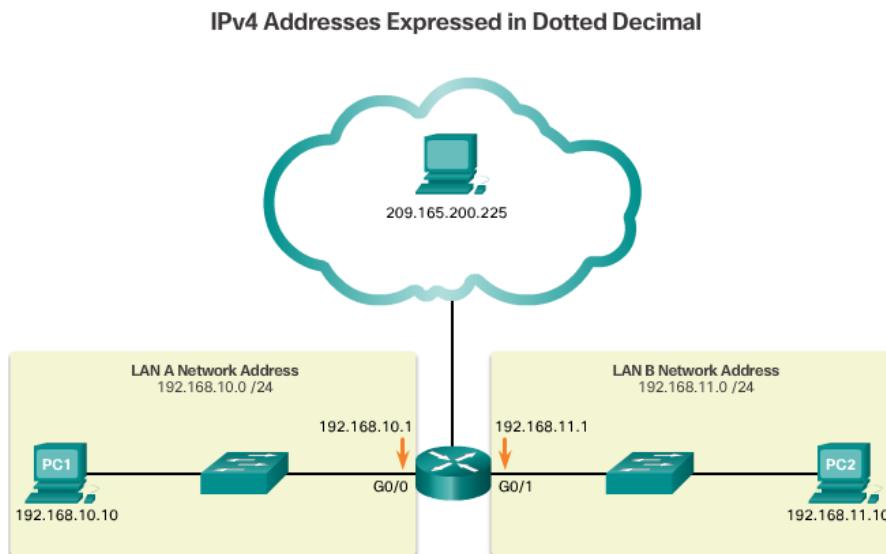
Biner penting bagi kita untuk mengerti karena host, server, dan perangkat jaringan menggunakan pengalamatan biner. Secara khusus, mereka menggunakan alamat IPv4 biner, seperti yang ditunjukkan pada Gambar 1, untuk mengidentifikasi satu sama lain.

Setiap alamat terdiri dari string 32 bit, dibagi menjadi empat bagian yang disebut oktet. Setiap oktet berisi 8 bit (atau 1 byte) yang dipisahkan dengan titik. Sebagai contoh, PC1 pada gambar tersebut diberi alamat IPv4 11000000.10101000.00001010.00001010. Alamat gateway defaultnya adalah antarmuka R1 Gigabit Ethernet 11000000.10101000.00001010.00000001.

IPv4 Addresses Expressed in Binary



Bekerja dengan bilangan biner bisa jadi tantangan. Untuk kemudahan penggunaan oleh orang, alamat IPv4 biasanya dinyatakan dalam notasi desimal bertitik seperti pada Gambar dibawah. PC1 diberi alamat IPv4 192.168.10.10, dan alamat gateway defaultnya adalah 192.168.10.1.



Gambar selanjutnya membandingkan alamat desimal bertitik dan alamat biner 32-bit PC1. Untuk pemahaman yang solid tentang pengalaman jaringan, perlu untuk mengetahui pengalaman biner dan mendapatkan keterampilan praktis untuk mengubah antara alamat IPv4 desimal biner dan titik-titik.

Bagian ini akan membahas bagaimana mengkonversi antara basis dua dan basis 10 sistem penomoran

Contrasting PC1 IPv4 Dotted Decimal and Binary Address

192	.	168	.	10	.	10
11000000		10101000		00001010		00001010

• POSITIONAL NOTATION

Belajar mengkonversi biner ke desimal memerlukan pemahaman tentang notasi posisional. Notasi posisi berarti bahwa digit mewakili nilai yang berbeda tergantung pada "posisi" digit yang menempati urutan nomor. Anda sudah tahu sistem penomoran yang paling umum, sistem notasi desimal (base 10).

Sistem notasi posisi desimal beroperasi seperti yang dijelaskan pada Gambar dibawah

Decimal Positional Notation

Radix	10	10	10	10
Position in #	3	2	1	0
Calculate	(10^3)	(10^2)	(10^1)	(10^0)
Positional Value	1000	100	10	1

Contoh pada Gambar dibawah mengilustrasikan bagaimana notasi posisional digunakan dengan angka desimal 1234.

Applying the Decimal Positional Notation



1234

	Thousands	Hundreds	Tens	Ones
Positional Value	1000	100	10	1
Decimal Number	1	2	3	4
Calculate	1×1000	2×100	3×10	4×1
Add them up ...	1000	+ 200	+ 30	+ 4
Result	1,234			

Sebaliknya, notasi posisi biner beroperasi seperti yang dijelaskan pada Gambar dibawah.

Binary Positional Notation

Radix	2	2	2	2	2	2	2	2
Position in #	7	6	5	4	3	2	1	0
Calculate	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)
Positional Value	128	64	32	16	8	4	2	1

Contoh pada Gambar dibawah mengilustrasikan bagaimana bilangan biner 11000000 sesuai dengan angka 192. Jika bilangan biner adalah 10101000, maka bilangan desimal yang sesuai adalah 168.

Applying the Binary Positional Notation

The diagram illustrates the conversion of the binary number 11000000 to its decimal equivalent, 192. An orange arrow points from the binary number to the first row of a table. The table has columns for Positional Value (128, 64, 32, 16, 8, 4, 2, 1) and Binary number (1, 1, 0, 0, 0, 0, 0, 0). The 'Calculate' column shows the multiplication of each binary digit by its corresponding positional value: 1 x 128, 1 x 64, 0 x 32, 0 x 16, 0 x 8, 0 x 4, 0 x 2, and 0 x 1. The 'Add them up ...' column shows the sum of these products: 128 + 64 + 0 + 0 + 0 + 0 + 0 + 0, resulting in 192. The 'Result' column simply contains the value 192.

Positional Value	128	64	32	16	8	4	2	1
Binary number	1	1	0	0	0	0	0	0
Calculate	1 x 128	1 x 64	0 x 32	0 x 16	0 x 8	0 x 4	0 x 2	0 x 1
Add them up ...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	192							

- **KONVERSI BINARY KE DECIMAL**

Untuk mengubah alamat IPv4 biner ke desimal desimal bertitik, bagilah alamat IPv4 menjadi empat oktet 8 bit. Selanjutnya menerapkan nilai posisi biner ke bilangan biner oktet pertama dan menghitungnya sesuai.

Sebagai contoh, pertimbangkan bahwa 11000000.10101000.00001011.00001010 adalah alamat IPv4 biner host. Untuk mengubah alamat biner menjadi desimal, mulailah dengan oktet pertama seperti yang ditunjukkan pada Gambar dibawah. Masukkan nomor biner 8 bit di bawah nilai posisi baris 1 dan kemudian hitung untuk menghasilkan bilangan desimal 192. Nomor ini masuk ke oktet pertama. notasi desimal bertitik.

Converting the First Octet to Decimal

The diagram shows the conversion of the first octet of the IPv4 address 11000000.10101000.00001011.00001010 to decimal 192. An orange arrow points from the first octet (11000000) to the first row of a table. The table follows the same structure as the one in the previous diagram, with columns for Positional Value (128, 64, 32, 16, 8, 4, 2, 1) and Binary number (1, 1, 0, 0, 0, 0, 0, 0). The 'Calculate' column shows the multiplication of each binary digit by its corresponding positional value: 1 x 128, 1 x 64, 0 x 32, 0 x 16, 0 x 8, 0 x 4, 0 x 2, and 0 x 1. The 'Add them up ...' column shows the sum of these products: 128 + 64 + 0 + 0 + 0 + 0 + 0 + 0, resulting in 192. The 'Result' column contains the value 192. Below the table, an orange arrow points down to the result 192, which is labeled as Dotted Decimal Notation.

Positional Value	128	64	32	16	8	4	2	1
Binary number	1	1	0	0	0	0	0	0
Calculate	1 x 128	1 x 64	0 x 32	0 x 16	0 x 8	0 x 4	0 x 2	0 x 1
Add them up ...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	192							

Dotted Decimal Notation

Selanjutnya ubah oktet kedua seperti yang ditunjukkan pada Gambar dibawah. Nilai desimal yang dihasilkan adalah 168, dan masuk ke oktet kedua.

11000000.10101000.00001011.00001010

Positional Value	128	64	32	16	8	4	2	1
Binary number	1	0	1	0	1	0	0	0
Calculate	1×128	0×64	1×32	0×16	1×8	0×4	0×2	0×1
Add them up ...	128	+ 0	+ 32	+ 0	+ 8	+ 0	+ 0	+ 0
Result	168							

Dotted Decimal Notation
192.168.11.10

Mengkonversi oktet ketiga seperti yang ditunjukkan pada Gambar dibawah dan oktet keempat seperti yang ditunjukkan pada Gambar selanjutnya yang melengkapi alamat IP dan menghasilkan 192.168.11.10.

11000000.10101000.00001011.00001010

Positional Value	128	64	32	16	8	4	2	1
Binary number	0	0	0	0	1	0	1	1
Calculate	0×128	0×64	0×32	0×16	1×8	0×4	1×2	1×1
Add them up ...	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 1
Result	11							

Dotted Decimal Notation
192.168.11.10

11000000.10101000.00001011.00001010

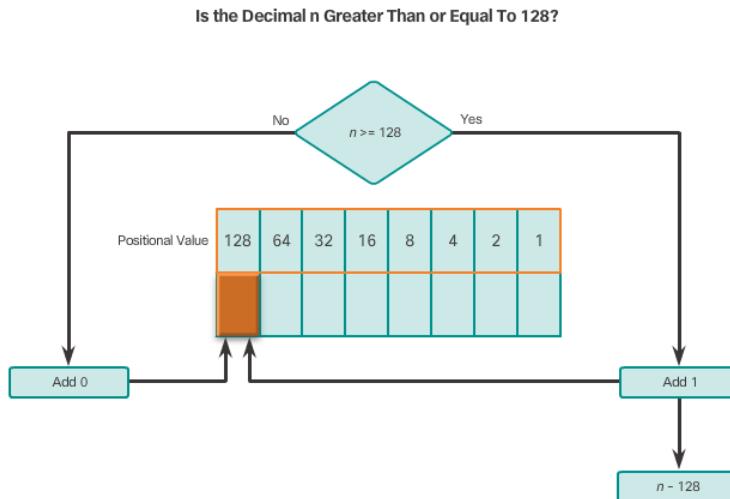
Positional Value	128	64	32	16	8	4	2	1
Binary number	0	0	0	0	1	0	1	0
Calculate	0×128	0×64	0×32	0×16	1×8	0×4	1×2	0×1
Add them up ...	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 0
Result	10							

Dotted Decimal Notation
192.168.11.10

- **KONVERSI DECIMAL KE BINARY**

Hal ini juga diperlukan untuk memahami bagaimana mengubah alamat desimal desimal bertitik menjadi biner. Alat yang berguna adalah tabel nilai posisi biner. Berikut ini menggambarkan bagaimana menggunakan tabel untuk mengubah desimal menjadi biner:

- ✓ Gambar dibawah pertanyaan jika bilangan desimal oktet (n) sama dengan atau lebih besar dari bit paling signifikan (128). Jika tidak, maka masukkan bilangan biner 0 pada nilai posisi 128. Jika iya, tambahkan satu biner 1 pada nilai posisi 128 dan kurangi 128 dari angka desimal.



- ✓ Selanjutnya pertanyaan jika sisanya (n) sama dengan atau lebih besar dari bit paling signifikan berikutnya (64). Jika tidak, maka tambahkan biner 0 pada nilai posisi 64, jika tidak tambahkan biner 1 dan kurangi 64 dari desimal.
- ✓ Selanjutnya jika sisanya (n) sama dengan atau lebih besar dari bit paling signifikan berikutnya (32). Jika tidak, maka tambahkan biner 0 ke dalam 32 nilai posisi, jika tidak tambahkan biner 1 dan kurangi 32 dari desimal.
- ✓ Lakukan sampai selesai terus mengevaluasi desimal sampai semua nilai posisi telah dimasukkan sehingga menghasilkan nilai biner ekuivalen

- **CONTOH KONVERSI DECIMAL KE BINARY**

Untuk membantu memahami prosesnya, pertimbangkan alamat IP 192.168.11.10. Dengan menggunakan proses yang dijelaskan sebelumnya, mulailah dengan tabel nilai posisi biner dan bilangan desimal pertama 192.

192 dibandingkan untuk melihat apakah itu sama dengan atau lebih besar dari bit orde tinggi 128. Karena 192 lebih besar dari 128, tambahkan nilai posisi 1 ke nilai orde tinggi untuk mewakili 128. Kemudian kurangi 128 dari 192 untuk menghasilkan sisa 64. kemudian membandingkan 64 dengan bit orde tinggi berikutnya 64. Karena keduanya sama, tambahkan nilai posisi ke urutan tinggi ke atas. Masukkan biner 0 di sisa nilai posisi seperti yang ditunjukkan pada Gambar 3. Nilai biner oktet pertama adalah 11000000.

Selanjutnya oktet 168. bandingkan 168 bit 128 orde tinggi. Karena 168 lebih besar dari 128, tambahkan 1 ke nilai posisi tingkat tinggi. Kemudian kurangi 128 dari 168 untuk menghasilkan sisa 40. kemudian membandingkan 40 dengan bit orde tinggi berikutnya 64. Karena 40 kurang, tambahkan 0 ke nilai posisi tingkat tinggi berikutnya 64. Bandingkan berikutnya bit orde tinggi 32. Karena 40 lebih besar dari 32, tambahkan nilai ke posisi 1, dan kurangi 32 dari 40 untuk menghasilkan sisa 8. Delapan sesuai dengan nilai posisi tertentu. Oleh karena itu, masukkan angka 0 untuk nilai posisi 16 dan tambahkan 1 ke nilai posisi 8, Tambahkan 0s ke semua nilai posisi yang tersisa. Nilai biner dari oktet ketiga adalah 10101000.

Oktet ketiga adalah 11. Dimungkinkan untuk memotong proses pengurangan dengan bilangan desimal yang lebih mudah atau lebih kecil. Perhatikan bahwa akan cukup mudah untuk menghitung jumlah ini tanpa benar-benar melalui proses pengurangan ($8 + 2 + 1 = 11$). Nilai biner oktet kedua adalah 00001011.

Kuartet keempat adalah 10 ($8 + 2$). Nilai biner oktet keempat adalah 00001010.

Konversi antara biner dan desimal mungkin terasa menantang pada awalnya, namun dengan latihan itu seharusnya menjadi lebih mudah seiring berjalannya waktu.

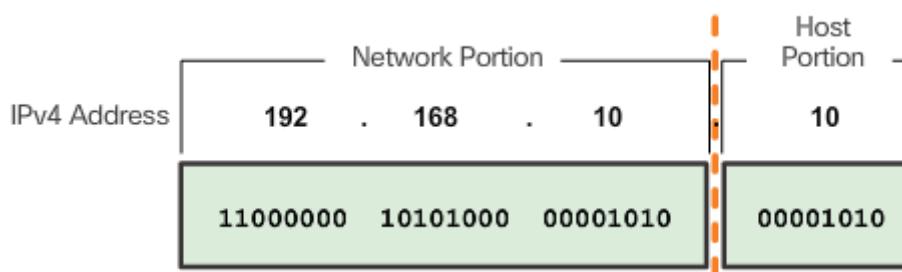
❖ IPv4 STRUKTUR ALAMAT

• NETWORK AND HOST PORTION

Memahami notasi biner penting saat menentukan apakah dua host berada dalam jaringan yang sama. Ingat bahwa alamat IPv4 adalah alamat hirarkis yang terdiri dari bagian jaringan dan bagian host. Saat menentukan bagian jaringan versus bagian host, perlu untuk melihat aliran 32-bit. Dalam aliran 32-bit, sebagian bit mengidentifikasi jaringan, dan sebagian bit mengidentifikasi host seperti yang ditunjukkan pada gambar.

Bit dalam bagian jaringan alamat harus sama untuk semua perangkat yang berada dalam jaringan yang sama. Bit dalam bagian host dari alamat harus unik untuk mengidentifikasi host tertentu dalam jaringan. Jika dua host memiliki pola bit yang sama pada bagian jaringan yang ditentukan dari aliran 32-bit, kedua host tersebut akan berada di jaringan yang sama.

Tapi bagaimana host mengetahui bagian 32 bit yang mengidentifikasi jaringan dan yang mengidentifikasi host? Itulah tugas *subnet mask*.



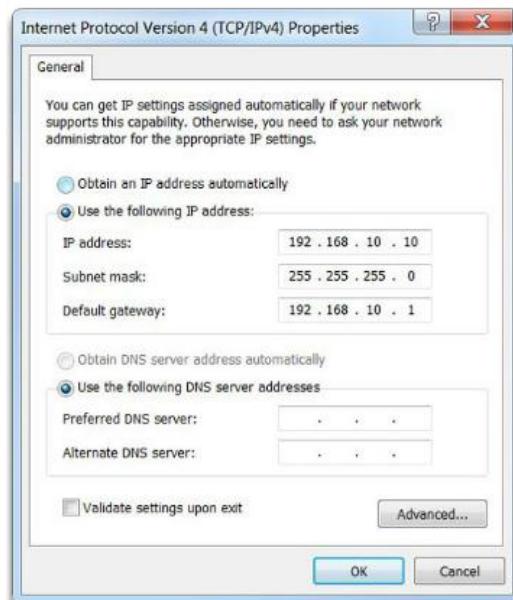
- **SUBNET MASK**

Seperti ditunjukkan pada Gambar dibawah, tiga alamat IPv4 desimal bertitik harus dikonfigurasi saat menetapkan konfigurasi IPv4 menjadi host:

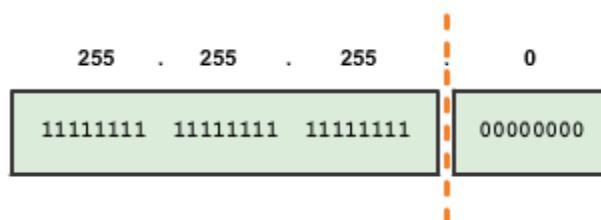
- ✓ **Alamat IPv4** - Alamat IPv4 yang unik dari host
- ✓ **Subnet mask** - Digunakan untuk mengidentifikasi bagian jaringan / host dari alamat IPv4
- ✓ **Default gateway** - Mengidentifikasi gateway lokal (yaitu alamat IPv4 router lokal IPv4) untuk menjangkau jaringan jarak jauh

Bila alamat IPv4 diberikan ke perangkat, subnet mask digunakan untuk menentukan alamat jaringan tempat perangkat berada. Alamat jaringan mewakili semua perangkat pada jaringan yang sama.

IP Configuration on a Host



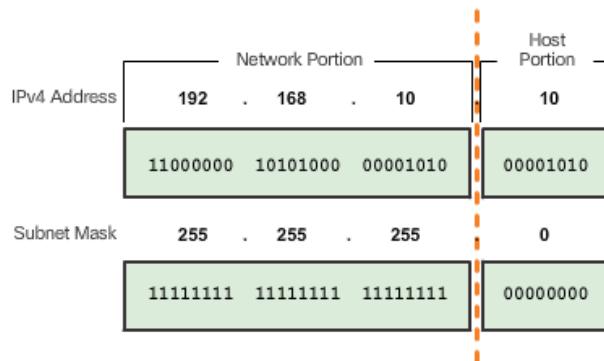
Gambar dibawah menampilkan alamat desimal bertitik dan subnet mask 32 bit. Perhatikan bagaimana subnet mask pada dasarnya adalah urutan 1 bit diikuti dengan urutan 0 bit.



Untuk mengidentifikasi bagian jaringan dan host dari sebuah alamat IPv4, subnet mask dibandingkan dengan bit alamat IPv4 sedikit, dari kiri ke kanan seperti yang ditunjukkan pada Gambar dibawah. 1s di subnet mask mengidentifikasi bagian jaringan sementara 0s mengidentifikasi porsi tuan rumah. Perhatikan bahwa subnet mask sebenarnya tidak mengandung bagian jaringan atau host dari sebuah alamat IPv4, ia hanya memberitahu komputer untuk mencari bagian-bagian ini dalam alamat IPv4 tertentu.

Proses aktual yang digunakan untuk mengidentifikasi bagian jaringan dan porsi host disebut **ANDing**.

Comparing the IP address and Subnet Mask

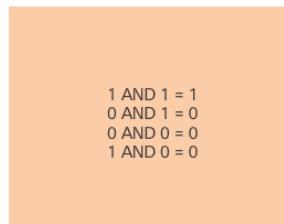


- **ANDing**

ANDING adalah satu dari tiga operasi biner dasar yang digunakan dalam logika digital. Dua lainnya OR dan TIDAK. Sedangkan ketiganya digunakan dalam jaringan data, hanya AND yang digunakan dalam menentukan alamat jaringan. Oleh karena itu, diskusi kita di sini akan terbatas pada operasi logika AND.

Logical AND adalah perbandingan dua bit yang menghasilkan hasil yang ditunjukkan pada Gambar dibawah. Perhatikan bagaimana hanya 1 DAN 1 yang menghasilkan 1.

Logical AND Operation



Untuk mengidentifikasi alamat jaringan host IPv4, alamat IPv4 secara logika ANDED, sedikit demi sedikit, dengan subnet mask. ANDING antara alamat dan subnet mask menghasilkan alamat jaringan.

Untuk menggambarkan bagaimana AND digunakan untuk menemukan alamat jaringan, pertimbangkan host dengan alamat IPv4 192.168.10.10 dan subnet mask 255.255.255.0. Gambar dibawah menampilkan host alamat IPv4 dan alamat biner yang dikonversi.

Alamat biner subnet mask host ditambahkan. Bagian yang disorot kuning mengidentifikasi bit AND yang menghasilkan biner 1 pada baris AND Results. Semua perbandingan bit lainnya

menghasilkan bilangan biner Os. Perhatikan bagaimana oktet terakhir tidak lagi memiliki biner 1 bit.

Akhirnya, alamat jaringan yang dihasilkan 192.168.10.0 255.255.255.0. Oleh karena itu, host 192.168.10.10 ada di jaringan 192.168.10.0 255.255.255.0

Resulting Network Address

IP address	192	.	168	.	10	.	10
Binary	11000000	10101000	00001010		00001010		
Subnet mask	255	.	255	.	255	.	0
	11111111	11111111	11111111		00000000		
AND Results	11000000	10101000	00001010		00000000		
Network Address	192	.	168	.	10	.	0

- **PANJANG PREFIX**

Mengekspresikan alamat jaringan dan alamat host dengan alamat subnet desimal bertitik desimal bisa menjadi tidak praktis. Untungnya, ada alternatif metode *shorthand* untuk mengidentifikasi subnet mask yang disebut ***prefix length***.

Secara khusus, *prefix length* adalah jumlah bit yang diset ke 1 di subnet mask. Hal ini ditulis dalam "notasi slash", yang merupakan "/" diikuti oleh jumlah bit yang diset ke 1. Oleh karena itu, hitung jumlah bit pada subnet mask dan tambahkan dengan slash.

Misalnya, lihat tabel pada gambar. Kolom pertama mencantumkan berbagai subnet mask yang bisa digunakan dengan alamat host. Kolom kedua menampilkan alamat binari 32-bit yang dikonversi. Kolom terakhir menampilkan *prefix length* yang dihasilkan.

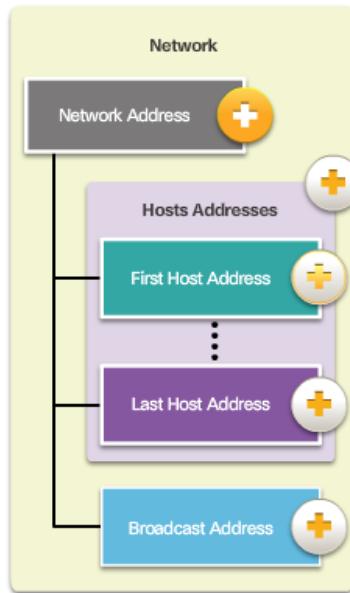
Menggunakan berbagai jenis *prefix length* akan dibahas nanti. Untuk saat ini, fokusnya adalah subnet mask / 24 (yaitu 255.255.255.0).

Comparing the Subnet Mask and Prefix Length

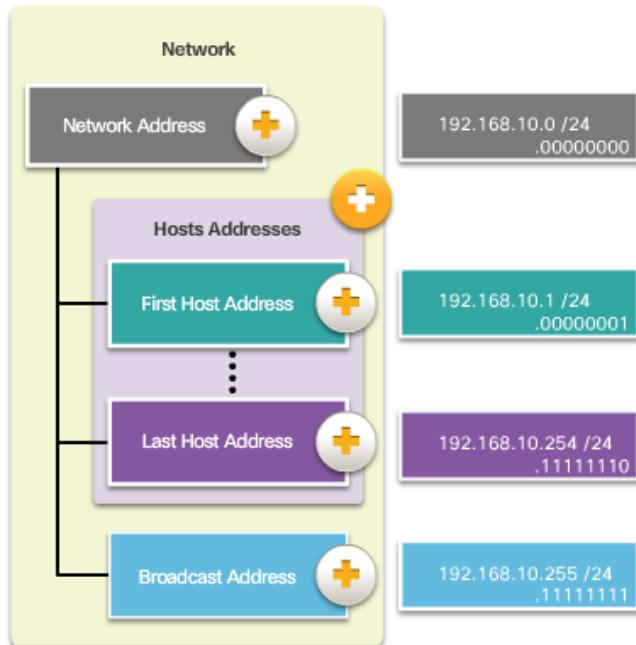
Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	1111111.0000000.0000000.0000000	/8
255.255.0.0	1111111.1111111.0000000.0000000	/16
255.255.255.0	1111111.1111111.1111111.0000000	/24
255.255.255.128	1111111.1111111.1111111.1000000	/25
255.255.255.192	1111111.1111111.1111111.1100000	/26
255.255.255.224	1111111.1111111.1111111.1110000	/27
255.255.255.240	1111111.1111111.1111111.1111000	/28
255.255.255.248	1111111.1111111.1111111.1111100	/29
255.255.255.252	1111111.1111111.1111111.1111100	/30

- **NETWORK, HOST AND BROADCAST ADDRESSES**

Setiap alamat jaringan berisi (atau mengidentifikasi) alamat host dan alamat broadcast.



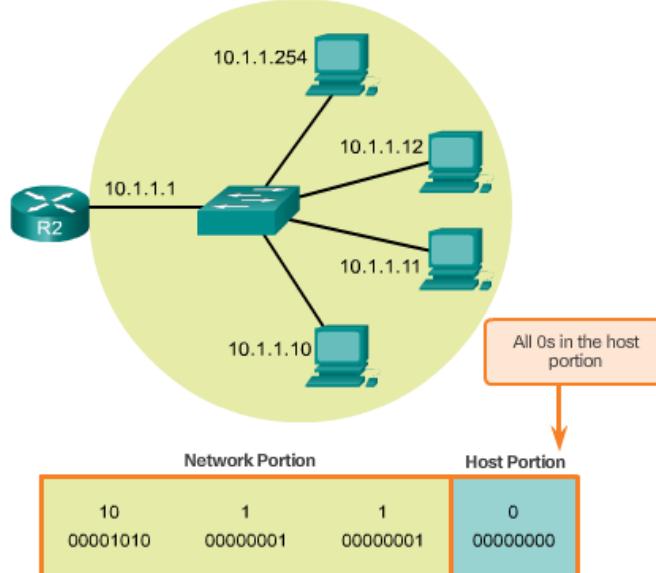
Gambar dibawah mencantumkan dan menjelaskan alamat spesifik di dalam jaringan 192.168.10.0 / 24.



Untuk contoh lain, Pada gambar selanjutnya, perhatikan bagaimana bagian jaringan dari alamat tetap sama sementara porsi host berubah:

Gambar dibawah menampilkan alamat jaringan 10.1.1.0 / 24. Bit host semuanya 0s.

Network Address



Alamat IPv4 dari host 10.1.1.10. Bit host adalah campuran dari 0s dan 1s.

Network Portion	Host Portion
10 00001010	10 00001010

alamat host pertama IPv4 10.1.1.1. Bit host semua 0s dengan 1. Perhatikan bahwa router tersebut ditugaskan ke antarmuka router, dan oleh karena itu, akan menjadi *default gateway* untuk semua host pada jaringan tersebut.

Network Portion	Host Portion
10 00001010	1 00000001

alamat host terakhir IPv4 10.1.1.254. Bit host semua 1s dan 0

Network Portion	Host Portion
10 00001010	254 11111110

alamat broadcast 10.1.1.255. Bit host semuanya 1s

Network Portion	Host Portion
10 00001010	255 11111111

Konsep yang dibahas dalam topik ini merupakan dasar untuk memahami pengalamanan IPv4. Pastikan Anda memahami bagaimana alamat jaringan mengidentifikasi bagian jaringan dan bagian host menggunakan subnet mask atau prefix dan operasi ANDING. Juga perhatikan berbagai jenis alamat jaringan dalam suatu jaringan.

❖ IPv4 UNICAST, BROADCAST, AND MULTICAST

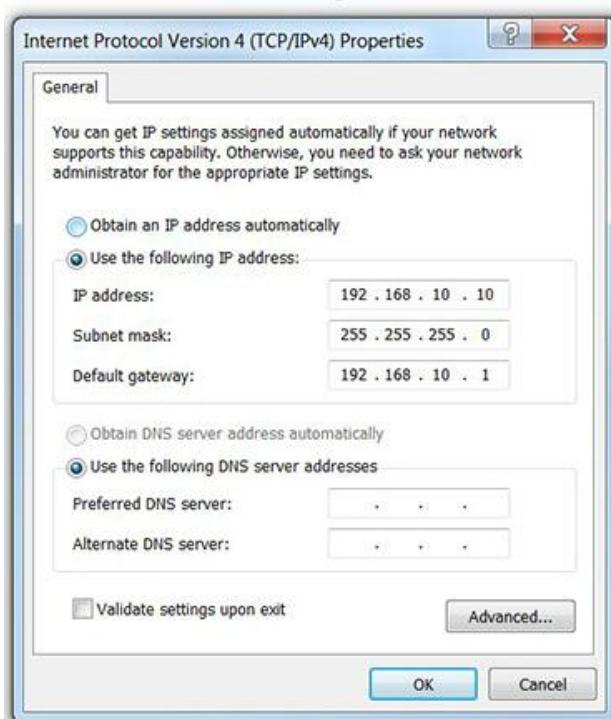
• STATISTIC IPV4 ADDRESS ASSIGNMENT TO A HOST

Perangkat bisa diberi alamat IP baik statis maupun dinamis.

Di jaringan, beberapa perangkat memerlukan alamat IP tetap. Misalnya, printer, server, dan perangkat jaringan membutuhkan alamat IP yang tidak berubah. Untuk alasan ini, perangkat ini biasanya diberi alamat IP statis.

Host juga dapat dikonfigurasi dengan alamat IPv4 statis seperti ditunjukkan pada gambar. Menugaskan host alamat IP statis dapat diterima di jaringan kecil. Namun, akan memakan waktu untuk memasukkan alamat statis pada setiap host dalam jaringan besar. Penting untuk menyimpan daftar alamat IP statis yang akurat yang ditetapkan ke masing-masing perangkat.

Static Assignment

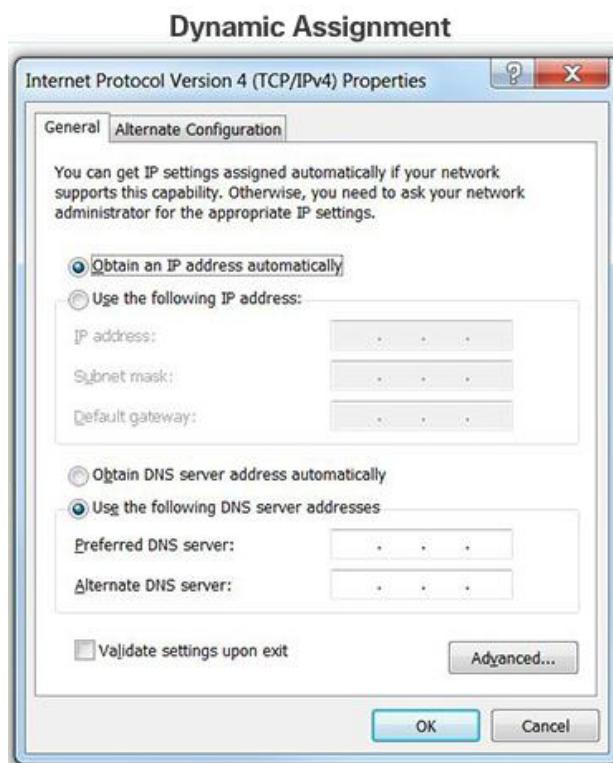


- **DYNAMIC IPV4 ADDRESS ASSIGNMENT TO A HOST**

Di sebagian besar jaringan data, jumlah host terbesar mencakup PC, tablet, smartphone, printer, dan telepon IP. Hal ini juga sering terjadi dimana populasi pengguna dan perangkat mereka sering berubah. Ini tidak praktis untuk menetapkan alamat IPv4 secara statis untuk setiap perangkat. Oleh karena itu, perangkat ini diberi alamat IPv4 secara dinamis menggunakan *Dynamic Host Configuration Protocol* (DHCP).

Seperti ditunjukkan pada gambar, host dapat memperoleh informasi pengalaman IP secara otomatis. Host adalah klien DHCP dan meminta informasi alamat IP dari server DHCP. Server DHCP menyediakan alamat IP, subnet mask, gateway default, dan informasi konfigurasi lainnya.

DHCP umumnya metode yang disukai untuk menetapkan alamat IPv4 ke host pada jaringan besar. Manfaat tambahan dari DHCP adalah alamat tidak ditugaskan secara permanen ke host tapi hanya "disewakan" untuk jangka waktu tertentu. Jika host dimatikan atau diambil dari jaringan, alamat dikembalikan ke kolam renang untuk digunakan kembali. Fitur ini sangat membantu bagi pengguna ponsel yang datang dan pergi pada jaringan.

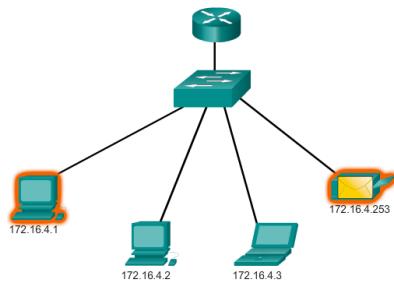


- **KOMUNIKASI IPV4**

Host yang berhasil terhubung ke jaringan dapat berkomunikasi dengan perangkat lain dengan salah satu dari tiga cara berikut:

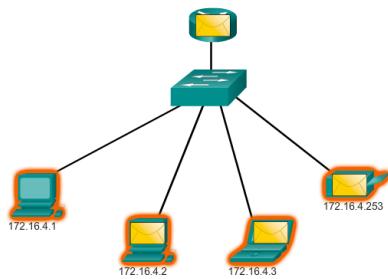
- ✓ **Unicast** - Proses pengiriman paket dari satu host ke host individu

Unicast Communication



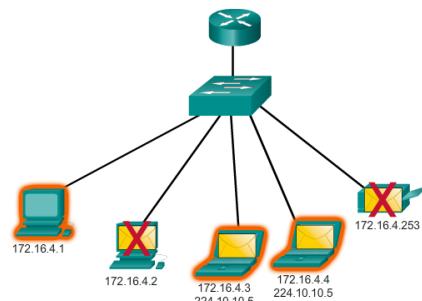
- ✓ **Broadcast** - Proses pengiriman paket dari satu host ke semua host dalam jaringan

Broadcast Communication



- ✓ **Multicast** - Proses pengiriman paket dari satu host ke host host yang dipilih, mungkin di jaringan yang berbeda

Multicast Communication



Ketiga jenis komunikasi ini digunakan untuk tujuan yang berbeda dalam jaringan data. Dalam ketiga kasus tersebut, alamat IPv4 dari host asal ditempatkan di header paket sebagai alamat sumber.

- **UNICAST TRANSMISSION**

Komunikasi Unicast digunakan untuk komunikasi host-to-host yang normal baik pada client / server dan jaringan peer-to-peer. Paket Unicast menggunakan alamat perangkat tujuan sebagai alamat tujuan dan bisa diarahkan melalui sebuah internetwork.

Dalam jaringan IPv4, alamat unicast yang dipraktikkan ke perangkat akhir disebut sebagai alamat host. Untuk komunikasi unicast, alamat yang ditugaskan ke dua perangkat akhir digunakan sebagai alamat sumber dan alamat tujuan IPv4. Selama proses enkapsulasi, host sumber menggunakan alamat IPv4 sebagai alamat sumber dan alamat IPv4 dari host tujuan sebagai alamat tujuan. Terlepas dari apakah tujuan menentukan paket sebagai unicast, broadcast atau multicast; alamat sumber dari setiap paket selalu merupakan alamat unicast dari host asal.

Catatan: Dalam bab ini, semua komunikasi antar perangkat bersifat unicast kecuali jika disebutkan lain.

Alamat host unicast IPv4 berada pada kisaran alamat 0.0.0.0 sampai 223.255.255.255. Namun, dalam rentang ini banyak alamat yang dipesan untuk tujuan khusus. Alamat tujuan khusus ini akan dibahas nanti di bab ini.

- **BROADCAST TRANSMISSION**

Lalu lintas *Broadcast* digunakan untuk mengirim paket ke semua host di jaringan menggunakan alamat broadcast untuk jaringan. Dengan siaran, paket berisi alamat IPv4 tujuan dengan semua yang (1s) di bagian host. Ini berarti bahwa semua host di jaringan lokal (broadcast domain) akan menerima dan melihat paketnya. Banyak protokol jaringan, seperti DHCP, menggunakan *broadcast*. Ketika sebuah host menerima sebuah paket yang dikirim ke alamat *broadcast* jaringan, host memproses paket seperti paket yang ditujukan ke alamat unicast-nya.

Broadcast dapat diarahkan atau dibatasi. *broadcast* terarah dikirim ke semua host di jaringan tertentu. Misalnya, host pada jaringan 172.16.4.0/24 mengirimkan sebuah paket ke 172.16.4.255. Siaran terbatas dikirim ke 255.255.255.255. Secara default, router tidak meneruskan *broadcast*.

Sebagai contoh, host dalam jaringan 172.16.4.0/24 akan *broadcast* ke semua host di jaringannya dengan menggunakan paket dengan alamat tujuan 255.255.255.255.

Ketika sebuah paket *dibroadcast*, ia menggunakan sumber daya pada jaringan dan menyebabkan setiap host penerima di jaringan memproses paket. Oleh karena itu, lalu lintas siaran harus dibatasi sehingga tidak mempengaruhi kinerja jaringan atau perangkat secara negatif. Karena router memisahkan domain siaran, jaringan yang membaginya dapat meningkatkan kinerja jaringan dengan menghilangkan lalu lintas *broadcast* yang berlebihan.

- **MULTICAST TRANSMISSION**

Transmisi multicast mengurangi lalu lintas dengan mengizinkan host mengirim satu paket ke satu set host yang dipilih yang berlangganan ke grup multicast.

IPv4 telah memesan 224.0.0.0 sampai 239.255.255.255 alamat sebagai rentang *multicast*. Alamat *multicast* IPv4 224.0.0.0 sampai 224.0.0.255 dicadangkan untuk multicasting hanya di jaringan lokal. Alamat ini akan digunakan untuk kelompok *multicast* di jaringan lokal. Router yang terhubung ke jaringan lokal mengetahui bahwa paket-paket ini ditujukan ke grup *multicast* jaringan lokal dan tidak akan meneruskannya lebih jauh. Penggunaan alamat *multicast* jaringan lokal yang dipesan secara umum ada pada protokol routing yang menggunakan transmisi *multicast* untuk bertukar informasi routing. Misalnya, 224.0.0.9 adalah alamat *multicast* yang digunakan oleh *Routing Information Protocol* (RIP) versi 2 untuk berkomunikasi dengan router RIPv2 lainnya.

Host yang menerima data multicast tertentu disebut *multicast clients*. Klien *multicast* menggunakan layanan yang diminta oleh program klien untuk berlangganan ke grup *multicast*.

Setiap kelompok *multicast* diwakili oleh satu alamat tujuan *multicast* IPv4 tunggal. Ketika host IPv4 berlangganan ke grup *multicast*, host memproses paket yang ditujukan ke alamat *multicast* ini, dan paket yang ditujukan ke alamat *unicast* yang dialokasikan secara unik.

❖ TIPE PENGALAMATAN IPv4

- **PUBLIC AND PRIVATE ADDRESSES**

Public IPv4 addresses adalah alamat yang dialihkan secara global antara router ISP (Internet Service Provider). Namun, tidak semua alamat IPv4 yang ada bisa digunakan di Internet. Ada blok alamat yang disebut alamat pribadi yang digunakan oleh sebagian besar organisasi untuk menetapkan alamat IPv4 ke host internal.

Pada pertengahan 1990-an alamat IPv4 pribadi diperkenalkan karena penipisan ruang alamat IPv4. Alamat IPv4 pribadi tidak unik dan dapat digunakan oleh jaringan internal.

Secara khusus, blok alamat pribadi adalah:

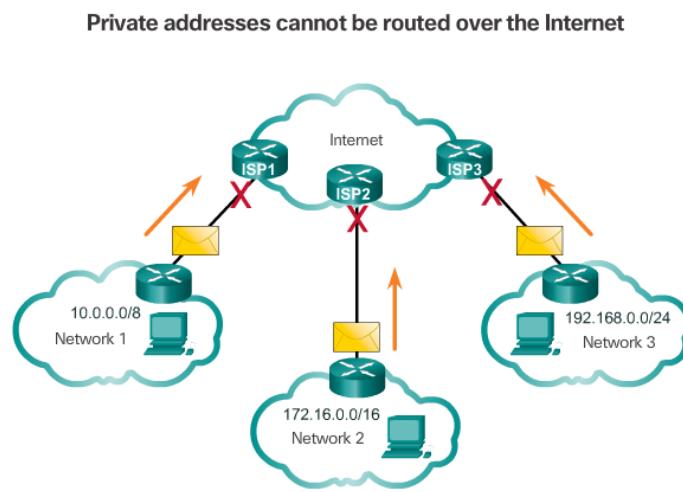
- ✓ 10.0.0 / 8 atau 10.0.0.0 sampai 10.255.255.255
- ✓ 172.16.0.0 / 12 atau 172.16.0.0 sampai 172.31.255.255
- ✓ 192.168.0.0 / 16 atau 192.168.0.0 sampai 192.168.255.255

Penting untuk diketahui bahwa alamat di dalam blok alamat ini tidak diperbolehkan di Internet dan harus disaring (dibuang) oleh router internet. Misalnya, pada gambar, pengguna di jaringan 1, 2, atau 3 mengirim paket ke tujuan terpencil. Router Internet Service Provider (ISP) akan melihat bahwa sumber alamat IPv4 dalam paket berasal dari alamat pribadi dan karena itu, akan membuang paketnya.

Catatan: Alamat pribadi didefinisikan dalam RFC 1918.

Sebagian besar organisasi menggunakan alamat IPv4 pribadi untuk host internal mereka. Namun, alamat RFC 1918 ini tidak routable di Internet dan harus diterjemahkan ke alamat IPv4 publik. Network Address Translation (NAT) digunakan untuk menerjemahkan antara IPv4 pribadi dan alamat IPv4 publik. Hal ini biasanya dilakukan pada router yang menghubungkan jaringan internal dengan jaringan ISP.

Home router memberikan kemampuan yang sama. Misalnya, sebagian besar router rumah menetapkan alamat IPv4 ke host kabel dan nirkabel mereka dari alamat pribadi 192.168.1.0 / 24. Antarmuka router rumah yang terhubung ke jaringan penyedia layanan Internet (ISP) diberi alamat IPv4 publik untuk digunakan di Internet.



- **SPESIAL USER IPV4 ADDRESSES**

Ada alamat tertentu seperti alamat jaringan dan alamat broadcast yang tidak bisa ditugaskan ke host. Ada juga alamat khusus yang dapat ditugaskan ke host, namun dengan batasan bagaimana host tersebut dapat berinteraksi dalam jaringan.

- ✓ Loopback addresses (127.0.0.0 /8 or 127.0.0.1 to 127.255.255.254) - Lebih umum diidentifikasi sebagai hanya 127.0.0.1, ini adalah alamat khusus yang digunakan oleh host untuk mengarahkan lalu lintas ke dirinya sendiri. Misalnya, dapat digunakan pada host untuk menguji apakah konfigurasi TCP / IP beroperasi, seperti ditunjukkan pada gambar. Perhatikan bagaimana alamat loopback 127.0.0.1 menjawab perintah ping. Perhatikan juga bagaimana setiap alamat dalam blok ini akan diulang kembali ke host lokal, seperti ditunjukkan pada ping kedua pada gambar.
- ✓ Link-Local addresses (169.254.0.0 /16 or 169.254.0.1 to 169.254.255.254) - Lebih umum dikenal dengan alamat Automatic Private IP Addressing (APIPA), mereka digunakan oleh klien Windows DCHP untuk mengkonfigurasi sendiri jika Tidak ada server DHCP yang tersedia. Ada koneksi peer-to-peer.
- ✓ TEST-NET addresses (192.0.2.0/24 or 192.0.2.0 to 192.0.2.255) - Alamat ini disisihkan untuk tujuan belajar mengajar dan dapat digunakan dalam contoh dokumentasi dan jaringan

Pinging the Loopback Interface

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad> ping 127.1.1.1

Pinging 127.1.1.1 with 32 bytes of data:
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad>
```

• PENANGANAN CLASSICAL LEGACY

Pada tahun 1981, alamat IPv4 Internet ditugaskan menggunakan pengalamatan kelas seperti yang didefinisikan dalam RFC 790, Assigned Numbers. RFC membagi rentang unicast menjadi kelas tertentu yang disebut:

- ✓ Kelas A (0.0.0.0/8 sampai 127.0.0.0/8) - Dirancang untuk mendukung jaringan yang sangat besar dengan lebih dari 16 juta alamat host. Ini menggunakan prefix tetap / 8 dengan oktet pertama untuk menunjukkan alamat jaringan dan tiga oktet sisanya untuk alamat host. Semua alamat kelas A mensyaratkan bahwa bit paling signifikan dari oktet orde tinggi menjadi nol yang menciptakan total 128 jaringan kelas A yang mungkin.

Class A Specifics	
Address block	0.0.0.0 – 127.0.0.0*
Default Subnet Mask	/8 (255.0.0.0)
Maximum Number of Networks	128
Number of Host per Network	16,777,214
High order bit	0xxxxxx.-----

* 0.0.0.0 and 127.0.0.0 are reserved and cannot be assigned

- ✓ Kelas B (128.0.0.0 / 16 - 191.255.0.0 / 16) - Dirancang untuk mendukung kebutuhan jaringan berukuran sedang hingga besar dengan sampai sekitar 65.000 alamat host. Ini menggunakan prefix tetap / 16 dengan dua oktet orde tinggi untuk menunjukkan alamat jaringan dan dua oktet sisanya untuk alamat host. Dua bit terpenting dari oktet orde tinggi harus 10 menciptakan lebih dari 16.000 jaringan.

Class B Specifics	
Address block	128.0.0.0 - 191.255.0.0
Default Subnet Mask	/16 (255.255.0.0)
Maximum Number of Networks	16,384
Number of Host per Network	65,534
High order bit	10xxxxxx._____._____._____

- ✓ Class C (192.0.0.0 / 24 - 223.255.255.0 / 24) - Dirancang untuk mendukung jaringan kecil dengan jumlah maksimum 254 host. Ini menggunakan prefix tetap / 24 dengan tiga oktet pertama untuk menunjukkan jaringan dan oktet yang tersisa untuk alamat host. Tiga bit paling penting dari oktet orde tinggi harus menghasilkan lebih dari 2 juta jaringan yang mungkin.

Class C Specifics	
Address block	192.0.0.0 - 223.255.255.0
Default Subnet Mask	/24 (255.255.255.0)
Maximum Number of Networks	2,097,152
Number of Host per Network	254
High order bit	110xxxxx._____._____._____

Catatan: Ada juga blok multicast Kelas D yang terdiri dari 224.0.0.0 sampai 239.0.0.0 dan blok alamat eksperimen Kelas E yang terdiri dari 240.0.0.0 - 255.0.0.0.

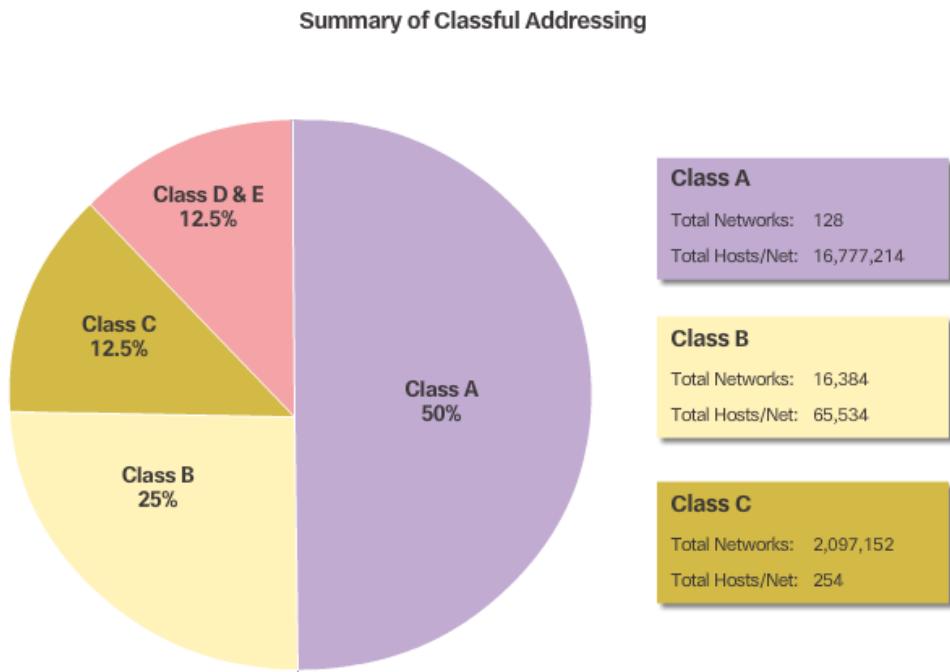
- **PENGALAMATAN TANPA KELAS**

Sistem classful mengalokasikan 50% alamat IPv4 yang tersedia ke 128 jaringan Kelas A, 25% alamat ke Kelas B dan kemudian Kelas C membagikan 25% sisanya dengan Kelas D dan E. Masalahnya adalah ini menyia-nyiakan banyak alamat dan kehabisan ketersediaan alamat IPv4. Tidak semua persyaratan organisasi sesuai dengan salah satu dari ketiga kelas ini. Misalnya, perusahaan yang memiliki jaringan dengan 260 host harus diberi alamat kelas B dengan lebih dari 65.000 alamat yang menghabiskan 64.740 alamat.

Pengalamatan kelas ditinggalkan pada akhir tahun 1990an untuk sistem pengalamatan kelas yang lebih baru dan sekarang. Namun, masih ada sisa-sisa yang berkelas di jaringan saat ini. Misalnya, ketika Anda menetapkan alamat IPv4 ke komputer, sistem operasi memeriksa alamat yang ditugaskan untuk menentukan apakah alamat ini adalah kelas A, kelas B, atau kelas C. Sistem operasi kemudian mengasumsikan prefix yang digunakan oleh kelas tersebut dan membuat subnet mask default.

Sistem yang digunakan saat ini disebut sebagai pengalamatan tanpa classless. Nama resmi adalah Classless Inter-Domain Routing (CIDR, diucapkan "sariawan"). Pada tahun 1993, IETF menciptakan seperangkat standar baru yang memungkinkan penyedia layanan mengalokasikan alamat IPv4 pada setiap batas bit alamat (panjang prefix), bukan hanya oleh alamat kelas A, B, atau C. Ini untuk membantu menunda penipisan dan akhirnya habisnya alamat IPv4.

IETF tahu bahwa CIDR hanyalah solusi sementara dan bahwa sebuah protokol IP baru harus dikembangkan untuk mengakomodasi pertumbuhan pesat jumlah pengguna Internet. Pada tahun 1994, IETF memulai pekerjaannya untuk menemukan penerus IPv4, yang akhirnya menjadi IPv6.



- **ASSIGNMENT OF IP ADDRESSES**

Bagi perusahaan atau organisasi untuk mendukung host jaringan, seperti server web yang dapat diakses dari Internet, organisasi tersebut harus memiliki blok alamat publik yang ditetapkan. Ingat bahwa alamat publik harus unik, dan penggunaan alamat publik ini diatur dan dialokasikan untuk setiap organisasi secara terpisah. Ini berlaku untuk alamat IPv4 dan IPv6.

Alamat IPv4 dan IPv6 dikelola oleh Internet Assigned Numbers Authority (IANA) (<http://www.iana.org>). IANA mengelola dan mengalokasikan blok alamat IP ke Regional Internet Registries (RIR). Klik masing-masing RIR pada gambar untuk melihat informasi lebih lanjut.

RIR bertanggung jawab untuk mengalokasikan alamat IP ke ISP yang pada gilirannya memberikan blok alamat IPv4 kepada organisasi dan ISP yang lebih kecil. Organisasi bisa mendapatkan alamat mereka langsung dari subjek RIR dengan kebijakan RIR itu.

7.3 IPv6 NETWORK ADDRESSES

❖ MASALAH IPV4

• KEBUTUHAN AKAN IPV6

IPv6 dirancang untuk menjadi penerus IPv4. IPv6 memiliki ruang alamat 128-bit yang lebih besar, menyediakan 340 alamat undecillion. (Itu adalah angka 340, diikuti oleh angka nol). Namun, IPv6 lebih dari sekedar alamat yang lebih besar. Ketika IETF memulai pengembangan penerus IPv4, ia menggunakan kesempatan ini untuk memperbaiki keterbatasan IPv4 dan menambahkan tambahan tambahan. Salah satu contohnya adalah Internet Control Message Protocol versi 6 (ICMPv6), yang mencakup resolusi alamat dan konfigurasi otomatis alamat yang tidak ditemukan di ICMP untuk IPv4 (ICMPv4).

Butuh untuk IPv6

Penipisan ruang alamat IPv4 telah menjadi faktor pendorong untuk pindah ke IPv6. Seiring Afrika, Asia dan wilayah lain di dunia menjadi lebih terhubung ke Internet, tidak ada cukup banyak alamat IPv4 untuk mengakomodasi pertumbuhan ini. Seperti ditunjukkan pada gambar, empat dari lima RIR telah kehabisan alamat IPv4.

IPv4 memiliki maksimum teoritis sebesar 4,3 miliar alamat. Alamat pribadi yang dikombinasikan dengan Network Address Translation (NAT) telah berperan penting dalam memperlambat penipisan ruang alamat IPv4. Namun, NAT memecahkan banyak aplikasi dan memiliki keterbatasan yang sangat menghambat komunikasi peer-to-peer.

Internet dari Segalanya

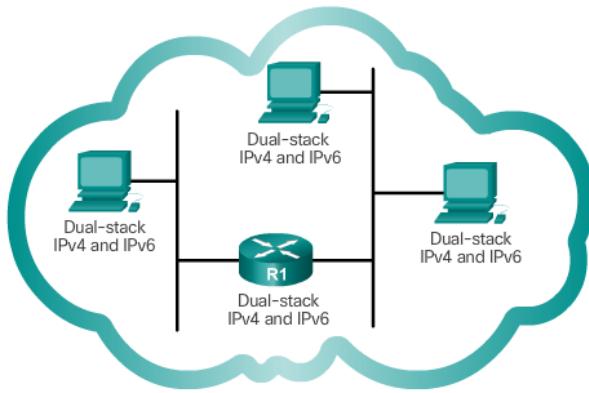
Internet saat ini berbeda secara signifikan dari Internet dalam beberapa dekade terakhir. Internet saat ini lebih dari sekedar email, halaman web, dan transfer file antar komputer. Internet yang berkembang menjadi internet hal. Tidak lagi satu-satunya perangkat yang mengakses internet adalah komputer, tablet, dan smartphone. Perangkat eksternal siap-serba sensor yang dilengkapi sensor, mencakup semua hal mulai dari mobil dan perangkat biomedis, hingga peralatan rumah tangga dan ekosistem alami.

Dengan populasi Internet yang meningkat, ruang alamat IPv4 yang terbatas, masalah dengan NAT dan Internet Segalanya, saatnya telah tiba untuk memulai transisi ke IPv6.

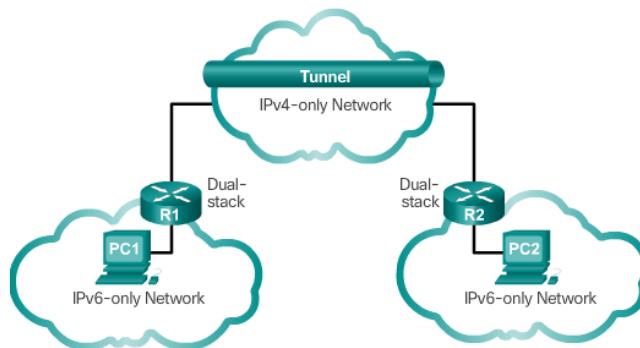
• KOEKSTENSI IPV4 DAN IPV6

Untuk masa yang akan datang, IPv4 dan IPv6 akan hidup berdampingan. Transisi ini diperkirakan akan memakan waktu bertahun-tahun. IETF telah menciptakan berbagai protokol dan alat untuk membantu administrator jaringan memindahkan jaringan mereka ke IPv6. Teknik migrasi dapat dibagi menjadi tiga kategori:

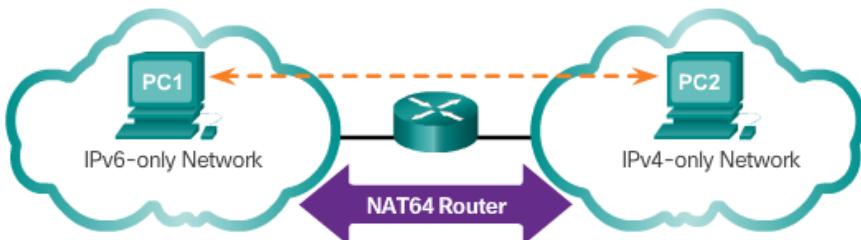
- ✓ **Dual Stack** - Seperti ditunjukkan pada Gambar 1, dual stack memungkinkan IPv4 dan IPv6 untuk hidup berdampingan pada segmen jaringan yang sama. Perangkat dual stack menjalankan kedua tumpukan protokol IPv4 dan IPv6 secara bersamaan.



- ✓ **Tunneling** - tunneling adalah metode untuk mengangkut paket IPv6 melalui jaringan IPv4. Paket IPv6 dienkapsulasi di dalam paket IPv4, mirip dengan jenis data lainnya.



- ✓ **Translation** - Network Address Translation 64 (NAT64) memungkinkan perangkat berkemampuan IPv6 untuk berkomunikasi dengan perangkat berkemampuan IPv4 menggunakan teknik terjemahan yang mirip dengan NAT untuk IPv4. Paket IPv6 diterjemahkan ke paket IPv4 dan sebaliknya.



Catatan: Tunneling dan terjemahan hanya digunakan bila diperlukan. Tujuannya adalah komunikasi native IPv6 dari sumber ke tujuan.

❖ PENGALAMATAN IPv6

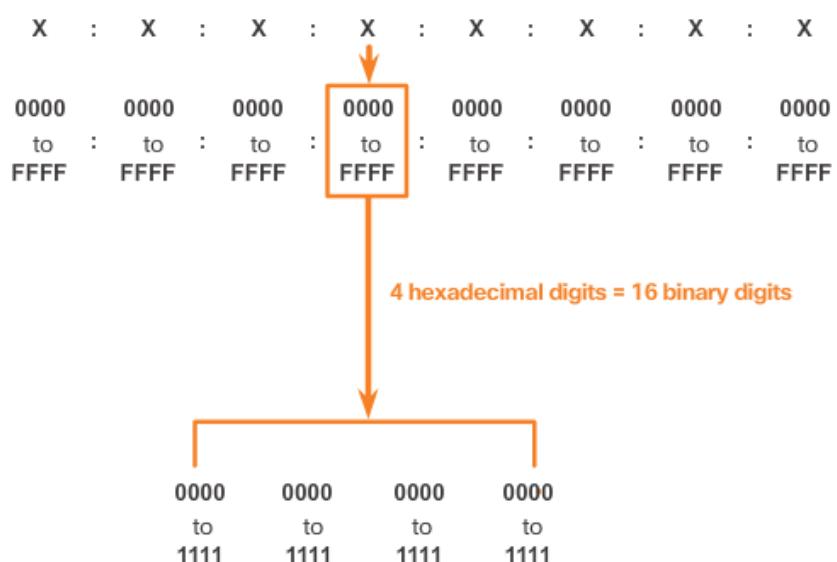
• REPRESENTASI PENGALAMATAN IPV6

Alamat IPv6 berukuran 128 bit dan ditulis sebagai string nilai heksadesimal. Setiap 4 bit diwakili oleh digit heksadesimal tunggal; untuk total 32 nilai heksadesimal. Alamat IPv6 tidak sensitif huruf dan dapat ditulis dengan huruf kecil atau huruf besar.

Preferred Format

Seperti yang ditunjukkan pada Gambar dibawah, format pilihan untuk menulis alamat IPv6 adalah x: x: x: x: x: x, dengan masing-masing "x" yang terdiri dari empat nilai heksadesimal. Bila mengacu pada 8 bit dari alamat IPv4 kita menggunakan istilah oktet. Di IPv6, hextet adalah istilah tidak resmi yang digunakan untuk merujuk ke segmen 16 bit atau empat nilai heksadesimal. Setiap "x" adalah satu hextet tunggal, 16 bit atau empat digit heksadesimal.

Hextets



Preferred Format berarti alamat IPv6 ditulis menggunakan 32 digit heksadesimal. Ini tidak berarti bahwa ini adalah metode ideal untuk mewakili alamat IPv6. Pada halaman berikut, kita akan melihat dua aturan untuk membantu mengurangi jumlah digit yang dibutuhkan untuk mewakili alamat IPv6.

Gambar dibawah adalah tinjauan hubungan antara desimal, biner dan heksadesimal. Gambar adalah contoh alamat IPv6 dalam format pilihan.

Hexadecimal Numbering			Preferred Format Examples												
Decimal and Binary equivalents of 0 to F Hexadecimal															
Decimal	Binary	Hexadecimal													
0	0000	0	2001	:	0DB8	:	0000	:	1111	:	0000	:	0000	:	0200
1	0001	1	2001	:	0DB8	:	0000	:	00A3	:	ABCD	:	0000	:	1234
2	0010	2	2001	:	0DB8	:	000A	:	0001	:	0000	:	0000	:	0100
3	0011	3	2001	:	0DB8	:	AAAA	:	0001	:	0000	:	0000	:	0200
4	0100	4	FE80	:	0000	:	0000	:	0123	:	4567	:	89AB	:	CDEF
5	0101	5	FE80	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
6	0110	6	FF02	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
7	0111	7	FF02	:	0000	:	0000	:	0000	:	0001	:	FF00	:	0200
8	1000	8	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
9	1001	9	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000
10	1010	A	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000
11	1011	B	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000
12	1100	C	0000	:	0000	:	0000	:	0000	:	0001	:	FF00	:	0200
13	1101	D	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000
14	1110	E	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000
15	1111	F	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000

• RULE 1 – OMIT LEADING 0S

Aturan pertama yang membantu mengurangi notasi alamat IPv6 adalah menghilangkan nol Os terdepan di bagian 16 bit atau hextet manapun. Sebagai contoh:

- ✓ 01AB dapat direpresentasikan sebagai 1AB
- ✓ 09F0 dapat direpresentasikan sebagai 9F0
- ✓ 0A00 dapat direpresentasikan sebagai A00
- ✓ 00AB dapat direpresentasikan sebagai AB

Aturan ini hanya berlaku untuk Os terdepan, BUKAN untuk mengikuti Os, jika tidak alamatnya akan ambigu. Misalnya, hextet "ABC" bisa berupa "0ABC" atau "ABC0", tapi ini tidak mewakili nilai yang sama.

Angka 1 sampai 8 menunjukkan beberapa contoh bagaimana menghilangkan Os yang dapat digunakan untuk mengurangi ukuran alamat IPv6. Untuk setiap contoh, format pilihan ditampilkan. Perhatikan bagaimana menghilangkan Os terdepan pada kebanyakan contoh menghasilkan representasi alamat yang lebih kecil.

Preferred	2001:0DB8:0000:1111:0000:0000:0000:0200
No leading 0s	2001: DB8: 0:1111: 0: 0: 0: 200

Preferred	2001:0DB8:0000:A300:ABCD:0000:0000:1234
No leading 0s	2001: DB8: 0:A300:ABCD: 0: 0:1234

Preferred	2001:0DB8:000A:1000:0000:0000:0000:0100
No leading 0s	2001: DB8: A:1000: 0: 0: 0: 100

Preferred	FE80: 0000:0000:0000:0123:4567:89AB:CDEF
No leading 0s	FE80: 0: 0: 0: 123:4567:89AB:CDEF

Preferred	FF02: 0000:0000:0000:0000:0000:0000:0001
No leading 0s	FF02: 0: 0: 0: 0: 0: 0: 1

Preferred	FF02: 0000:0000:0000:0000:0001:FF00:0200
No leading 0s	FF02: 0: 0: 0: 0: 1:FF00: 200

Preferred	0000:0000:0000:0000:0000:0000:0001
No leading 0s	0: 0: 0: 0: 0: 0: 0: 1

- **RULE 2 – OMIT ALL 0 SEGMENTS**

Aturan kedua untuk membantu mengurangi notasi alamat IPv6 adalah bahwa kolon ganda (:) dapat mengganti satu string tunggal dan bersebelahan dari satu atau lebih segmen 16 bit (hextets) yang terdiri dari semua 0s.

Kolom ganda (:) hanya dapat digunakan sekali dalam sebuah alamat, jika tidak, akan ada lebih dari satu alamat yang mungkin dihasilkan. Bila digunakan dengan teknik 0s yang mengabaikan, maka notasi alamat IPv6 seringkali sangat berkurang. Ini biasa dikenal dengan format terkompresi.

Alamat salah:

- ✓ 2001:0DB8 :: ABCD :: 1234

Kemungkinan perluasan alamat terkompresi ambigu:

- ✓ 2001:0DB8 :: ABCD:0000:0000:1234
- ✓ 2001:0DB8 :: ABCD:0000:0000:0000:1234
- ✓ 2001:0DB8:0000:ABCD :: 1234
- ✓ 2001:0DB8:0000:0000:ABCD :: 1234

Gambar dibawah menunjukkan beberapa contoh bagaimana menggunakan kolon ganda (:) dan menghilangkan faktor 0s dapat mengurangi ukuran alamat IPv6.

Preferred	2001: 0 DB8: 0000 :1111: 0000 : 0000 : 0000 :0200
No leading 0s	2001: DB8: 0:1111: 0: 0: 0: 200
Compressed	2001:DB8:0:1111::200

Preferred	2001: 0 DB8: 0000 : 0000 :ABCD: 0000 : 0000 : 0100
No leading 0s	2001: DB8: 0: 0:ABCD: 0: 0: 100
Compressed	2001:DB8::ABCD:0:0:100
or	
Compressed	2001:DB8:0:0:ABCD::100

Only one :: may be used.

Preferred	FE80: 0000 : 0000 : 0000 : 0123 :4567:89AB:CDEF
No leading 0s	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Compressed	FE80::123:4567:89AB:CDEF

Preferred	FF02: 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
No leading 0s	FF02: 0: 0: 0: 0: 0: 0: 0: 1
Compressed	FF02::1

Preferred	FF02: 0000 : 0000 : 0000 : 0000 : 0001 :FF00:0200
No leading 0s	FF02: 0: 0: 0: 0: 1:FF00: 200
Compressed	FF02::1:FF00:200

Preferred	0000:0000:0000:0000:0000:0000:0000:0001
No leading 0s	0: 0: 0: 0: 0: 0: 0: 1
Compressed	::1

Preferred	0000:0000:0000:0000:0000:0000:0000:0000
No leading 0s	0: 0: 0: 0: 0: 0: 0: 0
Compressed	::

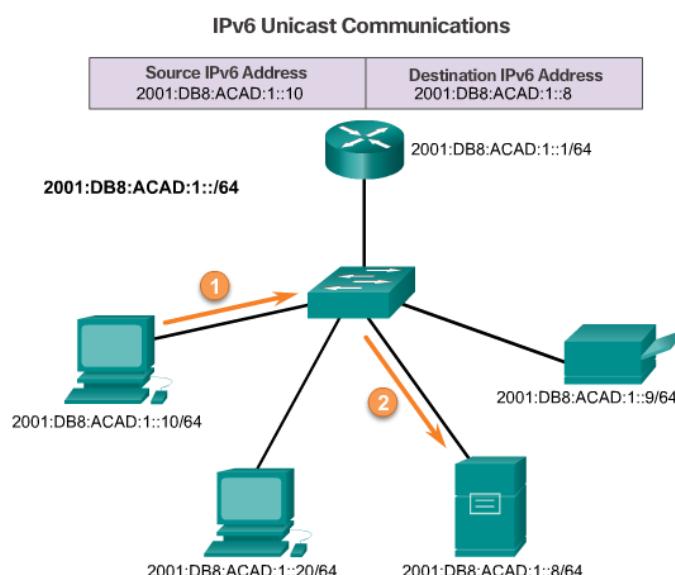
❖ TIPE PENGALAMATAN IPv6

- **TIPE ALAMAT IPV6**

Ada tiga jenis alamat IPv6:

- ✓ **Unicast** - Alamat unicast IPv6 mengidentifikasi secara unik sebuah antarmuka pada perangkat berkemampuan IPv6. Seperti yang ditunjukkan pada gambar, alamat IPv6 sumber harus berupa alamat unicast.
- ✓ **Multicast** - Alamat multicast IPv6 digunakan untuk mengirim satu paket IPv6 ke beberapa tujuan.
- ✓ **Anycast** - Alamat anycast IPv6 adalah alamat unicast IPv6 yang dapat ditugaskan ke beberapa perangkat. Sebuah paket yang dikirim ke alamat anycast diarahkan ke perangkat terdekat yang memiliki alamat itu. Alamat anycast berada di luar cakupan kursus ini.

Tidak seperti IPv4, IPv6 tidak memiliki alamat broadcast. Namun, ada alamat multicast IPv6 all-node yang pada dasarnya memberikan hasil yang sama.

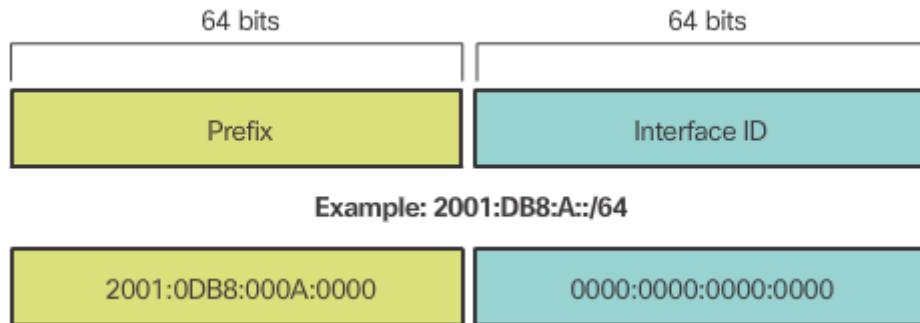


- **PANJANG PREFIX IPV6**

Prefix dari alamat IPv4, dapat diidentifikasi dengan subnet mask bertitik desimal atau panjang prefix (notasi slash). Misalnya, alamat IPv4 192.168.1.10 dengan subnet mask bertitik desimal 255.255.255.0 setara dengan 192.168.1.10/24.

IPv6 menggunakan prefix untuk mewakili bagian prefix dari alamat. IPv6 tidak menggunakan notasi subnet mask bertitik desimal. Prefix digunakan untuk menunjukkan bagian jaringan dari alamat IPv6 menggunakan alamat IPv6 / prefix.

Prefix bisa berkisar antara 0 sampai 128. Prefix IPv6 yang khas untuk LAN dan kebanyakan jenis jaringan lainnya adalah 64. Ini berarti prefix atau bagian jaringan dari alamat itu panjangnya 64 bit, meninggalkan 64 bit lagi untuk ID antarmuka (bagian host) dari alamat.



- **IPv6 UNICAST ADDRESSES**

Alamat unicast IPv6 mengidentifikasi secara unik sebuah antarmuka pada perangkat berkemampuan IPv6. Sebuah paket yang dikirim ke alamat unicast diterima oleh antarmuka yang diberi alamat itu. Serupa dengan IPv4, alamat IPv6 sumber harus berupa alamat unicast. Alamat IPv6 tujuan bisa berupa unicast atau alamat multicast.

Jenis alamat IPv4 IPv6 yang paling umum adalah alamat unicast global (GUA) dan alamat unicast link-local

Unicast global

Alamat unicast global mirip dengan alamat IPv4 publik. Ini adalah alamat routable internet yang unik secara global. Alamat unicast global dapat dikonfigurasi secara statis atau ditugaskan secara dinamis.

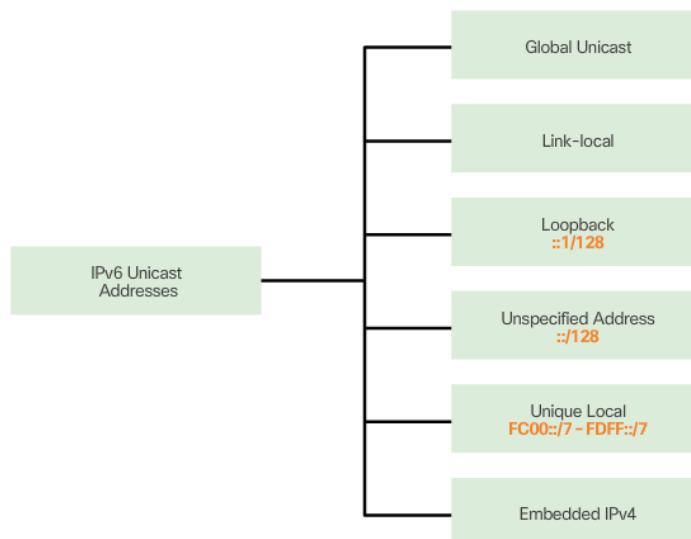
Link-lokal

Alamat link-lokal digunakan untuk berkomunikasi dengan perangkat lain pada link lokal yang sama. Dengan IPv6, istilah link merujuk ke subnet. Tautan-alamat lokal terbatas pada satu tautan. Keunikan mereka hanya bisa dikonfirmasi pada link itu karena tidak routable diluar link. Dengan kata lain, router tidak akan meneruskan paket dengan sumber link-local atau alamat tujuan.

Unik lokal

Jenis alamat unicast lainnya adalah alamat unicast lokal yang unik. Alamat lokal unik IPv6 memiliki kesamaan dengan alamat pribadi RFC 1918 untuk IPv4, namun ada perbedaan yang signifikan. Alamat lokal yang unik digunakan untuk pengalaman lokal di dalam suatu situs atau di antara sejumlah situs yang terbatas. Alamat ini tidak boleh routable di IPv6 global dan tidak boleh diterjemahkan ke alamat IPv6 global. Alamat lokal yang unik ada di kisaran FC00 :: / 7 sampai FDFF :: / 7.

Dengan IPv4, alamat pribadi digabungkan dengan NAT / PAT untuk menyediakan terjemahan antar-pribadi dari alamat private-to-public. Hal ini dilakukan karena terbatasnya ketersediaan ruang alamat IPv4. Banyak situs juga menggunakan sifat pribadi dari alamat RFC 1918 untuk membantu mengamankan atau menyembunyikan jaringan mereka dari risiko keamanan potensial. Namun, ini tidak pernah menjadi tujuan penggunaan teknologi ini, dan IETF selalu merekomendasikan agar situs tersebut melakukan tindakan pengamanan yang tepat di router yang menghadapi Internet mereka. Alamat lokal yang unik dapat digunakan untuk perangkat yang tidak memerlukan atau memiliki akses dari jaringan lain.



- **IPv6 LINK- LOCAL UNICAST ADDRESSES**

Alamat IPv6-local memungkinkan perangkat berkomunikasi dengan perangkat berkemampuan IPv6 lainnya pada link yang sama dan hanya pada link (subnet) tersebut. Paket dengan alamat sumber-tujuan atau alamat tujuan tidak dapat diarahkan melampaui tautan asal paket itu.

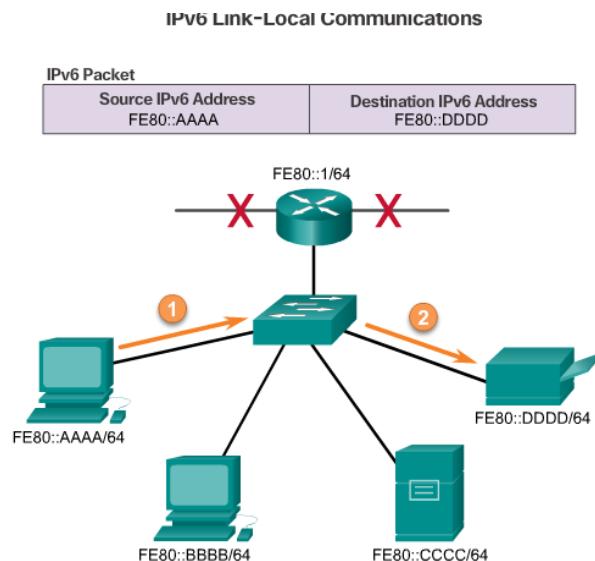
Alamat unicast global bukan keharusan. Namun, setiap antarmuka jaringan yang didukung IPv6 diperlukan untuk memiliki alamat link-lokal.

Jika alamat link-local tidak dikonfigurasi secara manual pada sebuah antarmuka, perangkat akan secara otomatis membuat sendiri tanpa berkomunikasi dengan server DHCP. Host berkemampuan IPv6 membuat alamat link-lokal IPv6 meskipun perangkat belum diberi alamat IPv4 unicast global. Ini memungkinkan perangkat berkemampuan IPv6 berkomunikasi

dengan perangkat berkemampuan IPv6 lainnya pada subnet yang sama. Ini termasuk komunikasi dengan gateway default (router).

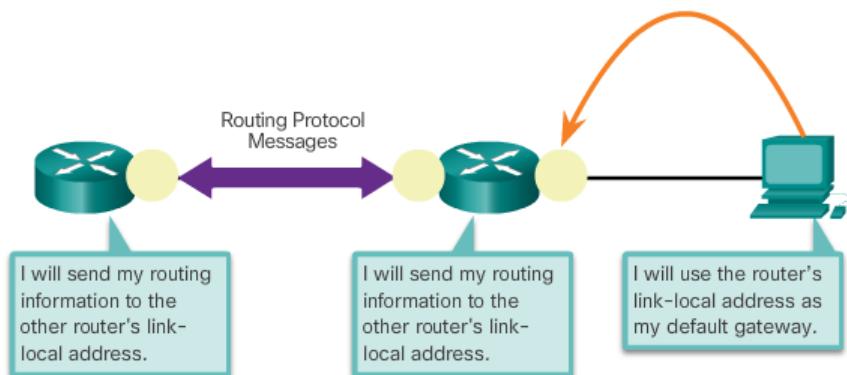
Alamat IPv6-local berada di kisaran FE80 :: / 10. The / 10 menunjukkan bahwa 10 bit pertama adalah 1111 1110 10xx xxxx. Hextet pertama memiliki jangkauan 1111 1110 1000 0000 (FE80) sampai 1111 1110 1011 1111 (FEBF).

- ✓ Contoh komunikasi menggunakan alamat IPv6-local.



- ✓ beberapa kegunaan untuk alamat link-local IPv6

Uses of an IPv6 Link-Local Address



Catatan: Biasanya, ini adalah alamat link-local dari router dan bukan alamat unicast global, yang digunakan sebagai gateway default untuk perangkat lain pada link.

❖ IPv6 UNICAST ADDRESSES

• STRUKTUR IPv6 GLOBAL UNICAST ADDRESSES

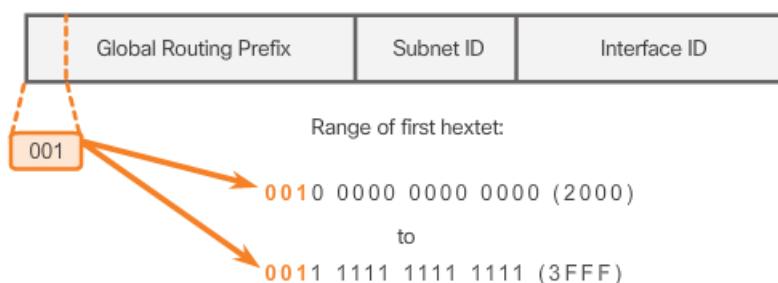
Alamat unicast IPv6 secara global unik dan routable di Internet IPv6. Alamat ini setara dengan alamat IPv4 publik. Komite Internet untuk Ditugaskan Nama dan Nomor (ICANN), operator untuk IANA, mengalokasikan blok alamat IPv6 ke lima RIR. Saat ini, hanya alamat unicast global dengan tiga bit pertama 001 atau 2000 :: / 3 yang ditugaskan. Ini hanya 1/8 dari total ruang alamat IPv6 yang tersedia, tidak termasuk bagian yang sangat kecil untuk jenis alamat unicast dan multicast lainnya.

Catatan: Alamat 2001: 0DB8 :: / 32 telah dipesan untuk tujuan dokumentasi, termasuk penggunaan di contoh.

struktur dan jangkauan alamat unicast global.

Alamat unicast global memiliki tiga bagian:

- ✓ **Global routing prefix**
- ✓ **Subnet ID**
- ✓ **Interface ID**



Global Routing Prefix

The global routing prefix adalah *prefix*, atau jaringan, bagian dari alamat yang diberikan oleh penyedia, seperti ISP, ke pelanggan atau situs. Biasanya, RIR menetapkan *prefix routing global* / 48 kepada pelanggan. Ini bisa mencakup semua orang dari jaringan bisnis perusahaan ke rumah tangga masing-masing.

Gambar dibawah menunjukkan struktur alamat *unicast global* menggunakan *prefix routing global* / 48. / 48 prefiks adalah *prefix routing global* yang paling umum yang ditugaskan.

Misalnya, alamat IPv6 2001: 0DB8: ACAD :: / 48 memiliki *prefix* yang menunjukkan bahwa 48 bit pertama (3 hextets) (2001: 0DB8: ACAD) adalah *prefix* atau bagian jaringan dari alamat. Kolom ganda (:) sebelum / 48 panjang *prefix* berarti sisa alamat berisi semua 0s.

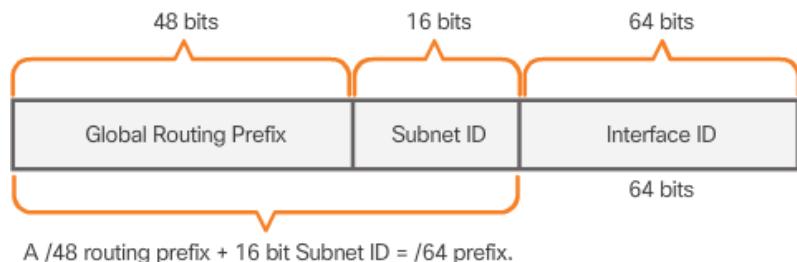
Ukuran *prefix routing global* menentukan ukuran ID subnet.

Subnet ID

Subnet ID digunakan oleh sebuah organisasi untuk mengidentifikasi subnet di dalam situsnya. Semakin besar subnet ID, semakin banyak subnet yang tersedia.

Interface ID

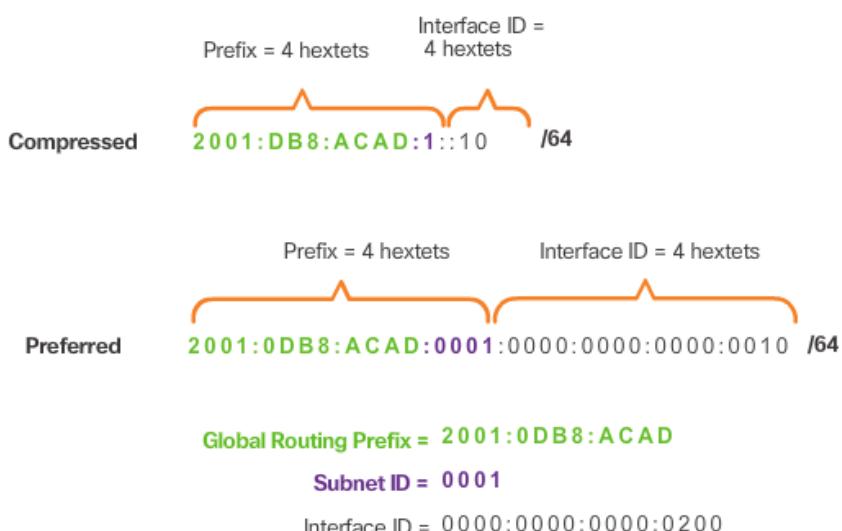
ID *interface* IPv6 setara dengan bagian host dari alamat IPv4. Istilah *Interface ID* digunakan karena satu host mungkin memiliki beberapa antarmuka, masing-masing memiliki satu atau lebih alamat IPv6. Sangat disarankan agar dalam kebanyakan kasus / 64 subnet harus digunakan. Dengan kata lain sebuah ID *interface* 64-bit



Catatan: Tidak seperti IPv4, di IPv6, alamat host all-0s dan all-1s dapat diberikan ke perangkat. Alamat all-1 dapat digunakan karena alamat broadcast tidak digunakan dalam IPv6. Alamat all-0s juga bisa digunakan, namun dicadangkan sebagai alamat anycast Subnet-Router, dan hanya ditugaskan ke router.

Cara mudah untuk membaca sebagian besar alamat IPv6 adalah menghitung jumlah hextet. Seperti ditunjukkan pada Gambar dibawah, dalam alamat unicast global / unicast empat hextet pertama adalah untuk bagian jaringan dari alamat, dengan hextet keempat menunjukkan ID Subnet. Empat hextets sisanya untuk Interface ID.

Reading a Global Unicast Address



- STATIC CONFIGURATION OF A GLOBAL UNICAST ADDRESSES

Konfigurasi Router

Sebagian besar perintah konfigurasi dan verifikasi IPv6 di Cisco IOS serupa dengan rekan IPv4 mereka. Dalam banyak kasus, satu-satunya perbedaan adalah penggunaan ipv6 di tempat ip di dalam perintah.

Perintah untuk mengkonfigurasi alamat unicast global IPv6 pada sebuah antarmuka adalah ipv6 address ipv6-address / prefix-length.

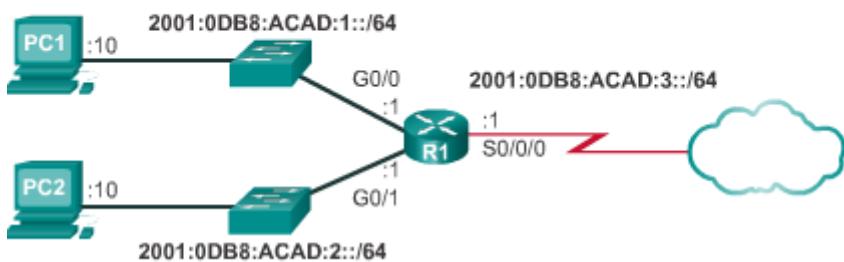
Perhatikan bahwa tidak ada ruang antara ipv6-address dan prefix-length.

Contoh konfigurasi menggunakan topologi yang ditunjukkan pada Gambar dibawah dan subnet IPv6 ini:

- ✓ 2001: 0DB8: ACAD: 0001: / 64 (atau 2001: DB8: ACAD: 1 :: 64)
- ✓ 2001: 0DB8: ACAD: 0002: / 64 (atau 2001: DB8: ACAD: 2 :: 64)
- ✓ 2001: 0DB8: ACAD: 0003: / 64 (atau 2001: DB8: ACAD: 3 :: 64)

Gambar dibawah juga menunjukkan perintah yang diperlukan untuk mengkonfigurasi alamat unicast global IPv6 pada antarmuka GigabitEthernet 0/0, GigabitEthernet 0/1, dan Serial 0/0/0 R1.

Configuring IPv6 on a Router



```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:3::1/64
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown
```

Konfigurasi Host

Mengkonfigurasi alamat IPv6 secara manual pada host sama dengan mengkonfigurasi alamat IPv4.

Seperti ditunjukkan pada Gambar dibawah, alamat gateway default yang dikonfigurasi untuk PC1 adalah 2001: DB8: ACAD: 1 :: 1. Ini adalah alamat unicast global dari antarmuka GigabitEthernet R1 pada jaringan yang sama. Sebagai alternatif, alamat gateway default dapat dikonfigurasi untuk mencocokkan alamat link-lokal dari antarmuka GigabitEthernet. Konfigurasi akan bekerja.

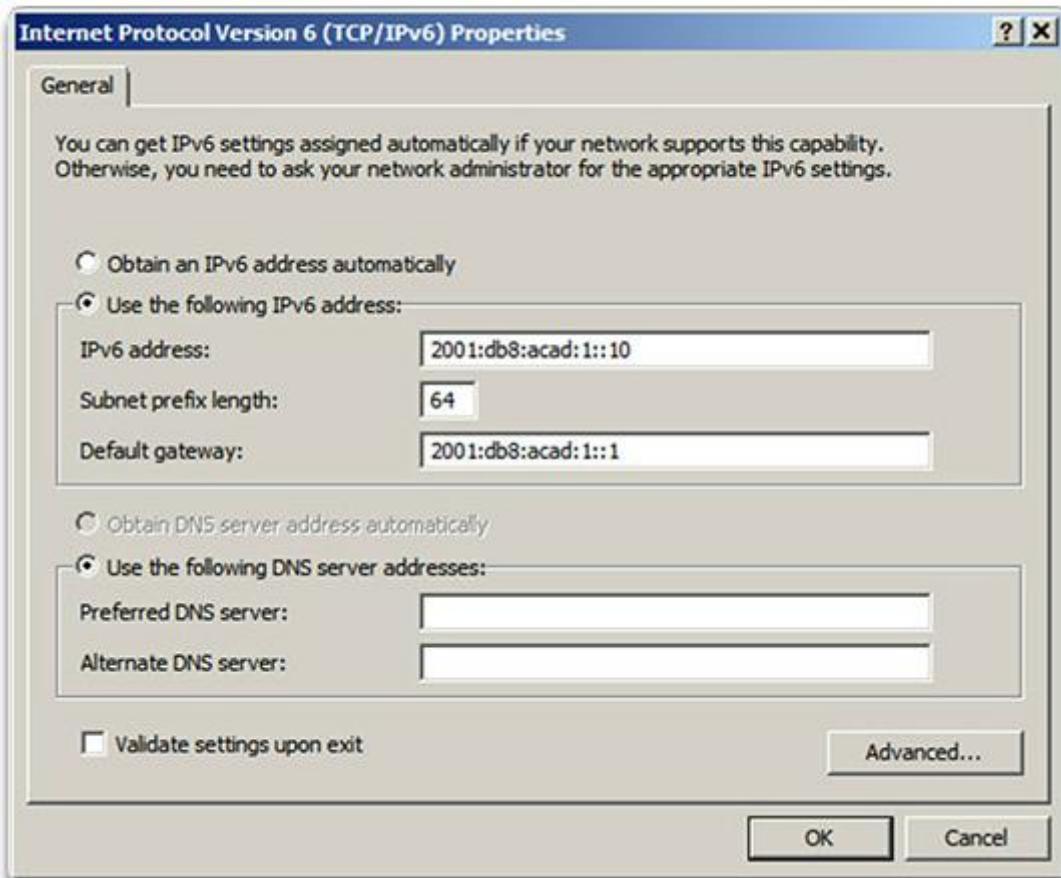
Gunakan Pemeriksa Sintaks untuk mengkonfigurasi alamat unicast global IPv6.

Sama seperti IPv4, konfigurasi alamat statis pada klien tidak berskala ke lingkungan yang lebih besar. Untuk alasan ini, sebagian besar administrator jaringan di jaringan IPv6 akan mengaktifkan penetapan alamat IPv6 dinamis.

Ada dua cara di mana perangkat dapat memperoleh alamat unicast global IPv6 secara otomatis:

- ✓ Stateless Address Autoconfiguration (SLAAC)
- ✓ DHCPv6

Catatan: Bila DHCPv6 atau SLAAC digunakan, alamat lokal-link router lokal akan secara otomatis ditetapkan sebagai alamat gateway default.



- **DYNAMIC CONFIGURATION – SLAAC**

Statified Address Autoconfiguration (SLAAC) adalah metode yang memungkinkan perangkat mendapatkan prefix, panjang prefix, alamat gateway default, dan informasi lainnya dari router IPv6 tanpa menggunakan server DHCPv6. Dengan menggunakan SLAAC, perangkat mengandalkan pesan ICMPv6 *Router Advertisement* (RA) router lokal untuk mendapatkan informasi yang diperlukan.

Router IPv6 mengirimkan pesan ICMPv6 RA secara berkala, setiap 200 detik, ke semua perangkat berkemampuan IPv6 di jaringan. Pesan RA juga akan dikirim sebagai tanggapan atas host yang mengirim pesan ICMPv6 Router Solicitation (RS).

Routing IPv6 tidak diaktifkan secara default. Untuk mengaktifkan router sebagai router IPv6, perintah konfigurasi global unicast-routing ipv6 harus digunakan.

Catatan: Alamat IPv6 dapat dikonfigurasi di router tanpa router IPv6.

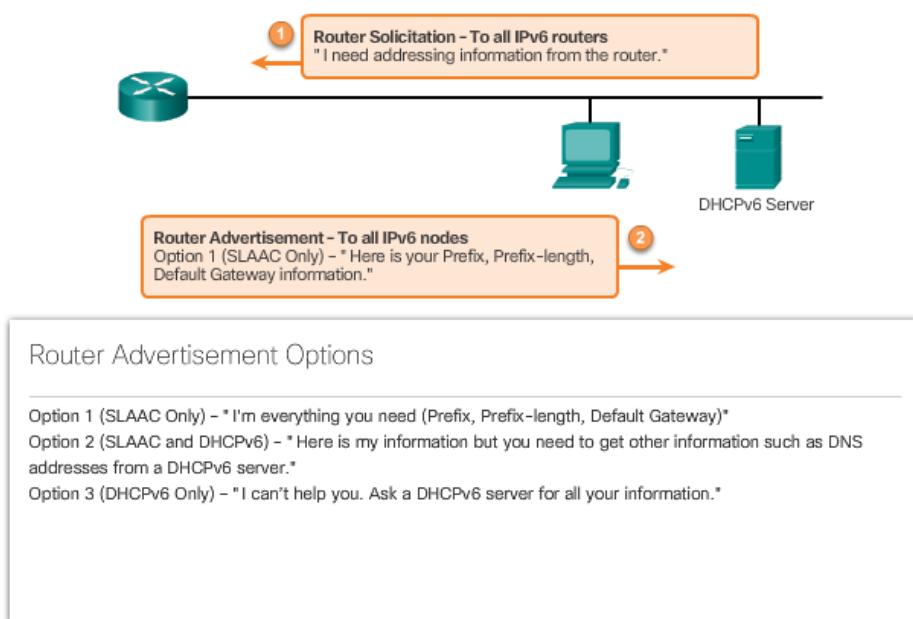
Pesan ICMPv6 RA adalah saran ke perangkat tentang cara mendapatkan alamat unicast global IPv6. Keputusan terakhir terserah pada sistem operasi perangkat. Pesan ICMPv6 RA meliputi:

- ✓ **Network prefix and prefix length** - Memberitahu perangkat di mana jaringan berada.
- ✓ **Default gateway address** - Ini adalah alamat link-lokal IPv6, alamat IPv6 sumber dari pesan RA.
- ✓ **DNS addresses and domain name** - Alamat server DNS dan nama domain

Seperti ditunjukkan pada Gambar, ada tiga pilihan untuk pesan RA:

- ✓ Opsi 1: SLAAC
- ✓ Opsi 2: SLAAC with a stateless DHCPv6 server
- ✓ Opsi 3: Stateful DHCPv6 (tidak ada SLAAC)

Router Solicitation and Router Advertisement Messages

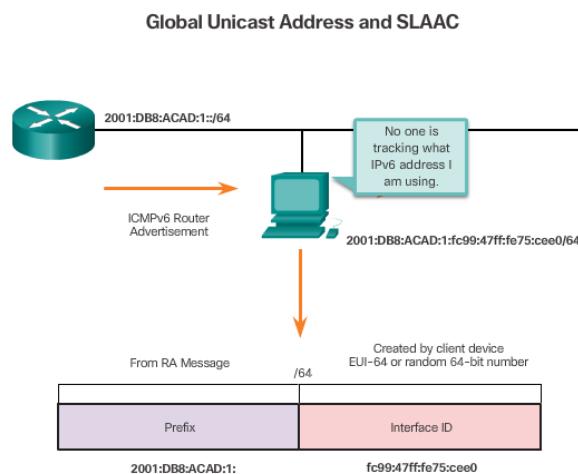


RA Opsi 1: SLAAC

Secara default, pesan RA menunjukkan bahwa perangkat penerima menggunakan informasi tersebut dalam pesan RA untuk membuat alamat unicast global IPv6 sendiri dan untuk semua informasi lainnya. Layanan server DHCPv6 tidak diperlukan.

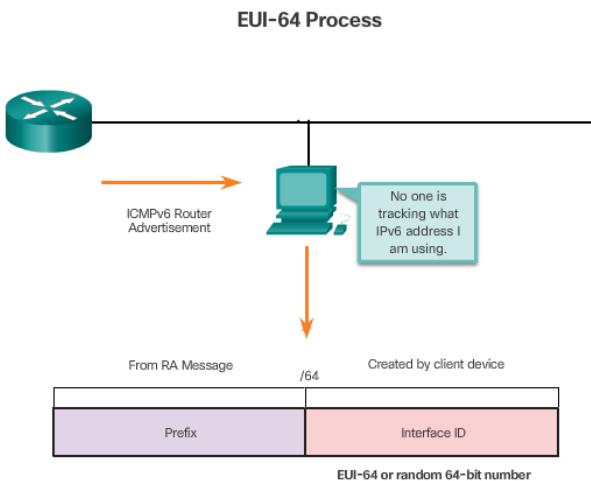
SLAAC is stateless, yang berarti tidak ada server pusat (misalnya, server DHCPv6 stateful) yang mengalokasikan alamat unicast global dan menyimpan daftar perangkat dan alamat mereka. Dengan SLAAC, perangkat klien menggunakan informasi dalam pesan RA untuk membuat alamat unicast globalnya sendiri. Seperti ditunjukkan pada Gambar dibawah, dua bagian alamat dibuat sebagai berikut:

- ✓ **Prefix** – Received in the RA message
- ✓ **Interface ID** – Uses the EUI-64 process or by generating a random 64-bit number



• EUI-64 PROCESS AND RANDOMLY GENERATED

Ketika pesan RA adalah SLAAC atau SLAAC dengan DHCPv6 stateless, klien harus membuat ID Interface-nya sendiri. Klien mengetahui prefix dari alamat dari pesan RA tapi harus membuat ID Interface-nya sendiri. ID interface dapat dibuat dengan menggunakan proses EUI-64 atau bilangan 64-bit yang dihasilkan secara acak, seperti yang ditunjukkan pada Gambar berikut.



Proses EUI-64

IEEE mendefinisikan Extended Unique Identifier (EUI) atau proses EUI-64 yang dimodifikasi. Proses ini menggunakan alamat MAC Ethernet 48-bit klien, dan memasukkan 16 bit lagi di tengah alamat MAC 48-bit untuk membuat ID Antarmuka 64-bit.

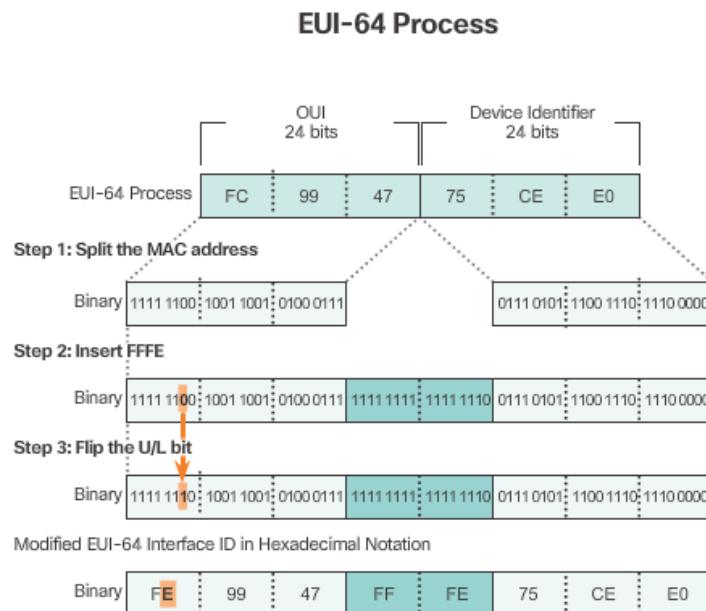
Alamat MAC Ethernet biasanya terwakili dalam heksadesimal dan terdiri dari dua bagian:

- ✓ **Organizationally Unique Identifier (OUI)** – OUI adalah kode vendor 24 bit (6 digit heksadesimal) yang ditugaskan oleh IEEE.
- ✓ **Device Identifier** - Device identifier adalah nilai 24-bit (6 heksadesimal digit) yang unik dalam OUI umum.

ID Antarmuka EUI-64 terwakili dalam biner dan terdiri dari tiga bagian:

- ✓ 24-bit OUI dari alamat MAC klien, tapi bit ke-7 (bit Universal / Lokal (U / L)) dibalik. Ini berarti bahwa jika bit ke-7 adalah 0, itu menjadi 1, dan sebaliknya.
- ✓ Nilai FFFE 16-bit dimasukkan (dalam heksadesimal)
- ✓ Device Identifier 24-bit dari alamat MAC klien

Proses EUI-64 diilustrasikan pada Gambar 2, menggunakan alamat MAC GigabitEthernet R1 dari FC99: 4775: CEE0.



1. Langkah 1: Bagilah alamat MAC antara OUI dan device identifier.
2. Langkah 2: Masukkan nilai heksadesimal FFFE, yang dalam biner adalah: 1111 1111 1111 1110.
3. Langkah 3: Mengkonversi 2 heksadesimal pertama nilai OUI ke biner dan flip U / L bit (bit 7). Dalam contoh ini, 0 di bit 7 diubah menjadi 1.

Hasilnya adalah ID Interface EUI-64 yang dihasilkan dari FE99: 47FF: FE75: CEE0.

Catatan: Penggunaan bit U / L, dan alasan untuk membalik nilainya, dibahas di RFC 5342.

Gambar dibawah menunjukkan alamat *unicast universal IPv6 global* yang dibuat secara dinamis dengan menggunakan SLAAC dan proses EUI-64. Cara mudah untuk mengidentifikasi bahwa alamat lebih dari kemungkinan dibuat dengan menggunakan EUI-64 adalah FFFE yang berada di tengah ID *interface*.

```
PCA> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection: From RA
                                         Message          EUI-64 generated
Connection-specific DNS Suffix : 2001:db8:acad:1:fc99:47ff:ffe75:cee0
IPv6 Address . . . . . : fe80::fc99:47FF:FE75:CEE0
Link-local IPv6 Address . . . . : fe80::1
Default Gateway . . . . . : fe80::1
```

Keuntungan dari EUI-64 adalah alamat MAC Ethernet yang bisa digunakan untuk menentukan Interface ID. Ini juga memungkinkan administrator jaringan untuk dengan mudah melacak alamat IPv6 ke perangkat akhir menggunakan alamat MAC yang unik. Namun, ini menyebabkan kekhawatiran privasi di antara banyak pengguna. Mereka khawatir paket mereka bisa dilacak ke komputer fisik yang sebenarnya. Karena masalah ini, ID *interface* yang dihasilkan secara acak dapat digunakan sebagai gantinya.

Randomly Generated Interface IDs

Bergantung pada sistem operasi, perangkat mungkin menggunakan ID *Interface* yang dibuat secara acak daripada menggunakan alamat MAC dan proses EUI-64. Misalnya, dimulai dengan Windows Vista, Windows menggunakan ID *Interface* yang dibuat secara acak, bukan yang dibuat dengan EUI-64. Windows XP dan sistem operasi Windows sebelumnya menggunakan EUI-64.

Setelah ID *Interface* dibuat, baik melalui proses EUI-64 atau melalui generasi acak, dapat dikombinasikan dengan prefix IPv6 dalam pesan RA untuk membuat alamat unicast global, seperti yang ditunjukkan pada Gambar dibawah.

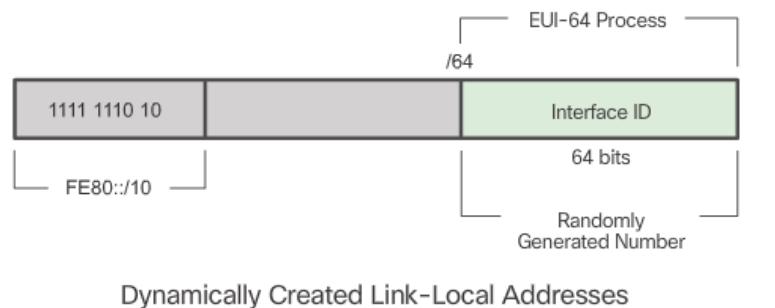
Catatan: Untuk memastikan keunikan alamat unicast IPv6, klien dapat menggunakan proses yang dikenal sebagai *Duplicate Address Detection* (DAD). Ini mirip dengan permintaan ARP untuk alamatnya sendiri. Jika tidak ada jawaban, maka alamatnya unik.

```
PCB> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection: From RA
                                         Message          Random 64-bit
                                         number
Connection-specific DNS Suffix : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
Link-local IPv6 Address . . . . : fe80::1
Default Gateway . . . . . : fe80::1
```

- **DYNAMIC LINK-LOCAL ADDRESSES**

Semua perangkat IPv6 harus memiliki alamat lokal-link IPv6. Alamat link-lokal dapat dibuat secara dinamis atau dikonfigurasi secara manual sebagai alamat link-lokal statis.

Gambar dibawah menunjukkan alamat link-lokal dibuat secara dinamis menggunakan prefix FE80 :: / 10 dan ID interface menggunakan proses EUI-64 atau nomor 64-bit yang dibuat secara acak. Sistem operasi biasanya menggunakan metode yang sama untuk SLAAC yang dibuat alamat unicast global dan alamat link-local yang ditetapkan secara dinamis.



EUI-64 generated Interface ID

```
PCA> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix :
  IPv6 Address . . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
  Link-local IPv6 Address . . . . : fe80::fc99:47ff:fe75:cee0
  Default Gateway . . . . . : fe80::1
```

Random 64-bit generated Interface ID

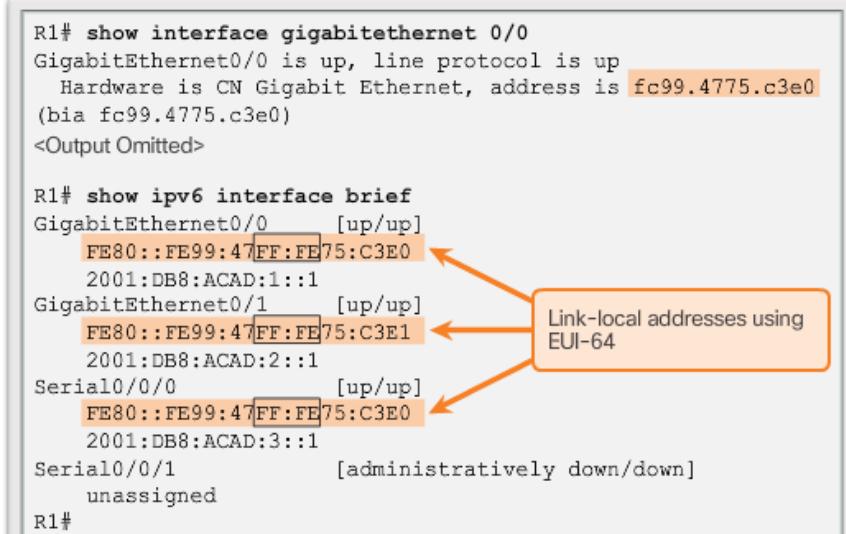
```
PCB> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix :
  IPv6 Address . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
  Link-local IPv6 Address . . . . : fe80::50a5:8a35:a5bb:66e1
  Default Gateway . . . . . : fe80::1
```

Router Cisco secara otomatis membuat alamat link-lokal IPv6 setiap kali alamat unicast global ditugaskan ke antarmuka. Secara default, router Cisco IOS menggunakan EUI-64 untuk menghasilkan Interface ID untuk semua alamat link-local pada interface IPv6. Untuk antarmuka serial, router akan menggunakan alamat MAC dari antarmuka Ethernet. Ingat bahwa alamat link-local harus unik hanya pada link atau jaringan itu. Namun, kelemahan untuk menggunakan alamat link-local yang ditugaskan secara dinamis adalah panjangnya, yang membuatnya menantang untuk mengidentifikasi dan mengingat alamat yang ditugaskan. Gambar dibawah menampilkan alamat MAC pada interface GigabitEthernet 0/0 router R1. Alamat ini digunakan untuk secara dinamis membuat alamat link-local pada interface yang sama.

Agar lebih mudah mengenali dan mengingat alamat ini di router, umumkan untuk mengkonfigurasi alamat IPv6 link-local secara statis pada router.

```
R1# show interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
(bia fc99.4775.c3e0)
<Output Omitted>

R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
  FE80::FE99:47FF:FE75:C3E1
  2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
  unassigned
R1#
```



- **STATIC LINK-LOCAL ADDRESSES**

Mengkonfigurasi alamat link-local secara manual memberikan kemampuan untuk membuat alamat yang mudah dikenali dan mudah diingat.

Alamat link-lokal dapat dikonfigurasi secara manual menggunakan perintah antarmuka yang sama yang digunakan untuk membuat alamat unicast global IPv6 namun dengan parameter link-local tambahan. Bila alamat diawali dengan hextet ini dalam kisaran FE80 ke FEBF, parameter tautan lokal harus mengikuti alamat.

Angka tersebut menunjukkan konfigurasi alamat link-local menggunakan perintah antarmuka alamat ipv6. Alamat link-local FE80 :: 1 digunakan untuk membuatnya mudah dikenali sebagai milik router R1. Alamat link-local IPv6 yang sama dikonfigurasi pada semua antarmuka R1. FE80 :: 1 dapat dikonfigurasi pada setiap tautan karena hanya harus unik pada tautan itu.

Serupa dengan R1, router R2 akan dikonfigurasi dengan FE80 :: 2 sebagai alamat link-local IPv6 pada semua antarmukanya

Configuring Link-local Addresses on R1

```
Router(config-if)#  
ipv6 address link-local-address link-local  
  
R1(config)#interface gigabitethernet 0/0  
R1(config-if)#ipv6 address fe80::1 ?  
  link-local  Use link-local address  
  
R1(config-if)#ipv6 address fe80::1 link-local  
R1(config-if)#exit  
R1(config)#interface gigabitethernet 0/1  
R1(config-if)#ipv6 address fe80::1 link-local  
R1(config-if)#exit  
R1(config)#interface serial 0/0/0  
R1(config-if)#ipv6 address fe80::1 link-local  
R1(config-if)#
```

- **VERIFIKASI IPv6 ADDRESS CONFIGURATION**

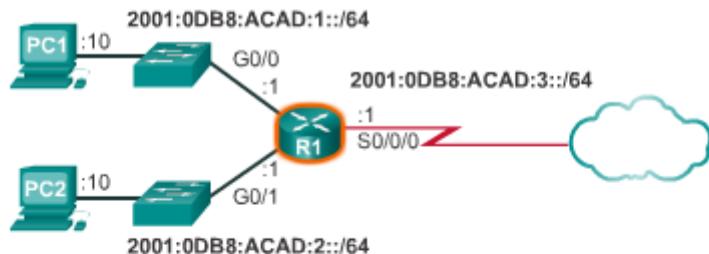
Seperti ditunjukkan pada Gambar, perintah untuk memverifikasi konfigurasi antarmuka IPv6 serupa dengan perintah yang digunakan untuk IPv4.

Perintah show menampilkan alamat MAC dari *interface Ethernet*. EUI-64 menggunakan alamat MAC ini untuk menghasilkan Interface ID untuk alamat link-local. Selain itu, perintah show ipv6 interface singkat menampilkan output yang disingkat untuk masing-masing antarmuka. Output [atas / atas] pada baris yang sama dengan antarmuka menunjukkan status antarmuka Layer 1 / Layer 2. Ini sama dengan kolom Status dan Protokol dalam perintah IPv4 yang setara.

Perhatikan bahwa setiap antarmuka memiliki dua alamat IPv6. Alamat kedua untuk setiap antarmuka adalah alamat unicast global yang dikonfigurasi. Alamat pertama, yang dimulai dengan FE80, adalah alamat unicast link-local untuk antarmuka. Ingat bahwa alamat link-lokal secara otomatis ditambahkan ke antarmuka saat alamat unicast global ditugaskan.

Juga, perhatikan bahwa alamat link-local R1 Serial 0/0/0 sama dengan interface GigabitEthernet 0/0 nya. Antarmuka serial tidak memiliki alamat MAC Ethernet, jadi Cisco IOS menggunakan alamat MAC dari antarmuka Ethernet pertama yang tersedia. Hal ini dimungkinkan karena antarmuka link-local hanya harus unik pada link itu.

Alamat link-local dari antarmuka router biasanya adalah alamat gateway default untuk perangkat pada link atau jaringan tersebut.



```
R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:ACAD:2::1
Serial0/0/0              [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1              [administratively down/down]
    unassigned
R1#
```

Seperti ditunjukkan pada Gambar dibawah, perintah *rute show ipv6* dapat digunakan untuk memverifikasi bahwa jaringan IPv6 dan alamat antarmuka IPv6 spesifik telah diinstal di tabel routing IPv6. Perintah perintah *ipv6* menunjukkan hanya akan menampilkan jaringan IPv6, bukan jaringan IPv4.

Dalam tabel rute, C di sebelah rute menunjukkan bahwa ini adalah jaringan yang terhubung langsung. Ketika *interface router* dikonfigurasi dengan alamat *unicast global* dan berada dalam status "naik / naik", prefix IPv6 dan panjang prefix ditambahkan ke tabel routing IPv6 sebagai rute yang terhubung.

Alamat unicast global IPv6 yang dikonfigurasi pada antarmuka juga dipasang di tabel routing sebagai rute lokal. Rute lokal memiliki prefix / 128. Rute lokal digunakan oleh tabel routing untuk memproses paket secara efisien dengan alamat tujuan dari alamat antarmuka router.

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - static, U - Per-user
Static

<output omitted>

C 2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0, receive
C 2001:DB8:ACAD:2::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
    via GigabitEthernet0/1, receive
C 2001:DB8:ACAD:3::/64 [0/0]
    via Serial0/0/0, directly connected
L 2001:DB8:ACAD:3::1/128 [0/0]
    via Serial0/0/0, receive
L FF00::/8 [0/0]
    via Null0, receive
R1#
```

Perintah ping untuk IPv6 identik dengan perintah yang digunakan dengan IPv4, kecuali bahwa alamat IPv6 digunakan. Seperti ditunjukkan pada Gambar dibawah, perintah digunakan untuk memverifikasi koneksi Layer 3 antara R1 dan PC1. Saat melakukan ping alamat link-local dari router, Cisco IOS akan meminta pengguna untuk keluar dari antarmuka. Karena alamat link-local tujuan bisa berada di satu atau lebih dari link atau jaringannya, router perlu mengetahui interface mana yang akan dikirim ping.

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5)
R1#
```

Gunakan Pemeriksa Sintaks memverifikasi konfigurasi alamat IPv6.

❖ IPv6 MULTICAST ADDRESSES

• ASSIGNED IPv6 MULTICAST ADDRESSES

Alamat *multicast* IPv6 mirip dengan alamat *multicast* IPv4. Ingat bahwa alamat *multicast* digunakan untuk mengirim satu paket ke satu atau beberapa tujuan (grup *multicast*). Alamat *multicast* IPv6 memiliki prefix FF00 :: / 8.

Catatan: Alamat *multicast* hanya bisa alamat tujuan dan bukan alamat sumber.

Ada dua jenis alamat *multicast* IPv6:

- ✓ Assigned multicast
- ✓ Solicited node multicast

Assigned Multicast

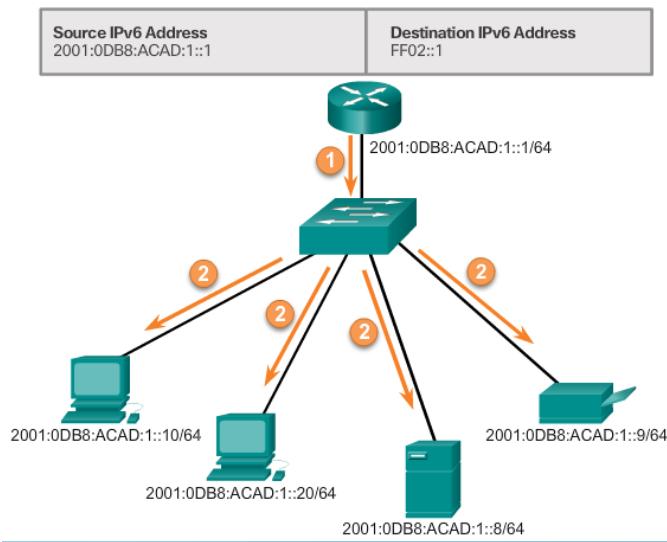
Alamat *multicast* yang ditugaskan merupakan alamat *multicast* yang dipesan untuk kelompok perangkat yang telah ditentukan. Alamat *multicast* yang ditugaskan adalah alamat tunggal yang digunakan untuk menjangkau sekelompok perangkat yang menjalankan protokol atau layanan umum. Alamat *multicast* yang ditugaskan digunakan dalam konteks dengan protokol spesifik seperti DHCPv6.

Dua kelompok multikast IPv6 yang umum ditugaskan meliputi:

- ✓ **FF02 :: 1 All-nodes multicast group** - Ini adalah grup *multicast* yang memungkinkan semua perangkat yang mendukung IPv6 bergabung. Sebuah paket yang dikirim ke grup ini diterima dan diproses oleh semua antarmuka IPv6 pada link atau jaringan. Ini memiliki efek yang sama dengan alamat broadcast di IPv4. Angka tersebut menunjukkan contoh komunikasi dengan menggunakan alamat *multicast* all-nodes. Router IPv6 mengirim pesan Message Control Protocol (Protokol Pesan Protokol TCP) jarak jauh (ICMPv6) RA ke grup *multicast* all-node. Pesan RA menginformasikan semua perangkat yang mendukung IPv6 pada jaringan tentang menangani informasi, seperti awalan, panjang awalan, dan gateway standar.
- ✓ **FF02 :: 2 All-routers multicast group** - Ini adalah grup *multicast* yang diikuti semua router IPv6. Router menjadi anggota grup ini saat diaktifkan sebagai router IPv6 dengan perintah konfigurasi global unicast-routing ipv6. Sebuah paket yang dikirim ke grup ini diterima dan diproses oleh semua router IPv6 pada link atau jaringan

Perangkat berkemampuan IPv6 mengirim pesan ICMPv6 Router Solicitation (RS) ke alamat *multicast* semua router. Pesan RS meminta pesan RA dari router IPv6 untuk membantu perangkat dalam konfigurasi alamatnya

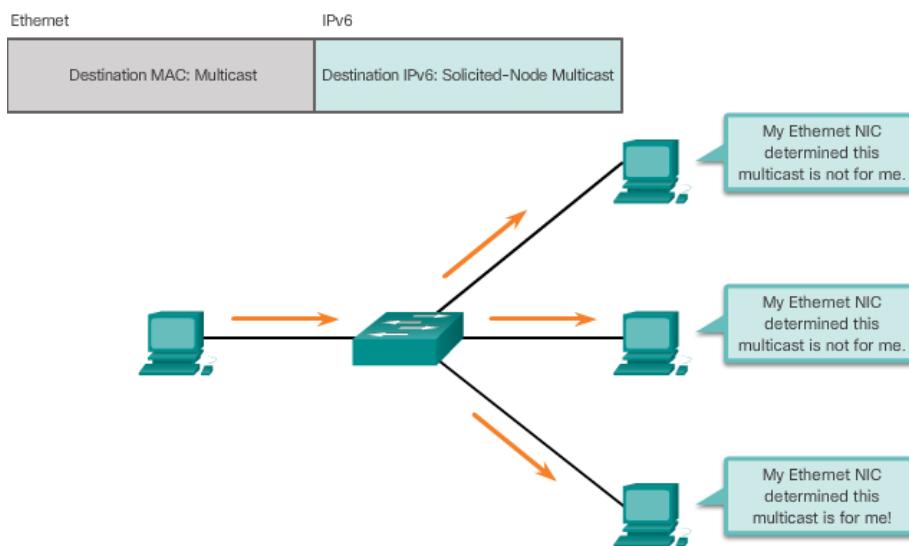
IPv6 All-Nodes Multicast Communications



- **SOLICITED-NODE IPv6 MULTICAST ADDRESSES**

A **solicited-node multicast address** adalah kemiripan dengan alamat multicast all-nodes. Keuntungan dari alamat multicast yang diminta oleh solicited adalah dipetakan ke alamat multicast Ethernet khusus. Hal ini memungkinkan NIC Ethernet untuk memfilter frame dengan memeriksa alamat MAC tujuan tanpa mengirimkannya ke proses IPv6 untuk melihat apakah perangkat tersebut adalah target yang dimaksud dari paket IPv6.

IPv6 Solicited-Node Multicast Address



7.4 VERIFIKASI KONEKTIFITAS

- ❖ ICMP
- ICMPv4 DAN ICMPv6

Meskipun IP bukanlah protokol yang andal, paket TCP / IP memang menyediakan agar pesan dikirim jika terjadi kesalahan tertentu. Pesan ini dikirim menggunakan layanan ICMP. Tujuan dari pesan ini adalah untuk memberikan umpan balik tentang isu-isu yang berkaitan dengan pengolahan paket IP dalam kondisi tertentu, agar IP tidak dapat diandalkan. Pesan ICMP tidak diperlukan dan sering tidak diizinkan masuk ke jaringan karena alasan keamanan.

ICMP tersedia untuk IPv4 dan IPv6. ICMPv4 adalah protokol perpesanan untuk IPv4. ICMPv6 menyediakan layanan yang sama untuk IPv6 namun mencakup fungsionalitas tambahan. Dalam kursus ini, istilah ICMP akan digunakan saat mengacu pada ICMPv4 dan ICMPv6.

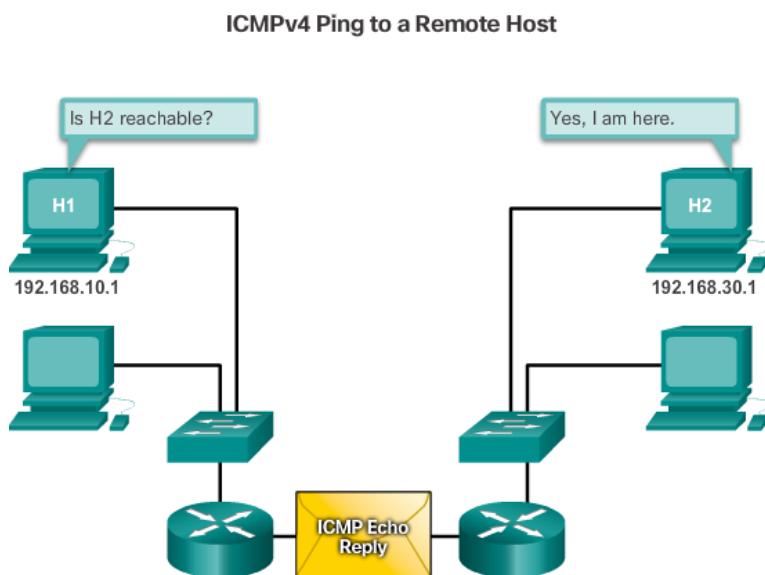
Jenis pesan ICMP dan alasan mengapa mereka dikirim, sangat luas. Kita akan membahas beberapa pesan yang lebih umum.

Pesan ICMP yang umum untuk ICMPv4 dan ICMPv6 meliputi:

- ✓ Host confirmation
- ✓ Destination or Service Unreachable
- ✓ Time exceeded
- ✓ Route redirection

Host Confirmation

Pesan ICMP Echo dapat digunakan untuk menentukan apakah host beroperasi. Host lokal mengirimkan Permintaan ICMP Echo ke host. Jika host tersedia, host tujuan merespons dengan Echo Reply. Pada gambar. Penggunaan pesan ICMP Echo ini adalah dasar utilitas ping.



Destination or Service Unreachable

Bila host atau gateway menerima paket yang tidak dapat dikirimnya, ia dapat menggunakan pesan *ICMP Destination Unreachable* untuk memberi tahu sumber bahwa tujuan atau layanan tidak dapat dijangkau. Pesan akan menyertakan kode yang menunjukkan mengapa paket tidak dapat dikirim.

Beberapa kode *Destination Unreachable* untuk ICMPv4 adalah:

- ✓ **0 - Net unreachable**
- ✓ **1 - Host unreachable**
- ✓ **2 - Protocol unreachable**
- ✓ **3 - Port unreachable**

Catatan: ICMPv6 memiliki kode yang mirip namun sedikit berbeda untuk pesan Destination Unreachable.

Time Exceeded

Pesan ICMPv4 Time Exceeded digunakan oleh router untuk menunjukkan bahwa paket tidak dapat diteruskan karena bidang Time to Live (TTL) paket dikurangi ke 0. Jika router menerima paket dan menolak bidang TTL dalam paket IPv4 ke nol, itu membuang paket dan mengirim pesan Time Exceeded ke host sumber.

ICMPv6 juga mengirimkan pesan Time Exceeded jika router tidak dapat meneruskan paket IPv6 karena paketnya telah kedaluwarsa. IPv6 tidak memiliki bidang TTL; ia menggunakan bidang batas hop untuk menentukan apakah paket telah kedaluwarsa.

- **ICMPv6 ROUTER SOLICITATION AND ROUTER ADVERTISEMENT MESSAGES**

Pesan informasi dan kesalahan yang ditemukan di ICMPv6 sangat mirip dengan pesan kontrol dan kesalahan yang diterapkan oleh ICMPv4. Namun, ICMPv6 memiliki fitur baru dan fungsionalitas yang tidak ditemukan di ICMPv4. Pesan ICMPv6 dienkapsulasi dalam IPv6.

ICMPv6 mencakup empat protokol baru sebagai bagian dari *Neighbor Discovery Protocol* (ND atau NDP). Pengiriman pesan antara router IPv6 dan perangkat IPv6:

- ✓ Router Solicitation (RS) message
- ✓ Router Advertisement (RA) message

Perpesanan antara perangkat IPv6:

- ✓ Neighbor Solicitation message
- ✓ Neighbor Advertisement message

Gambar dibawah menunjukkan contoh PC dan router bertukar pesan Periklanan dan Iklan Router. Permintaan Tetangga dan Tetangga Pesan iklan digunakan untuk resolusi Alamat dan Deteksi Alamat Duplikat (DAD).

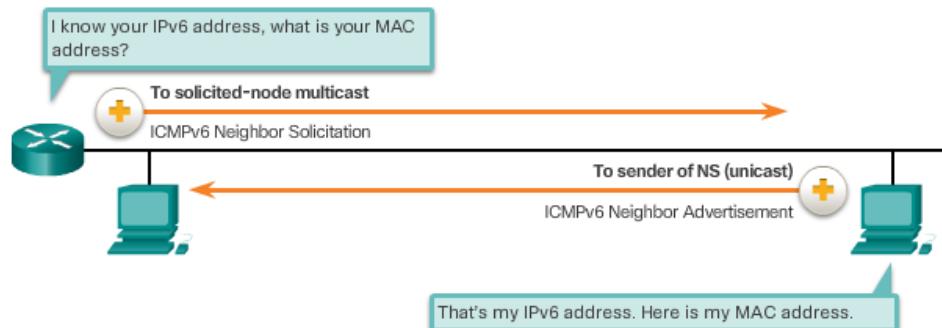
Messaging Between an IPv6 Router and an IPv6 Device



Address Resolution

Resolusi alamat digunakan saat perangkat di LAN mengetahui alamat unicast IPv6 dari sebuah tujuan namun tidak mengetahui alamat MAC Ethernet-nya. Untuk menentukan alamat MAC untuk tujuan, perangkat akan mengirim pesan NS ke alamat simpul yang diminta. Pesan tersebut akan mencakup alamat IPv6 (target) yang diketahui. Perangkat yang memiliki alamat IPv6 yang ditargetkan akan merespons dengan pesan NA yang berisi alamat MAC Ethernet-nya. Gambar dibawah menunjukkan dua PC bertukar pesan NS dan NA. Klik setiap pesan untuk informasi lebih lanjut.

Messaging Between IPv6 Devices

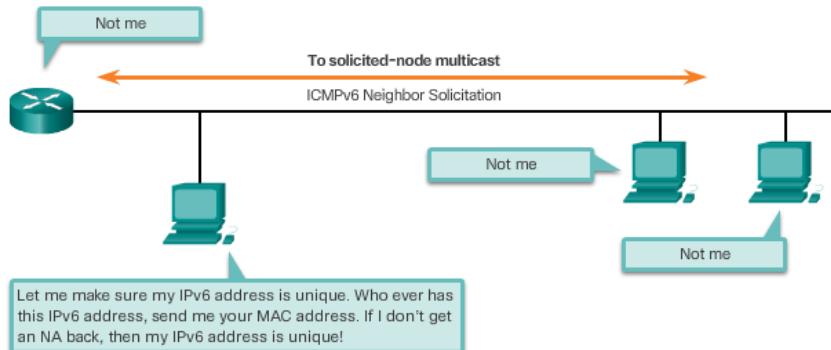


Duplicate Address Detection

Bila perangkat diberi alamat unicast global atau link-local unicast, disarankan agar DAD dilakukan di alamat untuk memastikannya unik. Untuk memeriksa keunikan alamat, perangkat akan mengirim pesan NS dengan alamat IPv6 sendiri sebagai alamat IPv6 yang ditargetkan, yang ditunjukkan pada Gambar dibawah. Jika perangkat lain di jaringan memiliki alamat ini, pesan akan merespons dengan pesan NA. Pesan NA ini akan memberitahukan perangkat pengirim bahwa alamat sedang digunakan. Jika pesan NA yang sesuai tidak dikembalikan dalam jangka waktu tertentu, alamat unicast unik dan dapat diterima untuk digunakan.

Catatan: DAD tidak diperlukan, namun RFC 4861 merekomendasikan agar DAD dilakukan pada alamat unicast.

Duplicate Address Detection (DAD)



❖ TESTING & VERIFIKASI

• PING – TESTING LOCAL STACK

Ping adalah utilitas pengujian yang menggunakan permintaan echo ICMP dan pesan echo reply untuk menguji koneksi antar host. Ping bekerja dengan host IPv4 dan IPv6.

Untuk menguji koneksi ke host lain di jaringan, permintaan echo dikirim ke alamat host menggunakan perintah ping. Jika host di alamat yang ditentukan menerima permintaan echo, ia merespons dengan echo reply. Karena setiap balasan gema diterima, ping memberi umpan balik pada waktu antara saat permintaan dikirim dan saat balasan diterima. Ini bisa menjadi ukuran kinerja jaringan.

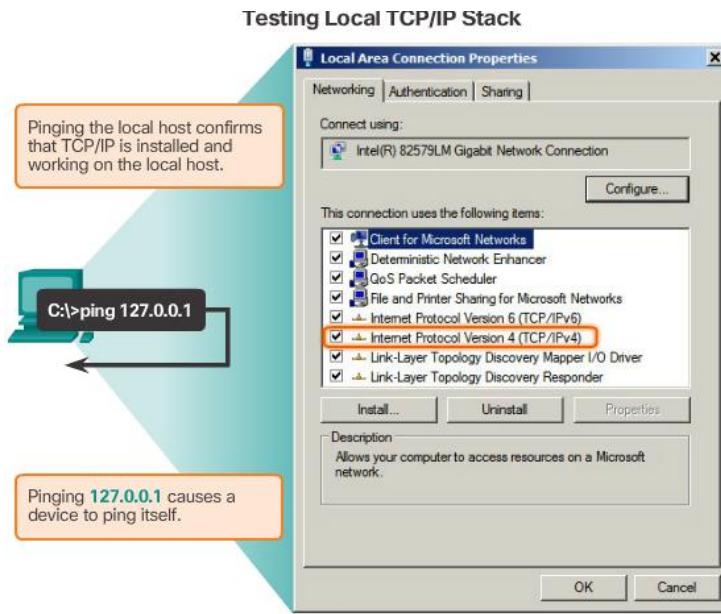
Ping memiliki nilai timeout untuk jawabannya. Jika balasan tidak diterima dalam batas waktu, ping memberikan pesan yang menunjukkan bahwa tanggapan tidak diterima. Ini biasanya menunjukkan bahwa ada masalah, namun bisa juga menunjukkan bahwa fitur keamanan yang memblokir pesan ping telah diaktifkan pada jaringan.

Setelah semua permintaan dikirim, utilitas ping menyediakan ringkasan yang mencakup tingkat keberhasilan dan waktu pulang-pergi rata-rata ke tempat tujuan.

Pinging the Local Loopback

Ada beberapa kasus pengujian dan verifikasi khusus yang bisa kita gunakan untuk melakukan ping. Satu kasus adalah untuk menguji konfigurasi internal IPv4 atau IPv6 di host lokal. Untuk melakukan tes ini, kami melakukan ping alamat loopback lokal 127.0.0.1 untuk IPv4 (:: 1 untuk IPv6). Menguji loopback IPv4 ditunjukkan pada gambar.

Tanggapan dari 127.0.0.1 untuk IPv4, atau :: 1 untuk IPv6, menunjukkan bahwa IP terpasang dengan benar pada host. Respon ini berasal dari lapisan jaringan. Namun, respons ini bukan indikasi bahwa alamat, masker, atau gateway telah dikonfigurasi dengan benar. Juga tidak menunjukkan apa-apa tentang status lapisan bawah tumpukan jaringan. Ini hanya tes IP turun melalui lapisan jaringan IP. Pesan kesalahan menunjukkan bahwa TCP / IP tidak beroperasi pada host.



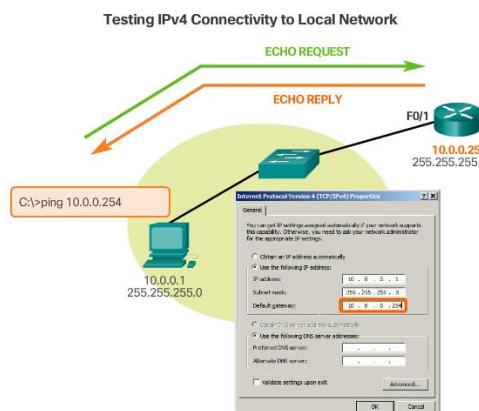
- **PING – TESTING CONNECTIVITY TO THE LOCAL LAN**

Anda juga bisa menggunakan ping untuk menguji kemampuan host untuk berkomunikasi di jaringan lokal. Hal ini umumnya dilakukan dengan melakukan ping alamat IP dari gateway host. Ping ke gateway menunjukkan bahwa host dan interface router berfungsi sebagai gateway keduanya beroperasi pada jaringan lokal.

Untuk pengujian ini, alamat gateway paling sering digunakan karena router biasanya selalu operasional. Jika alamat gateway tidak merespons, ping bisa dikirim ke alamat IP host lain di jaringan lokal yang diketahui beroperasi.

Jika gateway atau host lain merespons, host lokal dapat berhasil berkomunikasi melalui jaringan lokal. Jika gateway tidak merespon tapi host lain tidak, ini bisa menunjukkan adanya masalah dengan antarmuka router yang berfungsi sebagai gateway.

Salah satu kemungkinannya adalah alamat gateway yang salah telah dikonfigurasi pada host. Kemungkinan lain adalah bahwa antarmuka router mungkin beroperasi penuh namun memiliki keamanan yang diterapkan padanya sehingga mencegahnya memproses atau menanggapi permintaan ping.



- **PING – TESTING CONNECTIVITY TO REMOTE**

Ping juga bisa digunakan untuk menguji kemampuan host lokal untuk berkomunikasi antar internetwork. Host lokal dapat melakukan ping ke host IPv4 operasional jaringan jarak jauh.

Jika ping ini berhasil, pengoperasian sebagian besar internetwork bisa diverifikasi. Sebuah ping yang berhasil melintasi internetwork mengkonfirmasikan komunikasi pada jaringan lokal, pengoperasian router yang berfungsi sebagai gateway, dan pengoperasian semua router lain yang mungkin berada di jalur antara jaringan lokal dan jaringan host jarak jauh.

Selain itu, fungsi host jarak jauh dapat diverifikasi. Jika host jarak jauh tidak dapat berkomunikasi di luar jaringan lokalnya, hal itu tidak akan merespons.

Catatan: Banyak administrator jaringan membatasi atau melarang masuknya pesan ICMP ke dalam jaringan perusahaan; Oleh karena itu, kurangnya respons ping bisa jadi karena pembatasan keamanan.

LATIHAN SOAL 7

1. Jelaskan yang dimaksud dengan Ip addressing
2. Jelaskan yang dimaksud dengan subnetmask
3. Jelaskan yang dimaksud dengan ANDing
4. Gambarkan contoh komunikasi Unicast, Multicast & Broadcast
5. Jelaskan yang dimaksud dengan Multicast transmission
6. Apa itu Public IPv4 Addresses
7. Jelaskan yang dimaksud dengan IPv6
8. Jelaskan alasan mengapa diperlukan IPv6
9. Sebutkan dan jelaskan teknik migrasi dari IPv4 ke IPv6
10. Sebutkan tipe alamat IPv6
11. Jelaskan yang dimaksud dengan ICMP
12. Jelaskan apa itu PING
13. Jelaskan perbedaan antara Static Link local address dengan Dynamic Link local address

BAB 8 SUBNETTING IP NETWORKS

8.1 PENGANTAR

Merancang, menerapkan dan mengelola rencana pengalamatan IP yang efektif memastikan bahwa jaringan dapat beroperasi secara efektif dan efisien. Hal ini terutama berlaku karena jumlah koneksi host ke jaringan meningkat. Memahami struktur hierarkis dari alamat IP dan bagaimana memodifikasi hierarki tersebut agar lebih efisien memenuhi persyaratan routing merupakan bagian penting dari perencanaan skema pengalamatan IP.

Dalam alamat IPv4 yang asli, ada dua tingkat hierarki: jaringan dan host. Kedua tingkat pengalamatan ini memungkinkan pengelompokan jaringan dasar yang memudahkan dalam routing paket ke jaringan tujuan. Router meneruskan paket berdasarkan bagian jaringan dari sebuah alamat IP. Bila jaringan berada, bagian host dari alamat memungkinkan identifikasi perangkat tujuan.

Namun, seiring berkembangnya jaringan, dengan banyak organisasi menambahkan ratusan, dan bahkan ribuan host ke jaringan mereka, hierarki dua tingkat tidak mencukupi.

Membagi sebuah jaringan menambahkan level pada hierarki jaringan, menciptakan, pada dasarnya, tiga tingkat: jaringan, subnetwork, dan host. Memperkenalkan tingkat tambahan pada hierarki menciptakan sub-kelompok tambahan dalam jaringan IP yang memfasilitasi pengiriman paket lebih cepat dan penyaringan tambahan, dengan membantu meminimalkan lalu lintas 'lokal'.

Bab ini membahas, secara rinci, pembuatan dan penugasan jaringan IP dan alamat subnetwork melalui penggunaan subnet mask.

8.2 SUBNETTING IPv4 NETWORK

- ❖ **NETWORK SEGMENTATION**
- **BROADCAST DOMAINS**

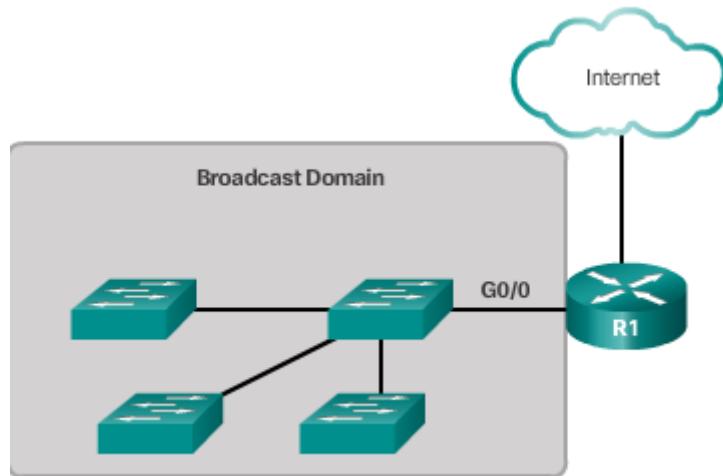
Di LAN Ethernet, perangkat menggunakan broadcast untuk mencari:

- ✓ **Other devices** - Perangkat menggunakan Address Resolution Protocol (ARP) yang mengirim broadcast Layer 2 ke alamat IPv4 yang diketahui pada jaringan lokal untuk menemukan alamat MAC yang terkait.
- ✓ **Layanan** - Host biasanya memperoleh konfigurasi alamat IP-nya menggunakan Dynamic Host Configuration Protocol (DHCP) yang mengirim siaran di jaringan lokal untuk mencari server DHCP.

Switch menyebarkan siaran semua antarmuka kecuali antarmuka yang menerimanya. Misalnya, jika sebuah tombol pada gambar tersebut menerima siaran, ia akan meneruskannya ke switch lain dan pengguna lain yang terhubung dalam jaringan.

Router tidak menyebarkan siaran. Saat router menerima siaran, ia tidak meneruskannya dari antarmuka lain. Misalnya, ketika R1 menerima siaran pada antarmuka Gigabit Ethernet 0/0 nya, ia tidak meneruskan antarmuka lain.

Oleh karena itu, setiap antarmuka router menghubungkan broadcast domain dan broadcast hanya disebarluaskan dalam domain broadcast spesifiknya.

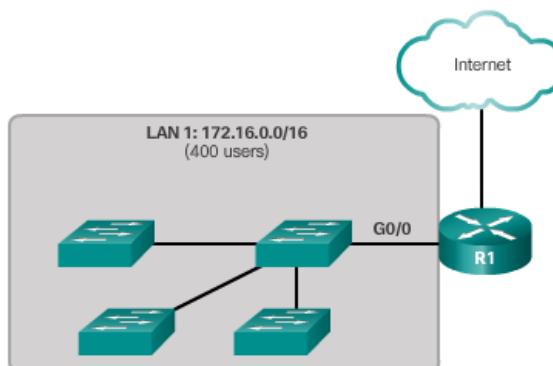


- **PROBLEM WITH LARGE BROADCAST DOMAINS**

Sebuah domain broadcast besar adalah jaringan yang menghubungkan banyak host. Masalah dengan domain siaran besar adalah host tersebut dapat menghasilkan siaran yang berlebihan dan berdampak negatif terhadap jaringan. Pada Gambar dibawah, LAN 1 menghubungkan 400 pengguna yang dapat menghasilkan lalu lintas siaran yang menghasilkan:

- ✓ Operasi jaringan yang lambat karena jumlah lalu lintas yang signifikan yang dapat menyebabkannya
- ✓ Operasi perangkat yang lambat karena perangkat harus menerima dan memproses setiap paket siaran

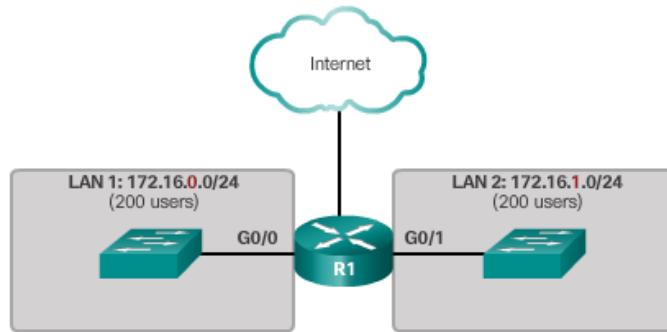
Solusinya adalah mengurangi ukuran jaringan untuk menciptakan domain broadcast yang lebih kecil dalam proses yang disebut **subnetting**. Ruang jaringan yang lebih kecil ini disebut **subnet**



Pada Gambar dibawah misalnya, 400 pengguna di LAN 1 dengan alamat jaringan 172.16.0.0 / 16 telah dibagi menjadi dua subnet dari 200 pengguna; 172.16.0.0 / 24 dan 172.16.1.0 / 24. Siaran hanya disebarluaskan dalam domain siaran yang lebih kecil. Oleh karena itu siaran di LAN 1 tidak akan menyebar ke LAN 2.

Perhatikan bagaimana panjang awalan telah berubah dari a / 16 ke a / 24. Ini adalah dasar subnetting; menggunakan bit host untuk membuat subnet tambahan.

Catatan: Istilah subnet dan jaringan sering digunakan secara bergantian. Sebagian besar jaringan adalah subnet dari beberapa blok alamat yang lebih besar.

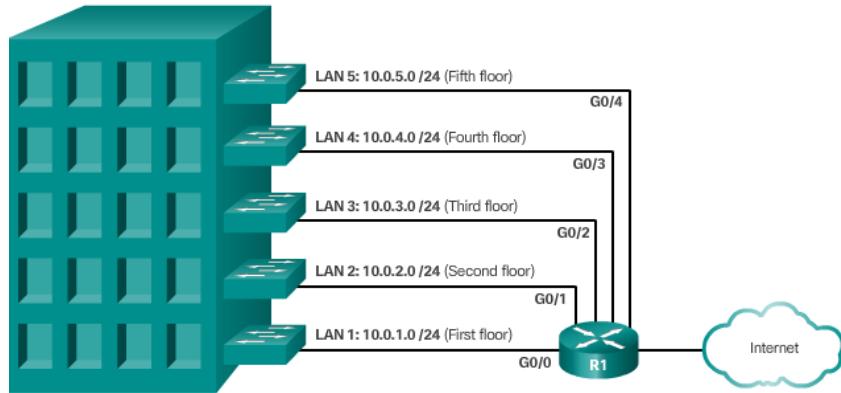


- **REASONS FOR SUBNETTING**

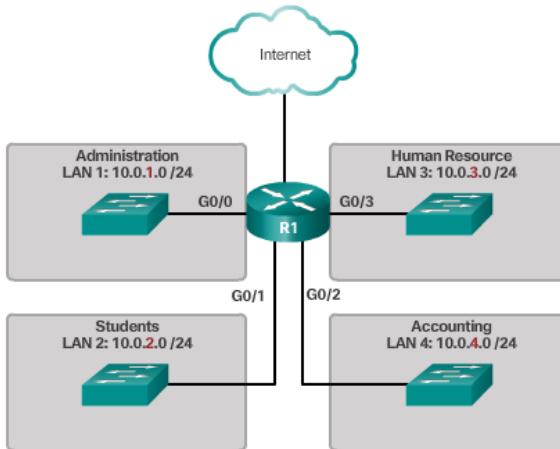
Subnetting mengurangi lalu lintas jaringan secara keseluruhan dan meningkatkan kinerja jaringan. Ini juga memungkinkan administrator untuk menerapkan kebijakan keamanan seperti subnet yang diizinkan atau tidak diizinkan berkomunikasi bersama.

Ada berbagai cara menggunakan subnet untuk membantu mengelola perangkat jaringan. Administrator jaringan dapat mengelompokkan perangkat dan layanan menjadi subnet yang ditentukan oleh:

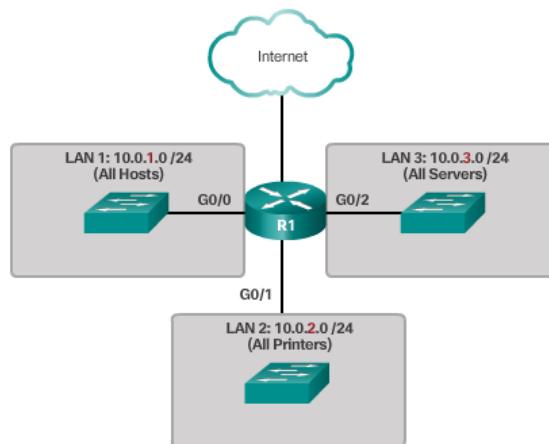
- ✓ **Location, such as floors in a building**



✓ Unit organisasi



✓ Device type



✓ Any other division that makes sense for the network

Perhatikan di setiap gambar, subnet menggunakan panjang awalan yang lebih lama untuk mengidentifikasi jaringan.

Bab ini menjelaskan bagaimana subnetting dilakukan. Memahami bagaimana jaringan subnet adalah keterampilan mendasar yang harus dimiliki oleh semua administrator jaringan. Berbagai metode telah dikembangkan untuk membantu memahami proses ini. Bab ini akan berfokus pada melihat metode biner. Meski sedikit banyak pada awalnya, fokus dan perhatikan detail dan dengan latihan, subnetting seharusnya menjadi lebih mudah.

❖ SUBNETTING IPv4 NETWORK

- OCTET BOUNDARIES

Setiap interface pada router terhubung ke jaringan. Alamat IP dan subnet mask yang dikonfigurasi pada antarmuka router digunakan untuk mengidentifikasi domain broadcast spesifik. Ingat bahwa panjang prefix dan subnet mask berbeda cara untuk mengidentifikasi bagian jaringan dari sebuah alamat.

Subnet IPv4 dibuat dengan menggunakan satu atau beberapa bit host sebagai bit jaringan. Hal ini dilakukan dengan memperluas subnet mask untuk meminjam beberapa bit dari bagian

host dari alamat untuk membuat bit jaringan tambahan. Semakin banyak bit host yang dipinjam, semakin banyak subnet yang bisa didefinisikan.

Jaringan paling mudah subnetted pada batas oktet / 8, / 16, dan / 24. Tabel pada gambar mengidentifikasi panjang awalan ini, subnet mask setara, bit jaringan dan host, dan jumlah host yang masing-masing subnet dapat terhubung. Perhatikan bahwa menggunakan panjang awalan yang lebih lama menurunkan jumlah host per subnet.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	255.0.0.0	<code>nnnnnnnn . hhhhhh . hhhhhh . hhhhhh 11111111 . 00000000 . 00000000 . 00000000</code>	16,777,214
/16	255.255.0.0	<code>nnnnnnnn . nnnnnnnn . hhhhhh . hhhhhh 11111111 . 11111111 . 00000000 . 00000000</code>	65,534
/24	255.255.255.0	<code>nnnnnnnn . nnnnnnnn . nnnnnnnn . hhhhhh 11111111 . 11111111 . 11111111 . 00000000</code>	254

• SUBNETTING ON THE OCTET BOUNDARIES

Untuk memahami bagaimana subnetting pada batas oktet bisa bermanfaat, perhatikan contoh berikut. Asumsikan sebuah perusahaan telah memilih alamat pribadi 10.0.0.0/8 sebagai alamat jaringan internalnya. Alamat jaringan tersebut dapat menghubungkan 16.777.214 host dalam satu domain broadcast. Jelas, ini tidak ideal.

Perusahaan dapat subnet lebih lanjut alamat 10.0.0.0/8 pada batas oktet 16/16 seperti yang ditunjukkan pada Gambar dibawah. Ini akan memberi perusahaan kemampuan untuk mendefinisikan 256 subnet (yaitu, 10.0.0.0/16 - 10.255.0.0 / 16) dengan masing-masing subnet mampu menghubungkan 65.534 host. Perhatikan bagaimana dua oktet pertama mengidentifikasi bagian jaringan dari alamat sementara dua oktet terakhir adalah untuk alamat IP host.

Subnet Address (256 Possible Subnets)	Host Range (65,534 possible hosts per subnet)	Broadcast
<u>10.0.0.0/16</u>	<u>10.0.0.1 - 10.0.255.254</u>	<u>10.0.255.255</u>
<u>10.1.0.0/16</u>	<u>10.1.0.1 - 10.1.255.254</u>	<u>10.1.255.255</u>
<u>10.2.0.0/16</u>	<u>10.2.0.1 - 10.2.255.254</u>	<u>10.2.255.255</u>
<u>10.3.0.0/16</u>	<u>10.3.0.1 - 10.3.255.254</u>	<u>10.3.255.255</u>
<u>10.4.0.0/16</u>	<u>10.4.0.1 - 10.4.255.254</u>	<u>10.4.255.255</u>
<u>10.5.0.0/16</u>	<u>10.5.0.1 - 10.5.255.254</u>	<u>10.5.255.255</u>
<u>10.6.0.0/16</u>	<u>10.6.0.1 - 10.6.255.254</u>	<u>10.6.255.255</u>
<u>10.7.0.0/16</u>	<u>10.7.0.1 - 10.7.255.254</u>	<u>10.7.255.255</u>
...
<u>10.255.0.0/16</u>	<u>10.255.0.1 - 10.255.255.254</u>	<u>10.255.255.255</u>

Sebagai alternatif, perusahaan dapat memilih subnet pada batas 24 oktet seperti yang ditunjukkan pada Gambar dibawah. Hal ini memungkinkan perusahaan untuk menentukan 65.536 subnet yang masing-masing mampu menghubungkan 254 host. Batas / 24 sangat populer di subnetting karena mengakomodasi jumlah host yang masuk akal dan subnet yang nyaman di batas oktet.

Subnet Address (65,536 Possible Subnets)	Host Range (254 possible hosts per subnet)	Broadcast
<u>10.0.0.0/24</u>	<u>10.0.0.1 – 10.0.0.254</u>	<u>10.0.0.255</u>
<u>10.0.1.0/24</u>	<u>10.0.1.1 – 10.0.1.254</u>	<u>10.0.1.255</u>
<u>10.0.2.0/24</u>	<u>10.0.2.1 – 10.0.2.254</u>	<u>10.0.1.255</u>
...
<u>10.0.255.0/24</u>	<u>10.0.255.1 – 10.0.255.254</u>	<u>10.0.255.255</u>
<u>10.1.0.0/24</u>	<u>10.1.0.1 – 10.1.0.254</u>	<u>10.1.0.255</u>
<u>10.1.1.0/24</u>	<u>10.1.1.1 – 10.1.1.254</u>	<u>1.1.1.0.255</u>
<u>10.1.2.0/24</u>	<u>10.1.2.1 – 10.1.2.254</u>	<u>10.1.2.0.255</u>
...
<u>10.100.0.0/24</u>	<u>10.100.0.1 – 10.100.0.254</u>	<u>10.100.0.255</u>
...
<u>10.255.255.0/24</u>	<u>10.255.255.1 – 10.255.255.254</u>	<u>10.255.255.255</u>

• CLASSLESS SUBNETTING

Contoh yang terlihat sejauh ini meminjam bit host dari awalan jaringan umum / 8, / 16 dan / 24. Namun, subnet dapat meminjam bit dari posisi bit host untuk membuat topeng lainnya. Sebagai contoh, alamat jaringan a / 24 biasanya disebarluaskan menggunakan awalan panjang yang lebih panjang dengan meminjam bit dari oktet keempat. Ini memberi administrator fleksibilitas tambahan saat menetapkan alamat jaringan ke sejumlah perangkat akhir yang lebih kecil. Seperti yang ditunjukkan pada gambar:

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn. n hhhhh 11111111.11111111.11111111. 1 0000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn. nn hhhhh 11111111.11111111.11111111. 11 000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn. nnn hhhhh 11111111.11111111.11111111. 111 00000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn. nnnn hhhh 11111111.11111111.11111111. 1111 0000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn. nnnn hh 11111111.11111111.11111111. 11111 000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn. nnnnn hh 11111111.11111111.11111111. 111111 00	64	2

- ✓ /25 row - Borrowing 1 bit from the fourth octet creates 2 subnets supporting 126 hosts each.
- ✓ /26 row - Borrowing 2 bits creates 4 subnets supporting 62 hosts each.
- ✓ /27 row – Borrowing 3 bits creates 8 subnets supporting 30 hosts each.
- ✓ /28 row – Borrowing 4 bits creates 16 subnets supporting 14 hosts each.
- ✓ /29 row – Borrowing 5 bits creates 32 subnets supporting 6 hosts each.
- ✓ /30 row – Borrowing 6 bits creates 64 subnets supporting 2 hosts each.

Untuk setiap bit yang dipinjam pada oktet keempat, jumlah subnetwork yang tersedia dua kali lipat sekaligus mengurangi jumlah alamat host per subnet.

- CLASSLESS SUBNETTING EXAMPLE

Untuk memahami bagaimana subnetting pada tingkat tanpa kelas bisa bermanfaat, perhatikan contoh berikut.

Perhatikan alamat jaringan pribadi 192.168.1.0/24 yang ditunjukkan pada Gambar dibawah. Tiga oktet pertama ditampilkan dalam desimal, sedangkan oktet terakhir ditampilkan dalam biner. Alasan untuk ini adalah karena kita akan meminjam bit dari oktet terakhir untuk membuat subnet dari jaringan 192.168.1.0/24.

192.168.1.0/24 Network

Address	192	168	1	0000	0000
Mask	255	255	255	0000	0000
					Network Portion Host Portion

With no host bits borrowed, the host portion of both the network address and mask are all 0 bits.

Subnet mask adalah 255.255.255.0 seperti yang ditunjukkan oleh / 24 awalan panjang. Ini mengidentifikasi tiga oktet pertama sebagai bagian jaringan dan 8 bit sisanya pada oktet terakhir sebagai bagian host. Tanpa subnet, jaringan ini mendukung satu antarmuka LAN yang menyediakan 254 alamat IP host. Jika LAN tambahan dibutuhkan, jaringan perlu subnetted.

Pada Gambar dibawah, 1 bit dipinjam dari bit paling signifikan (bit paling kiri) pada bagian host, sehingga memperpanjang bagian jaringan menjadi 25 bit atau / 25. Hal ini memungkinkan terciptanya dua subnet.

192.168.1.0/25 Network

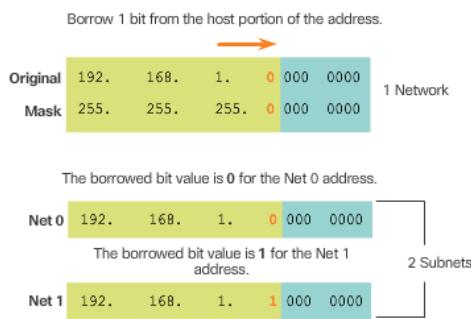
Borrow 1 bit from the host portion of the address.



Original	192.	168.	1.	0	000	0000	1 Network
Mask	255.	255.	255.	0	000	0000	

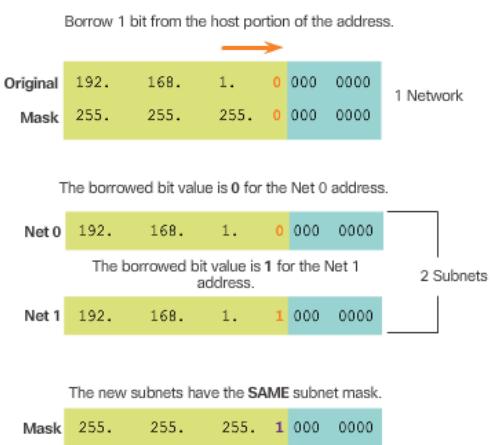
Gambar dibawah menampilkan dua subnet: 192.168.1.0/25 dan 192.168.1.128/25. Dua subnet diturunkan dari perubahan nilai bit yang dipinjam ke 0 atau 1. Karena bit yang dipinjam adalah 128 bit, nilai desimal dari oktet keempat untuk subnet ke-2 adalah 128.

192.168.1.0/25 Network



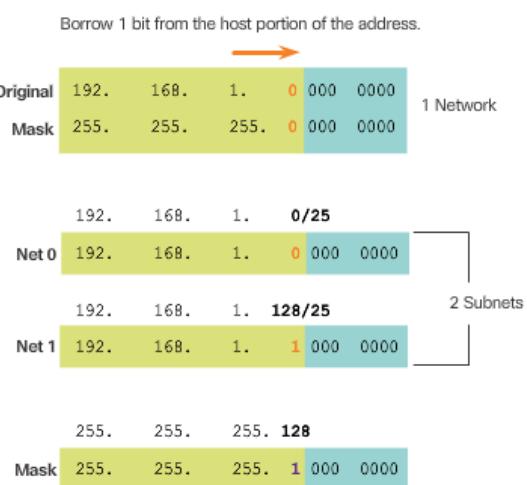
Gambar dibawah menampilkan subnet mask yang dihasilkan untuk kedua jaringan. Perhatikan bagaimana menggunakan 1 dalam posisi bit yang dipinjam untuk menunjukkan bahwa bit ini sekarang merupakan bagian dari bagian jaringan.

192.168.1.0/25 Network



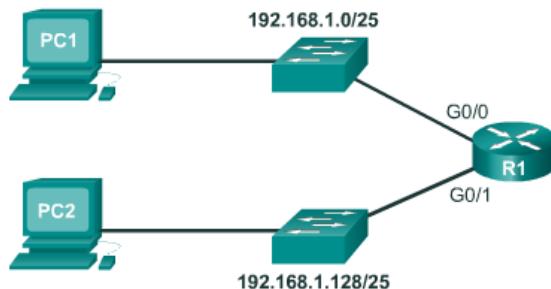
Gambar dibawah menampilkan representasi desimal bertitik dari dua alamat subnet dan subnet mask bersama mereka. Karena satu bit telah dipinjam, subnet mask untuk masing-masing subnet adalah 255.255.255.128 or / 25.

Dotted Decimal Addresses



- **CREATING 2 SUBNETS**

Untuk melihat bagaimana a / 25 subnet diterapkan dalam jaringan; pertimbangkan topologi pada Gambar dibawah. R1 memiliki dua segmen LAN yang terhubung ke antarmuka GigabitEthernet-nya. Setiap LAN ditugaskan salah satu subnet.



Alamat dari subnet pertama, 192.168.1.0/25. Perhatikan bagaimana:

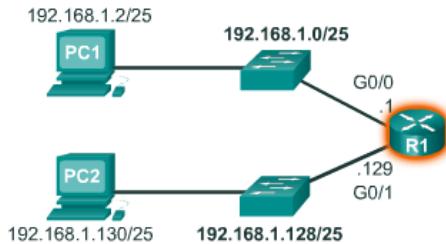
- ✓ **Network address** adalah 192.168.1.0 dan berisi semua 0 bit di bagian host dari alamat.
- ✓ **First host address** adalah 192.168.1.1 dan berisi semua 0 bit ditambah bit paling kanan 1 di bagian host dari alamat.
- ✓ **Last host address** adalah 192.168.1.126 dan berisi semua 1 bit ditambah bit paling kanan 0 di bagian host dari alamat.
- ✓ **Broadcast address** adalah 192.168.1.127 dan berisi semua 1 bit di bagian host dari alamat.

Network Address	<table border="1"><tr><td>192.</td><td>168.</td><td>1.</td><td>0</td><td>000 0000</td></tr></table>	192.	168.	1.	0	000 0000	= 192.168.1.0
192.	168.	1.	0	000 0000			
First Host Address	<table border="1"><tr><td>192.</td><td>168.</td><td>1.</td><td>0</td><td>000 0001</td></tr></table>	192.	168.	1.	0	000 0001	= 192.168.1.1
192.	168.	1.	0	000 0001			
Last Host Address	<table border="1"><tr><td>192.</td><td>168.</td><td>1.</td><td>0</td><td>111 1110</td></tr></table>	192.	168.	1.	0	111 1110	= 192.168.1.126
192.	168.	1.	0	111 1110			
Broadcast Address	<table border="1"><tr><td>192.</td><td>168.</td><td>1.</td><td>0</td><td>111 1111</td></tr></table>	192.	168.	1.	0	111 1111	= 192.168.1.127
192.	168.	1.	0	111 1111			

Alamat dari subnet kedua, 192.168.1.128/25.

Network Address	<table border="1"><tr><td>192.</td><td>168.</td><td>1.</td><td>1</td><td>000 0000</td></tr></table>	192.	168.	1.	1	000 0000	= 192.168.1.128
192.	168.	1.	1	000 0000			
First Host Address	<table border="1"><tr><td>192.</td><td>168.</td><td>1.</td><td>1</td><td>000 0001</td></tr></table>	192.	168.	1.	1	000 0001	= 192.168.1.129
192.	168.	1.	1	000 0001			
Last Host Address	<table border="1"><tr><td>192.</td><td>168.</td><td>1.</td><td>1</td><td>111 1110</td></tr></table>	192.	168.	1.	1	111 1110	= 192.168.1.254
192.	168.	1.	1	111 1110			
Broadcast Address	<table border="1"><tr><td>192.</td><td>168.</td><td>1.</td><td>1</td><td>111 1111</td></tr></table>	192.	168.	1.	1	111 1111	= 192.168.1.255
192.	168.	1.	1	111 1111			

Antarmuka router harus diberi alamat IP dalam kisaran host yang valid untuk subnet yang ditugaskan. Ini adalah alamat yang host pada jaringan tersebut akan digunakan sebagai gateway default mereka. Praktik yang sangat umum adalah menggunakan alamat pertama atau terakhir yang tersedia dalam jangkauan jaringan untuk alamat antarmuka router. Gambar dibawah menunjukkan konfigurasi untuk antarmuka R1 dengan alamat IP pertama untuk subnet masing-masing menggunakan perintah konfigurasi antarmuka alamat ip.

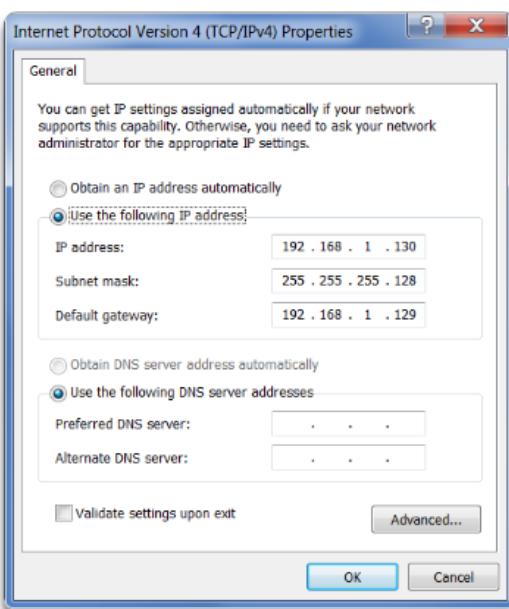


```

R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.128
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ip address 192.168.1.129 255.255.255.128
  
```

Host pada setiap subnet harus dikonfigurasi dengan alamat IP dan gateway default. Gambar dibawah menampilkan konfigurasi IP untuk host PC2 pada jaringan 192.168.1.128/25. Perhatikan bahwa alamat IP gateway default adalah alamat yang dikonfigurasikan pada antarmuka G0 / 1 dari R1, 192.168.1.129, dan subnet mask adalah 255.255.255.128.

Assign a Valid Host IP Address



- **SUBNETTING FORMULAS**

Untuk menghitung jumlah subnet yang dapat dibuat dari bit yang dipinjam, gunakan rumus yang ditunjukkan pada Gambar – gambar dibawah menampilkan kemungkinan jumlah subnet yang dapat dibuat saat meminjam 1, 2, 3, 4, 5, atau 6 bit.



Catatan: Dua bit terakhir tidak dapat dipinjam dari oktet terakhir karena tidak akan ada alamat host yang tersedia. Oleh karena itu, panjang awalan terpanjang mungkin saat subnetting adalah / 30 atau 255.255.255.252.

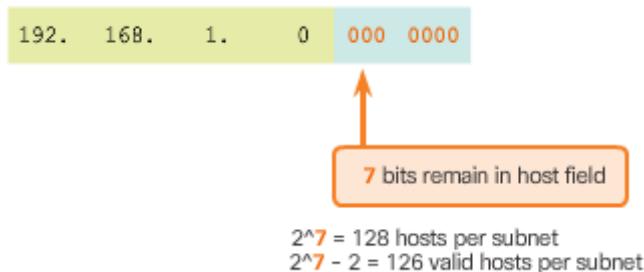
Untuk menghitung jumlah host yang bisa didukung, gunakan rumus yang ditunjukkan pada Gambar dibawah. Ada dua alamat subnet yang tidak bisa ditugaskan ke host, alamat jaringan dan alamat broadcast, jadi kita harus kurang 2.

$$2^{n-2}$$

n = the number of bits remaining in the host field

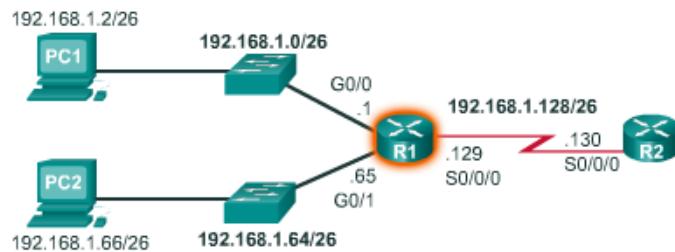
Seperti ditunjukkan pada Gambar dibawah, ada 7 bit host yang tersisa, jadi penghitungannya adalah $2^7 = 128 - 2 = 126$. Ini berarti masing-masing subnet memiliki 126 alamat host yang valid.

Oleh karena itu, meminjam 1 bit host ke jaringan menghasilkan 2 subnet, dan setiap subnet dapat memiliki total 126 host yang ditugaskan.



- CREATING 4 SUBNETS

Sekarang perhatikan topologi jaringan yang ditunjukkan pada Gambar dibawah. Perusahaan menggunakan alamat jaringan pribadi 192.168.1.0/24 dan memerlukan tiga subnet.



Meminjam satu bit hanya menyediakan 2 subnet; Oleh karena itu, bit host lain harus dipinjam seperti yang ditunjukkan pada Gambar dibawah. Menggunakan rumus 2^n untuk dua bit yang dipinjam menghasilkan $2^2 = 4$ subnet.

Borrowing 2 Bits

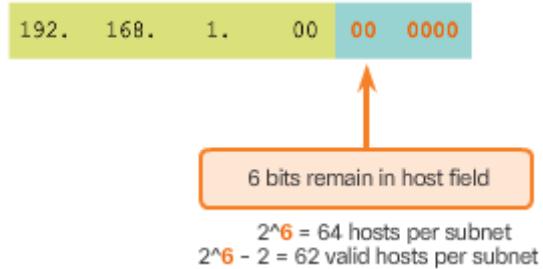
Borrowing 2 Bits							
Original	192.	168.	1.	00	00	0000	
Mask	255.	255.	255.	00	00	0000	

Spesifik dari empat subnet ditunjukkan pada Gambar dibawah. Subnet mask yang dihasilkan pada /26 atau 255.255.255.192 digunakan oleh keempat subnet.

Borrowing 2 Bits

Borrowing 2 Bits							
Original	192.	168.	1.	00	00	0000	
Mask	255.	255.	255.	00	00	0000	
Borrowing 2 bits creates 4 subnets:							
Net 0	192.	168.	1.	00	00	0000	192.168.1.0/26
Net 1	192.	168.	1.	01	00	0000	192.168.1.64/26
Net 2	192.	168.	1.	10	00	0000	192.168.1.128/26
Net 3	192.	168.	1.	11	00	0000	192.168.1.192/26
All 4 subnets use the same mask:							
Mask	255.	255.	255.	11	00	0000	Mask:255.255.255.192

Untuk menghitung jumlah host, periksa oktet terakhir seperti yang ditunjukkan pada Gambar dibawah. Setelah meminjam 2 bit untuk subnet, ada 6 bit host yang tersisa. Terapkan rumus penghitungan host $2^n - 2$ seperti yang ditunjukkan untuk mengungkapkan bahwa setiap subnet dapat mendukung 62 alamat host.



Alamat penting dari subnet pertama (yaitu, Net 0) akan ditampilkan pada Gambar dibawah.

Address Range for 192.168.1.0/26 Subnet

Network Address	192. 168. 1. 00 00 0000	= 192.168.1.0
First Host Address	192. 168. 1. 00 00 0001	= 192.168.1.1
Last Host Address	192. 168. 1. 00 11 1110	= 192.168.1.62
Broadcast Address	192. 168. 1. 00 11 1111	= 192.168.1.63

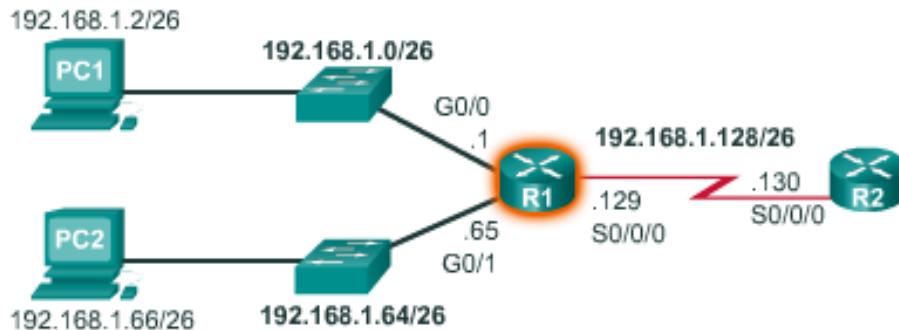
Hanya tiga subnet pertama yang dibutuhkan karena hanya ada tiga antarmuka. Gambar dibawah menampilkan spesifik dari tiga subnet pertama yang akan digunakan untuk memenuhi topologi pada Gambar awal.

Address Ranges Nets 0 - 2

Net 0	Network	192. 168. 1. 00 00 0000	192.168.1.0
	First	192. 168. 1. 00 00 0001	192.168.1.1
	Last	192. 168. 1. 00 11 1110	192.168.1.62
	Broadcast	192. 168. 1. 00 11 1111	192.168.1.63
Net 1	Network	192. 168. 1. 01 00 0000	192.168.1.64
	First	192. 168. 1. 01 00 0001	192.168.1.65
	Last	192. 168. 1. 01 11 1110	192.168.1.126
	Broadcast	192. 168. 1. 01 11 1111	192.168.1.127
Net 2	Network	192. 168. 1. 10 00 0000	192.168.1.128
	First	192. 168. 1. 10 00 0001	192.168.1.129
	Last	192. 168. 1. 10 11 1110	192.168.1.190
	Broadcast	192. 168. 1. 10 11 1111	192.168.1.191

Akhirnya, Gambar dibawah menerapkan alamat host yang valid pertama dari masing-masing subnet ke masing-masing antarmuka LAN R1.

Configuring the Interfaces with /26 Addresses



```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.192
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ip address 192.168.1.65 255.255.255.192
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 192.168.1.129 255.255.255.192
```

❖ SUBNETTING a/16 AND /8 PREFIX

- CREATING SUBNETS WITH a/16 PREFIX

Dalam situasi yang membutuhkan jumlah subnet yang lebih besar, dibutuhkan jaringan IP yang memiliki bit host lebih banyak untuk dipinjam. Misalnya, alamat jaringan 172.16.0.0 memiliki topeng default 255.255.0.0, atau /16. Alamat ini memiliki 16 bit di bagian jaringan dan 16 bit di bagian host. 16 bit di bagian host tersedia untuk dipinjam karena membuat subnet. Tabel di gambar menyoroti semua skenario yang mungkin untuk awalan subnetting a /16.

Meskipun penghafalan tabel tidak diperlukan, disarankan agar Anda memahami dengan baik bagaimana masing-masing nilai dalam tabel dihasilkan. Jangan biarkan ukuran meja mengintimidasi Anda. Alasannya besar adalah karena memiliki 8 bit tambahan yang bisa dipinjam, dan oleh karena itu, jumlah subnet dan host cukup besar.

Subnetting a /24 Network

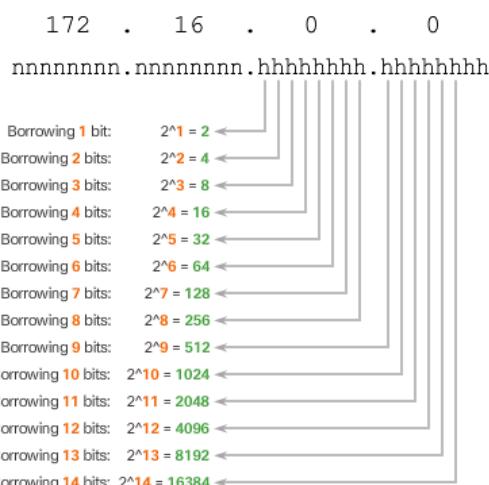
Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.10000000.00000000	2	32564
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.11000000.00000000	4	16282
/19	255.255.224.0	nnnnnnnn.nnnnnnnn.nnnhhhhh.hhhhhhhh 11111111.11111111.11100000.00000000	8	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn.nnnnhhhh.hhhhhhhh 11111111.11111111.11110000.00000000	16	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn.nnnnnhhh.hhhhhhhh 11111111.11111111.11111000.00000000	32	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn.nnnnnnhh.hhhhhhhh 11111111.11111111.11111100.00000000	64	1022
/23	255.255.254.0	nnnnnnnn.nnnnnnnn.nnnnnnnh.hhhhhhhh 11111111.11111111.11111110.00000000	128	510
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	256	254
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	512	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.11000000	1024	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	2048	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	4096	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhh 11111111.11111111.11111111.11111000	8192	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnnh 11111111.11111111.11111111.11111100	16384	2

- **CREATING 100 SUBNETS WITH a/16 NETWORK**

Misalkan sebuah perusahaan besar yang membutuhkan setidaknya 100 subnet dan telah memilih alamat pribadi 172.16.0.0/16 sebagai alamat jaringan internalnya.

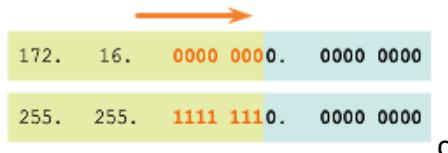
Saat meminjam bit dari alamat / 16, mulailah meminjam bit pada oktet ketiga, dari kiri ke kanan. Pinjam satu bit pada satu waktu sampai jumlah bit yang diperlukan untuk membuat 100 subnet tercapai.

Gambar dibawah menampilkan jumlah subnet yang dapat dibuat saat meminjam bit dari oktet ketiga dan oktet keempat. Perhatikan sekarang ada hingga 14 bit host yang bisa dipinjam.



Untuk memenuhi persyaratan perusahaan, 7 bit (yaitu, $2^7 = 128$ subnet) perlu dipinjam, seperti yang ditunjukkan pada Gambar dibawah.

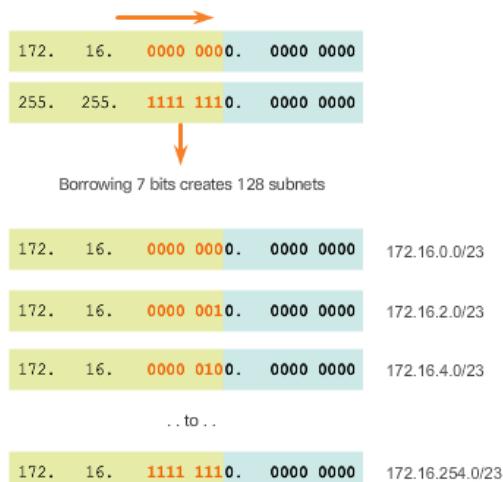
172.16.0.0/23 Network



c

Ingat bahwa subnet mask harus berubah untuk mencerminkan bit yang dipinjam. Dalam contoh ini, ketika 7 bit dipinjam, topeng diperpanjang 7 bit ke oktet ketiga. Dalam desimal, topeng diwakili sebagai 255.255.254.0, atau awalan / 23, karena oktet ketiga adalah 11111110 dalam biner dan oktet keempat adalah 00000000 dalam biner.

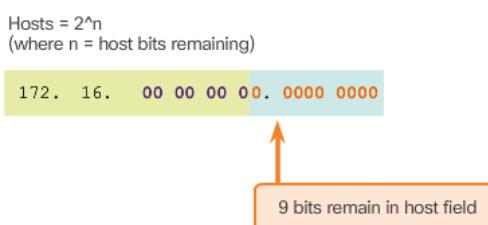
Gambar dibawah menampilkan subnet yang dihasilkan dari 172.16.0.0 / 23 sampai 172.16.254.0 / 23.



- CALCULATING THE HOSTS**

Untuk menghitung jumlah host masing-masing subnet dapat mendukung, periksa oktet ketiga dan keempat. Setelah meminjam 7 bit untuk subnet, ada satu bit host yang tersisa di oktet ketiga dan 8 bit host yang tersisa pada oktet keempat dengan total 9 bit yang tidak dipinjam.

Terapkan rumus penghitungan host seperti yang ditunjukkan pada Gambar dibawah. Hanya ada 510 alamat host yang tersedia untuk masing-masing / 23 subnet.



$$2^9 = 512 \text{ hosts per subnet}$$

$$2^9 - 2 = 510 \text{ valid hosts per subnet}$$

Seperti ditunjukkan pada Gambar dibawah, alamat host pertama untuk subnet pertama adalah 172.16.0.1, dan alamat host terakhir adalah 172.16.1.254.

Network Address	172. 16. 00 00 00 00. 0000 0000	= 172.16.0.0/23
First Host Address	172. 16. 00 00 00 00. 0000 0001	= 172.16.0.1/23
Last Host Address	172. 16. 00 00 00 01. 1111 1110	= 172.16.1.254/23
Broadcast Address	172. 16. 00 00 00 01. 1111 1111	= 172.16.1.255/23

❖ SUBNETTING TO MEET REQUIREMENTS

• SUBNETTING BASED ON HOST REQUIREMENTS

Inilah dua pertimbangan saat merencanakan subnet:

- ✓ jumlah alamat host yang dibutuhkan untuk setiap jaringan
- ✓ jumlah subnet masing-masing dibutuhkan

Tabel pada gambar menampilkan spesifik untuk subnetting a / 24 network. Perhatikan bagaimana ada hubungan terbalik antara jumlah subnet dan jumlah host. Semakin banyak bit yang dipinjam untuk membuat subnet, semakin sedikit bit host yang tersedia. Jika diperlukan lebih banyak alamat host, diperlukan lebih banyak bit host, yang menghasilkan subnet lebih sedikit.

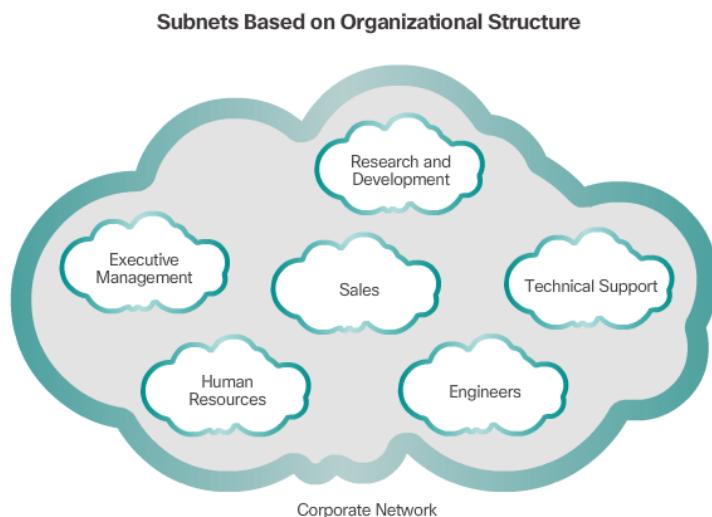
Jumlah alamat host yang dibutuhkan di subnet terbesar akan menentukan berapa bit yang tersisa di bagian host. Ingat bahwa dua alamat tidak dapat digunakan, sehingga jumlah alamat yang dapat digunakan dapat dihitung sebagai $2^n - 2$.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn. n hhhhh 11111111.11111111.11111111. 1 0000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn. nn hhhhh 11111111.11111111.11111111. 11 000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn. nnn hhh 11111111.11111111.11111111. 111 00000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn. nnnn hh 11111111.11111111.11111111. 1111 0000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn. nnnnn hh 11111111.11111111.11111111. 11111 000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn. nnnnnn hh 11111111.11111111.11111111. 111111 00	64	2

- **SUBNETTING BASED ON NETWORK REQUIREMENTS**

Terkadang sejumlah subnet diperlukan, dengan sedikit penekanan pada jumlah alamat host per subnet. Ini mungkin terjadi jika sebuah organisasi memilih untuk memisahkan lalu lintas jaringan mereka berdasarkan struktur internal atau pengaturan departemen, seperti yang ditunjukkan pada gambar. Misalnya, sebuah organisasi dapat memilih untuk meletakkan semua perangkat host yang digunakan oleh karyawan di departemen Teknik dalam satu jaringan, dan semua perangkat host yang digunakan oleh manajemen dalam jaringan terpisah. Dalam kasus ini, jumlah subnet paling penting dalam menentukan berapa banyak bit yang harus dipinjam.

Ingat jumlah subnet yang dibuat saat bit dipinjam dapat dihitung dengan menggunakan rumus 2^n (di mana n adalah jumlah bit yang dipinjam). Kuncinya adalah menyeimbangkan jumlah subnet yang dibutuhkan dan jumlah host yang dibutuhkan untuk subnet terbesar. Semakin banyak bit yang dipinjam untuk membuat subnet tambahan berarti host yang lebih sedikit tersedia per subnet.



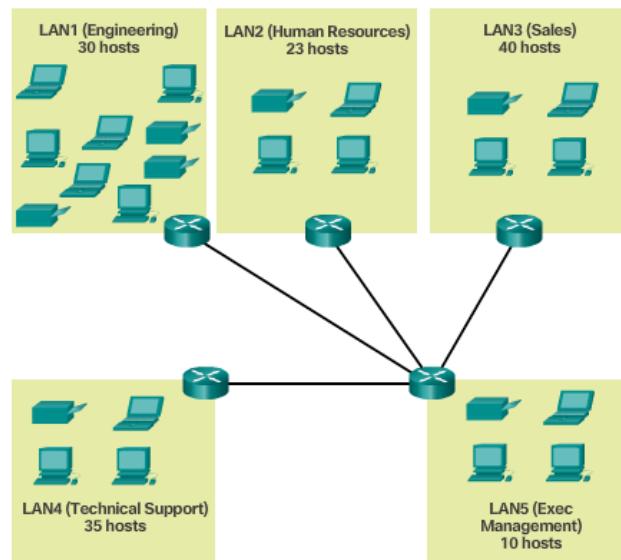
- **NETWORK REQUIREMENTS EXAMPLE**

Administrator jaringan harus merancang skema pengalaman jaringan untuk mengakomodasi jumlah host maksimum untuk setiap jaringan dan jumlah subnet. Skema pengalaman harus memungkinkan untuk pertumbuhan dalam jumlah kedua alamat host per subnet dan jumlah total subnet.

Dalam contoh ini, kantor pusat perusahaan telah mengalokasikan alamat jaringan pribadi 172.16.0.0/22 (10 bit host) ke lokasi cabang. Seperti ditunjukkan pada Gambar dibawah, ini akan menyediakan 1.022 alamat host.

Network portion	Host portion	
10101100.00010100.000000	00.00000000	172.16.0.0/22
10 host bits $2^{10} - 2 = 1,022$ hosts		

Topologi untuk lokasi cabang, ditunjukkan pada Gambar dibawah, terdiri dari 5 segmen LAN dan 4 koneksi internetwork antar router. Oleh karena itu diperlukan 9 subnet. Subnet terbesar membutuhkan 40 host.



Alamat jaringan 172.16.0.0/22 memiliki 10 bit host seperti yang ditunjukkan pada Gambar dibawah. Karena subnet terbesar membutuhkan 40 host, minimal 6 bit host dibutuhkan untuk menangani 40 host. Hal ini ditentukan dengan menggunakan rumus ini: $2^6 - 2 = 62$ host.

Menggunakan rumus untuk menentukan subnet, menghasilkan 16 subnet: $2^4 = 16$. Karena contoh internetwork membutuhkan 9 subnet, ini akan memenuhi persyaratan dan memungkinkan beberapa pertumbuhan tambahan.

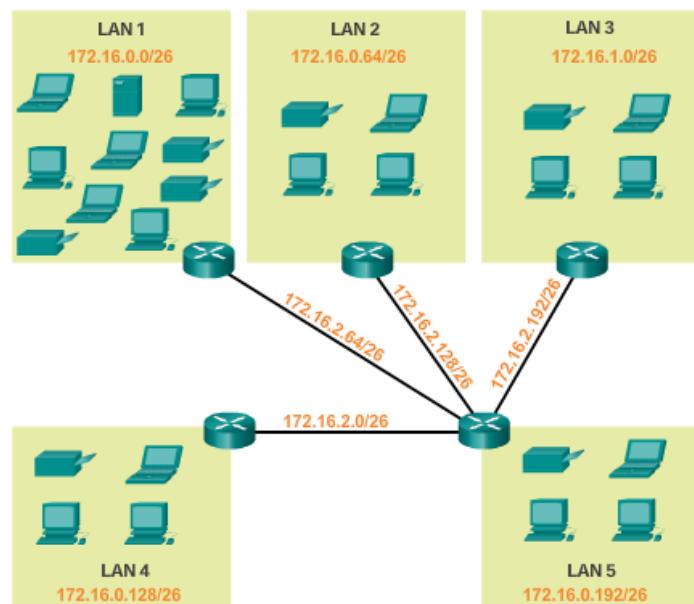
Network Portion	Host Portion	Dotted Decimal
10101100.00010000.000000	00.00 000000	172.16.0.0/22

Oleh karena itu, 4 bit host pertama dapat digunakan untuk mengalokasikan subnet, seperti yang ditunjukkan pada Gambar dibawah. Bila 4 bit dipinjam, awalan awalan baru adalah / 26 dengan subnet mask 255.255.255.192.

	Network Portion	Host Portion	Dotted Decimal
	10101100.00010000.000000	00.00 000000	172.16.0.0/22
0	10101100.00010000.000000	00.00 000000	172.16.0.0/26
1	10101100.00010000.000000	00.01 000000	172.16.0.64/26
2	10101100.00010000.000000	00.10 000000	172.16.0.128/26
3	10101100.00010000.000000	00.11 000000	172.16.0.192/26
4	10101100.00010000.000000	01.00 000000	172.16.1.0/26
5	10101100.00010000.000000	01.01 000000	172.16.1.64/26
6	10101100.00010000.000000	01.10 000000	172.16.1.128/26
Nets 7 - 13 not shown			
14	10101100.00010000.000000	11.10 000000	172.16.3.128/26
15	10101100.00010000.000000	11.11 000000	172.16.3.192/26

4 bits borrowed from host portion to create subnets

Seperti ditunjukkan pada Gambar dibawah, subnet dapat diberikan ke segmen LAN dan koneksi router-ke-router.

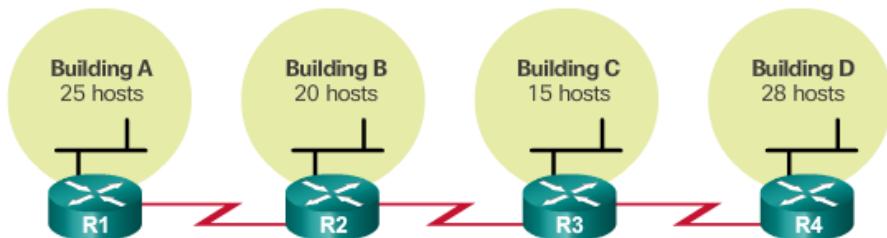


❖ BENEFITS OF VARIABLE LENGTH SUBNET MASKING

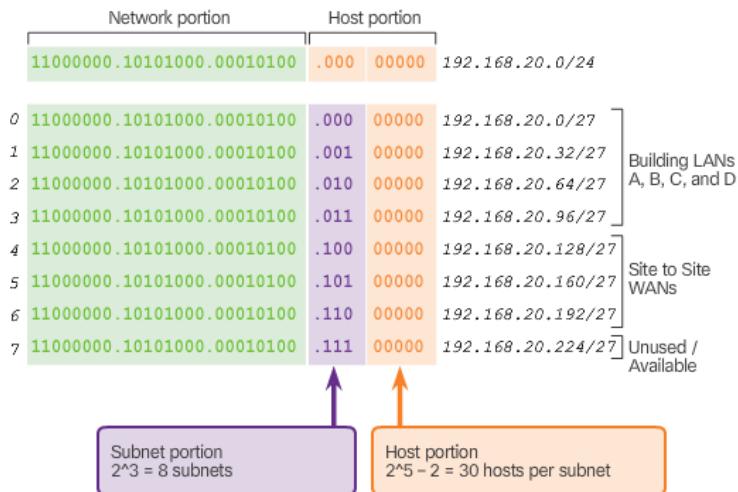
- TRADITIONAL SUBNETTING WASTES ADDRESSES

Dengan menggunakan subnetting tradisional, jumlah alamat yang sama dialokasikan untuk setiap subnet. Jika semua subnet memiliki persyaratan yang sama untuk jumlah host, blok alamat ukuran tetap ini akan efisien. Namun, paling sering itu tidak terjadi.

Sebagai contoh, topologi yang ditunjukkan pada Gambar dibawah membutuhkan tujuh subnet, satu untuk masing-masing dari empat LAN, dan satu untuk masing-masing dari tiga koneksi WAN di antara router.

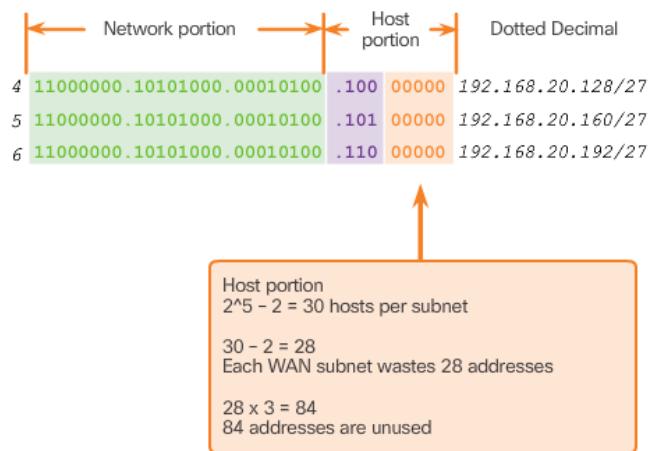


Dengan menggunakan subnetting tradisional dengan alamat 192.168.20.0/24, 3 bit dapat dipinjam dari porsi host pada oktet terakhir untuk memenuhi kebutuhan subnet dari tujuh subnet. Seperti ditunjukkan pada Gambar dibawah, meminjam 3 bit menciptakan 8 subnet dan meninggalkan 5 bit host dengan 30 host yang dapat digunakan per subnet. Skema ini menciptakan subnet yang dibutuhkan dan memenuhi persyaratan host LAN terbesar.



Meskipun subnetting tradisional ini memenuhi kebutuhan LAN terbesar dan membagi ruang alamat menjadi jumlah subnet yang memadai, namun hal ini mengakibatkan pemborosan alamat yang tidak terpakai.

Misalnya, hanya dua alamat yang dibutuhkan di setiap subnet untuk tiga link WAN. Karena setiap subnet memiliki 30 alamat yang dapat digunakan, ada 28 alamat yang tidak terpakai di masing-masing subnet ini. Seperti ditunjukkan pada Gambar dibawah, ini menghasilkan 84 alamat yang tidak terpakai (28×3).



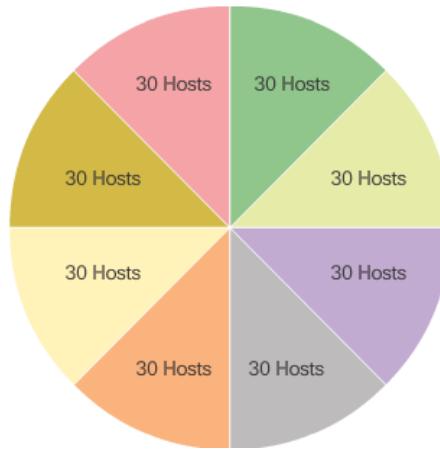
Selanjutnya, ini membatasi pertumbuhan di masa depan dengan mengurangi jumlah subnet yang tersedia. Penggunaan alamat yang tidak efisien ini merupakan ciri subnetting tradisional. Menerapkan skema subnetting tradisional untuk skenario ini tidak terlalu efisien dan boros.

Subnetting subnet, atau menggunakan Variable Length Subnet Mask (VLSM), dirancang untuk menghindari pemborosan alamat.

- **VARIABLE LENGTH SUBNET MASKS**

Dalam semua contoh subnetting sebelumnya, perhatikan bahwa subnet mask yang sama diterapkan untuk semua subnet. Ini berarti bahwa setiap subnet memiliki jumlah alamat host yang sama.

Seperti yang diilustrasikan pada Gambar dibawah, subnetting tradisional menciptakan subnet dengan ukuran yang sama. Setiap subnet dalam skema tradisional menggunakan subnet mask yang sama.

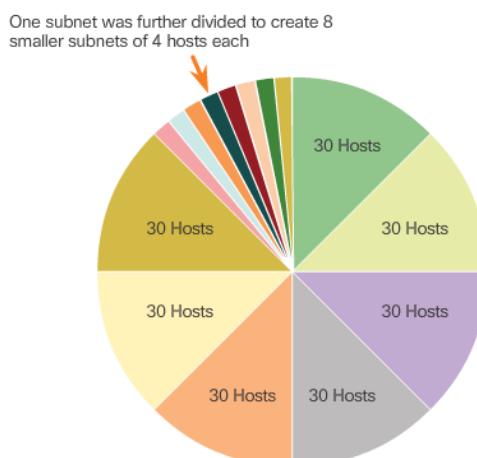


Seperti ditunjukkan pada Gambar dibawah, VLSM memungkinkan ruang jaringan dibagi menjadi bagian yang tidak sama. Dengan VLSM, subnet mask akan bervariasi tergantung pada berapa banyak bit yang telah dipinjam untuk subnet tertentu, sehingga bagian "variabel" dari VLSM.

Subnetting VLSM mirip dengan subnetting tradisional pada bit yang dipinjam untuk membuat subnet. Rumus untuk menghitung jumlah host per subnet dan jumlah subnet yang dibuat masih berlaku.

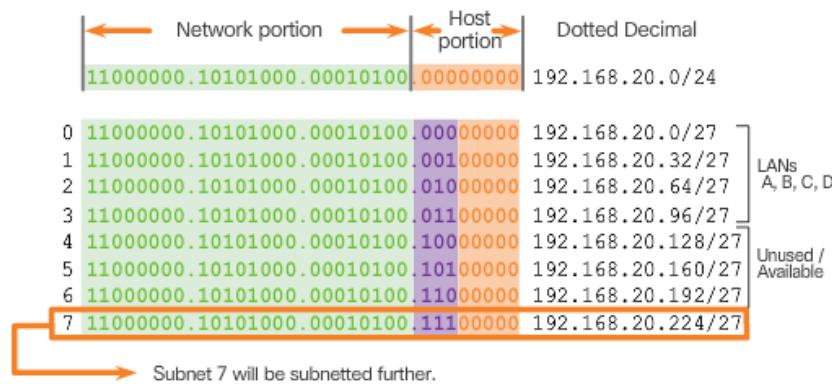
Perbedaannya adalah bahwa subnetting bukan aktivitas single pass. Dengan VLSM, jaringan pertama kali disaring, dan kemudian subnet disaring kembali. Proses ini bisa diulang berkali-kali untuk membuat subnet dengan berbagai ukuran.

Catatan: Bila menggunakan VLSM, selalu mulai dengan memenuhi persyaratan host dari subnet terbesar. Lanjutkan subnetting sampai persyaratan host dari subnet terkecil terpenuhi.



- **BASIC VLSM**

Untuk lebih memahami proses VLSM, kembali ke contoh sebelumnya, yang ditunjukkan pada Gambar dibawah. Jaringan 192.168.20.0/24 telah dibagi menjadi delapan subnet berukuran sama. Tujuh dari delapan subnet dialokasikan. Empat subnet digunakan untuk LAN dan tiga subnet untuk koneksi WAN di antara router. Ingat bahwa ruang alamat terbuang berada di subnet yang digunakan untuk koneksi WAN, karena subnet tersebut hanya membutuhkan dua alamat yang dapat digunakan: satu untuk setiap antarmuka router. Untuk menghindari limbah ini, VLSM dapat digunakan untuk membuat subnet yang lebih kecil untuk koneksi WAN.

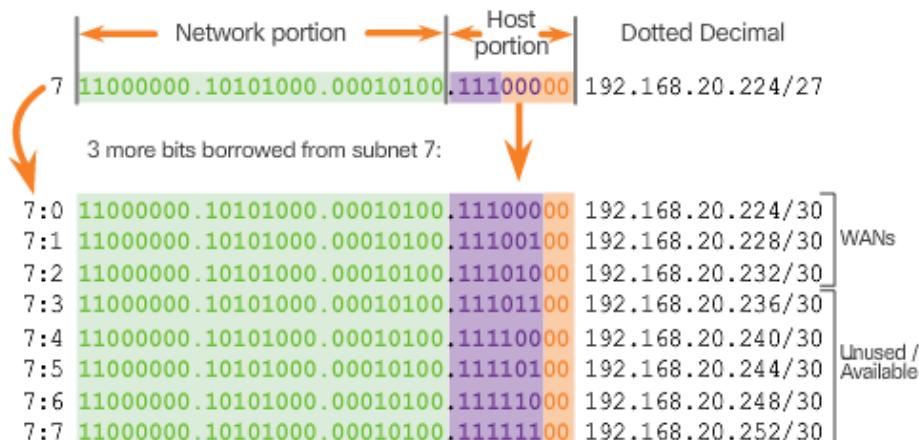


Untuk membuat subnet yang lebih kecil untuk link WAN, salah satu subnet akan dibagi. Dalam contoh ini, subnet terakhir, 192.168.20.224/27, akan di subnetted lebih lanjut.

Inginlah bahwa ketika jumlah alamat host yang dibutuhkan diketahui, rumus $2^n - 2$ (di mana n sama dengan jumlah bit host yang tersisa) dapat digunakan. Untuk menyediakan dua alamat yang dapat digunakan, 2 bit host harus tertinggal di bagian host.

Karena ada 5 bit host di ruang alamat 192.168.20.224/27 subnetted, 3 bit lagi dapat dipinjam, menghasilkan 2 bit di bagian host, seperti yang ditunjukkan pada Gambar dibawah. Perhitungan pada titik ini sama persis dengan yang digunakan untuk subnetting tradisional Bit dipinjam, dan rentang subnet ditentukan.

Skema subnetting VLSM ini mengurangi jumlah alamat per subnet ke ukuran yang sesuai untuk WAN. Subnetting subnet 7 untuk WAN, memungkinkan subnet 4, 5, dan 6 tersedia untuk jaringan masa depan, serta 5 subnet tambahan yang tersedia untuk WAN.



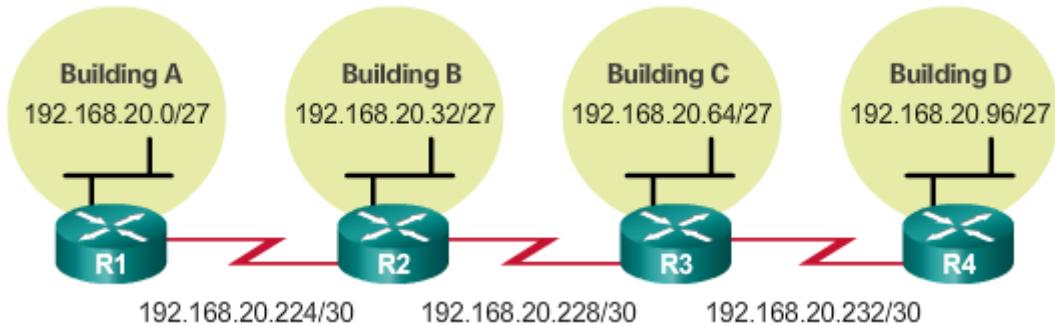
Subnetting a subnet

- **VLSM IN PRACTICE**

Dengan menggunakan subnet VLSM, segmen LAN dan WAN dapat ditangani tanpa limbah yang tidak perlu.

Seperti ditunjukkan pada Gambar dibawah, host di masing-masing LAN akan diberi alamat host yang valid dengan range subnet dan / 27 mask. Masing-masing dari keempat router tersebut akan memiliki interface LAN dengan subnet / 27 dan satu atau lebih interface serial dengan subnet / 30.

Dengan menggunakan skema pengalamanan umum, alamat IPv4 host pertama untuk setiap subnet ditugaskan ke antarmuka LAN router. Antarmuka WAN dari router diberi alamat IP dan topeng untuk / 30 subnet.



Gambar – gambar dibawah menunjukkan konfigurasi antarmuka untuk masing-masing router.

```

R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.20.1 255.255.255.224
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 192.168.20.225 255.255.255.252
R1(config-if)# end
R1#
  
```

```

R2(config)# interface gigabitethernet 0/0
R2(config-if)# ip address 192.168.20.33 255.255.255.224
R2(config-if)# exit
R2(config)# interface serial 0/0/0
R2(config-if)# ip address 192.168.20.226 255.255.255.252
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config-if)# ip address 192.168.20.229 255.255.255.252
R2(config-if)# end
R2#
  
```

```
R3(config)# interface gigabitethernet 0/0
R3(config-if)# ip address 192.168.20.65 255.255.255.224
R3(config-if)# exit
R3(config)# interface serial 0/0/0
R3(config-if)# ip address 192.168.20.230 255.255.255.252
R3(config-if)# exit
R3(config)# interface serial 0/0/1
R3(config)# ip address 192.168.20.233 255.255.255.252
R3(config-if)# end
R3#
```

```
R4(config)# interface gigabitethernet 0/0
R4(config-if)# ip address 192.168.20.97 255.255.255.224
R4(config-if)# exit
R4(config)# interface serial 0/0/0
R4(config-if)# ip address 192.168.20.234 255.255.255.252
R4(config-if)# end
R4#
```

Host pada setiap subnet akan memiliki alamat host IPv4 dari kisaran alamat host untuk subnet tersebut dan topeng yang sesuai. Host akan menggunakan alamat dari interface LAN router yang dilampirkan sebagai alamat gateway default.

- ✓ Default gateway untuk membangun host A (192.168.20.0/27) akan menjadi 192.168.20.1.
- ✓ Default gateway untuk host Building B (192.168.20.32/27) akan menjadi 192.168.20.33.
- ✓ Default gateway untuk host Building C (192.168.20.64/27) akan menjadi 192.168.20.65.
- ✓ Default gateway untuk host Building D (192.168.20.96/27) akan menjadi 192.168.20.97.

• VLSM CHART

Diagram pengalamanan dapat digunakan untuk mengidentifikasi blok alamat mana yang tersedia untuk digunakan dan mana yang sudah ditetapkan, seperti yang ditunjukkan pada Gambar dibawah. Metode ini membantu mencegah penetapan alamat yang telah dialokasikan.

	/27 Network	Hosts
Building A	.0	.1 - .30
Building B	.32	.33 - .62
Building C	.64	.65 - .94
Building D	.96	.97 - .126
WAN R1 - R2	.128	.129 - .158
WAN R2 - R3	.160	.161 - .190
WAN R3 - R4	.192	.193 - .222
Unused	.224	.225 - .254

Untuk menggunakan ruang alamat secara lebih efisien, / 30 subnet dibuat untuk tautan WAN, seperti yang ditunjukkan pada tabel VLSM pada Gambar dibawah. Untuk menyimpan blok alamat yang tidak terpakai bersama-sama di blok ruang alamat yang berdekatan, subnet terakhir / 27 selanjutnya diberi subnett untuk membuat / 30 subnet. 3 subnet pertama ditugaskan ke link WAN.

Merancang skema pengalamatan dengan cara ini meninggalkan 3 subnet yang tidak terpakai, bersebelahan / 27 dan 5 subnet yang tidak terpakai / 30.

VLSM Subnetting of 192.168.20.0/24

	/27 Network	Hosts
Bldg A	.0	.1 - .30
Bldg B	.32	.33 - .62
Bldg C	.64	.65 - .94
Bldg D	.96	.97 - .126
Unused	.128	.129 - .158
Unused	.160	.161 - .190
Unused	.192	.193 - .222
	.224	.225 - .254

	/30 Network	Hosts
WAN R1-R2	.224	.225 - .226
WAN R2-R3	.228	.229 - .230
WAN R3-R4	.232	.233 - .234
Unused	.236	.237 - .238
Unused	.240	.241 - .242
Unused	.244	.245 - .246
Unused	.248	.249 - .250
Unused	.252	.253 - .254

8.3 ADDRESSING SCHEMES

❖ STRUCTURED DESIGN

• NETWORK ADDRESSING PLANNING

Seperti yang ditunjukkan pada gambar, alokasi ruang alamat lapisan jaringan dalam jaringan perusahaan perlu dirancang dengan baik. Penugasan alamat tidak boleh acak.

Merencanakan subnet jaringan memerlukan pemeriksaan baik kebutuhan penggunaan jaringan organisasi, dan bagaimana subnet akan terstruktur. Melakukan studi kebutuhan jaringan adalah titik awal. Ini berarti melihat seluruh jaringan dan menentukan bagian utama jaringan dan bagaimana mereka akan tersegmentasi. Rencana alamat termasuk menentukan kebutuhan masing-masing subnet dalam hal ukuran, berapa host per subnet, bagaimana alamat host akan ditetapkan, host mana yang memerlukan alamat IP statis, dan host mana yang dapat menggunakan DHCP untuk mendapatkan informasi pengalaman mereka.

Ukuran subnet melibatkan perencanaan jumlah host yang memerlukan alamat host IP di setiap subnet dari jaringan pribadi terbagi. Misalnya, dalam desain jaringan kampus, Anda bisa mempertimbangkan berapa banyak host yang dibutuhkan di LAN Administratif, berapa banyak di Fakultas LAN, dan berapa banyak di LAN Mahasiswa. Di jaringan rumah, pertimbangan bisa dilakukan dengan jumlah host di Main House LAN dan jumlah host di Home Office LAN.

Seperti yang telah dibahas sebelumnya, kisaran alamat IP privat yang digunakan pada LAN adalah pilihan administrator jaringan dan perlu pertimbangan cermat untuk memastikan bahwa cukup banyak alamat host yang tersedia untuk host yang diketahui saat ini dan untuk perluasan di masa mendatang. Ingat rentang alamat IP pribadi adalah

- ✓ 10.0.0.0 - 10.255.255.255 dengan subnet mask 255.0.0.0 atau / 8
- ✓ 172.16.0.0 - 172.31.255.255 dengan subnet mask 255.240.0.0 atau / 12
- ✓ 192.168.0.0 - 192.168.255.255 dengan subnet mask 255.255.0.0 atau / 16

Mengetahui persyaratan alamat IP Anda akan menentukan rentang atau rentang alamat host yang Anda terapkan. Subnetting ruang alamat IP pribadi yang dipilih akan menyediakan alamat host untuk memenuhi kebutuhan jaringan Anda.

Alamat umum yang digunakan untuk terhubung ke Internet biasanya dialokasikan dari penyedia layanan. Jadi, sementara prinsip yang sama untuk subnetting akan berlaku, ini umumnya bukan tanggung jawab administrator jaringan organisasi.

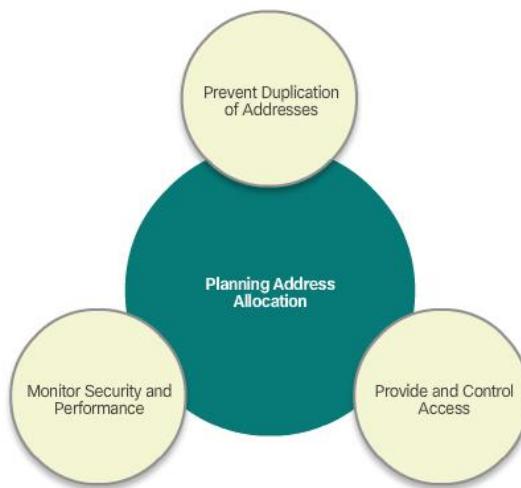
• PLANNING TO ADDRESS THE NETWORK

Tiga pertimbangan utama untuk perencanaan alokasi alamat ditampilkan pada gambar.

Mencegah duplikasi alamat mengacu pada fakta bahwa setiap host dalam sebuah internetwork harus memiliki alamat yang unik. Tanpa perencanaan dan dokumentasi yang tepat, sebuah alamat dapat ditugaskan ke lebih dari satu host, yang menghasilkan masalah akses untuk kedua host.

Menyediakan dan mengendalikan akses mengacu pada fakta bahwa beberapa host, seperti server, menyediakan sumber daya untuk host internal maupun host eksternal. Alamat Layer 3 yang ditugaskan ke server dapat digunakan untuk mengontrol akses ke server tersebut. Jika, bagaimanapun, alamatnya secara acak dan tidak terdokumentasi dengan baik, pengendalian akses lebih sulit.

Pemantauan keamanan dan kinerja host berarti lalu lintas jaringan diperiksa untuk alamat IP sumber yang menghasilkan atau menerima paket yang berlebihan. Jika ada perencanaan dan dokumentasi yang tepat untuk pengalaman jaringan, perangkat jaringan bermasalah harus mudah ditemukan.



- **ASSIGNING ADDRESSES TO DEVICES**

Dalam jaringan, ada berbagai jenis perangkat yang memerlukan alamat, termasuk:

- ✓ **End user clients** - Sebagian besar jaringan mengalokasikan alamat secara dinamis menggunakan Dynamic Host Configuration Protocol (DHCP). Hal ini mengurangi beban staf pendukung jaringan dan hampir menghilangkan kesalahan masuk. Selain itu, alamat hanya disewa untuk jangka waktu tertentu. Mengubah skema subnetting berarti server DHCP perlu dikonfigurasi ulang, dan klien harus memperbarui alamat IP mereka.
- ✓ **Servers and peripherals** - Ini harus memiliki alamat IP statis yang dapat diprediksi. Gunakan sistem penomoran yang konsisten untuk perangkat ini.
- ✓ **Servers that are accessible from the Internet** - Di banyak jaringan, server harus disediakan bagi pengguna jarak jauh. Dalam kebanyakan kasus, server ini diberi alamat pribadi secara internal, dan router atau firewall di sekeliling jaringan harus dikonfigurasi untuk menerjemahkan alamat internal menjadi alamat publik.
- ✓ **Intermediary devices** - Perangkat ini diberi alamat untuk pengelolaan, pemantauan, dan keamanan jaringan. Karena kita harus tahu bagaimana berkomunikasi dengan perangkat perantara, seharusnya alamat yang diprediksi dan statis.
- ✓ **Gateway** - Router dan firewall memiliki alamat IP yang ditetapkan ke setiap antarmuka yang berfungsi sebagai gateway untuk host di jaringan tersebut. Biasanya, antarmuka router menggunakan alamat terendah atau tertinggi dalam jaringan.

Tabel pada gambar tersebut memberikan contoh alokasi alamat untuk jaringan kecil.

Saat mengembangkan skema pengalaman IP, umumnya disarankan untuk memiliki seperangkat pola bagaimana alamat dialokasikan ke setiap jenis perangkat. Ini menguntungkan administrator saat menambahkan dan menghapus perangkat, memfilter lalu lintas berdasarkan IP, serta menyederhanakan dokumentasi.

Network: 192.168.1.0/24		
Use	First	Last
Host Devices	.1	.229
Servers	.230	.239
Printers	.240	.249
Intermediary Devices	.250	.253
Gateway (router LAN interface)	.254	

8.4 DESIGN CONSIDERATIONS FOR IPv6

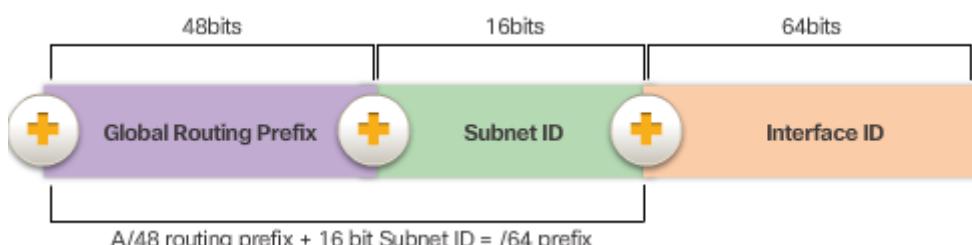
- ❖ SUBNETTING AN IPv6 NETWORK
- THE IPv6 GLOBAL UNICAST ADDRESS

Subnetting IPv6 memerlukan pendekatan yang berbeda dari subnetting IPv4. Alasan utamanya adalah bahwa dengan IPv6 ada begitu banyak alamat, sehingga alasan untuk subnetting benar-benar berbeda. Lihat gambar untuk tinjauan singkat tentang struktur alamat unicast global IPv6.

Subnetting IPv4 tidak hanya membatasi domain broadcast tapi juga tentang mengelola kelangkaan alamat. Menentukan subnet mask dan penggunaan VLSM dilakukan untuk membantu melestarikan alamat IPv4. Subnetting IPv6 tidak peduli dengan melestarikan ruang alamat. ID subnet mencakup lebih dari cukup subnet. Subnetting IPv6 adalah tentang membangun hirarki pengalaman berdasarkan jumlah subnetwork yang dibutuhkan.

Ingat bahwa ada dua jenis alamat IPv6 yang dapat dialihkan. Alamat lokal-link IPv6 tidak akan pernah di subnett karena hanya ada pada link lokal. Namun, alamat unicast global IPv6 bisa di subnetted.

Alamat unicast global IPv6 biasanya terdiri dari awalan routing global 48, subnet ID 16 bit, dan ID antarmuka 64 bit.



- **SUBNETTING USING THE SUBNET ID**

Bagian subnet ID 16 bit dari alamat unicast global IPv6 dapat digunakan oleh sebuah organisasi untuk membuat subnet internal.

Subnet ID menyediakan lebih dari cukup subnet dan dukungan host daripada yang dibutuhkan di satu subnet. Misalnya, bagian 16 bit dapat:

- ✓ Buat hingga 65.536 / 64 subnet. Ini tidak termasuk kemungkinan meminjam bit dari ID antarmuka alamat.
- ✓ Mendukung hingga 18 quintillion host alamat IPv6 per subnet (yaitu, 18.000.000.000.000.000,000).

Catatan: Subnetting ke ID Interface 64 bit (atau porsi host) juga mungkin tapi jarang diperlukan.

Subnetting IPv6 juga lebih mudah diimplementasikan daripada IPv4, karena tidak ada konversi ke biner yang dibutuhkan. Untuk menentukan subnet yang tersedia berikutnya, hitung saja heksadesimal.

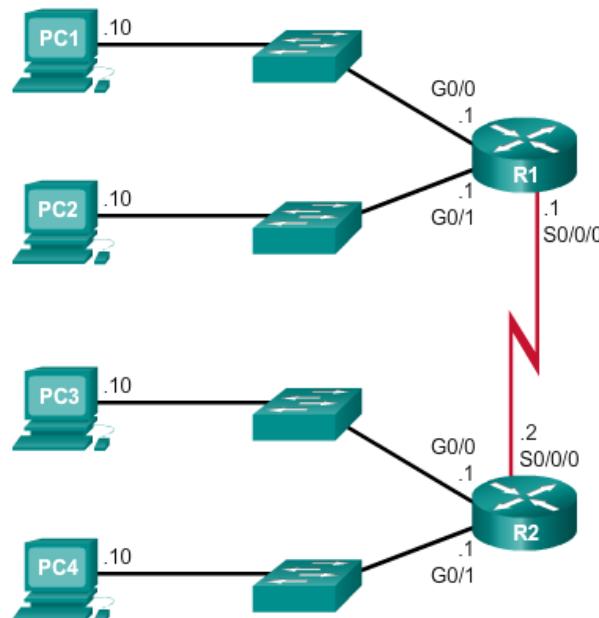
Sebagai contoh, anggap sebuah organisasi telah menetapkan jeda routing global 2001: 0DB8: ACAD :: / 48 dengan subnet ID 16 bit. Ini akan memungkinkan organisasi membuat / 64 subnet, seperti yang ditunjukkan pada gambar. Perhatikan bagaimana awalan routing global sama untuk semua subnet. Hanya subnet ID hextet yang bertambah secara heksadesimal untuk setiap subnet.



- **IPv6 SUBNET ALLOCATION**

Dengan lebih dari 65.000 subnet untuk dipilih, tugas administrator jaringan menjadi salah satu perancangan skema logis untuk mengatasi jaringan.

Seperti ditunjukkan pada Gambar dibawah, topologi contoh akan memerlukan subnet untuk setiap LAN dan juga untuk hubungan WAN antara R1 dan R2. Tidak seperti contoh untuk IPv4, dengan IPv6 subnet link WAN tidak akan subnetted lebih lanjut. Meskipun ini mungkin "membuang" alamat, itu bukan masalah saat menggunakan IPv6.

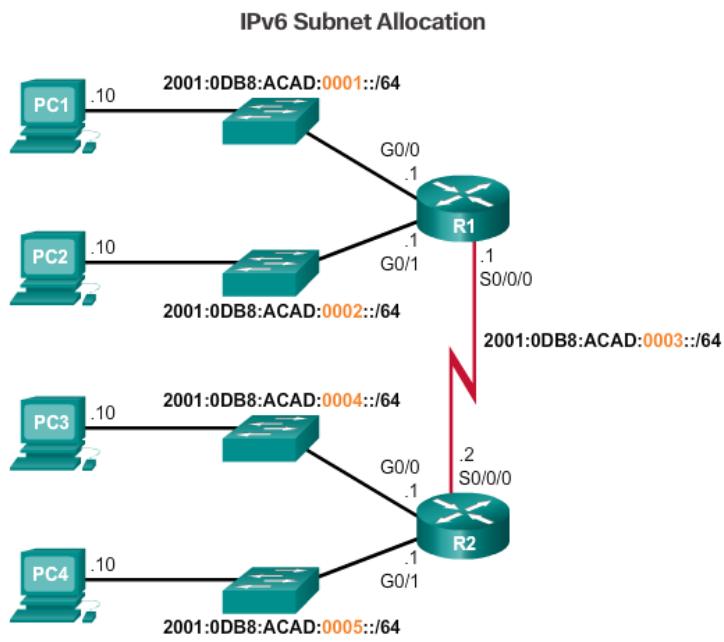


Seperti ditunjukkan pada Gambar dibawah, alokasi lima subnet IPv6, dengan field subnet ID 0001 sampai 0005 akan digunakan untuk contoh ini. Masing-masing / 64 subnet akan menyediakan lebih banyak alamat daripada yang dibutuhkan.

Address Block: 2001:0DB8:ACAD::/48

5 subnets allocated from 65,536 available subnets	2001:0DB8:ACAD:0000::/64 2001:0DB8:ACAD:0001::/64 2001:0DB8:ACAD:0002::/64 2001:0DB8:ACAD:0003::/64 2001:0DB8:ACAD:0004::/64 2001:0DB8:ACAD:0005::/64 2001:0DB8:ACAD:0006::/64 2001:0DB8:ACAD:0007::/64 2001:0DB8:ACAD:0008::/64 ... 2001:0DB8:ACAD:FFFF::/64
---	---

Seperti ditunjukkan pada Gambar dibawah, setiap segmen LAN dan link WAN diberi subnet / 64.



Mirip dengan konfigurasi IPv4, Gambar dibawah menunjukkan bahwa masing-masing interface router telah dikonfigurasi untuk berada pada subnet IPv6 yang berbeda.

Lihat Bab Lampiran untuk informasi lebih lanjut yang memasukkan IPv6 ke dalam ID antarmuka.

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# end
R1#
```

LATIHAN SOAL 8

1. Jelaskan yang dimaksud dengan Subnetting
2. Sebutkan cara menggunakan subnet untuk membantu mengelola jaringan
3. Jelaskan yang dimaksud dengan Classless subnetting
4. Jelaskan cara membuat 2 Subnets
5. Jelaskan perbedaan antara membuat 2 subnets dan 4 subnets
6. Jelaskan yang dimaksud dengan VLSM
7. Jelaskan faktor yang mempengaruhi dalam merencanakan alamat jaringan
8. Sebutkan jenis-jenis perangkat yang memerlukan address
9. Jelaskan langkah-langkah konfigurasi interface router
10. Jelaskan kelebihan dari VLSM

BAB 9 TRANSPORT LAYER

9.1 PENGANTAR

Jaringan data dan internet mendukung jaringan manusia dengan menyediakan komunikasi yang andal antar manusia. Pada satu perangkat, orang dapat menggunakan beberapa aplikasi dan layanan seperti email, web, dan pesan instan untuk mengirim pesan atau mengambil informasi. Data dari masing-masing aplikasi ini dikemas, diangkut dan dikirim ke aplikasi yang sesuai pada perangkat tujuan.

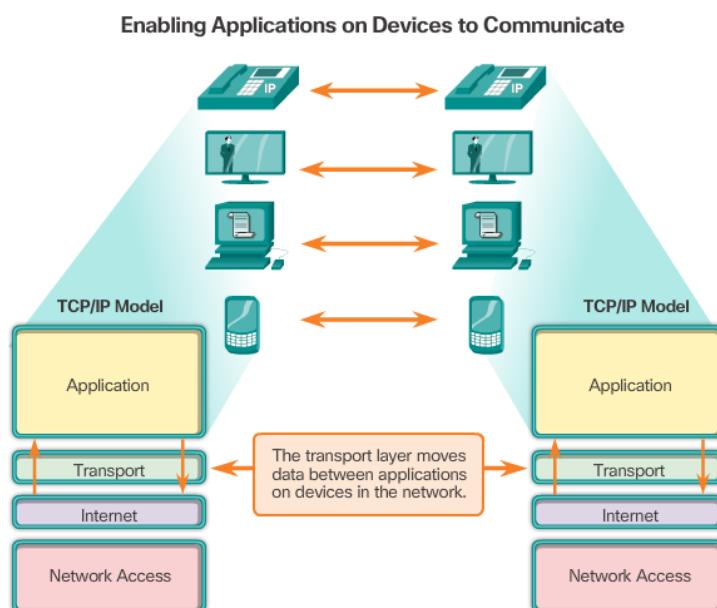
Proses yang dijelaskan dalam lapisan transport OSI menerima data dari lapisan aplikasi dan mempersiapkannya untuk pengalaman pada lapisan jaringan. Komputer sumber berkomunikasi dengan komputer penerima untuk memutuskan bagaimana memecah data menjadi beberapa segmen, bagaimana memastikan tidak ada segmen yang hilang, dan bagaimana memverifikasi semua segmen yang ada. Saat memikirkan lapisan transport, pikirkan sebuah departemen pengiriman yang menyiapkan satu pesanan beberapa paket untuk pengiriman.

9.2 TRANSPORT LAYER PROTOCOLS

❖ TRANSPORT OF DATA

• ROLE OF THE TRANSPORT LAYER

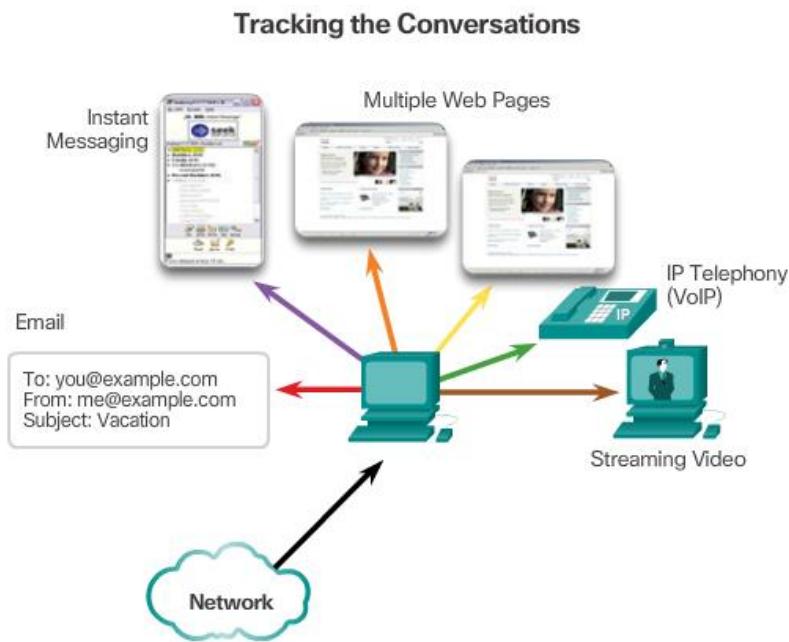
Lapisan transport bertanggung jawab untuk membentuk sesi komunikasi sementara antara dua aplikasi dan mengirimkan data di antara keduanya. Aplikasi menghasilkan data yang dikirim dari aplikasi pada host sumber ke aplikasi di host tujuan. Ini tanpa memperhatikan tipe host tujuan, jenis media dimana data harus melakukan perjalanan, jalur yang ditempuh oleh data, kemacetan pada link, atau ukuran jaringan. Seperti ditunjukkan pada gambar, lapisan transport adalah penghubung antara lapisan aplikasi dan lapisan bawah yang bertanggung jawab untuk transmisi jaringan.



- **TRANSPORT LAYER RESPONSIBILITIES**

Tracking Individual Conversations

Pada lapisan transport, setiap rangkaian data yang mengalir antara aplikasi sumber dan aplikasi tujuan dikenal sebagai percakapan (Gambar dibawah). Host mungkin memiliki beberapa aplikasi yang berkomunikasi di seluruh jaringan secara bersamaan. Masing-masing aplikasi ini berkomunikasi dengan satu atau lebih aplikasi pada satu atau lebih host jarak jauh. Ini adalah tanggung jawab lapisan transport untuk mempertahankan dan melacak beberapa percakapan ini.



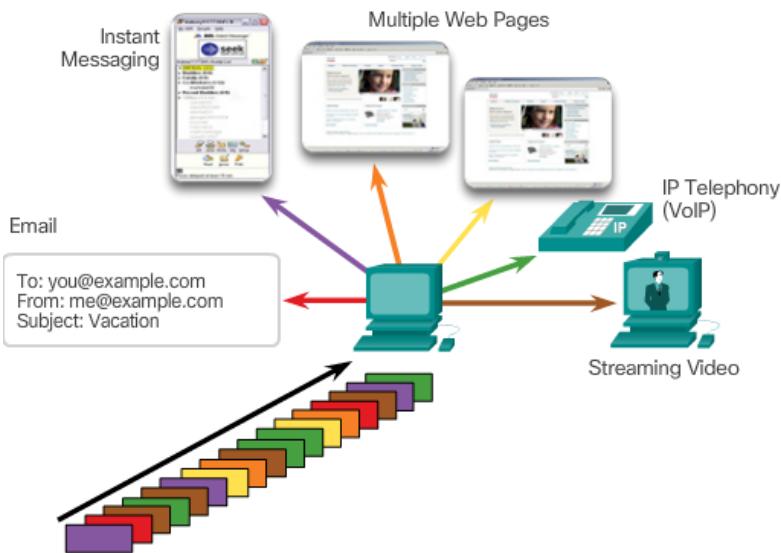
The transport layer tracks each individual conversation flowing between a source application and a destination application separately.

Segmenting Data and Reassembling Segments

Data harus dipersiapkan untuk dikirim ke media secara terkelola. Sebagian besar jaringan memiliki keterbatasan pada jumlah data yang dapat disertakan dalam satu paket. Transport layer protocols memiliki layanan yang mengelompokkan data aplikasi menjadi blok yang ukurannya sesuai (Gambar dibawah). Layanan ini mencakup enkapsulasi yang diperlukan pada setiap potongan data. Header yang digunakan untuk reassembly ditambahkan ke setiap blok data. Header ini digunakan untuk melacak arus data.

Di tempat tujuan, lapisan transport harus bisa merekonstruksi potongan data menjadi aliran data yang lengkap yang berguna untuk lapisan aplikasi. Protokol pada lapisan pengangkutan menggambarkan bagaimana informasi header lapisan transport digunakan untuk memasang kembali potongan data ke dalam aliran yang akan dilewatkan ke lapisan aplikasi.

Segmentation



The transport layer divides the data into segments that are easier to manage and transport.

Identifying the Applications

Untuk melewaskan arus data ke aplikasi yang tepat, lapisan transport harus mengidentifikasi aplikasi target (Gambar dibawah). Untuk mencapai hal ini, lapisan transport memberi setiap aplikasi sebuah identifier yang disebut nomor port. Setiap proses perangkat lunak yang perlu mengakses jaringan diberi nomor port yang unik ke host tersebut.

Identifying the Application



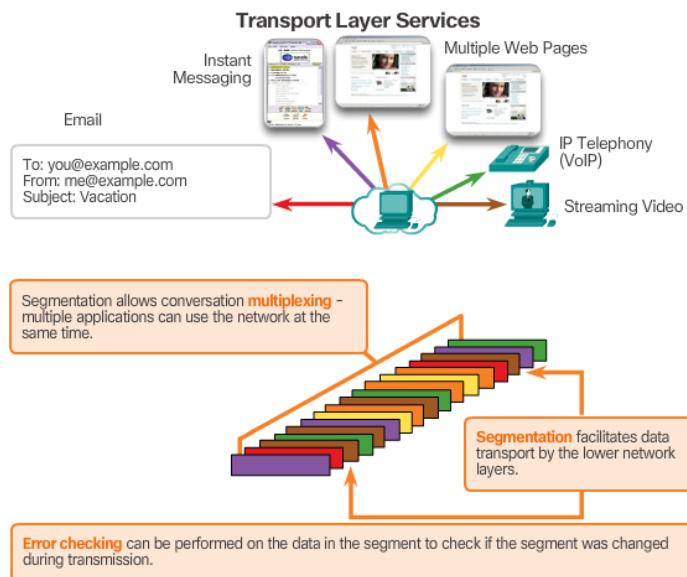
The transport layer ensures that even with multiple applications running on a device, all applications receive the correct data.

• CONVERSATION MULTIPLEXING

Mengirim beberapa jenis data (misalnya, video streaming) di seluruh jaringan, sebagai salah satu aliran komunikasi yang lengkap, dapat menghabiskan semua bandwidth yang tersedia. Hal ini akan mencegah komunikasi lainnya terjadi pada saat bersamaan. Hal itu juga akan membuat error recovery dan retransmission data yang rusak menjadi sulit.

Angka tersebut menunjukkan bahwa mengelompokkan data ke dalam potongan yang lebih kecil memungkinkan banyak komunikasi yang berbeda, dari banyak pengguna yang berbeda, untuk disisipkan (multiplexing) pada jaringan yang sama.

Untuk mengidentifikasi setiap segmen data, lapisan transport menambahkan sebuah header berisi data biner yang disusun dalam beberapa bidang. Ini adalah nilai di bidang ini yang memungkinkan berbagai protokol lapisan transport untuk melakukan fungsi yang berbeda dalam mengelola komunikasi data.

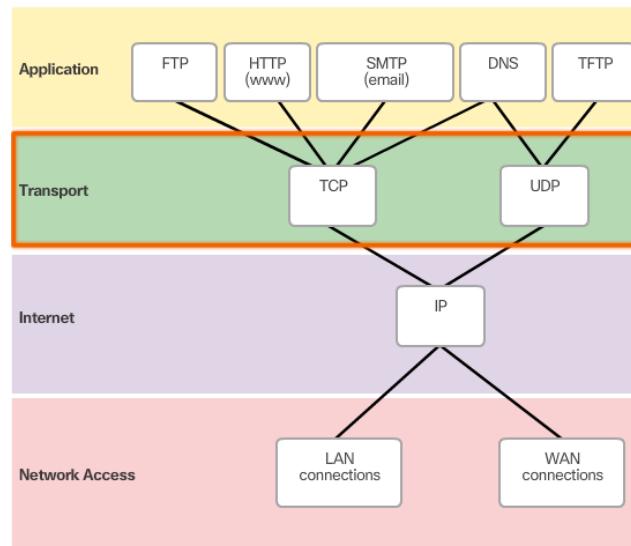


• TRANSPORT LAYER RELIABILITY

Lapisan transport juga bertanggung jawab untuk mengelola persyaratan keandalan percakapan. Aplikasi yang berbeda memiliki persyaratan keandalan transportasi yang berbeda.

IP hanya terkait dengan struktur, pengalamatan, dan perutean paket. IP tidak menentukan bagaimana pengiriman atau pengangkutan paket berlangsung. Protokol transportasi menentukan cara untuk mentransfer pesan antar host. TCP / IP menyediakan dua protokol lapisan transport, Transmission Control Protocol (TCP) dan User Datagram Protocol (UDP), seperti yang ditunjukkan pada gambar. IP menggunakan protokol transport ini untuk memungkinkan host berkomunikasi dan mentransfer data.

TCP dianggap sebagai protokol lapisan transport berfitur lengkap yang andal, yang memastikan bahwa semua data sampai di tempat tujuan. Sebaliknya, UDP adalah protokol lapisan transport yang sangat sederhana yang tidak menyediakan keandalan apapun.



Transport TCP analog dengan pengiriman paket yang dilacak dari sumber ke tujuan. Jika pesanan pengiriman dipecah menjadi beberapa paket, pelanggan dapat memeriksa secara online untuk melihat urutan pengiriman.

Dengan TCP, ada tiga operasi dasar keandalan:

- ✓ Penomoran dan pelacakan segmen data dikirim ke host tertentu dari aplikasi tertentu
- ✓ Acknowledging received data
- ✓ Retransmitting any unacknowledged data after a certain period of time

• UDP

Sementara fungsi keandalan TCP memberikan komunikasi yang lebih kuat antara aplikasi, mereka juga mengalami overhead tambahan dan kemungkinan penundaan transmisi. Ada trade-off antara nilai reliabilitas dan beban yang ditempatinya pada sumber daya jaringan. Menambahkan overhead untuk memastikan keandalan beberapa aplikasi bisa mengurangi kegunaan aplikasi dan bahkan bisa merugikan. Dalam kasus tersebut, **UDP** adalah protokol transport yang lebih baik.

UDP menyediakan fungsi dasar untuk menyampaikan segmen data antara aplikasi yang sesuai, dengan sedikit overhead dan pengecekan data. UDP dikenal sebagai protokol pengiriman best-effort. Dalam konteks jaringan, pengiriman best-effort disebut tidak dapat diandalkan karena tidak ada pengakuan bahwa data diterima di tempat tujuan. Dengan UDP, tidak ada proses lapisan transport yang menginformasikan pengirim tentang pengiriman yang berhasil.

UDP mirip dengan menempatkan surat biasa, tidak terdaftar, melalui surat. Pengirim surat tersebut tidak mengetahui ketersediaan penerima untuk menerima surat tersebut. Kantor pos juga tidak bertanggung jawab untuk melacak surat tersebut atau memberitahukan pengirimnya jika surat tersebut tidak sampai pada tujuan akhir.

- THE RIGHT TRANSPORT LAYER PROTOCOL FOR THE RIGHT APPLICATION

Untuk beberapa aplikasi, segmen harus sampai pada urutan yang sangat spesifik untuk diproses dengan sukses. Dengan aplikasi lain, semua data harus sepenuhnya diterima sebelum ada yang dianggap bermanfaat. Dalam kedua kasus ini, TCP digunakan sebagai protokol transport. Pengembang aplikasi harus memilih tipe protokol transport yang sesuai dengan persyaratan aplikasi.

Misalnya, aplikasi seperti database, browser web, dan klien email, mengharuskan semua data yang dikirim tiba di tempat tujuan dalam kondisi aslinya. Setiap data yang hilang dapat menyebabkan komunikasi korup yang tidak lengkap atau tidak terbaca. Aplikasi ini dirancang untuk menggunakan TCP.

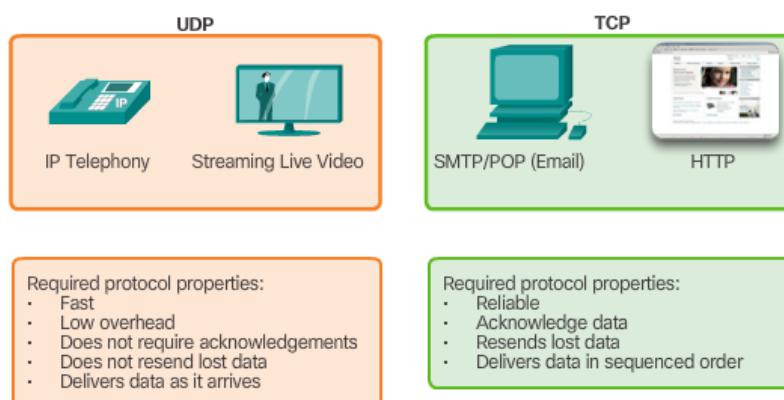
Dalam kasus lain, aplikasi dapat mentolerir beberapa kehilangan data selama pengiriman melalui jaringan, namun penundaan transmisi tidak dapat diterima. UDP adalah pilihan yang lebih baik untuk aplikasi ini karena lebih sedikit overhead jaringan yang diperlukan. UDP lebih disukai untuk aplikasi seperti streaming live audio, live video, dan Voice over IP (VoIP). Ucapan terima kasih dan pengiriman ulang akan memperlambat pengiriman.

Misalnya, jika satu atau dua segmen aliran video langsung gagal tiba, hal itu akan menciptakan gangguan sesaat di arus. Ini mungkin tampak sebagai distorsi pada gambar atau suara, namun mungkin tidak terlihat oleh pengguna. Jika perangkat tujuan harus memperhitungkan data yang hilang, arus dapat tertunda sambil menunggu transmisi ulang, sehingga menyebabkan gambar atau suara menjadi sangat terdegradasi. Dalam kasus ini, lebih baik membuat media sebaik mungkin dengan segmen yang diterima, dan menghilangkan keandalan.

Catatan: Aplikasi yang mengalirkan audio dan video yang tersimpan menggunakan TCP. Misalnya, jika jaringan Anda tiba-tiba tidak dapat mendukung bandwidth yang dibutuhkan untuk menonton film sesuai permintaan, aplikasi akan menghentikan pemutaran. Selama jeda, Anda mungkin melihat pesan "buffering ..." sementara TCP bekerja untuk membangun kembali arus. Setelah semua segmen berada dalam urutan dan tingkat minimum bandwidth dipulihkan, sesi TCP Anda dilanjutkan dan film mulai diputar.

Transport Layer Protocols

Application developers choose the appropriate transport layer protocol based on the nature of the application.



❖ TCP DAN UDP OVERVIEW

• TCP FEATURES

Untuk memahami perbedaan antara TCP dan UDP, penting untuk memahami bagaimana masing-masing protokol menerapkan fitur keandalan tertentu dan bagaimana mereka melacak percakapan. Selain mendukung fungsi dasar segmentasi data dan reassembly, TCP, seperti yang ditunjukkan pada gambar, juga menyediakan layanan lainnya.

Establishing a Session

TCP adalah protokol connection-oriented. Protokol berorientasi koneksi adalah protokol yang menegosiasikan dan menetapkan koneksi permanen (atau sesi) antara perangkat sumber dan tujuan sebelum meneruskan lalu lintas. Melalui pembentukan sesi, perangkat menegosiasikan jumlah lalu lintas yang dapat diteruskan pada waktu tertentu, dan data komunikasi antara keduanya dapat dikelola dengan baik.

Reliable Delivery

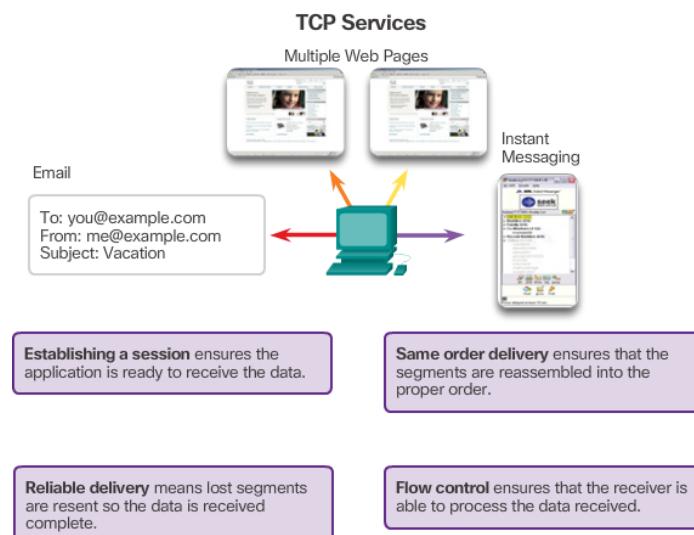
Dalam istilah jaringan, keandalan berarti memastikan bahwa setiap segmen yang dikirim sumbernya sampai di tempat tujuan. Karena berbagai alasan, adalah mungkin bagi segmen untuk menjadi rusak atau hilang sepenuhnya, karena dikirimkan melalui jaringan.

Same-Order Delivery

Karena jaringan dapat menyediakan banyak rute yang dapat memiliki tingkat transmisi yang berbeda, data bisa sampai pada urutan yang salah. Dengan penomoran dan pengurutan segmen, TCP dapat memastikan bahwa segmen ini dipasang kembali ke urutan yang benar.

Flow Control

Host jaringan memiliki sumber daya yang terbatas, seperti memori dan daya pemrosesan. Ketika TCP menyadari bahwa sumber daya ini terlalu banyak, ia dapat meminta agar aplikasi pengirim mengurangi laju aliran data. Hal ini dilakukan oleh TCP yang mengatur jumlah data yang dikirimkan sumber. Pengendalian aliran dapat mencegah kebutuhan transmisi kembali data saat sumber daya penerima menerima kewalahan.

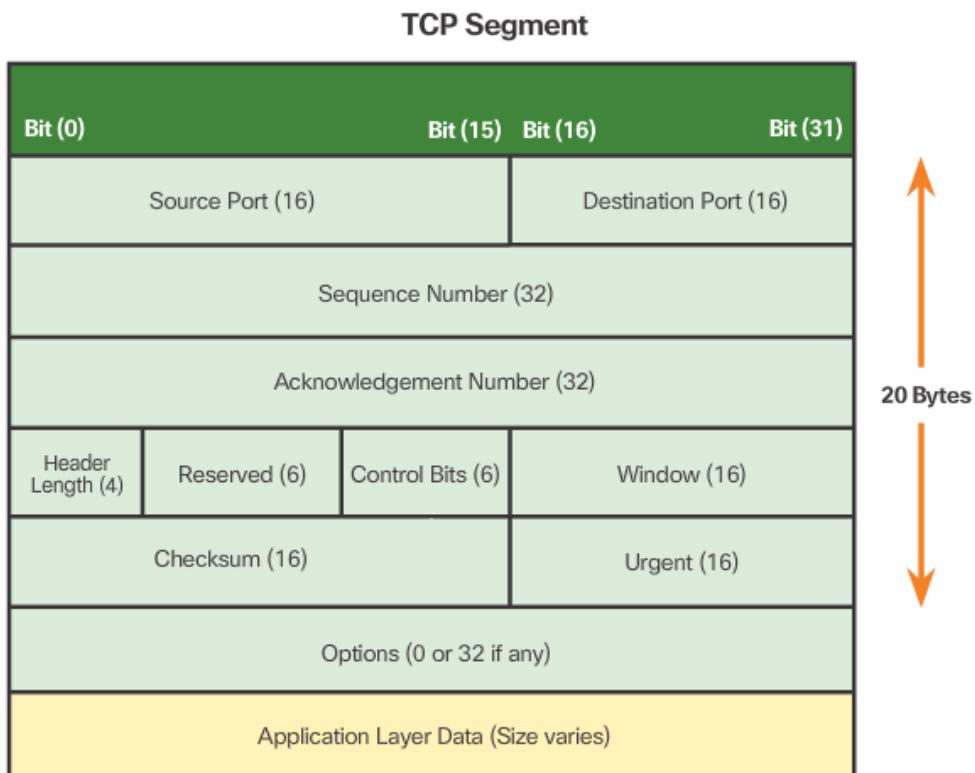


- **TCP HEADER**

TCP adalah protokol stateful. Protokol stateful adalah protokol yang melacak keadaan sesi komunikasi. Untuk melacak keadaan sebuah sesi, TCP mencatat informasi mana yang telah dikirim dan informasi mana yang telah diketahui. Sesi stateful dimulai dengan pembentukan sesi dan berakhir saat ditutup dengan penghentian sesi.

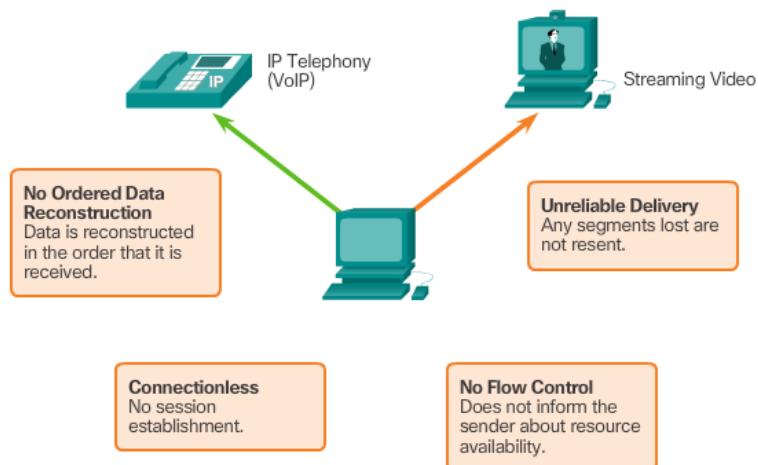
Seperti ditunjukkan pada gambar, setiap segmen TCP memiliki 20 byte overhead di header yang mengenkapsulasi data lapisan aplikasi:

- ✓ Source Port (16 bit) dan Destination Port (16 bit) - Digunakan untuk mengidentifikasi aplikasi.
- ✓ Sequence number (32 bits) - Digunakan untuk keperluan pengumpulan data.
- ✓ Acknowledgment number (32 bits) - Menunjukkan data yang telah diterima.
- ✓ Header length (4 bits) - Dikenal sebagai "data offset ". Menunjukkan panjang header segmen TCP.
- ✓ Reserved (6 bit) - Bidang ini dicadangkan untuk masa depan.
- ✓ Bit kontrol (6 bit) - Termasuk kode bit, atau flag, yang menunjukkan tujuan dan fungsi segmen TCP.
- ✓ Window size (16 bits) - Menunjukkan jumlah byte yang bisa diterima sekaligus.
- ✓ Checksum (16 bit) - Digunakan untuk pengecekan kesalahan pada header segmen dan data.
- ✓ Urgent (16 bit) - Mengindikasikan jika data mendesak.



- **UDP FEATURES**

User Datagram Protocol (UDP) dianggap sebagai protokol transport best-effort. **UDP** adalah protokol transport ringan yang menawarkan segmentasi data dan reassembly yang sama seperti TCP, namun tanpa keandalan dan kontrol aliran TCP. UDP adalah protokol sederhana yang biasanya dijelaskan dalam hal apa yang tidak dilakukannya dibandingkan dengan TCP.

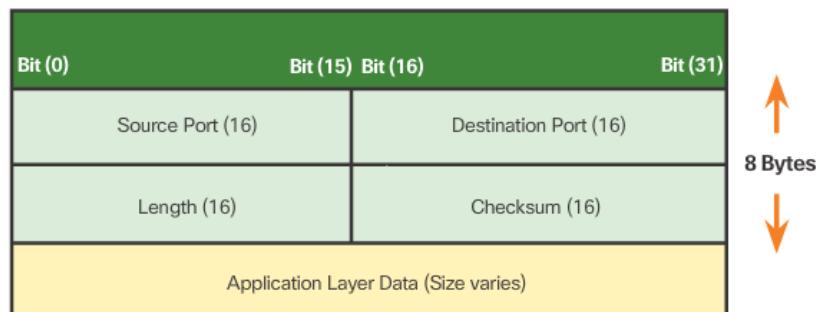


- **UDP HEADER**

UDP adalah protokol tanpa kewarganegaraan, yang berarti baik klien, maupun server, berkewajiban untuk melacak keadaan sesi komunikasi. Jika reliabilitas diperlukan saat menggunakan UDP sebagai transport protocol, maka harus ditangani oleh aplikasi.

Salah satu persyaratan terpenting untuk menghadirkan video langsung dan suara melalui jaringan adalah data terus mengalir dengan cepat. Aplikasi video dan suara langsung dapat mentolerir beberapa kehilangan data dengan efek minimal atau tidak nyata, dan sangat sesuai untuk UDP.

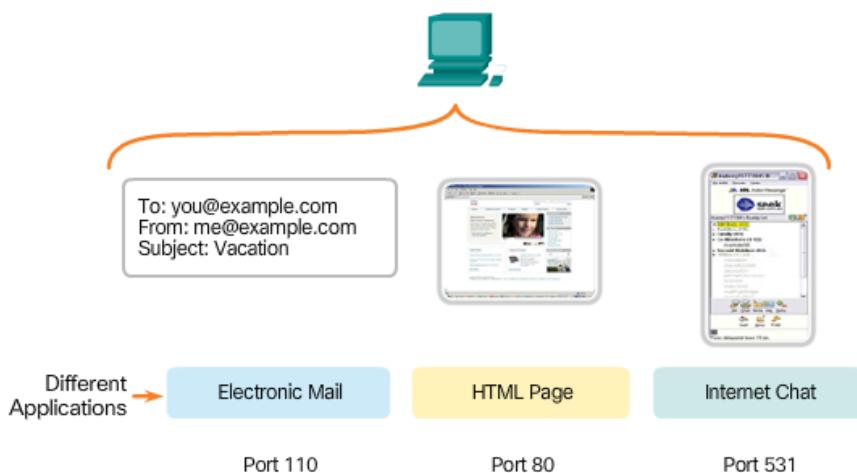
Potongan komunikasi dalam UDP disebut datagrams, seperti yang ditunjukkan pada gambar. Datagram ini dikirim sebagai upaya terbaik oleh protokol lapisan transport. UDP memiliki overhead rendah 8 byte.



- **MULTIPLE SEPARATE CONVERSATIONS**

Lapisan transport harus dapat memisahkan dan mengelola beberapa komunikasi dengan kebutuhan kebutuhan transportasi yang berbeda. Pengguna berharap dapat secara bersamaan menerima dan mengirim email dan pesan instan, melihat situs web, dan melakukan panggilan telepon VoIP. Masing-masing aplikasi ini mengirim dan menerima data melalui jaringan pada saat bersamaan, terlepas dari persyaratan keandalan yang berbeda. Selain itu, data dari panggilan telepon tidak ditujukan ke browser web, dan teks dari pesan instan tidak muncul dalam email.

TCP dan UDP mengelola beberapa percakapan simultan ini dengan menggunakan bidang header yang dapat mengidentifikasi aplikasi ini secara unik. Pengenal unik ini adalah nomor port.



- **PORT NUMBERS**

Nomor port sumber dikaitkan dengan aplikasi yang berasal dari host lokal. Nomor port tujuan dikaitkan dengan aplikasi tujuan pada host jarak jauh.

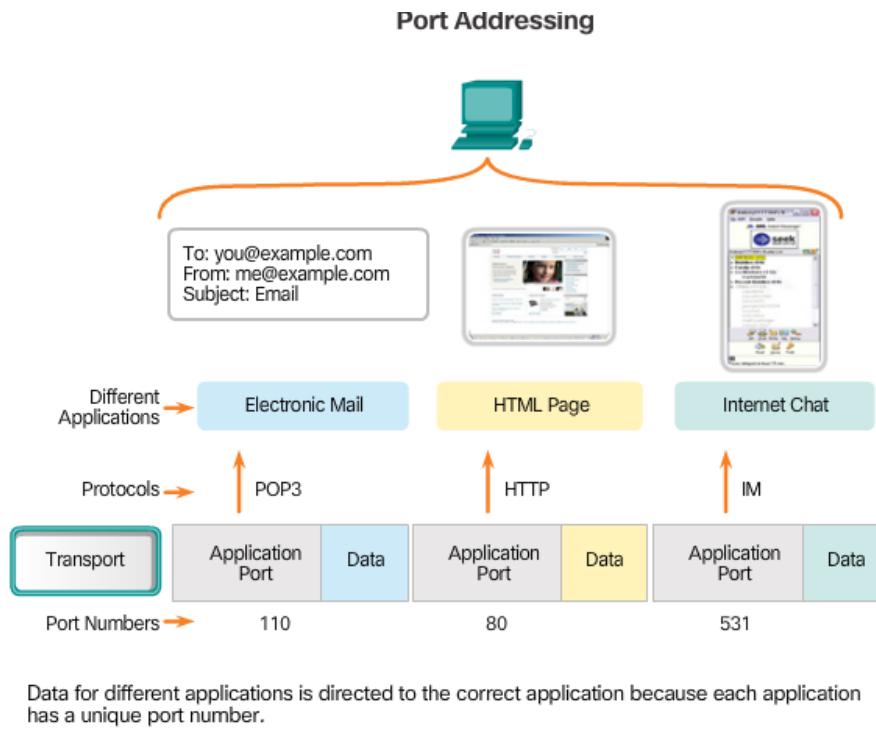
Source Port

Nomor port sumber secara dinamis dihasilkan oleh perangkat pengirim untuk mengidentifikasi percakapan antara dua perangkat. Proses ini memungkinkan beberapa percakapan terjadi secara simultan. Adalah umum bagi perangkat untuk mengirim beberapa permintaan layanan HTTP ke server web secara bersamaan. Setiap percakapan HTTP terpisah dilacak berdasarkan port sumber.

Destination Port

Klien menempatkan nomor port tujuan di segmen tersebut untuk memberi tahu server tujuan tentang layanan apa yang diminta, seperti yang ditunjukkan pada gambar. Misalnya, ketika klien menentukan port 80 di port tujuan, server yang menerima pesan mengetahui bahwa layanan web diminta. Sebuah server dapat menawarkan lebih dari satu layanan secara

bersamaan seperti layanan web pada port 80 pada saat yang bersamaan dengan menawarkan koneksi File Transfer Protocol (FTP) pada port 21.



- **SOCKET PAIRS**

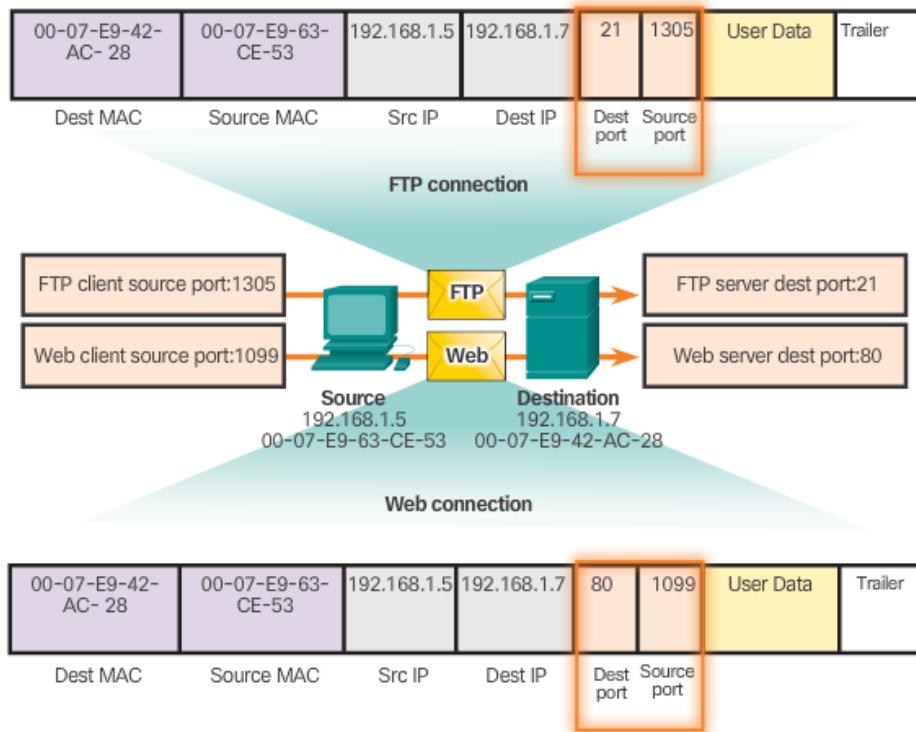
Port sumber dan tujuan ditempatkan di dalam segmen. Segmen kemudian dienkapsulasi dalam paket IP. Paket IP berisi alamat IP dari sumber dan tujuan. Kombinasi alamat IP sumber dan nomor port sumber, atau alamat IP tujuan dan nomor port tujuan dikenal sebagai soket. Soket digunakan untuk mengidentifikasi server dan layanan yang diminta oleh klien. Soket klien mungkin terlihat seperti ini, dengan 1099 mewakili nomor port sumber: 192.168.1.5:1099

The socket on a web server might be: 192.168.1.7:80

Together, these two sockets combine to form a socket pair: 192.168.1.5:1099, 192.168.1.7:80

Sockets memungkinkan beberapa proses, berjalan pada klien, untuk membedakan diri mereka satu sama lain, dan beberapa koneksi ke proses server untuk dibedakan satu sama lain.

Nomor port sumber bertindak sebagai alamat pengirim untuk aplikasi peminta. Lapisan transport melacak port ini dan aplikasi yang menginisiasi permintaan sehingga ketika respons dikembalikan, pesan tersebut dapat diteruskan ke aplikasi yang benar.



• PORT NUMBER GROUPS

Internet Assigned Numbers Authority (IANA) adalah badan standar yang bertanggung jawab untuk menetapkan berbagai standar pengalaman, termasuk nomor port. Ada berbagai jenis nomor port;

Port Number Range	Port Group
0 to 1023	Well-known Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

Well-known Ports (Numbers 0 to 1023) - Nomor ini dicadangkan untuk layanan dan aplikasi. Mereka biasanya digunakan untuk aplikasi seperti browser web, klien email, dan klien akses jarak jauh. Dengan mendefinisikan port-port yang terkenal untuk aplikasi server ini, aplikasi klien dapat diprogram untuk meminta koneksi ke port tertentu dan layanan yang terkait dengannya.

Registered Ports (Numbers 1024 to 49151) - Nomor port ini ditugaskan oleh IANA ke entitas peminta untuk digunakan dengan proses atau aplikasi tertentu. Proses ini terutama merupakan aplikasi individual yang dipilih pengguna untuk dipasang, bukan aplikasi umum yang akan menerima nomor port yang terkenal. Sebagai contoh, Cisco telah mendaftarkan port 1985 untuk proses Hot Standby Routing Protocol (HSRP).

Dynamic or Private Ports (Numbers 49152 to 65535) - Juga dikenal sebagai port fana, ini biasanya diberikan secara dinamis oleh OS klien saat koneksi ke layanan dimulai. Port dinamis kemudian digunakan untuk mengidentifikasi aplikasi klien selama komunikasi berlangsung.

Catatan: Beberapa sistem operasi klien mungkin menggunakan nomor port terdaftar, bukan nomor port dinamis untuk menugaskan port sumber.

Gambar dibawah menampilkan beberapa nomor port terkenal dan aplikasinya. Beberapa aplikasi mungkin menggunakan TCP dan UDP. Misalnya, DNS menggunakan UDP saat klien mengirim permintaan ke server DNS. Namun, komunikasi antara dua server DNS selalu menggunakan TCP.

Port Number	Protocol	Application	Acronym
20	TCP	File Transfer Protocol (data)	FTP
21	TCP	File Transfer Protocol (control)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	-
25	TCP	Simple Mail Transfer Protocol	SMTP
53	UDP, TCP	Domain Name Service	DNS
67	UDP	Dynamic Host Configuration Protocol (server)	DHCP
68	UDP	Dynamic Host Configuration Protocol (client)	DHCP
69	UDP	Trivial File Transfer Protocol	TFTP
80	TCP	Hypertext Transfer Protocol	HTTP
110	TCP	Post Office Protocol version 3	POP3
143	TCP	Internet Message Access Protocol	IMAP
161	UDP	Simple Network Management Protocol	SNMP
443	TCP	Hypertext Transfer Protocol Secure	HTTPS

• THE NETSTAT COMMAND

Koneksi TCP yang tidak dapat dijelaskan dapat menjadi ancaman keamanan utama. Mereka dapat menunjukkan bahwa ada sesuatu atau seseorang yang terhubung dengan host lokal. Terkadang perlu diketahui koneksi TCP aktif mana yang terbuka dan berjalan pada host jaringan. Netstat adalah utilitas jaringan penting yang dapat digunakan untuk memverifikasi koneksi tersebut. Seperti ditunjukkan pada gambar, masukkan perintah netstat ke daftar protokol yang digunakan, alamat lokal dan nomor port, alamat asing dan nomor port, dan status koneksi.

Secara default, perintah netstat akan mencoba untuk menyelesaikan alamat IP ke nama domain dan nomor port ke aplikasi yang terkenal. Opsi -n dapat digunakan untuk menampilkan alamat IP dan nomor port dalam bentuk numeriknya.

```
C:\> netstat
Active Connections

  Proto  Local Address        Foreign Address          State
  TCP    kenpc:3126           192.168.0.2:netbios-ssn  ESTABLISHED
  TCP    kenpc:3158           207.138.126.152:http   ESTABLISHED
  TCP    kenpc:3159           207.138.126.169:http   ESTABLISHED
  TCP    kenpc:3160           207.138.126.169:http   ESTABLISHED
  TCP    kenpc:3161           sc.msn.com:http       ESTABLISHED
  TCP    kenpc:3166           www.cisco.com:http     ESTABLISHED

C:\>
```

9.3 TCP DAN UDP

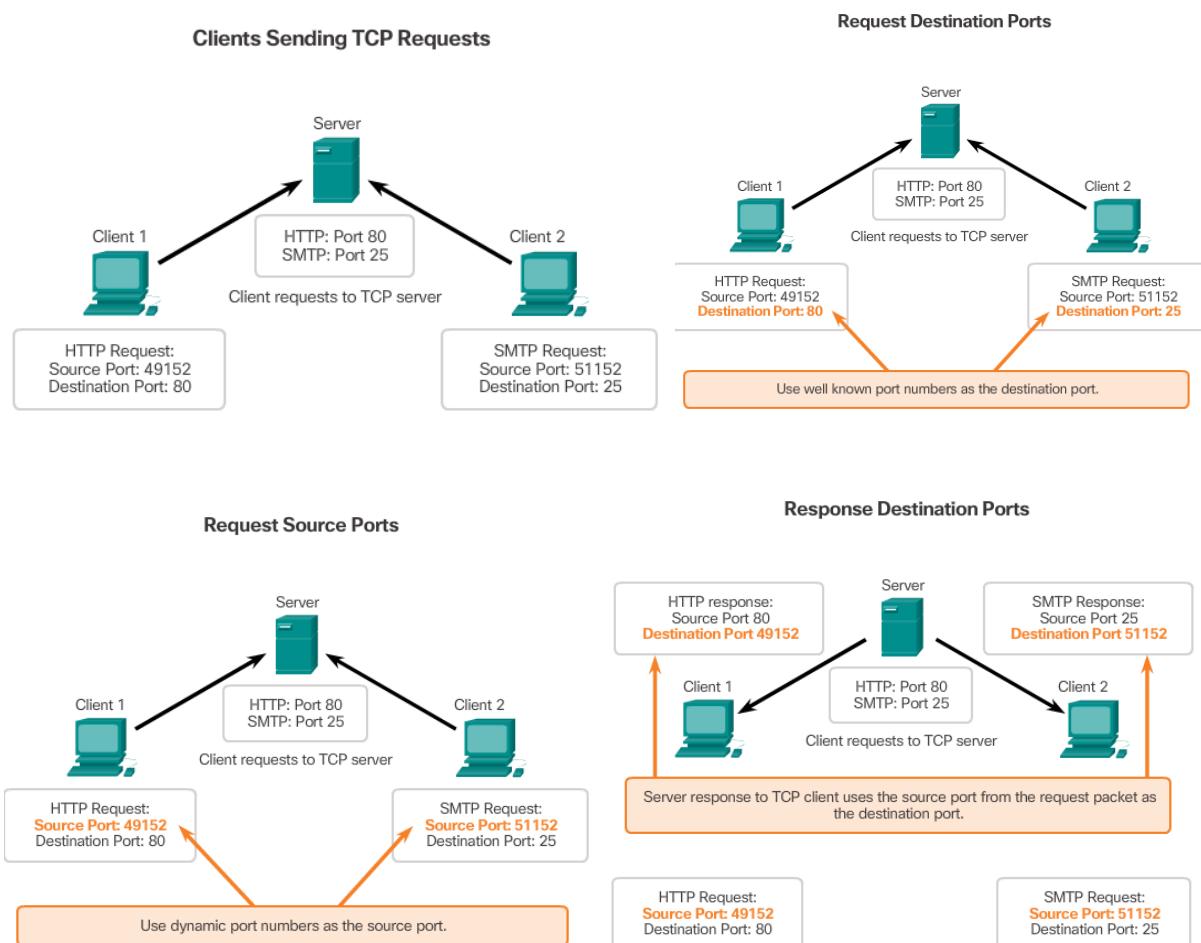
❖ TCP COMMUNICATION PROCESS

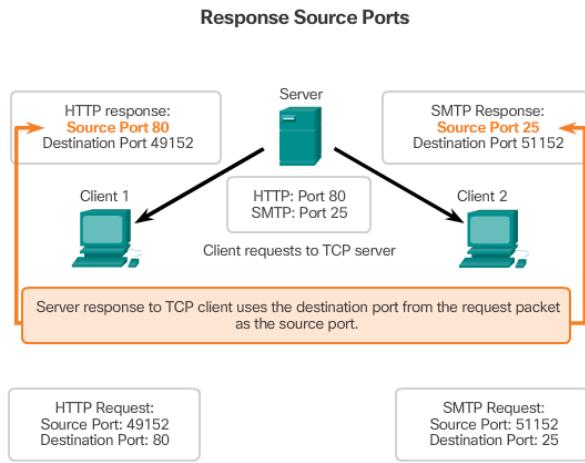
• TCP SERVER PROCESSES

Setiap proses aplikasi yang berjalan di server dikonfigurasi untuk menggunakan nomor port, baik secara default atau manual, oleh administrator sistem. Server individual tidak dapat memiliki dua layanan yang ditugaskan ke nomor port yang sama dalam lapisan transport yang sama.

Misalnya, host yang menjalankan aplikasi server web dan aplikasi transfer file tidak dapat dikonfigurasi untuk menggunakan port yang sama (misalnya, port TCP 80). Aplikasi server aktif yang ditugaskan ke port tertentu dianggap terbuka, yang berarti bahwa lapisan transport menerima dan memproses segmen yang ditujukan ke port tersebut. Setiap permintaan klien masuk yang ditujukan ke soket yang benar diterima, dan data dilewatkan ke aplikasi server. Ada banyak port yang terbuka secara bersamaan di server, satu untuk setiap aplikasi server yang aktif.

Lihat urutan untuk melihat alokasi khas port sumber dan tujuan pada operasi klien / server TCP.



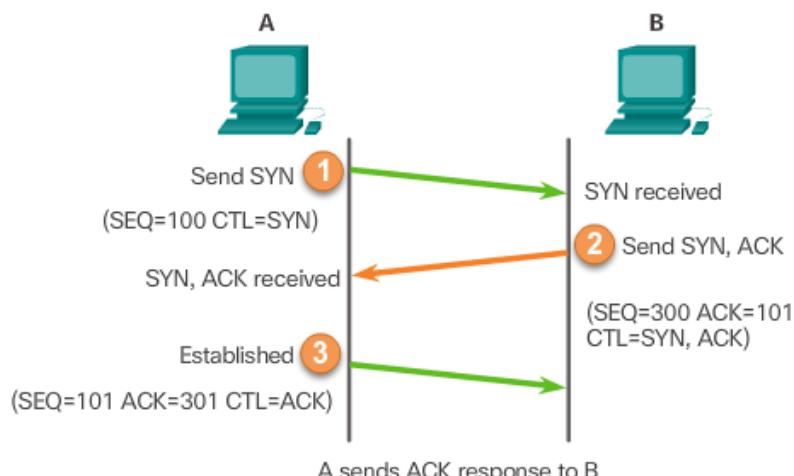


- **TCP CONNECTION ESTABLISHMENT**

Dalam beberapa budaya, ketika dua orang bertemu, mereka sering saling menyapa dengan berjabat tangan. Tindakan berjabat tangan dipahami oleh kedua belah pihak sebagai sinyal untuk ucapan ramah. Koneksi pada jaringan serupa. Dalam koneksi TCP, host client mengatur koneksi dengan server.

Sambungan TCP dibuat dalam tiga langkah:

- ✓ Langkah 1 - Klien inisiasi meminta sesi komunikasi client-to-server dengan server.
- ✓ Langkah 2 - Server mengenali sesi komunikasi client-to-server dan meminta sesi komunikasi server-to-client.
- ✓ Langkah 3 - Klien inisiasi mengenali sesi komunikasi server-to-client.



- **TCP SESSION TERMINATION**

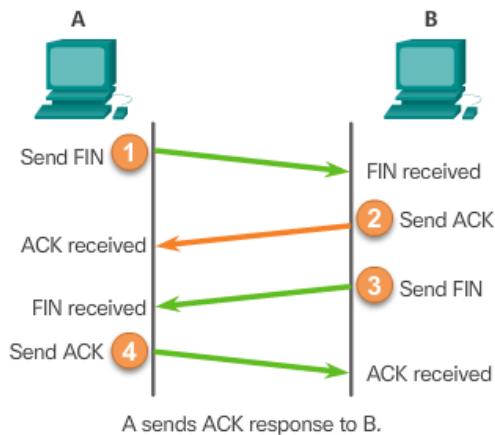
Untuk menutup koneksi, bendera kontrol Finish (FIN) harus disetel di header segmen. Untuk mengakhiri setiap sesi TCP satu arah, jabat tangan dua arah, yang terdiri dari segmen FIN dan Acknowledgement (ACK), digunakan. Oleh karena itu, untuk menghentikan satu percakapan yang didukung oleh TCP, dibutuhkan empat pertukaran untuk mengakhiri kedua sesi.

Catatan: Dalam penjelasan ini, istilah client dan server digunakan sebagai referensi untuk kesederhanaan, namun proses penghentian dapat dimulai oleh dua host yang memiliki sesi terbuka:

- ✓ Langkah 1 - Bila klien tidak memiliki lebih banyak data untuk dikirim ke arus, ia mengirim segmen dengan set bendera FIN.
- ✓ Langkah 2 - Server mengirimkan ACK untuk mengetahui penerimaan FIN untuk mengakhiri sesi dari client ke server.
- ✓ Langkah 3 - Server mengirimkan FIN ke klien untuk mengakhiri sesi server-ke-klien.
- ✓ Langkah 4 - Klien merespons ACK untuk mengenali FIN dari server.

Bila semua segmen telah diakui, sesi ditutup.

TCP Connection Establishment and Termination



- **TCP THREE-WAY HANDSHAKE ANALYSIS**

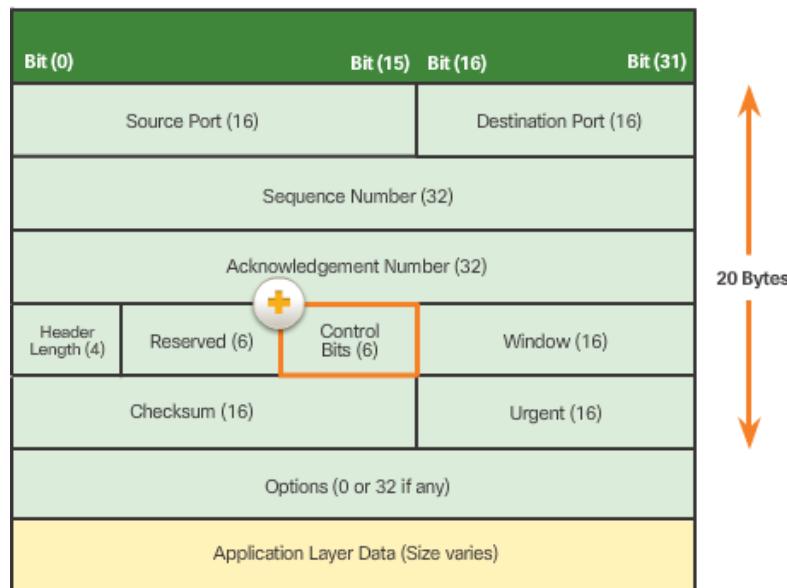
Host melacak setiap segmen data dalam sebuah sesi dan bertukar informasi tentang data apa yang diterima dengan menggunakan informasi di header TCP. TCP adalah protokol full-duplex, di mana setiap koneksi mewakili dua jalur komunikasi satu arah atau sesi. Untuk menjalin koneksi, host melakukan jabat tangan tiga arah. Bit kontrol pada header TCP menunjukkan kemajuan dan status koneksi.

The three-way handshake:

- ✓ Menetapkan bahwa perangkat tujuan ada pada jaringan
- ✓ Memverifikasi bahwa perangkat tujuan memiliki layanan aktif dan menerima permintaan pada nomor port tujuan yang akan digunakan oleh klien pemula
- ✓ Menginformasikan perangkat tujuan bahwa klien sumber bermaksud untuk membentuk sesi komunikasi pada nomor port tersebut

Setelah komunikasi selesai, sesi ditutup, dan koneksi dihentikan. Mekanisme koneksi dan sesi memungkinkan fungsi keandalan TCP.

Enam bit di bidang Control Bits dari header segmen TCP juga dikenal sebagai flag. Bendera sedikit yang diatur ke aktif atau nonaktif. Klik bidang Kontrol Bits pada gambar untuk melihat keenam flag. Kita telah membahas SYN, ACK, dan FIN. Flag RST digunakan untuk mengatur ulang koneksi saat terjadi kesalahan atau batas waktu. Klik di sini untuk mempelajari lebih lanjut tentang flag PSH dan URG



❖ UDP COMMUNICATION PROCESS

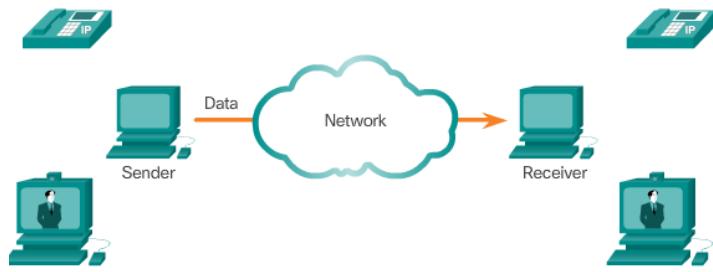
• UDP LOW OVERHEAD VERSUS RELIABILITY

UDP adalah protokol sederhana yang menyediakan fungsi lapisan transport dasar. Ini memiliki overhead jauh lebih rendah daripada TCP karena tidak berorientasi koneksi dan tidak menawarkan mekanisme pengiriman ulang, sequencing, dan flow control yang canggih yang memberikan keandalan.

Ini tidak berarti bahwa aplikasi yang menggunakan UDP selalu tidak dapat diandalkan, juga tidak berarti bahwa UDP adalah protokol yang inferior. Ini hanya berarti bahwa fungsi ini tidak disediakan oleh protokol lapisan transport dan harus diterapkan di tempat lain jika diperlukan.

Rendahnya biaya overhead UDP membuatnya sangat diinginkan untuk protokol yang membuat permintaan sederhana dan transaksi balasan. Misalnya, menggunakan TCP untuk DHCP akan mengenalkan lalu lintas jaringan yang tidak perlu. Jika ada masalah dengan permintaan atau balasan, perangkat akan mengirim permintaan lagi jika tidak ada jawaban yang diterima.

UDP Low Overhead Data Transport



UDP does not establish a connection before sending data.

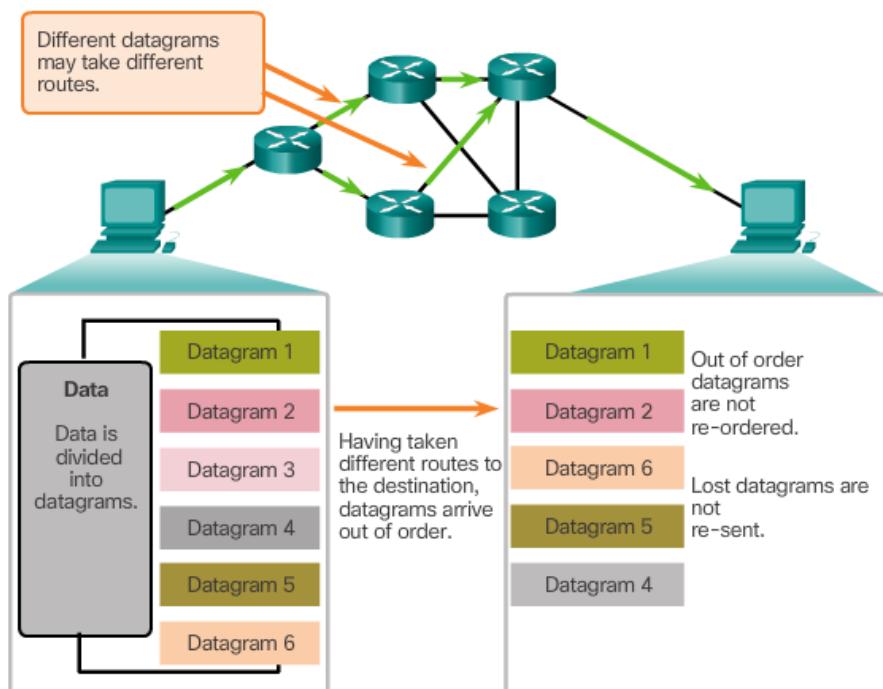
UDP provides low overhead data transport because it has a small datagram header and no network management traffic.

- **UDP DATAGRAM REASSEMBLY**

Seperti segmen dengan TCP, ketika datagram UDP dikirim ke tujuan, mereka sering mengambil jalur yang berbeda dan sampai pada urutan yang salah. UDP tidak melacak nomor urut seperti TCP. UDP tidak memiliki cara untuk menyusun ulang datagram ke dalam urutan transmisi mereka, seperti yang ditunjukkan pada gambar.

Oleh karena itu, UDP hanya menyusun kembali data sesuai urutan penerimaan dan meneruskannya ke aplikasi. Jika urutan data penting untuk aplikasi, aplikasi harus mengidentifikasi urutan yang benar dan menentukan bagaimana data harus diproses.

UDP: Connectionless and Unreliable

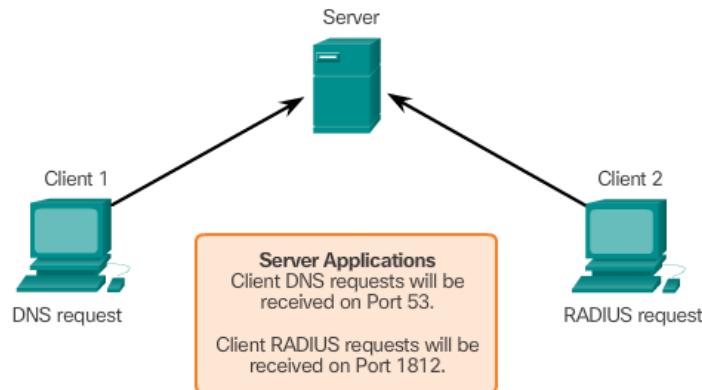


- **UDP SERVER PROCESSES AND REQUEST**

Seperti aplikasi berbasis TCP, aplikasi server berbasis UDP diberikan nomor port yang terkenal atau terdaftar, seperti yang ditunjukkan pada gambar. Saat aplikasi atau proses ini berjalan di

server, mereka menerima data yang sesuai dengan nomor port yang ditetapkan. Ketika UDP menerima datagram yang ditujukan untuk salah satu port ini, maka akan meneruskan data aplikasi ke aplikasi yang sesuai berdasarkan nomor portnya.

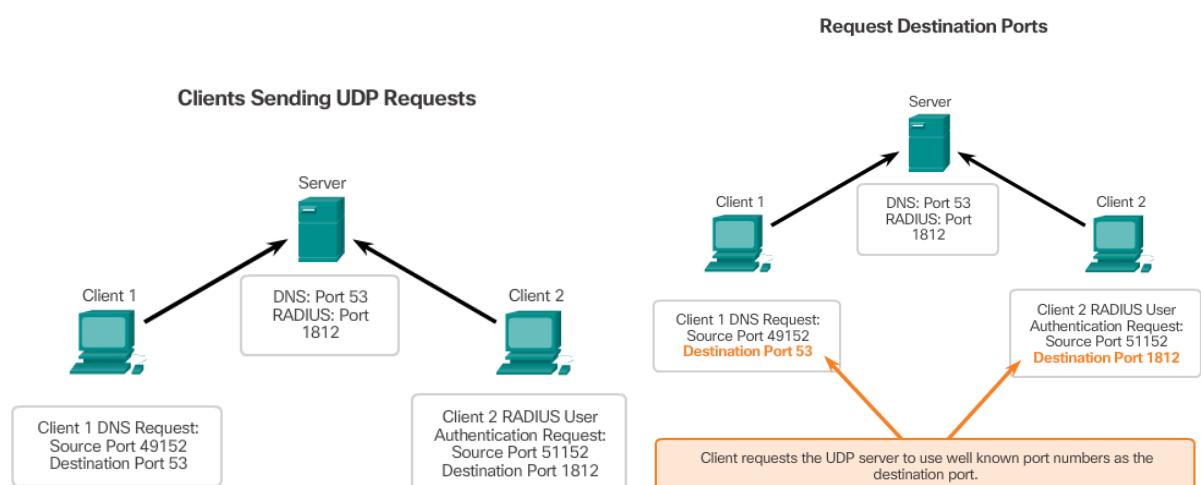
Catatan: Server layanan pengguna Dial-in User Service (RADIUS) Remote Authentication yang ditunjukkan pada gambar menyediakan layanan otentikasi, otorisasi, dan akuntansi untuk mengelola akses pengguna.

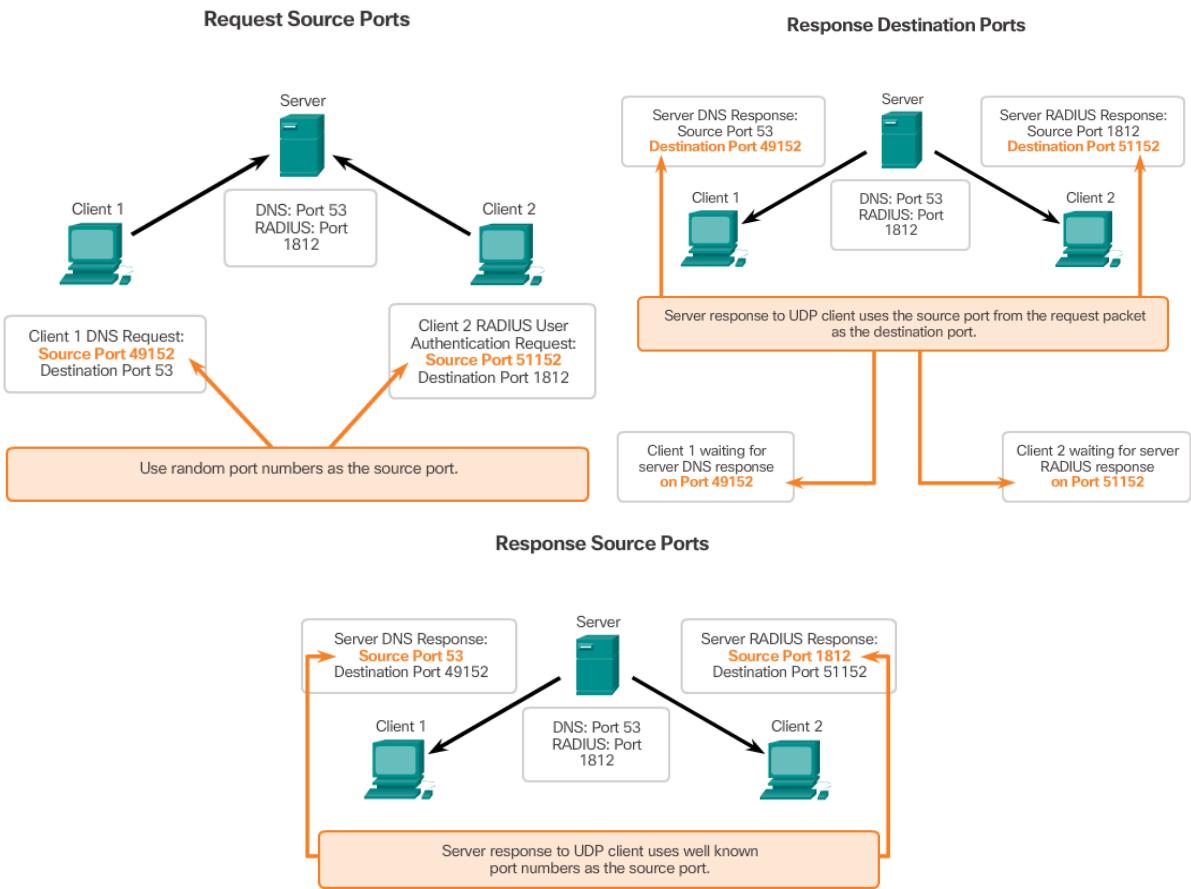


- **UDP CLIENT PROCESSES**

Seperi TCP, komunikasi client-server diprakarsai oleh aplikasi klien yang meminta data dari proses server. Proses klien UDP secara dinamis memilih nomor port dari kisaran nomor port dan menggunakan ini sebagai port sumber untuk percakapan. Port tujuan biasanya adalah nomor port yang terkenal atau terdaftar yang ditugaskan ke proses server.

Setelah klien memilih port sumber dan tujuan, pasangan port yang sama digunakan di header semua datagram yang digunakan dalam transaksi. Untuk data yang kembali ke client dari server, source dan destination port numbers pada datagram header dibalik.



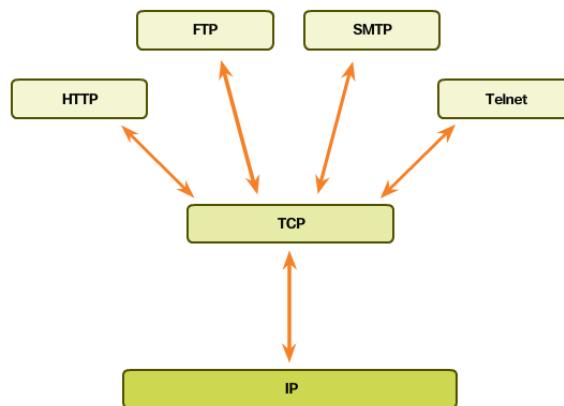


❖ TCP ATAU UDP

• APPLICATION THAT USE TCP

TCP adalah contoh bagus bagaimana lapisan-lapisan protokol TCP / IP yang berbeda memiliki peran yang spesifik. TCP menangani semua tugas yang terkait dengan membagi arus data menjadi beberapa segmen, memberikan keandalan, mengendalikan arus data, dan penataan ulang segmen. TCP membebaskan aplikasi dari keharusan mengelola salah satu tugas ini. Aplikasi, seperti yang ditunjukkan pada gambar, cukup mengirim aliran data ke lapisan transport dan menggunakan layanan TCP.

Applications that use TCP

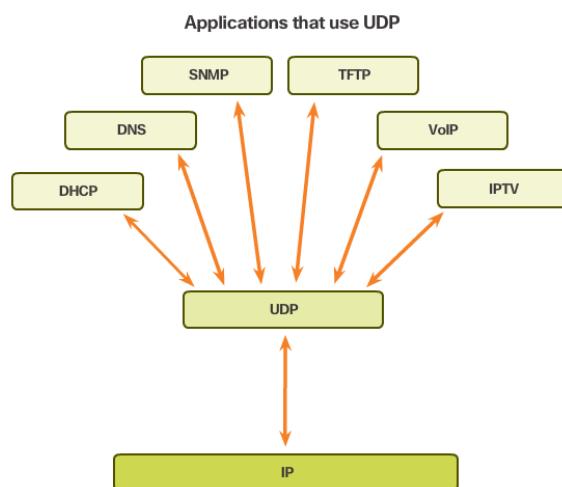


- **APPLICATION THAT USE UDP**

Ada tiga jenis aplikasi yang paling cocok untuk UDP:

- ✓ **Live video and multimedia applications** : Dapat mentolerir beberapa kehilangan data, namun memerlukan sedikit atau tanpa penundaan. Contohnya termasuk VoIP dan live streaming video.
- ✓ **Simple request and reply applications** - Aplikasi dengan transaksi sederhana dimana host mengirim permintaan dan mungkin atau mungkin tidak menerima balasan. Contohnya termasuk DNS dan DHCP.
- ✓ **Applications that handle reliability themselves** - Komunikasi searah dimana kontrol aliran, deteksi kesalahan, ucapan terima kasih, dan pemulihan kesalahan tidak diperlukan atau dapat ditangani oleh aplikasi. Contohnya termasuk SNMP dan TFTP.

Meski DNS dan SNMP menggunakan UDP secara default, keduanya juga bisa menggunakan TCP. DNS akan menggunakan TCP jika permintaan DNS atau response DNS lebih dari 512 byte, seperti ketika respon DNS mencakup sejumlah besar resolusi nama. Demikian pula, dalam beberapa situasi administrator jaringan mungkin ingin mengkonfigurasi SNMP untuk menggunakan TCP.



LATIHAN SOAL 9

1. Jelaskan fungsi transport Layer
2. Jelaskan yang dimaksud dengan TCP
3. Jelaskan yang dimaksud dengan UDP
4. Jelaskan perbedaan antara TCP dan UDP
5. sebutkan dan jelaskan layanan / service yang dimiliki oleh TCP
6. Sebutkan bagian dari header TCP
7. Sebutkan bagian dari header UDP
8. Jelaskan fungsi dari port number
9. Jelaskan yang dimaksud dengan NESTAT Command
10. Jelaskan proses TCP server

BAB 10 APPLICATION LAYER

10.1 PENGANTAR

Aplikasi, seperti web browser, game online, chatting dengan dan email teman, memungkinkan kita untuk mengirim dan menerima data dengan relatif mudah. Biasanya kita bisa mengakses dan menggunakan aplikasi ini tanpa mengetahui cara kerjanya. Namun, bagi profesional jaringan, penting untuk mengetahui bagaimana aplikasi dapat memformat, mentransmisikan dan menafsirkan pesan yang dikirim dan diterima di seluruh jaringan.

Memvisualisasikan mekanisme yang memungkinkan komunikasi antar jaringan menjadi lebih mudah jika kita menggunakan kerangka kerja model OSI berlapis.

Dalam bab ini, kita akan mengeksplorasi peran lapisan aplikasi dan bagaimana aplikasi, layanan, dan protokol di dalam lapisan aplikasi membuat komunikasi yang kuat di seluruh jaringan data menjadi mungkin.

10.2 APPLICATION LAYER PROTOCOLS

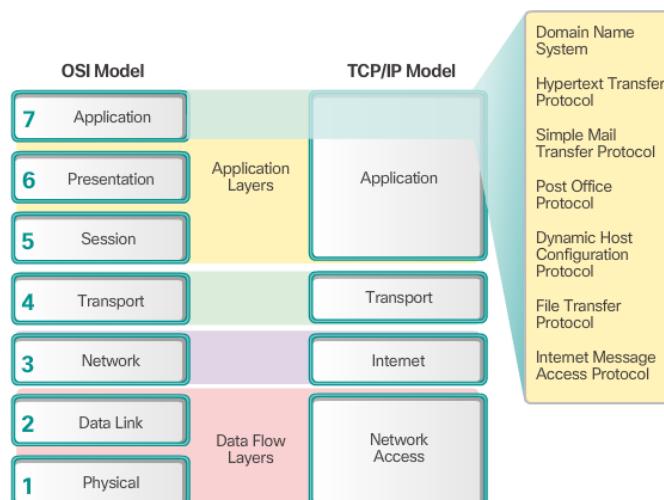
- ❖ APPLICATION, PRESENTATION AND SESSION
- APPLICATION LAYER

Lapisan Aplikasi

Lapisan aplikasi paling dekat dengan pengguna akhir. Seperti yang ditunjukkan pada gambar, itu adalah lapisan yang menyediakan antarmuka antara aplikasi yang digunakan untuk berkomunikasi dan jaringan dasar dimana pesan dikirimkan. Protokol lapisan aplikasi digunakan untuk bertukar data antar program yang berjalan pada sumber dan host tujuan.

Tiga lapisan atas model OSI (aplikasi, presentasi, dan sesi) menentukan fungsi lapisan aplikasi TCP / IP tunggal.

Ada banyak protokol lapisan aplikasi, dan protokol baru selalu dikembangkan. Beberapa protokol lapisan aplikasi yang paling banyak dikenal meliputi Hypertext Transfer Protocol (HTTP), Protokol Transfer File (FTP), protokol Transfer Berkas Trivial (TFTP), Protokol Akses Pesan Internet (IMAP), dan Protokol Nama Domain (DNS).



- PRESENTATION AND SESSION LAYER

Lapisan Presentasi

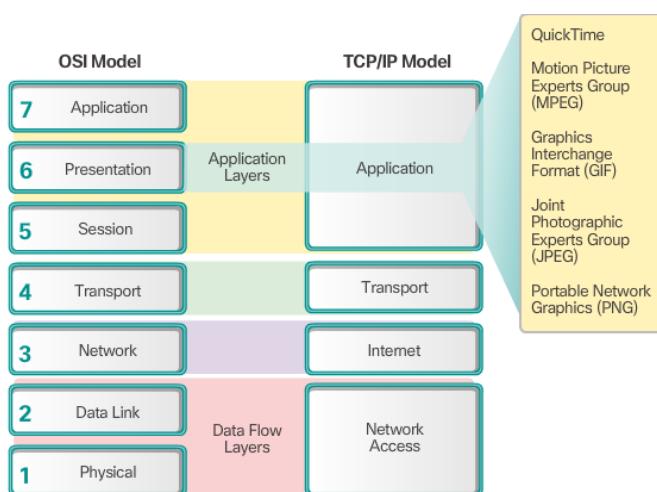
Lapisan presentasi memiliki tiga fungsi utama:

- ✓ Memformat, atau menyajikan, data pada perangkat sumber ke dalam bentuk yang kompatibel agar diterima oleh perangkat tujuan
- ✓ Mengompresi data dengan cara yang bisa didekompresi oleh perangkat tujuan
- ✓ Enkripsi data untuk transmisi dan dekripsi data setelah diterima

Seperti ditunjukkan pada gambar, lapisan presentasi memformat data untuk lapisan aplikasi, dan menetapkan standar untuk format file. Beberapa standar video yang terkenal termasuk QuickTime and Motion Picture Experts Group (MPEG). Beberapa format gambar grafis yang terkenal yang digunakan pada jaringan adalah Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), dan format Portable Network Graphics (PNG).

Lapisan Sesi

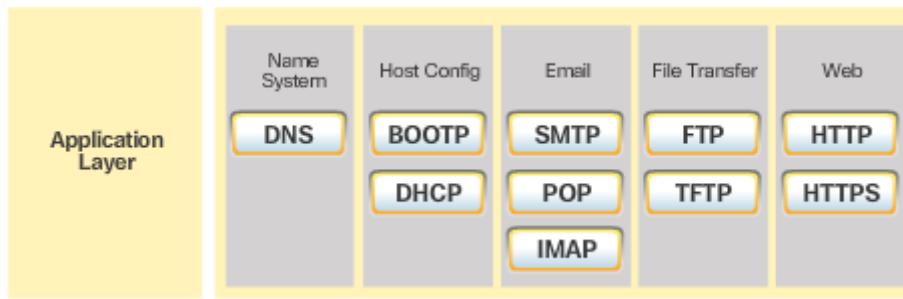
Sesuai namanya, fungsi pada lapisan sesi membuat dan memelihara dialog antara aplikasi sumber dan tujuan. Lapisan sesi menangani pertukaran informasi untuk memulai dialog, membuat mereka tetap aktif, dan memulai kembali sesi yang terganggu atau menganggur dalam jangka waktu yang lama.



- TCP / IP APPLICATION LAYER PROTOCOLS

Protokol aplikasi TCP / IP menentukan format dan informasi kontrol yang diperlukan untuk banyak fungsi komunikasi Internet yang umum. Klik setiap protokol aplikasi pada gambar untuk mempelajari lebih lanjut tentangnya.

Protokol lapisan aplikasi digunakan oleh perangkat sumber dan tujuan selama sesi komunikasi. Agar komunikasi berhasil, protokol lapisan aplikasi yang diterapkan pada host sumber dan tujuan harus kompatibel.



❖ HOW APPLICATION PROTOCOLS INTERACT WITH END-USER APPLICATIONS

- **CLIENT-SERVER MODEL**

Pada model client-server, perangkat yang meminta informasi tersebut disebut klien dan perangkat yang merespons permintaan disebut server. Proses client dan server dianggap berada di lapisan aplikasi. Klien memulai pertukaran dengan meminta data dari server, yang merespons dengan mengirimkan satu atau beberapa aliran data ke klien. Protokol lapisan aplikasi menggambarkan format permintaan dan tanggapan antara klien dan server. Selain transfer data yang sebenarnya, pertukaran ini juga memerlukan otentikasi pengguna dan identifikasi file data yang akan ditransfer.

Salah satu contoh jaringan client-server menggunakan layanan email ISP untuk mengirim, menerima dan menyimpan email. Klien email di komputer rumahan mengeluarkan permintaan ke server email ISP untuk setiap surat yang belum dibaca. Server merespons dengan mengirimkan email yang diminta ke klien. Seperti yang ditunjukkan pada gambar, transfer data dari client ke server disebut sebagai upload dan data dari server ke client sebagai download.

- **PEER-TO-PEER NETWORKS**

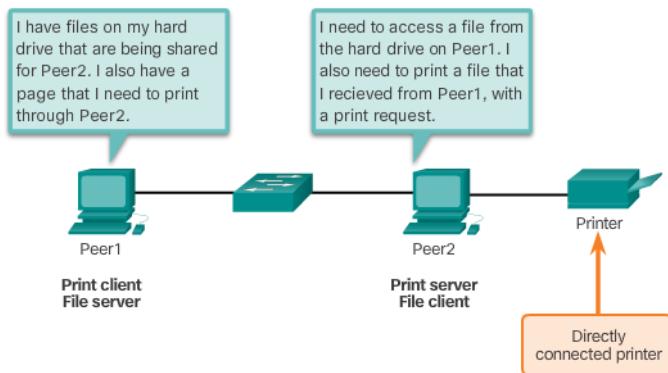
Dalam model jaringan peer-to-peer (P2P), data diakses dari perangkat peer tanpa menggunakan dedicated server.

Model jaringan P2P melibatkan dua bagian: jaringan P2P dan aplikasi P2P. Kedua bagian memiliki fitur serupa, namun dalam praktiknya bekerja cukup berbeda.

Dalam jaringan P2P, dua atau lebih komputer terhubung melalui jaringan dan dapat berbagi sumber daya (seperti printer dan file) tanpa dedicated server. Setiap perangkat akhir terhubung (dikenal sebagai peer) dapat berfungsi baik sebagai server dan klien. Satu komputer mungkin menganggap peran server untuk satu transaksi sekaligus melayani sebagai klien yang lain. Peran klien dan server ditetapkan berdasarkan permintaan per permintaan.

Contoh sederhana dari jaringan P2P ditunjukkan pada gambar. Selain berbagi file, jaringan seperti ini memungkinkan pengguna mengaktifkan permainan berjejaring, atau berbagi koneksi Internet.

Peer-to-Peer Networking



In a peer-to-peer exchange, both devices are considered equal in the communication process.

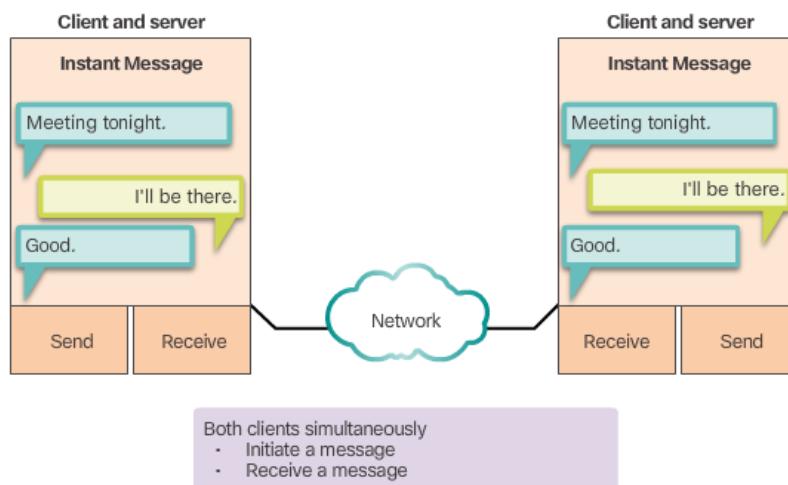
- **PEER-TO-PEER APPLICATIONS**

Aplikasi P2P memungkinkan perangkat bertindak sebagai klien dan server dalam komunikasi yang sama, seperti yang ditunjukkan pada gambar. Dalam model ini, setiap client adalah server dan setiap server client. Aplikasi P2P mengharuskan setiap perangkat akhir menyediakan antarmuka pengguna dan menjalankan layanan latar belakang.

Beberapa aplikasi P2P menggunakan sistem hibrida dimana resource sharing didesentralisasikan, namun indeks yang mengarah ke lokasi sumber daya disimpan dalam direktori terpusat. Dalam sistem hibrida, setiap peer mengakses server indeks untuk mendapatkan lokasi sumber daya yang tersimpan di peer lain.

Peer-to-Peer Applications

Client and server in the same communication



- **COMMON P2P APPLICATIONS**

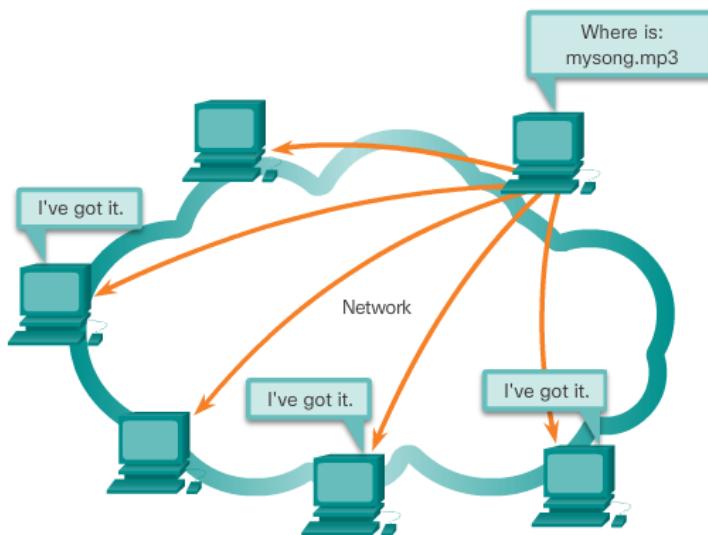
Dengan aplikasi P2P, setiap komputer dalam jaringan yang menjalankan aplikasi dapat bertindak sebagai client atau server untuk komputer lain dalam menjalankan aplikasi jaringan. Jaringan P2P yang umum meliputi:

- ✓ eDonkey
- ✓ G2
- ✓ BitTorrent
- ✓ Bitcoin

Beberapa aplikasi P2P didasarkan pada protokol Gnutella, di mana setiap pengguna membagikan keseluruhan file dengan pengguna lain. Seperti ditunjukkan pada gambar, perangkat lunak klien yang kompatibel dengan Gnutella memungkinkan pengguna untuk terhubung ke layanan Gnutella melalui Internet dan untuk mencari dan mengakses sumber daya yang dimiliki oleh rekan Gnutella lainnya. Banyak aplikasi klien Gnutella tersedia, termasuk gtk-gnutella, WireShare, Shareaza, dan Bearshare.

Banyak aplikasi P2P memungkinkan pengguna berbagi beberapa file dengan satu sama lain secara bersamaan. Klien menggunakan file kecil yang disebut file torrent untuk mencari pengguna lain yang memiliki potongan yang mereka butuhkan sehingga mereka dapat terhubung langsung dengan mereka. File ini juga berisi informasi tentang komputer pelacak yang melacak pengguna mana yang memiliki file apa. Klien meminta potongan dari beberapa pengguna sekaligus, yang dikenal sebagai kawan. Teknologi ini disebut BitTorrent. Ada banyak klien BitTorrent termasuk BitTorrent, uTorrent, Frostwire, dan qBittorrent.

Gnutella Supports P2P Applications



Gnutella allows P2P applications to search for shared resources on peers.

10.3 WELL-KNOWN APPLICATION LAYER PROTOCOLS AND SERVICES

❖ WEB AND EMAIL PROTOCOLS

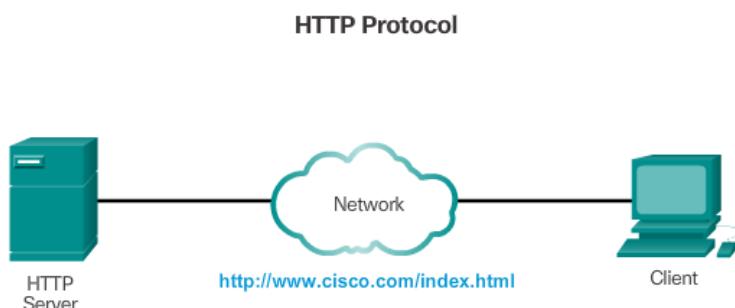
• HYPERTEXT TRANSFER PROTOCOL AND HYPERTEXT MARKUP LANGUAGE

Ketika alamat web atau uniform resource locator (URL) diketikkan ke dalam browser web, browser web menetapkan koneksi ke layanan web yang berjalan pada server menggunakan protokol HTTP. URL dan Uniform Resource Identifier (URI) adalah nama yang kebanyakan orang kaitkan dengan alamat web.

Untuk lebih memahami bagaimana browser web dan server web berinteraksi, kita bisa memeriksa bagaimana sebuah halaman web dibuka di browser. Untuk contoh ini, gunakan <http://www.cisco.com/index.html> URL.

Pertama, seperti yang ditunjukkan pada Gambar, browser menafsirkan tiga bagian URL

1. http (protokol atau skema)
2. www.cisco.com (nama server)
3. index.html (nama file tertentu yang diminta)



Browser kemudian memeriksa dengan server nama untuk mengubah www.cisco.com menjadi alamat numerik, yang digunakannya untuk terhubung ke server. Dengan menggunakan persyaratan HTTP, browser mengirimkan permintaan GET ke server dan meminta file index.html. Server, mengirimkan kode HTML untuk halaman web ini ke browser. Akhirnya, browser menentukan kode HTML dan memformat halaman untuk jendela browser.

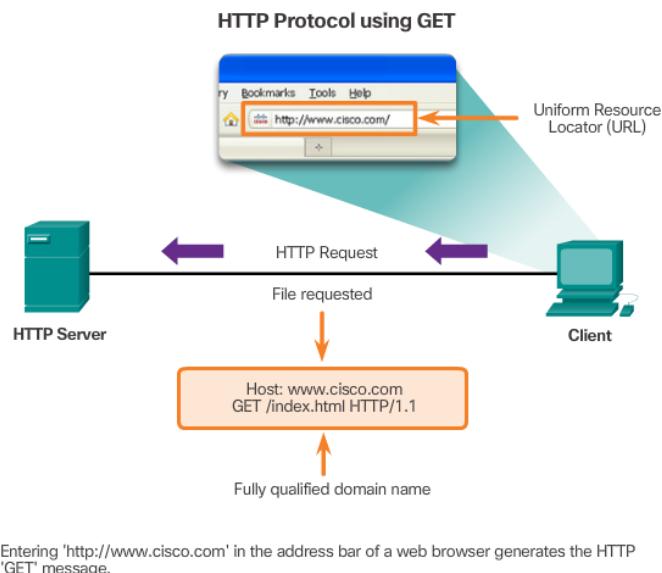
• HTTP AND HTTPS

HTTP adalah request / response protocol. Ketika klien, biasanya browser web, mengirim permintaan ke server web, HTTP menentukan jenis pesan yang digunakan untuk komunikasi tersebut. Tiga jenis pesan umum adalah GET, POST, dan PUT

- ✓ GET - Permintaan klien untuk data. Klien (browser web) mengirim pesan GET ke server web untuk meminta halaman HTML.
- ✓ POST - Upload file data ke server web seperti data form.
- ✓ PUT - Mengunggah sumber daya atau konten ke server web

Meskipun HTTP sangat fleksibel, ini bukan protokol yang aman. Pesan permintaan mengirimkan informasi ke server dalam teks biasa yang bisa dicegat dan dibaca. Tanggapan server, biasanya halaman HTML, juga tidak terenkripsi.

Untuk komunikasi aman di Internet, protokol HTTP Secure (HTTPS) digunakan. HTTPS menggunakan otentikasi dan enkripsi untuk mengamankan data saat melakukan perjalanan antara klien dan server. HTTPS menggunakan proses respons server permintaan klien yang sama seperti HTTP, namun aliran data dienkripsi dengan Secure Socket Layer (SSL) sebelum dikirim melalui jaringan.

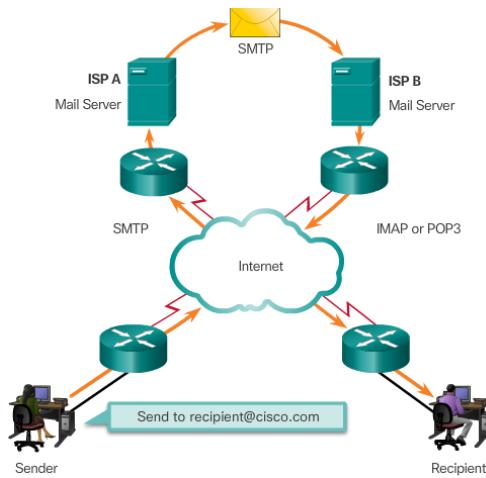


• EMAIL PROTOCOLS

Salah satu layanan utama yang ditawarkan oleh ISP adalah email hosting. Untuk berjalan di komputer atau perangkat akhir lainnya, email memerlukan beberapa aplikasi dan layanan, seperti yang ditunjukkan pada gambar. Email adalah metode pengiriman dan penyimpanan, dan menyimpan pesan elektronik melalui jaringan. Pesan email disimpan di database pada server email.

Klien email berkomunikasi dengan server surat untuk mengirim dan menerima email. Server email berkomunikasi dengan server email lain untuk mengangkut pesan dari satu domain ke domain lainnya. Klien email tidak berkomunikasi langsung dengan klien email lain saat mengirim email. Sebagai gantinya, kedua klien mengandalkan server surat untuk mengangkut pesan.

Email mendukung tiga protokol yang terpisah untuk operasi: Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), dan IMAP. Proses lapisan aplikasi yang mengirim email menggunakan SMTP. Seorang klien mengambil email, namun menggunakan salah satu dari dua protokol lapisan aplikasi: POP atau IMAP.

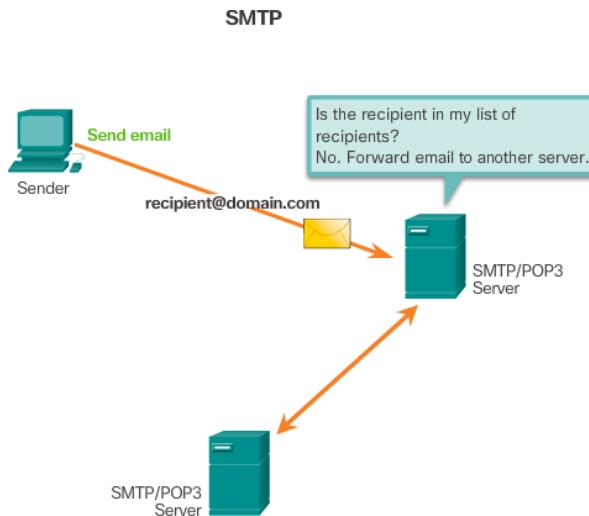


- **SMTP OPERATION**

Format pesan SMTP memerlukan header pesan dan badan pesan. Sementara badan pesan dapat berisi sejumlah teks, header pesan harus memiliki alamat email penerima yang diformat dengan benar dan alamat pengirim.

Saat klien mengirim email, proses SMTP klien terhubung dengan proses SMTP server pada port 25 yang terkenal. Setelah koneksi dilakukan, klien mencoba mengirim email ke server melalui koneksi. Saat server menerima pesan, pesan tersebut akan ditayangkan di akun lokal, jika penerima lokal, atau meneruskan pesan ke server surat lain untuk pengiriman, seperti yang ditunjukkan pada gambar.

Server email tujuan mungkin tidak online atau mungkin sibuk saat pesan email dikirim. Oleh karena itu, SMTP mengirimkan pesan yang akan dikirim di lain waktu. Secara berkala, server memeriksa antrian untuk pesan dan mencoba mengirimnya lagi. Jika pesan masih belum terkirim setelah waktu kadaluarsa yang telah ditentukan, pesan tersebut dikembalikan ke pengirim sebagai tidak terkirim.

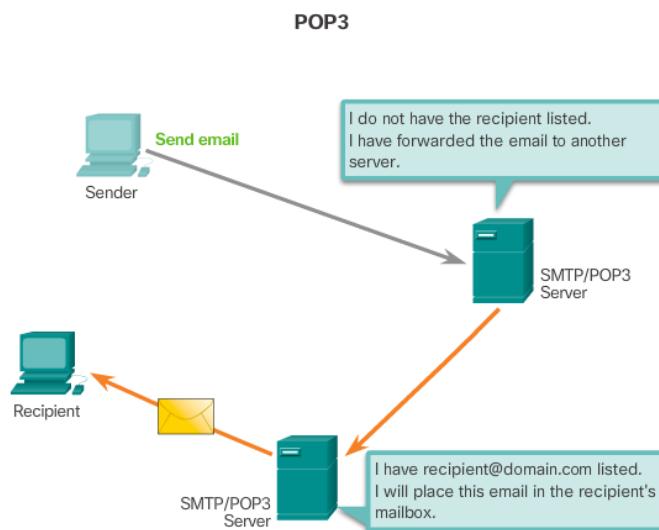


- **POP OPERATION**

POP digunakan oleh aplikasi untuk mengambil email dari server surat. Dengan POP, mail didownload dari server ke client dan kemudian dihapus di server. Ini adalah bagaimana POP beroperasi, secara default.

Server memulai layanan POP dengan mendengarkan secara pasif pada port TCP 110 untuk permintaan koneksi klien. Ketika klien ingin menggunakan layanan ini, ia mengirim permintaan untuk membuat koneksi TCP dengan server. Saat koneksi dibuat, server POP mengirimkan sapaan. Klien dan server POP kemudian bertukar perintah dan tanggapan sampai koneksi ditutup atau dibatalkan.

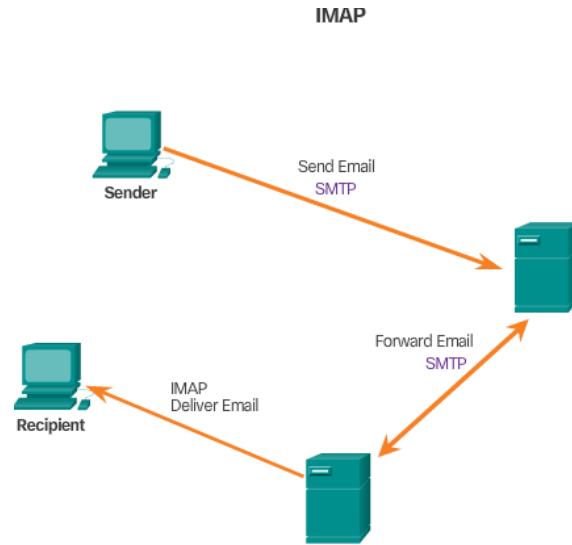
Dengan POP, pesan email didownload ke klien dan dihapus dari server, jadi tidak ada lokasi terpusat dimana pesan email disimpan. Karena POP tidak menyimpan pesan, tidak disarankan bagi usaha kecil yang memerlukan solusi backup terpusat.



- **IMAP OPERATION**

IMAP adalah protokol lain yang menjelaskan metode untuk mengambil pesan email. Tidak seperti POP, ketika pengguna terhubung ke server yang berkemampuan IMAP, salinan pesan diunduh ke aplikasi klien. Pesan asli disimpan di server sampai dihapus secara manual. Pengguna melihat salinan pesan dalam perangkat lunak klien email mereka.

Pengguna dapat membuat hierarki file pada server untuk mengatur dan menyimpan email. Struktur file itu juga diduplikasi pada klien email. Saat pengguna memutuskan untuk menghapus pesan, server akan menyinkronkan tindakan tersebut dan menghapus pesan dari server.



❖ IP ADDRESSING SERVICES

- DOMAIN NAME SERVICE

Di jaringan data, perangkat diberi label dengan alamat IP numerik untuk mengirim dan menerima data melalui jaringan. Nama domain dibuat untuk mengubah alamat numerik menjadi nama yang mudah dikenali.

Di Internet, nama domain ini, seperti <http://www.cisco.com>, jauh lebih mudah diingat orang daripada 198.133.219.25, yang merupakan alamat numerik sebenarnya untuk server ini. Jika Cisco memutuskan untuk mengubah alamat numerik www.cisco.com, itu transparan bagi pengguna karena nama domainnya tetap sama. Alamat baru ini hanya terhubung dengan nama domain dan koneksi yang ada.

Protokol DNS mendefinisikan layanan otomatis yang sesuai dengan nama sumber daya dengan alamat jaringan numerik yang diperlukan. Ini termasuk format untuk pertanyaan, tanggapan, dan data. Protokol DNS menggunakan format tunggal yang disebut pesan. Format pesan ini digunakan untuk semua jenis pertanyaan klien dan tanggapan server, pesan kesalahan, dan transfer informasi catatan sumber daya antar server.

- DNS MESSAGE FORMAT

Server DNS menyimpan berbagai jenis catatan sumber daya yang digunakan untuk menyelesaikan nama. Catatan ini berisi nama, alamat, dan jenis rekaman. Beberapa jenis rekaman ini adalah:

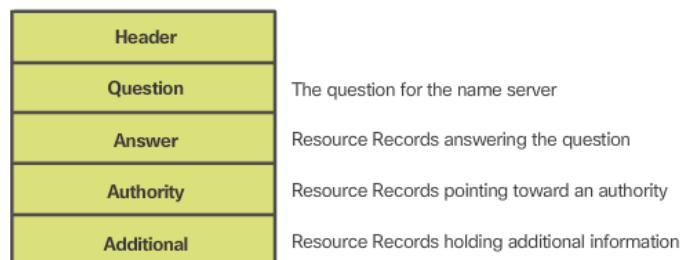
- ✓ A - Alamat perangkat akhir IPv4
- ✓ NS - server nama berwibawa
- ✓ AAAA - Perangkat akhir alamat IPv6 (diucapkan quad-A)
- ✓ MX - catatan pertukaran surat

Saat klien membuat kueri, proses DNS server pertama-tama melihat catatannya sendiri untuk menyelesaikan namanya. Jika tidak dapat menyelesaikan nama menggunakan catatan tersimpan, ia menghubungi server lain untuk menyelesaikan nama tersebut. Setelah ditemukan kecocokan dan dikembalikan ke server peminta yang asli, server sementara menyimpan alamat bernomor tersebut jika nama yang sama diminta lagi.

Layanan Klien DNS pada PC Windows juga menyimpan nama-nama yang sebelumnya dipecahkan di memori. Perintah ipconfig / displaydns menampilkan semua entri DNS yang di-cache.

DNS uses the same message format for:

- all types of client queries and server responses
- error messages
- the transfer of resource record information between servers



• DNS HIERARCHY

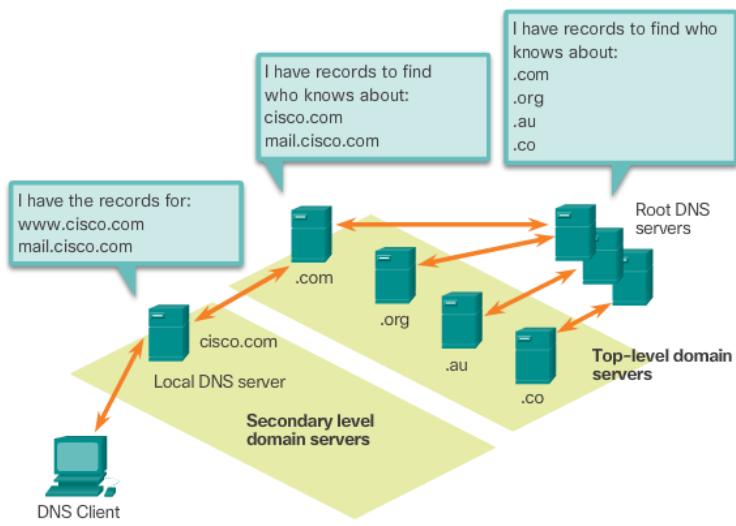
Protokol DNS menggunakan sistem hirarkis untuk membuat database untuk memberikan resolusi nama. Hirarki terlihat seperti pohon terbalik dengan akar di bagian atas dan cabang di bawahnya (lihat gambarnya). DNS menggunakan nama domain untuk membentuk hirarki.

Struktur penamaan dipecah menjadi zona kecil yang mudah dikelola. Setiap server DNS menyimpan file database tertentu dan hanya bertanggung jawab untuk mengelola pemetaan nama-ke-IP untuk sebagian kecil keseluruhan struktur DNS. Ketika server DNS menerima permintaan untuk terjemahan nama yang tidak berada dalam zona DNS-nya, server DNS meneruskan permintaan ke server DNS lain di zona yang tepat untuk diterjemahkan.

Catatan: DNS terukur karena resolusi hostname tersebar di beberapa server.

Domain tingkat atas yang berbeda mewakili jenis organisasi atau negara asal. Contoh domain tingkat atas adalah:

- ✓ .com - a business or industry
- ✓ .org - a non-profit organization
- ✓ .au – Australia
- ✓ .co – Colombia



A hierarchy of DNS servers contains the resource records that match names with addresses.

• NSLOOKUP COMMAND

Saat mengkonfigurasi perangkat jaringan, satu atau beberapa alamat DNS Server disediakan agar klien DNS dapat menggunakan resolusi nama. Biasanya penyedia layanan Internet (ISP) menyediakan alamat yang akan digunakan untuk server DNS. Saat aplikasi pengguna meminta untuk terhubung ke perangkat jarak jauh berdasarkan namanya, klien DNS yang meminta menanyakan server nama untuk menyelesaikan nama tersebut ke alamat numerik.

Sistem operasi komputer juga memiliki utilitas yang disebut nslookup yang memungkinkan pengguna untuk secara manual meminta nama server untuk menyelesaikan nama host yang diberikan. Utilitas ini juga dapat digunakan untuk memecahkan masalah resolusi nama dan untuk memverifikasi status server nama saat ini.

Pada Gambar dibawah, ketika perintah nslookup dikeluarkan, server DNS default yang dikonfigurasi untuk host Anda ditampilkan. Nama host atau domain dapat dimasukkan pada prompt nslookup. Utilitas nslookup memiliki banyak pilihan yang tersedia untuk pengujian ekstensif dan verifikasi proses DNS.

```
C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\bradfjoh>cd..
C:\Documents and Settings>nslookup
Default Server: dns-sj.cisco.com
Address: 171.70.168.183

> www.cisco.com
Server: dns-sj.cisco.com
Address: 171.70.168.183
Name: www.cisco.com
Address: 198.133.219.25

> cisco.netacad.net
Server: dns-sj.cisco.com
Address: 171.70.168.183
Non-authoritative answer:
Name: cisco.netacad.net
Address: 128.107.229.50
>
```

- **DYNAMIC HOST CONFIGURATION PROTOCOL**

Dynamic Host Configuration Protocol (DHCP) untuk layanan IPv4 mengotomatisasi penugasan alamat IPv4, subnet mask, gateway, dan parameter jaringan IPv4 lainnya. Ini disebut sebagai dynamic addressing. Alternatif pengalaman dinamis adalah pengalaman statis. Saat menggunakan pengalaman statis, administrator jaringan secara manual memasukkan informasi alamat IP pada host.

Saat host terhubung ke jaringan, server DHCP dihubungi, dan sebuah alamat diminta. Server DHCP memilih alamat dari serangkaian alamat yang dikonfigurasi yang disebut kolam dan menugaskan (menyewakan) ke host.

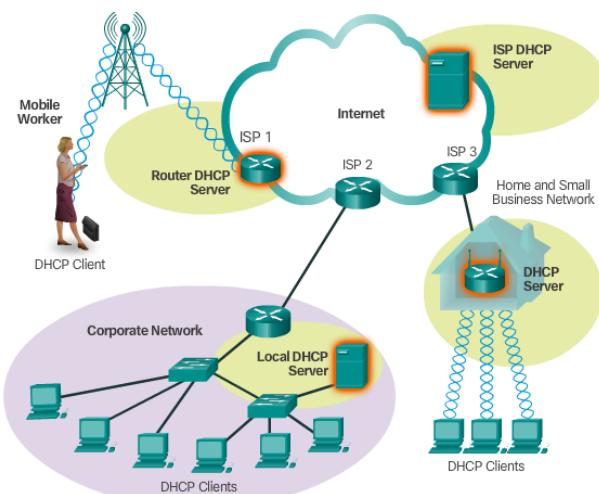
Pada jaringan yang lebih besar, atau di mana populasi pengguna sering berubah, DHCP lebih disukai untuk tugas alamat. Pengguna baru mungkin datang dan membutuhkan koneksi; Orang lain mungkin memiliki komputer baru yang harus terhubung. Daripada menggunakan pengalaman statis untuk setiap koneksi, lebih efisien jika alamat IP ditetapkan secara otomatis menggunakan DHCP.

Alamat terdistribusi DHCP disewa untuk jangka waktu tertentu. Bila masa sewa habis, alamat dikembalikan ke kolam untuk digunakan kembali jika host telah dimatikan atau diambil dari jaringan. Pengguna dapat dengan bebas berpindah dari lokasi ke lokasi dan dengan mudah membangun kembali koneksi jaringan melalui DHCP.

Seperti ditunjukkan oleh gambar, berbagai jenis perangkat bisa berupa server DHCP. Server DHCP di sebagian besar jaringan menengah-ke-besar biasanya merupakan server berbasis PC khusus lokal. Dengan jaringan rumah, server DHCP biasanya terletak di router lokal yang menghubungkan jaringan rumah ke ISP.

Banyak jaringan menggunakan DHCP dan pengalaman statis. DHCP digunakan untuk host tujuan umum, seperti perangkat pengguna akhir. Pengalaman statis digunakan untuk perangkat jaringan, seperti gateway, switch, server, dan printer.

DHCPv6 (DHCP untuk IPv6) menyediakan layanan serupa untuk klien IPv6. Salah satu perbedaan penting adalah bahwa DHCPv6 tidak menyediakan alamat gateway default. Ini hanya bisa didapat secara dinamis dari pesan Router Advertisement Router.



- **DHCP OPERATION**

Seperti ditunjukkan pada gambar, saat perangkat IPv4 yang dikonfigurasi DHCP memasang atau menghubungkan ke jaringan, klien menyiarkan pesan DHCP menemukan (DHCPDISCOVER) untuk mengidentifikasi server DHCP yang tersedia di jaringan. Server DHCP membalas dengan pesan DHCP (DHCPOFFER), yang menawarkan sewa kepada klien. Pesan penawaran berisi alamat IPv4 dan subnet mask yang akan ditetapkan, alamat IPv4 dari server DNS, dan alamat IPv4 dari gateway default. Penawaran sewa juga mencakup masa sewa.

Klien mungkin menerima beberapa pesan DHCPOFFER jika ada lebih dari satu server DHCP di jaringan lokal. Oleh karena itu, ia harus memilih di antara keduanya, dan mengirimkan pesan DHCP request (DHCPREQUEST) yang mengidentifikasi server eksplisit dan penawaran sewa yang diterima klien. Seorang klien juga dapat memilih untuk meminta alamat yang sebelumnya telah dialokasikan oleh server.

Dengan asumsi bahwa alamat IPv4 yang diminta oleh klien, atau yang ditawarkan oleh server, masih tersedia, server mengembalikan pesan konfirmasi DHCP (DHCPACK) yang mengakui klien bahwa masa sewa telah selesai. Jika penawaran tidak berlaku lagi, server yang dipilih akan merespons dengan pesan konfirmasi negatif DHCPNAK. Jika pesan DHCPNAK dikembalikan, proses seleksi harus dimulai lagi dengan pesan DHCPDISCOVER baru yang sedang dikirim. Setelah klien memiliki masa sewa, maka harus diperbarui sebelum masa sewa habis masa berlakunya melalui pesan DHCPREQUEST lainnya.

Server DHCP memastikan bahwa semua alamat IP unik (alamat IP yang sama tidak dapat diberikan ke dua perangkat jaringan yang berbeda secara bersamaan). Sebagian besar penyedia layanan internet menggunakan DHCP untuk mengalokasikan alamat kepada pelanggan mereka.

DHCPv6 memiliki kumpulan pesan yang serupa dengan yang ditunjukkan pada gambar untuk DHCP untuk IPv4. Pesan DHCPv6 adalah SOLICIT, ADVERTISE, INFORMATION REQUEST, dan REPLY



❖ FILE SHARING SERVICES

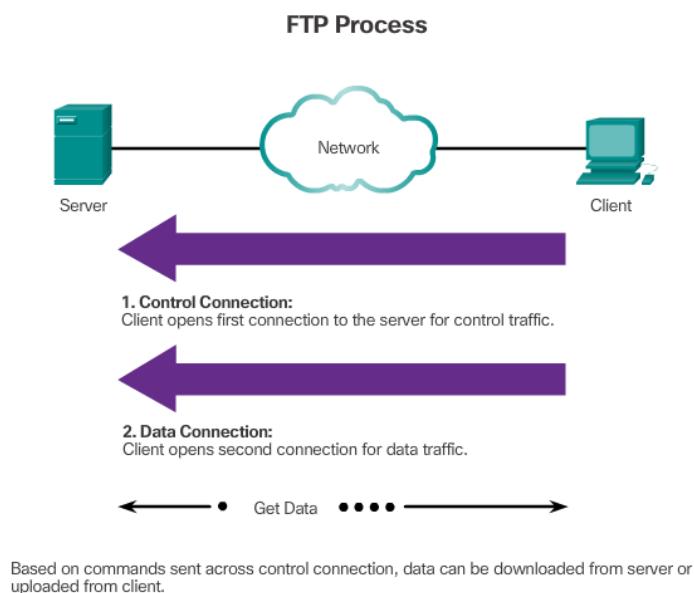
• FILE TRANSFER PROTOCOL

FTP adalah protokol lapisan aplikasi yang umum digunakan lainnya. FTP dikembangkan untuk memungkinkan transfer data antara klien dan server. Klien FTP adalah aplikasi yang berjalan di komputer yang digunakan untuk mendorong dan menarik data dari server yang menjalankan daemon FTP (FTPd).

Seperti gambar yang diilustrasikan, untuk berhasil mentransfer data, FTP memerlukan dua koneksi antara klien dan server, satu untuk perintah dan balasan, yang lainnya untuk transfer file yang sebenarnya:

- ✓ Klien menetapkan koneksi pertama ke server untuk lalu lintas kontrol menggunakan port TCP 21, yang terdiri dari perintah klien dan balasan server.
- ✓ Klien menetapkan koneksi kedua ke server untuk transfer data aktual menggunakan port TCP 20. Sambungan ini dibuat setiap kali ada data yang akan ditransfer.

Transfer data bisa terjadi di kedua arah. Klien bisa mendownload (pull) data dari server, atau klien bisa mengupload (push) data ke server.



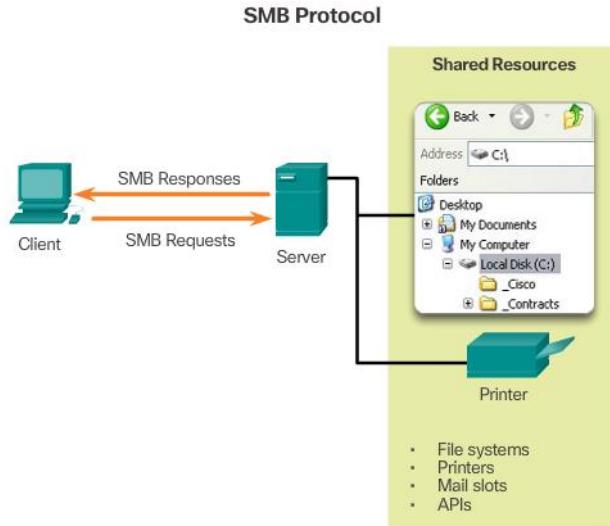
• SERVER MESSAGE BLOCK

Server Message Block (SMB) adalah protokol berbagi file klien / server yang menggambarkan struktur sumber daya jaringan bersama, seperti direktori, file, printer, dan port serial. Ini adalah protokol request-response. Semua pesan SMB berbagi format umum. Format ini menggunakan header berukuran tetap, diikuti oleh parameter berukuran variabel dan komponen data.

Pesan SMB dapat:

- ✓ Mulai, autentikasi, dan akhiri sesi
- ✓ Kontrol file dan akses printer
- ✓ Mengizinkan aplikasi mengirim atau menerima pesan ke atau dari perangkat lain

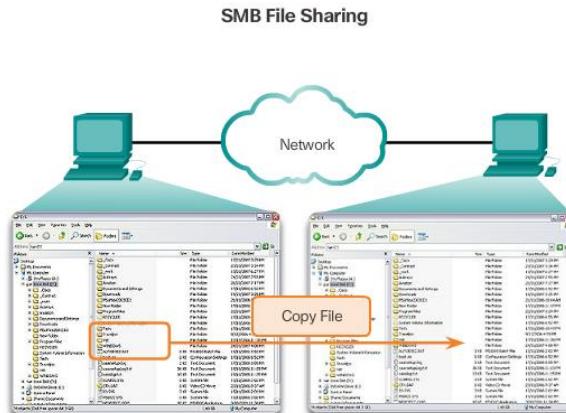
Layanan berbagi file dan cetak SMB telah menjadi andalan jaringan Microsoft. Dengan diperkenalkannya seri perangkat lunak Windows 2000, Microsoft mengubah struktur dasar penggunaan SMB. Pada versi sebelumnya produk Microsoft, layanan SMB menggunakan protokol non-TCP / IP untuk menerapkan resolusi nama. Dimulai dengan Windows2000, semua produk Microsoft berikutnya menggunakan penamaan DNS, yang memungkinkan protokol TCP / IP untuk secara langsung mendukung pembagian sumber daya SMB, seperti yang ditunjukkan pada Gambar dibawah.



SMB is a client-server, request-response protocol. Servers can make their resources available to clients on the network.

Berbeda dengan file sharing yang didukung oleh FTP, klien membangun koneksi jangka panjang ke server. Setelah koneksi dibuat, pengguna klien dapat mengakses sumber daya di server seolah-olah sumber daya lokal ke host klien.

Sistem operasi LINUX dan UNIX juga menyediakan metode untuk berbagi sumber daya dengan jaringan Microsoft yang menggunakan versi SMB yang disebut SAMBA. Sistem operasi Apple Macintosh juga mendukung pembagian sumber daya menggunakan protokol SMB.



A file may be copied from PC to PC with Windows Explorer using the SMB protocol.

LATIHAN SOAL 10

1. Jelaskan yang dimaksud dengan aplikasi layer
2. Jelaskan yang dimaksud dengan protokol aplikasi
3. Jelaskan bagaimana protokol aplikasi berinteraksi dengan aplikasi end-user
4. Jelaskan perbedaan antara HTTP & HTTPS
5. Apa itu SMTP Operation
6. Jelaskan yang dimaksud dengan IMAP Operation
7. Jelaskan yang dimaksud dengan POP Operation
8. Jelaskan apa itu DNS
9. Apa itu DHCP
10. Jelaskan cara kerja FTP