

CCNA 1

Daftar Isi

| | |
|--|-----------|
| Chapter 1 Introducing to Networking | 2 |
| Chapter 2 Networking Fundamentals | 5 |
| Chapter 3 Networking Media | 7 |
| Chapter 4 Cable Testing | 15 |
| Chapter 5 Cabling LAN and WAN | 18 |
| Chapter 6 Ethernet Fundamental | 23 |
| Chapter 7 Ethernet Technologies | 26 |
| Chapter 8 Ethernet Switching | 28 |
| Chapter 9 TCP/IP Protocol Suite & IP Addressing | 33 |
| Chapter 10 Routing Fundamental & Subnet | 39 |
| Chapter 11 TCP / IP Transport and Application Layer | 42 |

Chapter 1

Introduction to Networking

Jaringan

Komputer yang saling berhubungan dan dapat berkomunikasi dengan menggunakan protokol tertentu dan memakai alat misalnya *Network Internet Card (NIC)*, modem, dll. Contohnya yaitu internet.

Tipe koneksi internet ada 3 :

- | | | |
|--------------------------------------|---|---|
| <input type="checkbox"/> Physical | : | Dengan modem atau NIC. |
| <input type="checkbox"/> Logical | : | Protokol, misalnya TCP/IP (Transmission Control Protocol/Internet Protocol) |
| <input type="checkbox"/> Application | : | Menggunakan browser, contoh IE atau Netscape Navigator |

Bagian-bagian PC :

- | | | |
|---|---|--|
| <input type="checkbox"/> Resistor | : | Hambatan. |
| <input type="checkbox"/> Transistor | : | Memperkuat sinyal & membuka & menutup circuit. |
| <input type="checkbox"/> Capacitor | : | Menyimpan energi. |
| <input type="checkbox"/> Integrated Circuit | : | Kumpulan transistor. |
| TM Expansion slot | | |
| TM Floppy Disk | | |
| TM Hard Disk | | |
| TM CD-ROM | | |
| TM Video & Audio port | | |
| TM Serial Port | | |
| TM Parallel port | | |
| TM Motherboard | | |

Serial port digunakan untuk menghubungkan PC ke console router guna manajemen router.

Koneksi internet memerlukan modem yang dapat berupa internal maupun eksternal.

Koneksi internet local dapat menggunakan NIC, yang perlu diperhatikan adalah

- | |
|--|
| TM Protokol (ethernet, token ring, FDDI) |
| TM Type of media (coaxial, wireless, twisted pair) |
| TM Type of bus (PCI, ISA) |

Untuk notebook dapat menggunakan PCMCIA, adapun koneksi network dengan PING (Pocket Internetwork Gropher) apakah sudah connect / belum.

Network Math

- | | | |
|---|---|-----------|
| <input type="checkbox"/> Basis 2 (Binary) | : | 1100 0000 |
| <input type="checkbox"/> Basis 10 (Decimal) | : | 192 |
| <input type="checkbox"/> Basis 16 (Hexadecimal) | : | C2 |

Konversi Basis

Contoh :

1. Ubahlah 16 ke binary !

$$\begin{array}{r} 16 \\ 2 \overline{) } \quad 0 \\ 8 \\ 2 \overline{) } \quad 0 \\ 4 \\ 2 \overline{) } \quad 0 \\ 2 \\ 2 \overline{) } \quad 0 \\ 1 \end{array}$$

2. Ubahlah 0001 0000 ke decimal !

$$\begin{array}{ccccccc} & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ & | & | & | & | & | & | & | \\ 2^7 & 2^6 & 2^5 & 2^4 & 2^3 & 2^2 & 2^1 & 2^0 \end{array}$$

$2^4 = 16$

Konversi Basis 10 ke Basis 16

Bil. Basis 16

| | |
|-------|--------|
| 0 > 0 | 9 > 9 |
| 1 > 1 | 10 > A |
| 2 > 2 | 11 > B |
| 3 > 3 | 12 > C |
| 4 > 4 | 13 > D |
| 5 > 5 | 14 > E |
| 6 > 6 | 15 > F |
| 7 > 7 | |
| 8 > 8 | |

Contoh :

- a) Ubahlah 49 ke hexadecimal !

$$\begin{array}{r} 49 \\ 16 \overline{) } \quad 1 \\ 3 \end{array}$$

jadi hexadecimal dari 49 adalah 31

- b) Ubahlah hexadecimal 31 ke decimal !

$$\begin{array}{r} 31 \\ | \quad | \\ 3 \times 16^1 + 1 \times 16^0 \\ 48 \quad + \quad 1 = 49 \end{array}$$

Konversi Basis 2 ke 16

- a) Ubahlah 1100 0010 ke hexadecimal !

$$\begin{array}{r} 1100 \quad 0010 \\ \underbrace{\quad}_{12} \quad \underbrace{\quad}_{2} \end{array}$$

---> C 2

atau ---> 0xC2

b) Ubahlah 0xC2 ke binary !

| | |
|-----------------|------|
| C | 2 |
| 12 | 2 |
| 1100 | 0010 |
| ----> 1100 0010 | |

Operasi AND

| | | |
|--------|--------|--------|
| 11 > 1 | 11 > 1 | 11 > 0 |
| 10 > 0 | 10 > 1 | 10 > 1 |
| 01 > 0 | 01 > 1 | 01 > 1 |
| 00 > 0 | 00 > 0 | 00 > 0 |

Operasi OR

| | | |
|--------|-----------|-----------|
| 11 > 1 | 1100 1001 | 1100 1001 |
| 10 > 1 | 0100 1010 | 0100 1010 |
| 01 > 1 | ----- OR | ----- XOR |
| 00 > 0 | 1100 1011 | 1000 0011 |

Operasi XOR

Contoh :

| | | |
|-----------|-----------|-----------|
| 1100 1001 | ----- AND | 1100 1001 |
| 0100 1010 | | 0100 1010 |
| 0100 1000 | | 1000 0011 |

Chapter 2

Networking Fundamentals

Peralatan-peralatan jaringan:

1. End-user device

Peralatan seperti computer, NIC, printer pada user.

2. Network device

- repeater / hub: layer 1 OSI layer, mengirim data ke semua yang terkoneksi selain port asal data.
- bridge / switch: layer 2 OSI layer, mengirim data bentuk frame ke tujuan berdasarkan MAC address.
- router: layer 3 OSI layer, menghubungkan 2 network yang berbeda; mengirim data ke tujuan bedasarkan IP address.

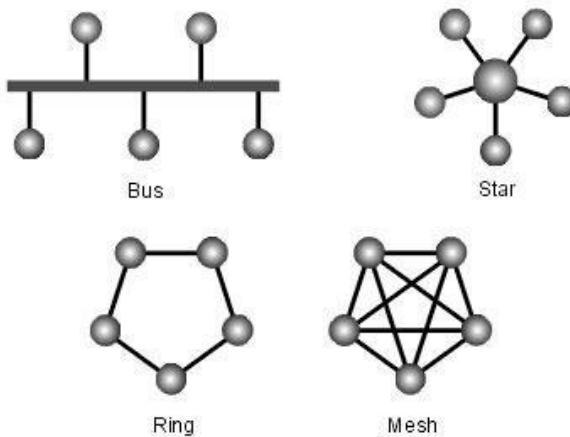
Istilah-istilah jaringan:

- A. **Sneaker net** : istilah untuk sekumpulan computer yang tidak terkoneksi jaringan.
- B. **Local Area Network (LAN)** : jaringan skala kecil, biasanya dalam 1 bangunan atau area.
- C. **Wide Area Network (WAN)** : jaringan skala besar, contohnya: antar kota atau antar negara.

Protokol digunakan sebagai aturan dalam berkomunikasi. Contoh protocol:

1. FTP untuk mengirim dan membuka data pada FTP server.
2. TFTP untuk recovery system pada router atau switch.
3. DHCP untuk dynamic IP address.
4. DNS untuk memetakan domain name ke IP address.
5. Telnet untuk remote login ke komputer lain.
6. SNMP untuk manajemen jaringan.
7. SMTP untuk menangani email.
8. HTTP untuk menangan request halaman web.

Macam-macam network topology:



OSI Layer

OSI Layer adalah standarisasi layer pada jaringan yang paling umum, terdiri dari:

1. Application
2. Presentation
3. Session
4. Transport: Datanya dalam bentuk segment.
5. Network: Memecah segment ke dalam beberapa packet. Di packet ada ada informasi IP address untuk dikirim lewat routing table.
6. Data Link: Data dikirim dalam bentuk frame dan ada informasi MAC address.
7. Physical: Layer paling bawah yang menggambarkan koneksi titik jaringan misalnya cable. Data dikirim dalam bentuk bits.

TCP/IP

TCP/IP adalah network protocol yang paling sering dipakai untuk jaringan, salah satunya adalah jaringan Internet. Layer TCP/IP terdiri dari:

1. Application: Penggabungan layer Application, Presentation dan Session pada OSI Layer.
2. Transport: Sama dengan layer Transport pada OSI Layer.
3. Internet: Sama dengan layer Network pada OSI Layer.
4. Network Access: Penggabungan layer Data Link dan Physical pada OSI Layer.

Bandwidth

Bandwidth adalah besar jalur data.

$$T = S / Bw$$

T = waktu untuk transfer

S = size dari file

Bw = Bandwidth

Chapter 3

Networking Media

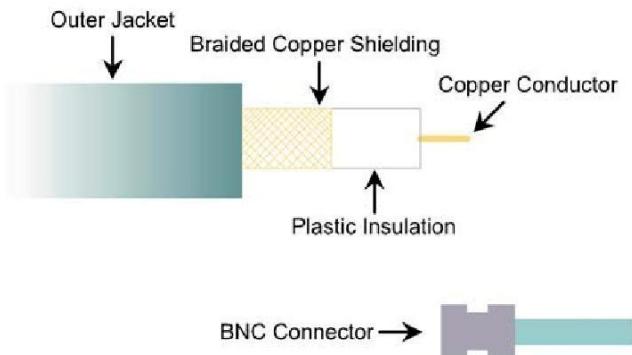
Networking Media

- Copper media
- Optical media
- Wireless media

Copper media.

Media yang paling banyak digunakan dalam jaringan LAN adalah copper cable/ kabel tembaga. Terdiri dari banyak macam jenis seperti:

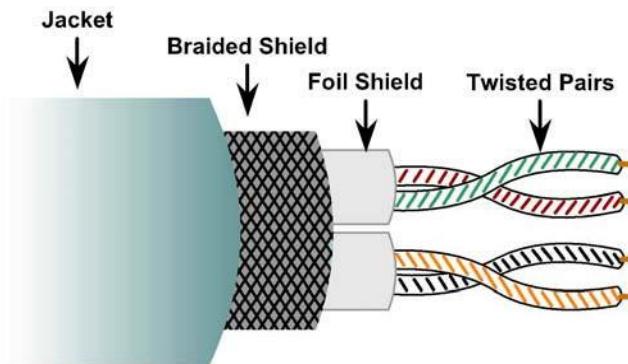
- Coaxial kabel



- Bandwidth: 10Mbps
- Biaya tidak terlalu mahal
- Media dan connector size: Medium
- Jarak maximum kabel: 500m

Dalam LAN, kabel coaxial mempunyai nilai plus yang tidak dipunyai kabel STP dan UTP, yaitu *jarak maximum* yang dapat digunakan tanpa menggunakan bantuan repeater. Repeater adalah alat yang memperkuat signal di dalam jaringan agar bisa meng-cover jarak yang jauh. Coaxial kabel lebih murah dari fiber optic dan teknologinya lebih dikenal umum. Kebanyakan digunakan pada alat-alat telekomunikasi, seperti: Telivisi kabel (kabel vision). Saat sekarang ini jenis Coaxial kabel sudah jarang dipakai pada jaringan Ethernet.

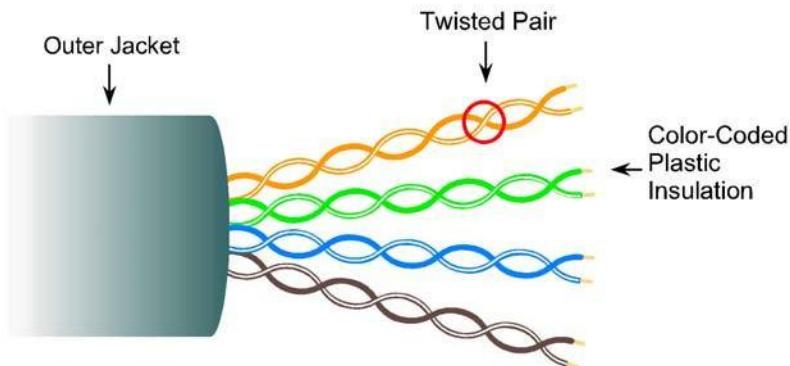
- Shielded twisted-pair (STP) kabel



- Bandwidth: 0-100 Mbps
- Biaya: Moderate/ agak mahal
- Media dan connector size: Sedang sampai Besar
- Maximum panjang kabel: 100m

Jarang digunakan pada jaringan, karena faktor harga dan perlu di-grounded/pembumian pada kedua ujungnya untuk mengurangi/menghilangkan noise.

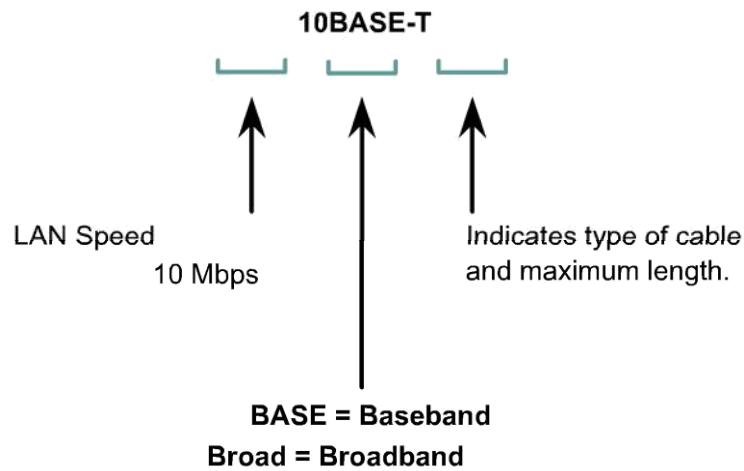
-Unshielded twisted-pair (UTP)



- Bandwidth: 10 – 100 – 1000 Mbps(tergantung dari kualitas/ katagori kabel)
- Biaya: lebih murah
- Media dan connector size: kecil
- Maximum panjang kabel: 100m

Spesifikasi Kabel:

- 10 BASE-T
- 10 BASE5
- 10 BASE2



10BASE-T

Bandwidth 10Mbps, type transmission baseband (transmitted digitally), T for twisted cable (maximum cable length 100m).

10 BASE5

Bandwidth 10Mbps, type transmission baseband, 5 for maximum length 500m, using coaxial cable type thicknet.

10 BASE2

Bandwidth 10Mbps, type transmission baseband, 2 for maximum length approximately 185m, using coaxial cable type thinnet.

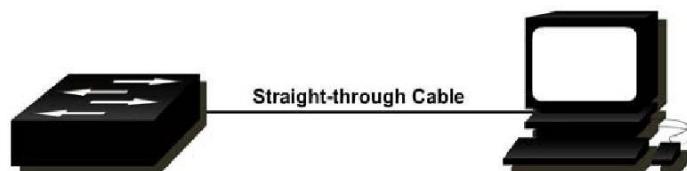
These three specifications above are also known as LEGACY of ETHERNET (the first specification used in networks).

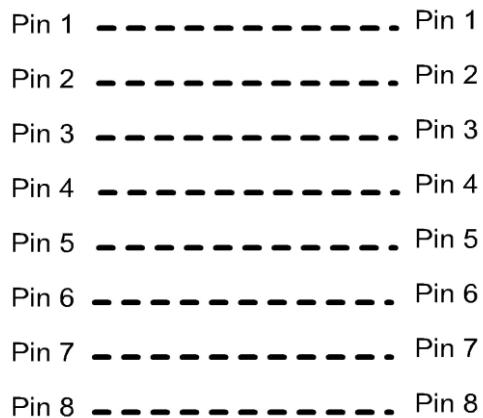
UTP cable, the medium that is most commonly used in today's networks. The main advantage is its small size (easy to install in ducting or anywhere). Bandwidth that can reach up to 1000 Mbps, of course, the price is not very expensive.

Some connection types used between network devices:

- Straight-through cable

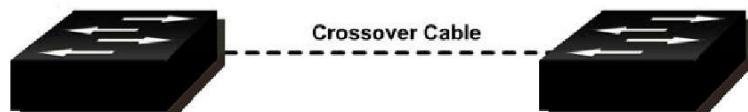
Used on devices that are not the same, such as switch-PC, hub-PC.



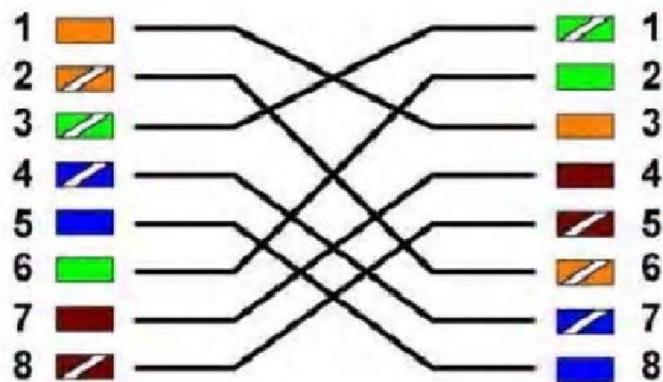


- Crossover kabel

Digunakan untuk menghubungi device-device yang sama/sejenis seperti, switch-switch, switch-hub, router-pc.

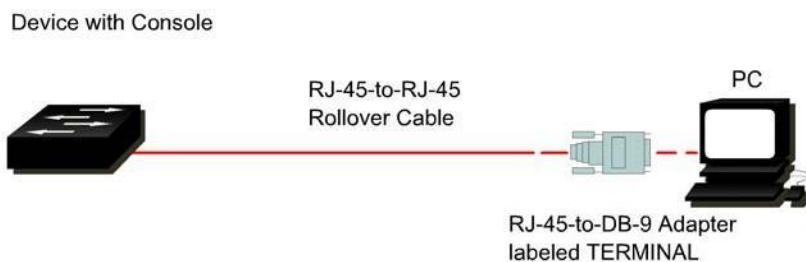


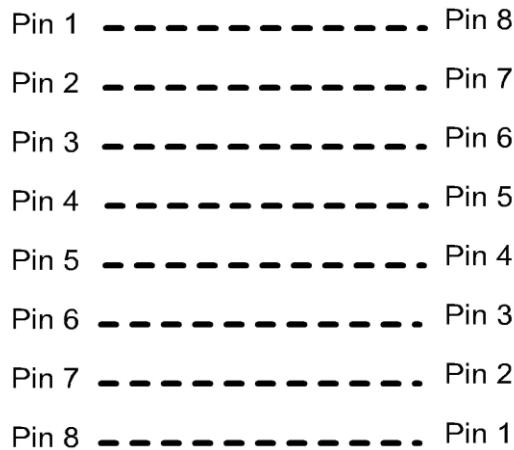
EIA/TIA T568B Crossover Diagram



- Rollover kab

Digunakan hanya untuk converter DB9(port serial pc) ke port console, biasanya untuk melakukan manajemen. Menghubungkan switch (manageable)-pc dan Router-pc.

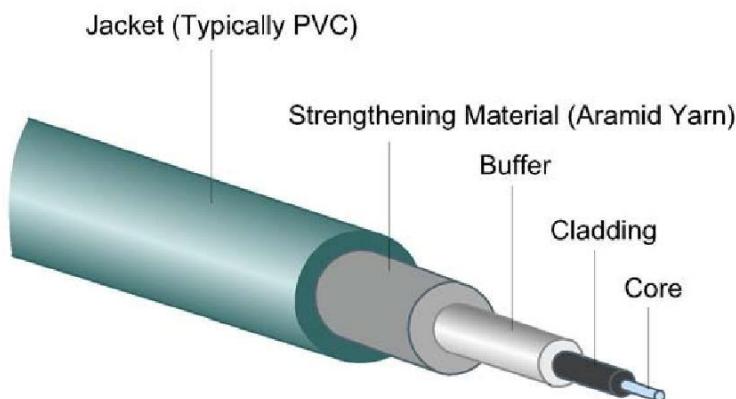




- Optical media

Cahaya yang digunakan dalam jaringan fiber optic adalah sinar laser. Fiber optic adalah medium yang paling sering digunakan karena jaraknya yang jauh, bandwidth yang tinggi, transmisi point to point yang dibutuhkan pada backbone LAN dan WAN.

Energi cahaya di gunakan untuk mengirim sejumlah besar data dengan aman dan dalam jarak yang jauh. Signal cahaya di dalam fiber ini dihasilkan dari transmitter yang merubah dari signal listrik menjadi signal cahaya. Receiver merubah cahaya yang datang dari ujung kabel kembali menjadi signal listrik.



Setiap fiber optic kabel yang digunakan untuk jaringan terdiri dari 2 core fiber yang terpisah. Seperti kabel twisted pair, kabel yang terpisah digunakan untuk men transmit dan receive, fiber optic juga menggunakan satu fiber untuk men transmit/mengirim dan satu lagi untuk me receive/menerima.





Gambar: ujung/connector kabel optic(1 untuk transmit dan 1 untuk receive)

- Wireless Media

Wireless teknologi memiliki kelebihan dibandingkan dengan media kabel seperti, device dapat dibawa ke mana saja/mobile, sedangkan kabel dan fiber terbatas. Terdapat standart dan regulasi yang harus disepakati bersama agar wireless teknologi dapat saling terkoneksi dan ini distandarisasi dengan IEEE 802.11, standart untuk WLANs. Terbagi atas:

- 802.11b
- 802.11a
- 802.11g

802.11b disebut juga dengan *Wi-Fi* Wireless Fidelity, bekerja pada frekwensi 2,4 Ghz, speed 11 Mbps, throughput 1-2 Mbps, menggunakan Direct Sequence Spread Spectrum (DSSS), yang berkembang menjadi Frequency Hopping Spread Spectrum (FHSS).

802.11a bekerja pada frekwensi 5 Ghz, speed 54-108 Mbps, throughput 20-26Mbps, tidak compatible dengan Wi-Fi

802.11g bekerja pada frekwensi 2,4GHZ, speed 54-108 Mbps, throughput 20-26 Mbps, menggunakan Orthogonal Frequency Division Multiplexing(OFDM), compatible dengan Wi-Fi

Macam-macam topologi wireless:

- Independent Basic Service Set (IBSS)

Hubungan terjadi antara 2 devices wireless,tanpa menggunakan acces point sebagai sentral ‘ad-hoc’ topologi, seperti peer to peer dalam jaringan kabel, banyak permasalahan pada compatibility antara beberapa merk.



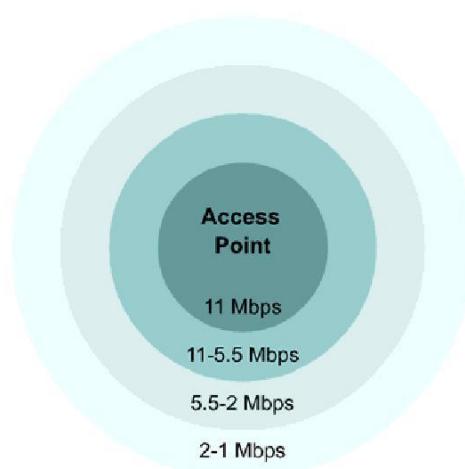
Gambar. Internal wireless NIC untuk desktop atau server

- Basic Service Net (BSS)

Untuk mengatasi masalah kompatibilitas antar devices maka digunakan Access Point(AP) sebagai sentral hub dari jaringan WLAN, AP dihubungkan pada jaringan kabel LAN. Range efektif 90-150m.

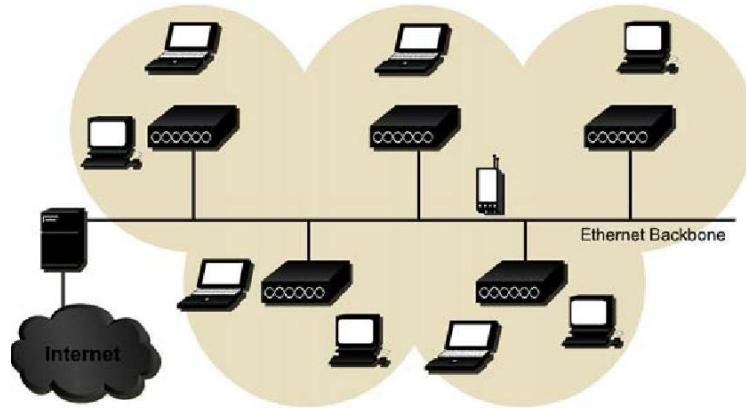


Gambar. Access point



- Extended Service Set (ESS)

Untuk mengatasi range tadi, maka digunakan beberapa Access point agar wilayah yang dicover menjadi luas/overlaping.



Komunikasi Wireless menggunakan tiga type frame: control (contoh authentication request frame dan association request frame), management(frame berupa SSid dari Access point ke client), dan data frame(data yang akan dikirim).

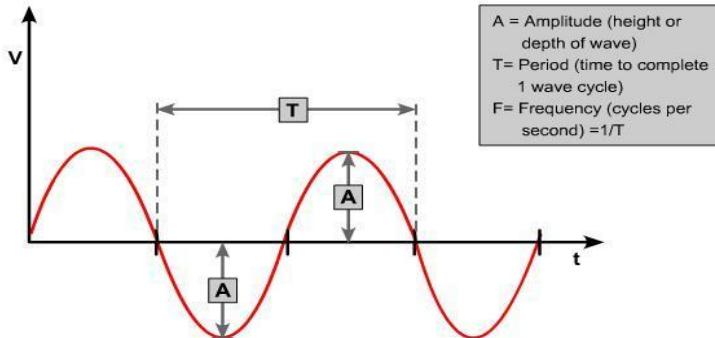
Untuk mencegah collision dalam sharing radio frekwensi, WLAN menggunakan Carrier Sense Multiple Access/Collision Avoidence (CSMA/CA), untuk memastikan request to send/ clear to send (RTS/CTS) terjadi sebelum data dikirim.

Chapter 4 Cable Testing

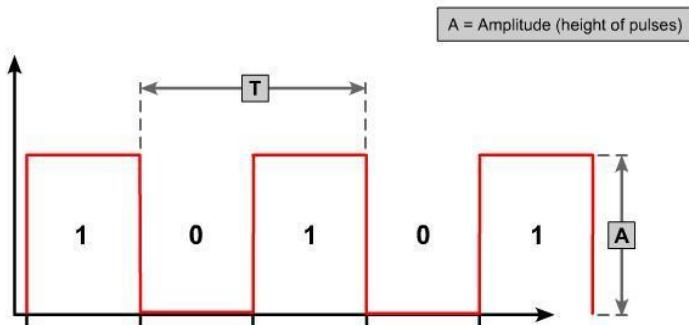
Waves atau gelombang dalam bahasa Indonesia adalah energi yang merambat dari 1 tempat ke tempat lain.

Terdapat 2 jenis gelombang,yaitu:

- Sine Waves yang mirip signal Analog
Contoh:



- Square Waves yang mirip signal Digital
Contoh:



Seluruh jenis gelombang memiliki atribut yang sama yaitu:

- Frequency:Banyaknya gelombang dalam 1 periode
- Amplitudo:Tingginya 1 gelombang,dan
- Pulses

Desibel adalah besaran dari power signal.bila nilainya negatif maka signal tersebut mengalami loss(kehilangan) dan bila nilainya positif maka signal bertambah atau malah besarnya kelebihan.

Rumus perhitungan decibel:

- Fiber & Wireless :

$$db = 10 \log \frac{P_{\text{new}}}{P_{\text{old}}}$$

- Copper Media :

$$db = 20 \log \frac{V_{\text{new}}}{V_{\text{old}}}$$

Gangguan pada signal biasa disebut Noise yang bias berasal dari:

- Kabel yang saling berdekatan
- Electro Magnetic Interference(EMI)
- Radio Frequency Interference(RFI)

Noise dapat mempengaruhi Keseluruhan signal yang ditransmisikan(white noise), dan juga dapat pula hanya sebagian (Narrow band Interference).

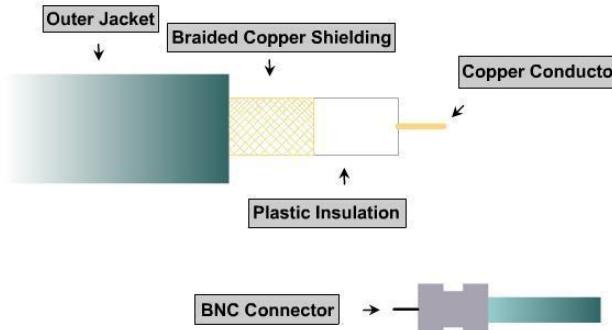
Bandwidth dibagi menjadi 2,yaitu:

- Analog Bandwidth,biasanya pada Radio atau Amplifier
- Digital Bandwidth,biasanya digunakan pada pengiriman data pada computer

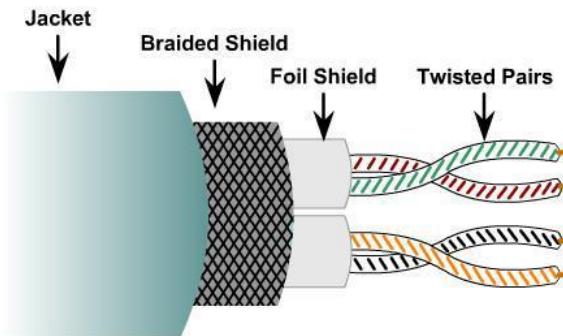
Terdapat 2 jenis kabel,yaitu:

A. Copper

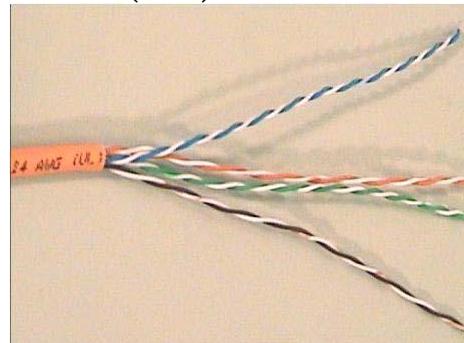
a. Coaxial Cable



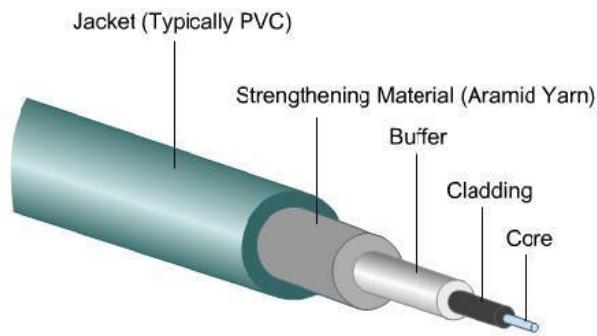
b. Shielded Twisted Pair(STP)



c. UnShielded Twisted Pair(UTP)



B. Fiber Optic



Berkurangnya kualitas suatu signal (degradasi signal) dapat disebabkan oleh beberapa hal, seperti:

- Attenuation
- Impedance mismatch
- Noise
- Crosstalk, beberapa macam crosstalk, antara lain:
 - Near End Crosstalk(NEXT)
 - Far End Crosstalk(FEXT)
 - Power Sum Near End Crosstalk(PS-NEXT)

TIA/EIA-568-B standart menspesifikasi 10 test yang harus dilewati oleh Cooper cable bila akan digunakan untuk high-speed Ethernet LANs. Optical Fiber juga harus melewati test sesuai dengan standar network yang ada.

CHAPTER 5

Cabling LAN and WAN

Standard-standard IEEE untuk Ethernet

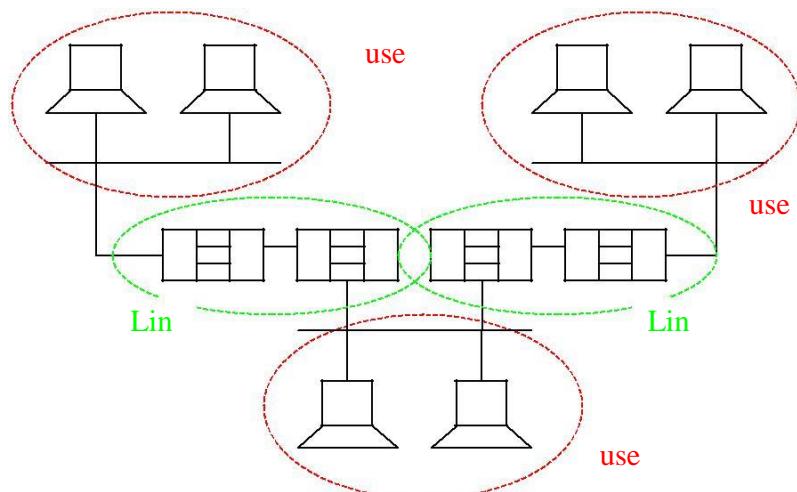
- : a.) 802.3 – Ethernet
- b.) 802.3u – Fast Ethernet
- c.) 802.3z – Gigabit Ethernet

Pada Ethernet, terdapat istilah AUI (Attachment Unit Interface) yang terdiri dari 15 pin, gunanya sebagai converter misalnya Ethernet router yang tidak support RJ-45 harus memakai AUI sebagai perantara.

Standard Ethernet untuk media:

- a.) 10 Base 2 : 10 Mbps, Baseband, 200 m(185 m), bus topology
- b.) 10 Base 5 : 10 Mbps, Baseband, 500 m, bus topology
- c.) 10 Base T : 10 Mbps, BAseband, 100 m, star topology
- d.) 100 Base TX: 100 Mbps, BAseband, memakai UPT
- e.) 100 Base FX : 100 Mbps, Baseband, memakai Fiber Optic
- f.) 100 Base SX dan 1000 Base LX : 1000 Mbps, Baseband, memakai Fiber Optic
- g.) 1000 Base T : 1000 Mbps, Baseband, memakai UTP

Pada Hub terdapat aturan 5-4-3 dimana, terdapat 5 segment, maksimal 4 Repeater, hanya 3 segment yang terkoneksi user.



koneksinya ada 2 :

- User : populated
- Link : non-populated

Hub terbagi atas 3 tipe :

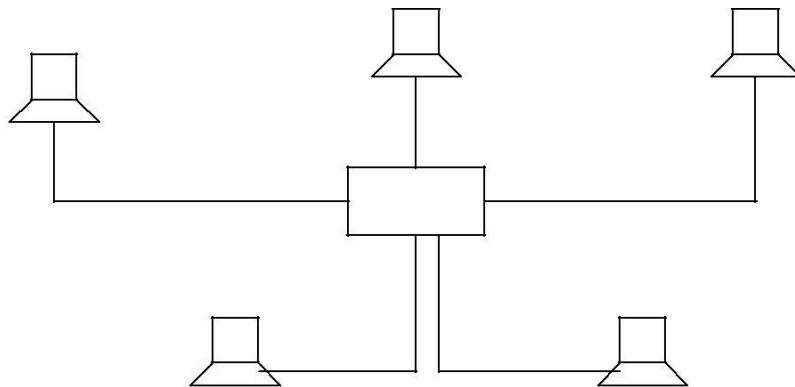
- a.) Passive : langsung operasi setelah colok power dan host
- b.) Active : dapat diatur
- c.) Intelligent : dapat diatur

Media wireless biasanya menggunakan Radio Frequency (RF), Infrared (IF), Microwave, dan Satellite. Ada dua metode spectrum : Direct Sequence Spread Spectrum (DSSS) dan Frequency Hopping Spread Spectrum (FHSS).

Switch dan Bridge bekerja based on destination MAC Address, memiliki CAM (Content Addressable memory) untuk menyimpan MAC dan portnya.

3 Operasi Switch dan Bridge :

- a) Flooding, saat destination MAC tidak ada di CAM, maka frame akan diforward ke semua port kecuali port asal & source MAC di catat, proses ini dinamakan flooding.
- b) Forward, frame langsung dikirim ke tujuan bila destination MAC ada di CAM table
- c) Filter, frame ke tujuan yang MAC-nya telah ada pada CAM aka difilter agar tidak keluar ke port lain selain tujuannya.



CAM :

| MAC | PORT |
|-----|------|
| A1 | 0/1 |
| E5 | 0/5 |

<= misal dari A dikirim pesan ke E...

Pertama dia kirim sampe alamat destinationnya benar
Tapi kalo udah ada diCAM, gak dikirim kesemua,
langsung ke destination

↑
Yang dicatat itu SOURCE-nya Tambahan:

Dua oprasi dasar swict;

- A) switching data frame
- B) maintaining switching operation

Pengertian Broadcast Domain dan Collision Domain

Broadcast domain akan meneruskan broadcast transmission pada domain tsb, contoh: request DHCP client thd. DHCP server. Collision domain memungkinkan terjadinya collision yang lebih banyak pada domain tsb.

- ™ **Device layer 1** yaitu repeater dan hub tidak memisahkan collision domain dan tidak memisahkan broadcast domain.
- ™ **Device layer 2** yaitu switch dan bridge memisahkan collision domain tapi tidak memisahkan broadcast domain.
- ™ **Device layer 3** yaitu router memisahkan collision domain dan memisahkan broadcast domain.

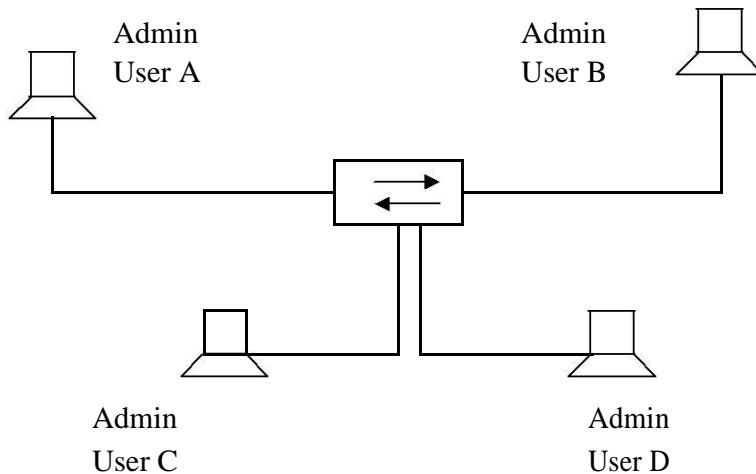
Perbandingan Mode Client-Server dgn Mode Peertoper Pada Local Area Network

Peer to peer disebut juga work group mode, tidak ada sistem penyimpanan data terpusat diserver, semua data dan user account disimpan pada komputer lokal

Cara melihat nama workgroup:

Klik kanan icon MY Computer => properties=>Computer name=>changes Cara melihat dan membuat user account:
Klik kanan icon MY Computer=>mange=>local user and groups untuk membuatnya klik kanan pada folder Local Users and Group lalu New Users.

Work Group:



Setiap host computer pada peer to peer (workgroup) mempunyai peran yang sama dalam. Sharing dan mapping data

Sharing: share thd folder agar dapat diakses oleh host lainnya dlm network yang sama
Mapping: proses pengambilan folder yang dishare o/ sebuah computer

Sharing, ada beberapa cara:

- *) klik kanan foldernya lalu pilih “Sharing and Security”, maksudnya nama folder sharenya.
- *)start=> run => cnd

Net share name = path

Mapping ada beberapa cara:

*) start => Run => ketik:

\ \ ip tujuan \ folder share

*) start => run => cmd => ketik:

Net_use_*_\ \ ip tujuan \ folder share _/user: name _ password

Tanda folder yang di share yaitu:

Gambar tangan dibawah folder



Komputer B mapping ke A dengan cara

: Start => run => ketik:

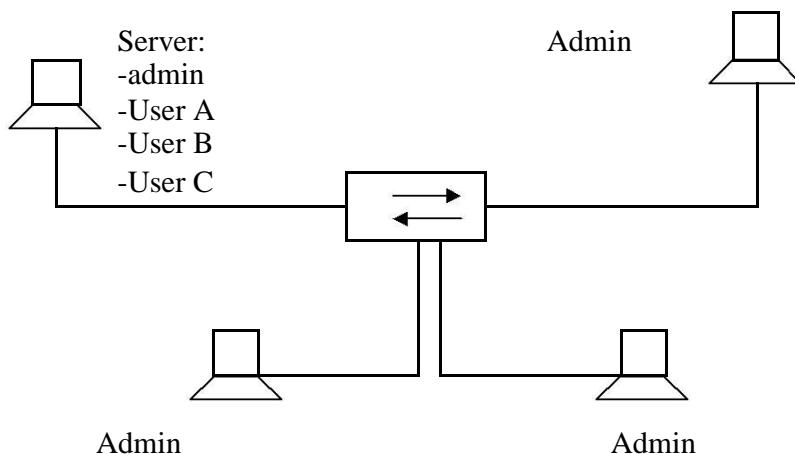
\ \ 192.168.10.10 \ folder

Mode Server

Client-server mempunyai sistem penyimpanan terpusat dengan nomor active Directory pada komputer server.

Bila server menjalankan sistem operasi:

- windows NT40 => Security Account Manager (SAM)
- windows 2000 dan setelahnya => Active Directory



Client dapat log in dari computer manapun sebab account dibuat diserver

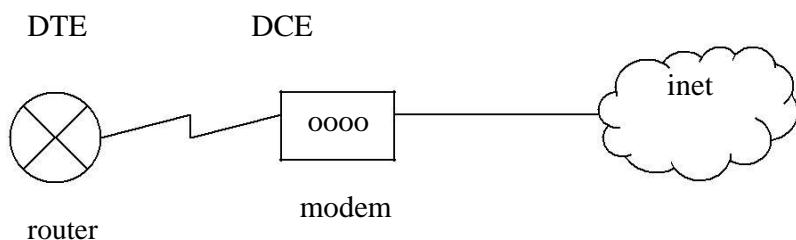
Penetapan u/ security dan apa saja yang dapat diakses client dibuat dengan Group Policy Object (GPO) pada server.

Pengantar WAN

Wide Area Network meliputi skala yg luas & menggunakan teknologi spt; frame relay,

150N, TI ,dll

Alat2x pada WAN misalnya modem, router, communication server (provider)



Terhadap cable serial yang dapat berupa DTE (connector-nya male) Maupun DCE (connector female)

Router dihubungkan dgn serial yg berupa DTE, lalu dihubungkan ke modem yg interfocenya DCE.

Chapter 6

Ethernet Fundamental

Ethernet memungkinkan berbagai host untuk berbagi medium yang sama tanpa collision yang signifikan.

Mengenal metode CSMA/CD (Carrier Sense Multiple Access / Collision Detection).

Ethernet diciptakan oleh DIX (Digital Corporation, Intel, dan Xerox) dan memiliki standar IEEE 802.3

Terdapat isitilah legacy ethernet yaitu ethernet yang beroperasi pada 10

Mbps Pada OSI Layer, ethernet bekerja pada layer physical dan data link.

Layer data link membuat ethernet menggunakan frame dalam mengirim data.

Pengiriman frame pada layer 2 berdasarkan MAC address, MAC terdiri dari 48 bits, 12 hexadecimal, dan 6 bytes.

Tipe-tipe frame ethernet :

a) 802.3

| Preamble | SFD | Destination | Source | Type/ Length | Data | FCS |
|----------|-----|-------------|--------|-----------------|---------|-----|
| 7 | 1 | 6 | 6 | 2 | 46-1500 | 4 |

b) Ethernet II

| Preamble | Destination | Source | Type/ Length | Data | FCS |
|----------|-------------|--------|-----------------|---------|-----|
| 8 | 6 | 6 | 2 | 46-1500 | 4 |

Preamble digunakan sebagai timing information pada ethernet 10 Mbps atau kurang.

SFD adalah Smart Frame of Delimiter > akhir timing information, bentuknya 10101011.

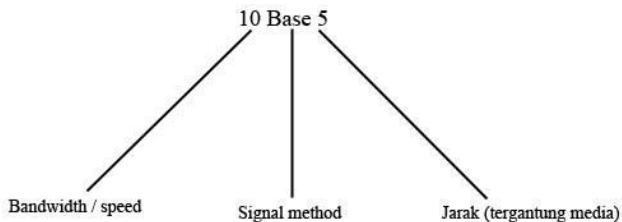
Destination dan sourcanya merupakan destination dan source MAC address.

FCS adalah check sequence yang digunakan untuk pengecekan kesalahan.

MAC address terbagi menjadi 2 tipe :

- Deterministic** : collisionless, misalnya pada token ring dengan metode token passing.
- Non-Deterministic** : dapat terjadi collision, contohnya pada ethernet.

Bentuk penulisan method pada ethernet :



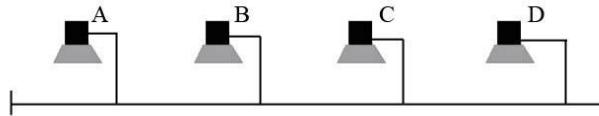
Ethernet juga mengenal Logical Link Control (LLC) pada layer data link guna menghubungkan dengan layer diatasnya.

Ethernet menjalankan fungsi :

- Mengirim dan menerima data frame.
- Mendeteksi error.

Cara kerja CSMA/CA pada ethernet

CSMA/CD merupakan metode pengontrolan collision, misalnya terdapat topologi :

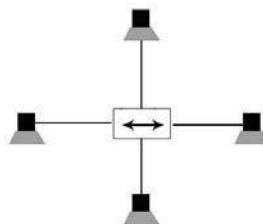


Host A ingin mengirimkan data ke host B, pada saat yang bersamaan, host C mengirim data ke host B, akan terjadi collision dan menyebabkan signal dalam media jaringan meningkat, lalu pengiriman dihentikan dan waktu untuk setiap host dalam mengirim kembali diacak. Host C yang menyebabkan collision tidak akan mendapat prioritas pertama dalam mengirim data.

Macam-macam jenis collision yaitu :

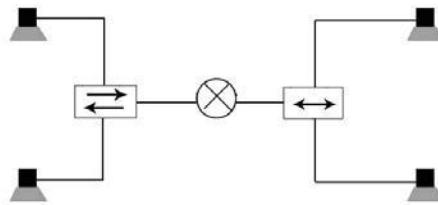
a. **Local**

Collision yang terjadi di segmen yang sama; penggambarannya :



b. Remote

Collision yang terjadi di segmen yang berbeda, penggambarannya :



c. Late

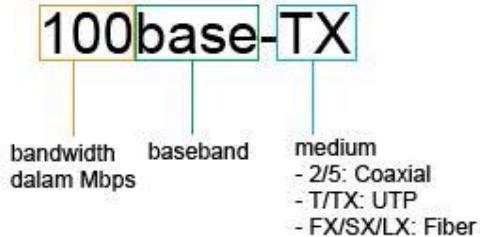
Collision yang terjadi setelah 64 bytes pertama dari satu frame di pandang dari sisi si frame-nya.

Jenis-jenis gangguan pada frame :

1. Short frame
2. Long frame

Chapter 7

Ethernet Technologies



Legacy Ethernet

Bandwidth Legacy Ethernet: 10Mbps (20Mbps bila full-duplex). Legacy Ethernet menggunakan Manchester encoding.

10Base5

- Maximum distance: 500m
- Medium: Coaxial cable

10Base2

- Maximum distance: 185m
- Medium: Coaxial cable

10Base-T

- Maximum distance: 100m
- Medium: UTP

Fast Ethernet

Bandwidth Fast Ethernet: 100Mbps (200Mbps bila full-duplex).

100Base-TX

- Maximum distance: 100m
- Medium: UTP

100Base-FX

- Maximum distance: 228-412m
- Medium: Fiber

Gigabit Ethernet

Bandwidth Gigabit Ethernet: 1000Mbps. Gigabit Ethernet menggunakan 4 pasang kabel untuk transfer dan menerima data secara bersamaan. (full-duplex) Gigabit Ethernet mempunyai keuntungan: bebas noise, jarak tempuh yang lebih jauh dan bandwidth yang lebih besar sehingga sering dipakai untuk teknologi backbone.

1000Base-T

- Maximum distance: 100m
- Medium: UTP

1000Base-SX

- Maximum distance: 220-550m
- Medium: Fiber

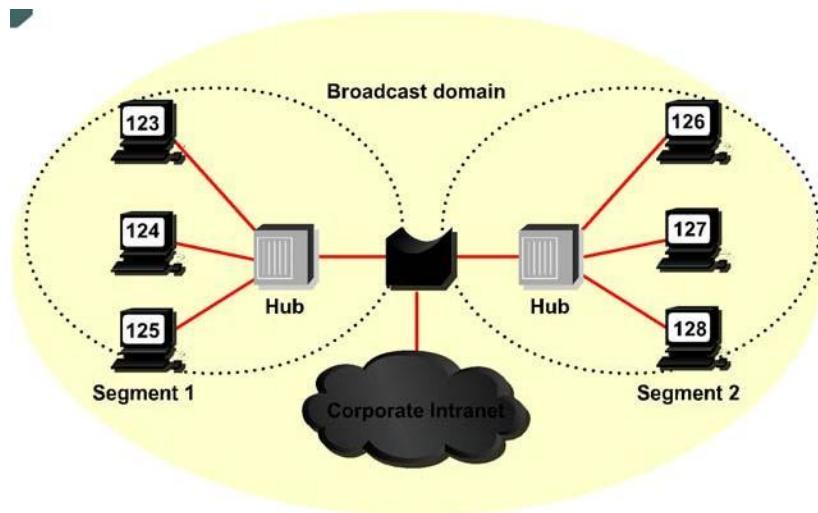
1000Base-LX

- Maximum distance: 550-5000m
- Medium: Fiber

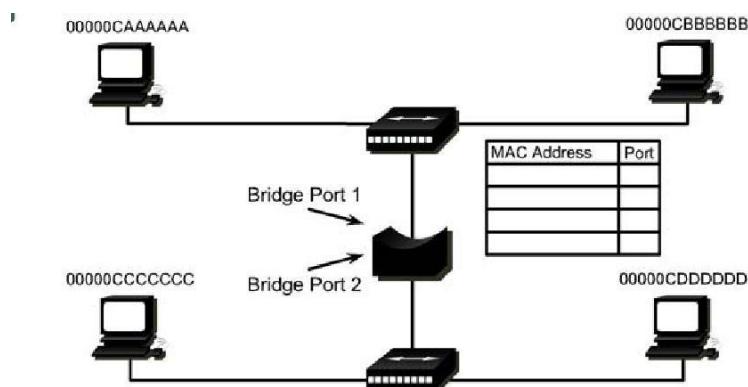
Chapter 8

Ethernet Switching

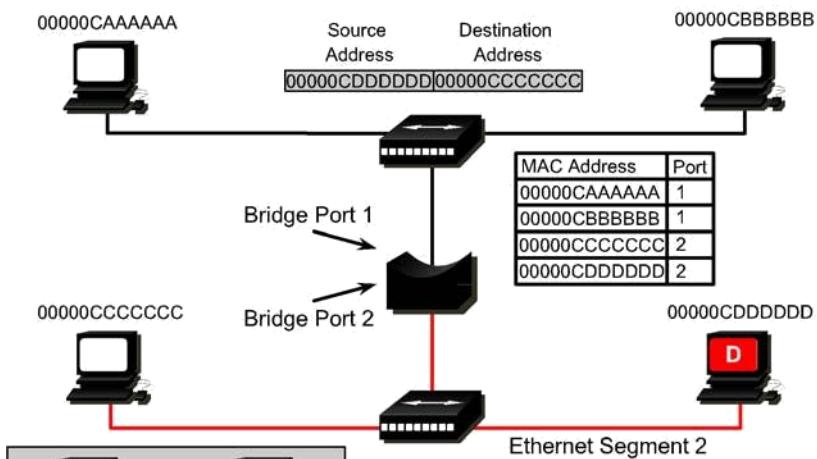
Ethernet adalah sharing media, baseband teknologi, yang artinya hanya satu node dapat mentransmit satu data pada saat itu juga. Untuk meningkatkan jumlah node dalam single segment akan berakibat pada kebutuhan bandwidth yang harus ditingkatkan juga. Hal ini dapat meningkatkan terjadinya collision. Pemecahan dari masalah ini adalah membagi suatu segment network yang besar menjadi beberapa bagian dan memisahkannya menjadi collision domain yang terpisah. *Bridges* dan *switches* dipakai untuk memecah network menjadi multiple collision domains.



Bridge membuat bridge table dari source address suatu packets yang diproses. Address tersebut berhubungan dengan frame port yang masuk. Akhirnya bridge table mempunyai informasi dari address-address yang memungkinkan bridge untuk meneruskan frame keluar melalui port yang didasarkan pada destination address.

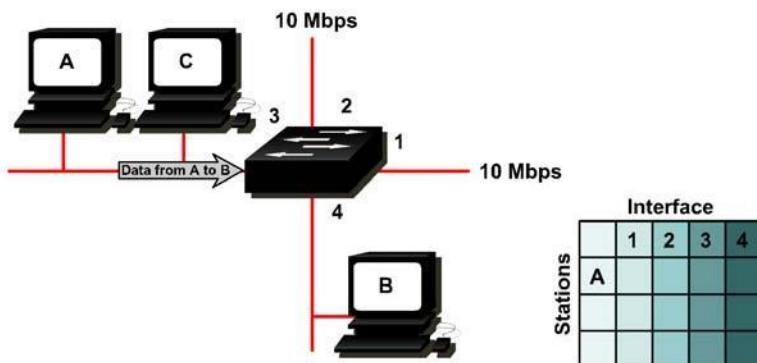


Gambar. Keadaan default (bridge table kosong)



Gambar. Bridge table sudah terisi

Switch adalah bridge dengan banyak port, mempunyai cara kerja yang sama dengan bridge tapi juga dilengkapi dengan virtual connection yang langsung menghubungkan antara source dan destination node, dibandingkan antara source collision domain dan destination collision domain. Setiap portnya membuat collision domain. Switch membuat secara dinamik dan memelihara Content Addressable Memory (CAM) table, menjaga semua informasi MAC yang dibutuhkan untuk tiap port. CAM adalah memory yang pada hakikatnya bekerja mulai dari belakang dibanding dengan conventional memory.

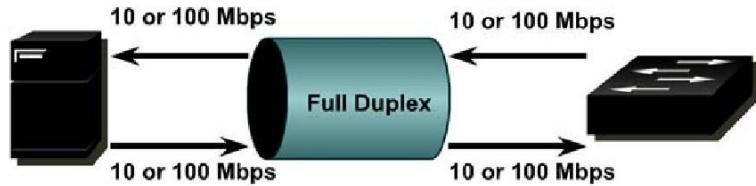


Tiga proses Switch based on CAM table

- Flooding, disebarluaskan ke semua port kecuali port asalnya, bila destination Mac belum ada di CAM table
- Forward, frame langsung dikirim ke tujuan berdasarkan destination Mac, bila destination telah ada.
- Filter, frame tidak dikirim ke port yang bukan terdapat Mac address tujuan.

Dua device yang dihubungkan ke port Switch menyebabkan small collision domain. Small physical segments ini dinamakan microsegments. Microsegments dihubungkan dengan menggunakan twisted pair kabel yang sanggup berkomunikasi

secara full-duplex. Dalam mode full duplex , ketika kabel yang terpisah digunakan untuk transmit dan receive diantara host, tidak terdapat konflik dalam media tersebut, oleh sebab itu collision domain tidak terbentuk lagi.



Full Duplex

- bandwidth menjadi double diantara node
- Transmisi bebas collision
- Dua 10 atau 100 Mbps jalur data

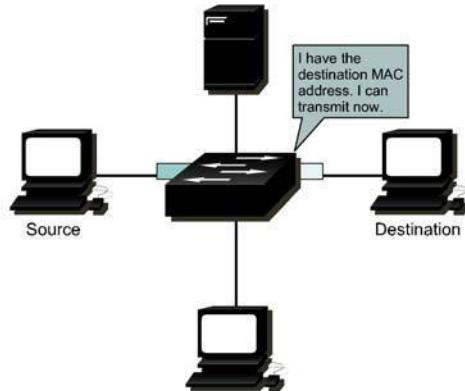
Kebanyakan Switch support untuk komunikasi dalam mode full duplex, begitu juga NIC, dalam teorinya bandwidth akan menjadi double ketika digunakan mode full duplex.

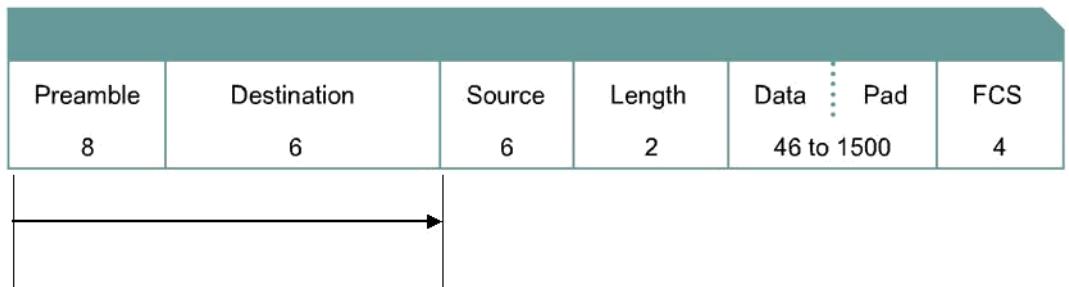
Terdapat 3 jenis SWITCH:

- Cut Through Switch
- Store and Forward Switch
- Fragment Free Switch

Cut Through Switch.

Switch dapat segera meneruskan frame ke tujuan begitu destination address terbaca, tidak terdapat error cheking, latency yang rendah.

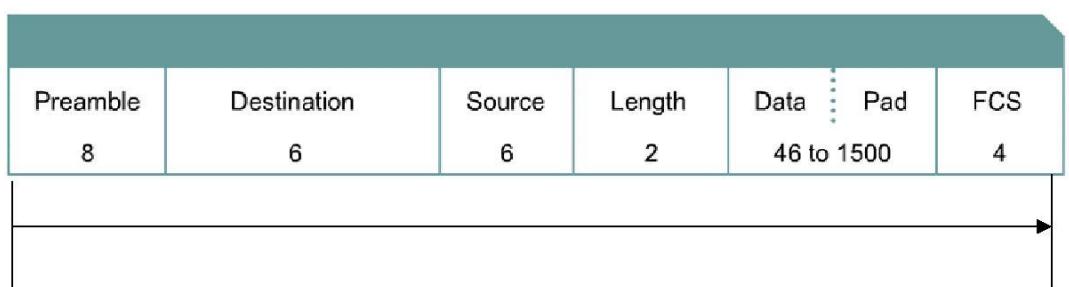
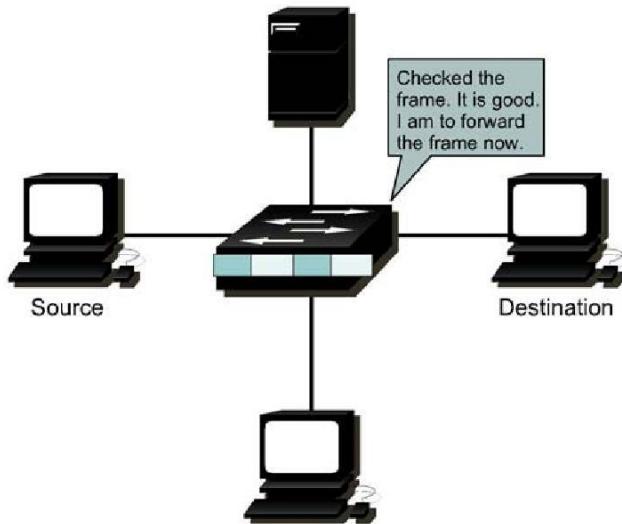




Cut Through mode

Store and Forward Switch

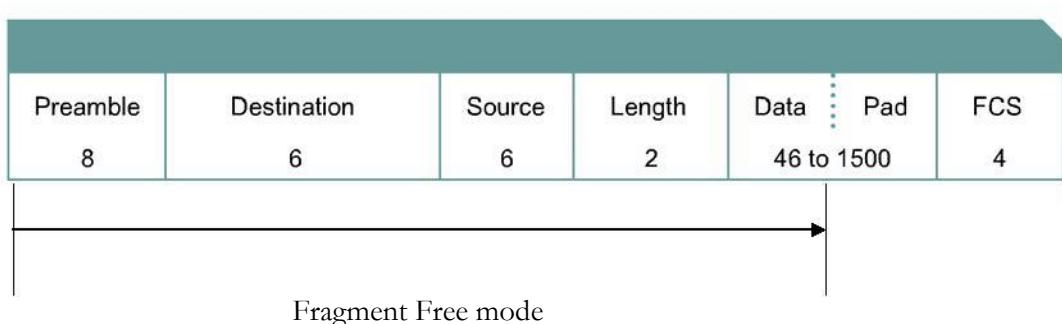
Switch menerima keseluruhan frame sebelum mengirim kembali ke port tujuan, memeriksa sampai Frame check Sequence (FCS), kalau frame valid, Switch melihat ke alamat tujuan apa ada di table, yang kemudian frame dikirimkan ke port tujuan. Delay paling tinggi



Store and Forward mode

Fragment-free switching

Fragment free switch membaca dan memeriksa 64 bytes pertama dari frame sebelum meneruskannya ke port tujuan.



Switch pada network biasanya menggunakan Spanning-Tree Protocol (STP) untuk mengidentifikasi dan mematikan jalur yang terlalu banyak yang melalui suatu network (broadcast storm). Hasilnya adalah jalur untuk melalui network terbebas dari loop (dengan memblok port menggunakan Spanning Tree Algorithm)

Layer 2 tidak mempunyai Time To Live (TTL) seperti pada Layer 3 dalam mengatasi looping, maka digunakan STP. Proses-proses dalam STP:

- Blocking
- Listening
- Learning
- Forwarding
- Disabled

Proses cara kerja STP pada suatu port

- From initialization to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

Menggunakan layer 2 device(switch) untuk memecah LAN ke dalam multi Collision domain dapat meningkatkan bandwith yang ada pada tiap-tiap host. Tapi device layer 2(switch) meneruskan Broadcast, seperti ARP. Device layer 3(router) dibutuhkan untuk mengontrol broadcast dan membagi broadcast domain.

Data bergerak melintasi traffic manajemen suatu device pada layer 1, 2, dan 3 pada OSI model. Layer 1 digunakan untuk transmisi melintasi fisik media, layer 2 untuk collision domain manajemen, dan Layer 3 untuk broadcast domain manajemen.

Chapter 9

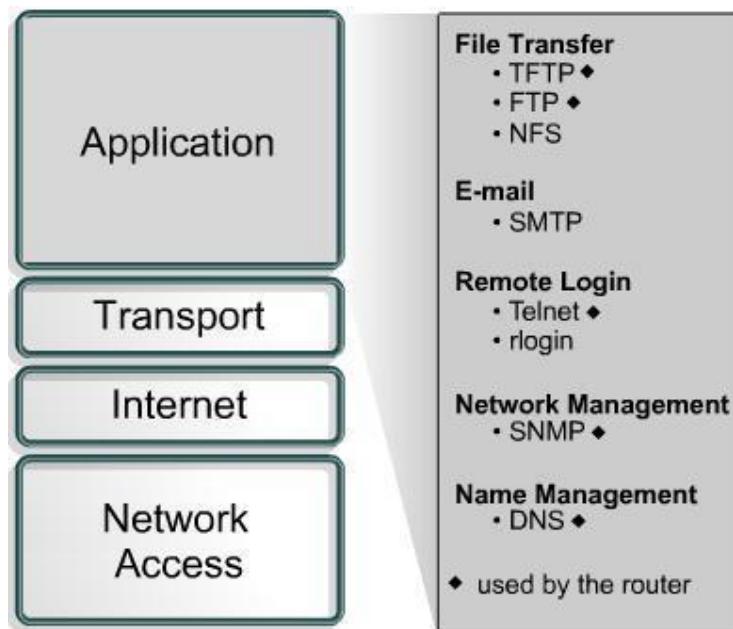
TCP/IP Protocol Suite & IP Addressing

Protocol ini dikembangkan oleh Departement of Defense(DOD) untuk menghasilkan Network yang terpercaya.

Pada TCP/IP terdapat 4 Layer,yang terdiri dari:

- **APPLICATION Layer**

Contohnya antara lain:FTP,TFTP,NFS,SMTP,TelNet,SNMP,dan masih banyak yang lain



- **TRANSPORT Layer**

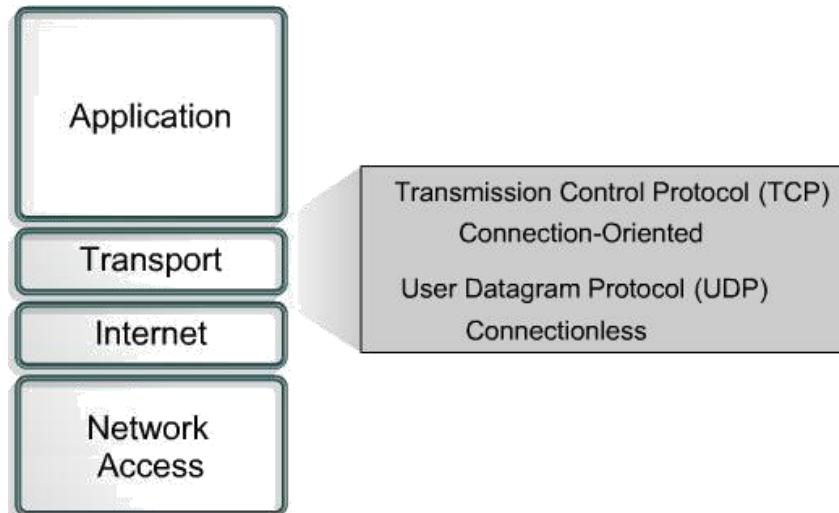
Pada Layer ini terdapat 2 protocol utama,yaitu

- **TCP(Transmission Control Protocol)**

Sifatnya Reable,Connection Oriented

- **UDP(User Datagram Protocol)**

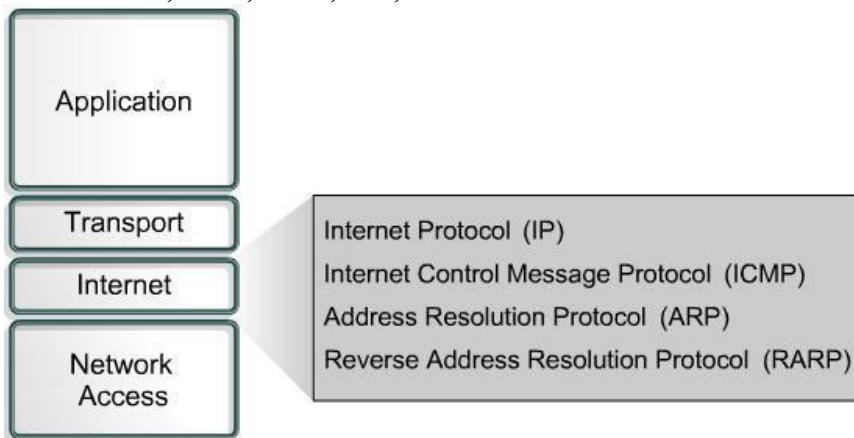
Sifatnya UnReable,Connectionless



- **INTERNET Layer**

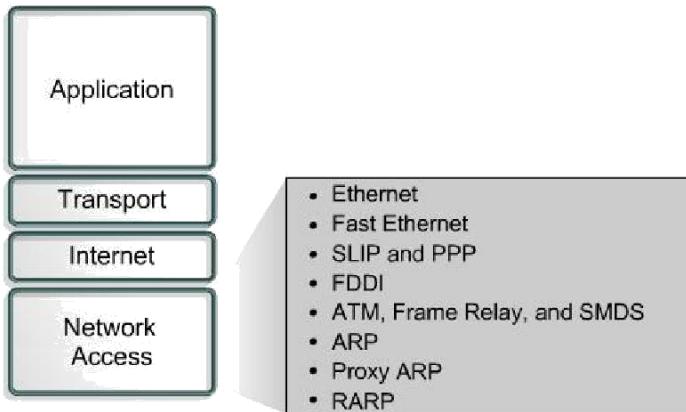
Berfungsi untuk menentukan jalur yang paling baik pada Network saat pengirim data dilakukan

Beberapa protocol yang beroperasi pada layer ini, antara lain:
IP, ICMP, RARP, ARP, dll



- **NETWORK ACCESS Layer**

Berfungsi untuk mengijinkan Packet IP melakukan koneksi fisik dengan Media Network.



| Address Class | Number of Networks | Number of Host per Network |
|---------------|--------------------|----------------------------|
| A | 126 * | 16,777,216 |
| B | 16,384 | 65,535 |
| C | 2,097,152 | 254 |
| D (Multicast) | N/A | N/A |

| IP Address Class | High Order Bits | First Octet Address Range | Number of Bits in the Network Address |
|------------------|-----------------|---------------------------|---------------------------------------|
| Class A | 0 | 0 - 127 * | 8 |
| Class B | 10 | 128 - 191 | 16 |
| Class C | 110 | 192 - 223 | 24 |
| Class D | 1110 | 224 - 239 | 28 |

IP Addressing Dibedakan menjadi 2,yaitu:

- **Private**

Private IP digunakan untuk jaringan lokal yang terkoneksi dengan internet Kelas A:10.0.0.0 – 10.255.255.255
 Kelas B:172.16.0.0 - 172.31.255.255
 Kelas C:192.168.0.0 – 192.168.255.255

- **Public**

Digunakan untuk Jaringan Internet,misalnya untuk Situs-situs/website.
 Ada 3 macam cara untuk memberikan IP pada suatu computer.

1. Static,disetting secara manual
2. Dynamic,penyetingan dilakukan menggunakan DHCP
3. Reservation,juga dengan DHCP dan secara permanent

SubNet Mask berguna untuk mengetahui terdapat di network manakah sebuah IP.

Caranya yaitu IP di AND dengan SubNet Mask maka akan menghasilkan Network ID.

| Decimal Notation for First Host Octet | Number of Subnets | Number of Class A Hosts per Subnet | Number of Class B Hosts per Subnet | Number of Class C Hosts per Subnet |
|---------------------------------------|-------------------|------------------------------------|------------------------------------|------------------------------------|
| .192 | 2 | 4,194,302 | 16,382 | 62 |
| .224 | 6 | 2,097,150 | 8,190 | 30 |
| .240 | 14 | 1,048,574 | 4,094 | 14 |
| .248 | 30 | 524,286 | 2,046 | 6 |
| .252 | 62 | 262,142 | 1,022 | 2 |
| .254 | 126 | 131,070 | 510 | - |
| .255 | 254 | 65,534 | 254 | - |

Selain IP TCP/ IP Protocol juga menyediakan beberapa protocol yang fungsinya untuk melakukan pengalamanan.

- **RARP(Reverse Address Resolution Protocol)**

RARP Digunakan untuk mendapatkan IP address dari MAC.

| 0 - 15 bits | | 16 - 31 bits |
|-------------------------|--|------------------------|
| Hardware Type | | Protocol Type |
| HLen (1 byte) | | Operation |
| Sender HA (bytes 1 - 4) | | |
| Sender HA (byte 5- 6) | | Sender PA (byte 1 - 2) |
| Sender PA (byte 3 - 4) | | Target HA (byte 1 -2) |
| Target HA (bytes 3 - 6) | | |
| Target PA (bytes 1 - 4) | | |
| RARP header structure | | |

- **BOOTP(BOOTstrap Protocol)**

Beroperasi pada lingkungan Client-server,dan hanya memerlukan 1 buah paket untuk mengumpulkan/mecari IP.

BOOTP sudah jarang digunakan dan digantikan oleh DHCP sebagai pemberi IP secara dinamis.

| 0 -7 bits | 8 -15 bits | 16 - 23 bits | 24 - 31 bits |
|---------------------------------|------------|--------------|--------------|
| Op (1) | Htype (1) | HLen (1) | Hops (1) |
| Xid (4 bytes) | | | |
| Seconds (2 bytes) | | | Unused |
| Ciaddr (4 bytes) | | | |
| Yiaddr (4 bytes) | | | |
| Siaddr (4 bytes) | | | |
| Giaddr (4 bytes) | | | |
| Chaddr (16 bytes) | | | |
| Server Host Name (64 bytes) | | | |
| Boot File Name (128 bytes) | | | |
| Vendor Specific Area (64 bytes) | | | |
| BOOTP message structure | | | |

- **DHCP(Dynamic Host Configuration Protocol)**

Berbeda dengan BOOTP,DHCP mengizinkan host untuk melakukan pengesetan alamat IP secara dinamis.

| 0 -7 bits | 8 -15 bits | 16 - 23 bits | 24 - 31 bits |
|---------------------------------|------------|--------------|-----------------|
| Op (1) | Htype (1) | HLen (1) | Hops (1) |
| Xid (4bytes) | | | |
| Seconds (2 bytes) | | | Flags (2 bytes) |
| Ciaddr (4 bytes) | | | |
| Yiaddr (4 bytes) | | | |
| Siaddr (4 bytes) | | | |
| Giaddr (4 bytes) | | | |
| Chaddr (16 bytes) | | | |
| Server Host Name (64 bytes) | | | |
| Boot File Name (128 bytes) | | | |
| Vendor Specific Area (variable) | | | |
| DHCP message structure | | | |

- **ARP(Address Resolution Protocol)**

ARP digunakan untuk menetapkan MAC Address dari IP Address.

| ARP Table Entry | | |
|------------------|-------------------|---------|
| Internet Address | Physical Address | Type |
| 68.2.168.1 | 00-50-57-00-76-84 | dynamic |

| Arp Table 198.150.11.36 | |
|-------------------------|---------------|
| MAC | IP |
| FE:ED:F9:44:45:66 | 198.150.11.34 |
| DD:EC:BC:00:04:AC | 198.150.11.33 |
| DD:EC:BC:00:94:D4 | 198.150.11.35 |

CHAPTER 10

Routing Fundamental & Subnet

Pengertian Protocol

Protocol : sekumpulan aturan yang mendefinisikan bagaimana computer atau host dapat berkomunikasi, aturan yang dideskripsikan:

- a.) format yang dipertukarkan b.)
cara computer bertukar pesan

Dalam network terdapat 2 protocol utama, yaitu

: a.) Routing protocol

Protocol yang digunakan untuk membangun routing table overall network dan memilih best path. Routing table digunakan sebagai panduan dalam melakukan routing (meneruskan paket ke network yang berbeda)

Routing table berisi network yang directly connected maupun network

remote b.) Routing protocol

berguna untuk meneruskan paket ke tujuan atau router berikutnya berdasarkan informasi pada routing table, contohnya IP

Routing sendiri mempunyai 2 jenis, yaitu

- a.) static routing
- b.) dynamic routing

Static Routing

Static Routing berguna untuk membangun routing table secara manual, jadi tidak menggunakan routing protocol dalam membuat routing table, memiliki kelemahan bila network ada banyak (harus memasukkan satu-satu)

Contoh membangun static routing pada topology sebelumnya:

```
A(config)#ip route 192.168.20.0 255.255.255.0 200.10.10.20
```

```
A(config)#ip route 200.20.20.0 255.255.255.0 200.10.10.20
```

```
A(config)#ip route 192.168.30.0 255.255.255.0 200.20.20.10
```

```
B(config)#ip route 192.168.10.0 255.255.255.0 200.10.10.10
```

```
B(config)#ip route 192.168.30.0 255.255.255.0 200.20.20.20
```

```
A(config)#ip route 192.168.20.0 255.255.255.0 200.20.20.10
```

```
A(config)#ip route 200.10.10.0 255.255.255.0 200.20.20.10
```

```
A(config)#ip route 192.168.20.0 255.255.255.0 200.10.10.10
```

Dynamic routing

Dynamic Routing menggunakan routing protocol dalam membangun routing table dan memudahkan bila network atau route yang terdapat ada banyak:

- a.) routing Information Protocol (RIP)
- b.) Interior Gateway Rating Protocol (IGRP)
- c.) OpenOpen Shortest Path First (OSPF)
- d.) Enhanced Interior Gateway Routing Protocol (EIGRP)
- e.) Border Gateway Protocol(BGP)
- f.) Intermediate System to Intermediate System, (IS-IS)

2 Algoritma routing, yaitu

- : a.) distance over
- b.) link state

Distance Vector Routing

Distance vector mengirimkan routing update secara estafet kepada router-router tetangganya, setiap kali melewati sebuah router, maka hop akan ditambahkan (hop =router yang dilalui).

Routing update mengirimkan copy routing table secara lengkap pada router tetangganya. Router-router dalam jaringan distance vector hanya tahu network dari tetangganya saja. Contoh routing protocol distance vector :

- a.) RIP v1 & RIP v2
- b.) IGRP
- c.) BGP

Link State Routing

Link state tidak terbatas jumlah hop dalam mengirim update, jadi dapat menjangkau network yang lebih luas.

Link state mengirimkan link state advertisement (LSA) secara broadcast(flooding) ke semua router dalam jaringan.

Info LSA disimpan oleh setiap router dalam databasenya sehingga setiap router tahu topologi jaringan secara overall.

Istilah-istilah link state :

- a.) Link State Advertisement (LSA)
- b.) Djikstra
- c.) Routing Table
- d.) Neighbor table
- e.) Database/ topologi table

Info LSA disimpan pada database/ topological table, kemudian Djikstra digunakan dalam menghitung cost atau best path dan perhitungan diletakkan dalam routing table.

Link State juga mempunyai neighbor table yang berisi daftar router tetangganya. Link State mengenal periodic update, update hanya dilakukan bila ada perubahan(event triggered update) dengan mengirim LSA lagi ke semua router.

Perubahan diketahui dengan pengiriman Link State Refresh berupa hellos messages secara periodik (ukuran lebih kecil dari pada routing update distance vector)

Contoh Link State Routing Protocol

- : a.) OSPF
- b.) IS-IS

Selain berdasarkan algoritma, routing protocol juga dapat dibedakan menjadi 2 dari AS(Autonomous System = Network yg Policy sama) yaitu:

- a.) IGP
- b.) EGP

Informasi lain pada routing protocol mendefinisikan:

- a.) protocol-type : jenis routing protocol
- b.) next hop association : apakah suatu network directly connected atau remote
- c.) outbound interface : ke interface mana routing dilakukan
- d.) routing metric : perhitungan best route

Pengantar Subnetting

Subnetting adalah proses memcah-mecah network yang besar menjadi network-network yang lebih kecil.

Subnet mask yang dipakai oleh suatu class dapat menjadi tidak default. Network-network kecil yang diperoleh hasil dari subnet mask tidak dapat berhubungan tanpa melalui router.

Subnetting memiliki rumus:

$$\text{subnet bit} \quad \text{Total subnet} = 2^{\text{subnet bit}}$$

$$\text{Usable subnet} = 2^{\text{subnet bit} - 2}$$

$$\text{Total host per subnet} = 2^{\text{host bit}}$$

$$\text{Usable host per subnet} = 2^{\text{host bit}} - 2$$

Keterangan :

- Usable subnet yaitu total subnet dikurang dua sebab menurut aturan cisco, subnet pertama & terakhir tidak boleh digunakan.

Subnet pertama disebut juga subnet zero

- Usable host per subnet yaitu total host per subnet dikurang dua sebab alamat network dan alamat terakhir dari subnetwork adalah alamat broadcast.

Berdasarkan subnet mask secara default:

a.) Class A

11111111.00000000.00000000.00000000

Network bit host bit

b.) Class B

11111111.11111111.00000000.00000000

Network bit host bit

c.) Class C

11111111.11111111.11111111.00000000

Network bit host bit

Subnet bit akan muncul setelah subnetting dilakukan

Chapter 11

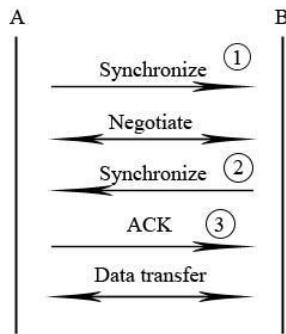
TCP / IP Transport and Application Layer

Fungsi dari transport layer :

- Meregulasikan aliran informasi secara akurat dan terpercaya dengan sliding window, sequence number, dan ACK.
- Menjamin Reliability dan melakukan flow control.

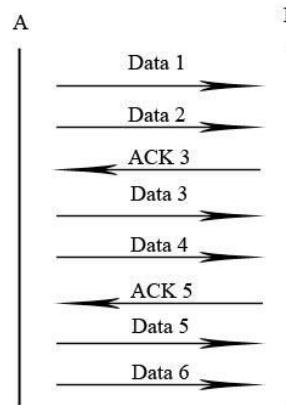
TCP / IP merupakan gabungan dari dua layer yaitu TCP pada layer 4 dan IP pada layer 3.

TCP membentuk virtual circuit, sifatnya connection oriented dan membentuk koneksi dengan three way handshake :



Flow control digunakan untuk mengatur jumlah data yang dikirim pada suatu waktu, ditentukan oleh window size.

Contoh window size 2 yang sudah membentuk sliding window :



Sequence number digunakan untuk mengurutkan data agar sampai pada tujuan sesuai urutannya.

Bila pada selang waktu tertentu ACK tidak diterima oleh host sumber dari host tujuan, maka akan dilakukan *retransmission* atau pengiriman kembali ke tujuan.

Transport layer berkomunikasi dengan application layer dengan menggunakan port number.

Port dibawah 1024 disebut juga *well-known* port number.

Protocol-protocol yang memakai TCP :

- **HTTP :**

Bekerja sama dengan www digunakan untuk merequest halaman web dari web server untuk ditampilkan pada browser client.

Halaman web dapat dibuat dengan Hypertext Markup Language (HTML) yang merupakan web static ataupun dengan web dinamis seperti PHP, ASP, atau JSP
- > port 80.

- **FTP :**

Digunakan untuk melakukan transfer file dari server FTP ke client FTP (port 20 dan 21).

- **SMTP :**

Digunakan untuk email server (port 25).

- **TelNet :**

Digunakan untuk remote ke komputer lain (port 32).

User Datagram Protocol (UDP)

UDP yaitu protocol yang sifatnya connectionless, tidak membentuk koneksi atau virtual circuit, pengiriman langsung dilakukan tanpa memperdulikan data sampai pada tujuan atau tidak.

Protocol yang memakai UDP :

- **SNMP :**

Untuk manajemen network (port 161).

- **TFTP :**

Backup IOS dan configuration file pada router dan switch Cisco (port 69).

- **DHCP : (Membagi IP address)**

Membagi IP secara dinamik (port 67 dan 68).

DNS memakai TCP dan UDP sekaligus, untuk menterjemahkan nama ke IP dan sebaliknya (port 53).

CCNA 2

| | |
|---|-----------|
| Daftar Isi | 1 |
| Chapter 1 WAN and ROUTER | 2 |
| Chapter 2 Introduction to Routers | 4 |
| Chapter 3 Configuring a Router | 7 |
| Chapter 4 Learning About Other Devices | 13 |
| Chapter 5 Router and Routing Basics | 18 |
| Chapter 6 Routing and Routing Protocol | 22 |
| Chapter 7 Distance Vector Routing Protocols | 24 |
| Chapter 8 TCP/IP Suite Error and Control Messanges | 27 |
| Chapter 9 Basic Router Troubleshooting | 35 |
| Chapter 10 Intermediate TCP/IP | 41 |
| Chapter 11 Access Control List | 44 |

CHAPTER 1

WAN and ROUTER

Wide area network (WAN) yaitu jaringan yang meliputi area geografis yang luas dan memiliki karakteristik yang berbeda dengan Local Area Network (LAN). WAN menggunakan router yang terdiri dari physical layer component yang memiliki fungsi masing-masing

Karakteristik WAN :

- a) Memiliki area geografis yang luas
- b) Menggunakan jasa provider
- c) Menggunakan serial connection dari berbagai tipe

Komponen-komponen yang ada pada WAN :

- a) Router
- b) Switch
- c) Modem
- d) Communication Server (Provider)

Standard WAN dikembangkan oleh :

- a) ITU-T (International Telecommunication Union-Telecommunication Standardization Sector), awalnya bernama CCITT (Consultative Committee for International Telegraph and Telephone)
- b) ISO (International Organization for Standardization)
OS switch dan router yang tidak memiliki keyboard dan monitor, yang dikonfigurasikan dengan PC dengan kabel rollover.
- c) IETF (Internet Engineering Task Force)
- d) EIA (Electronic Industry Association)

Physical layer component router :

- a) RAM (DRAM)
- b) NVRAM
- c) Flash
- d) ROM
- e) Interface

Random Access Memory (RAM) / Dynamic RAM (DRAM)

- a) Menyimpan routing table
- b) Menyimpan ARP cache
- c) Fast-switching cache
- d) Packet buffering
- e) Sifatnya volatile
- f) Running-config

Non Volatile Random Access Memory (NVRAM)

- a) Menyimpan startup-configuration
- b) Sifatnya non volatile

Flash memory

- a) Menyimpan Internetworking Operating System (IOS)
- b) Sifatnya non volatile

Read Only Memory (ROM)

- a) Berguna untuk Power On Self Test (POST)
- b) Menyimpan konfigurasi IOS basic

WAN berada pada layer physical dan data link pada OSI layer. Layer physical WAN menyangkut DTE, DCE, V35, EIA/TIA-232

Layer data link WAN menyangkut encapsulation seperti High Level Data Link Control (HDLC), Point-to-Point Protocol (PPP), frame relay.

Cara menghubungkan router agar dapat dikonfigurasikan dengan komputer :

- a) Siapkan rollover cable
- b) Hubungkan rollover cable dengan console port router
- c) Hubungkan ujung rollover cable satunya dengan DB9 connector untuk converter dari RJ-45 ke serial port pada komputer
- d) Pada komputer, buka terminal emulation software Hyper Terminal untuk konfigurasi IOS
- e) Buat agar restore default pada Hyper terminal
- f) Masukkan command-command IOS.

Router berada pada Layer 3 (network layer) dan dapat melakukan fungsi routing yang meliputi :

- a) Best path
- b) Switching to destination based on network (pada routing table)

Router memiliki 3 buah interface utama :

- a) LAN interface : contohnya fast ethernet
- b) WAN interface : serial connection
- c) Management port : console untuk konfigurasi router

CHAPTER 2

Introduction to Routers

Router dan Switch Cisco membutuhkan Internetworking Operating System untuk dapat beroperasi, fungsinya:

- Akses ke network -
- Network scalability
- Basic routing and switching

Command-Line Interface (CLI) pada IOS dapat diakses melalui console, auxiliary atau telnet. Pada CLI terdapat command interpreter yang disebut dengan command executive (EXEC), dan mempunyai 2 tingkatan utama: user mode dan privileged mode.

User mode

Tingkatan awal pada EXEC. Hanya command-command basic yang diperbolehkan, dan tidak dapat mengganti konfigurasi pada router. Prompt pada CLI dapat diidentifikasi dengan: >.

Privileged mode

Tingkat selanjutnya pada EXEC. Dapat melakukan seluruh command-command yang tersedia pada router termasuk konfigurasi. Prompt pada CLI: #.

Untuk dapat mengakses privileged mode dari user mode, pada prompt >, ketik command **enable**.

Perpindahan dari user mode ke privileged:

| | |
|-----------------|---|
| Router> enable | ↳ ketik enable untuk masuk ke privileged mode |
| Router# | ↳ privileged mode |
| Router# disable | ↳ ketik disable untuk keluar ke user mode |
| Router> | ↳ user mode |

Penamaan pada IOS:



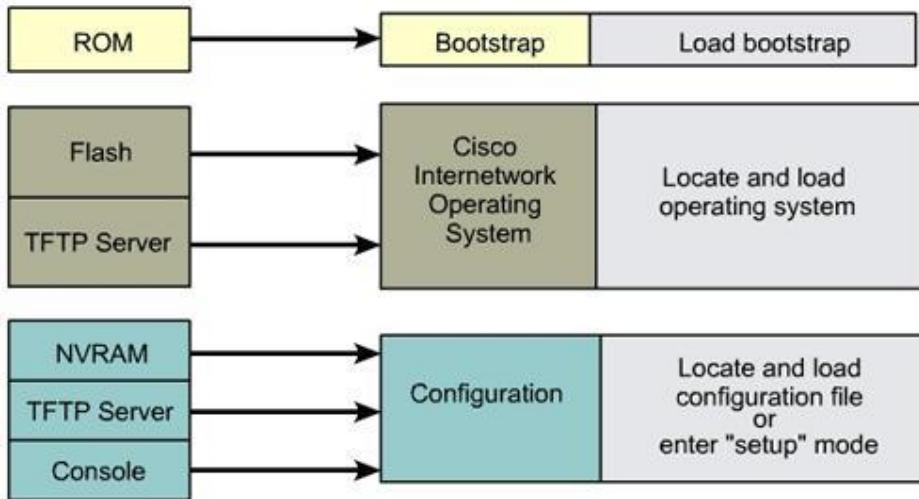
IOS mempunyai 3 environment utama, yaitu: ROMMON (Rom Monitor), Boot ROM dan IOS.

| Operating Environment | Prompt | Usage |
|-----------------------|----------------|------------------------------|
| ROM monitor | > or ROMMON> | Failure or password recovery |
| Boot ROM | Router (boot)> | Flash image upgrade |
| Cisco IOS | Router> | Normal operation |

Router melakukan POST (Power On Self Test) yang tujuannya:

- memastikan hardware berjalan dengan baik
- mencari dan load IOS dari flash ke ROM
- mencari dan load configuration file dari NVRAM

Urutan POST:



Saat router melakukan initial bootup, ada info tentang:

- jenis interface
- jumlah interface
- jumlah flash memory
- jumlah / kapasitas NVRAM

Tanda tanya (?) berfungsi sebagai pembantu pada CLI. Dapat digunakan pada user atau privileged mode untuk memunculkan daftar perintah-perintah yang bisa dipakai.

Contoh: Router> sh? ↵ memunculkan daftar perintah yang berawalan sh ,seperti show Router> show ? ↵ memunculkan daftar perintah yang ada setelah show, seperti version, ip route, controllers

Fungsi-fungsi IOS Editing:

Ctrl-A : Pindah ke awal baris perintah.

Esc-B : Mundur 1 kata

Ctrl-B atau Left Arrow : Mundur 1 huruf

Ctrl-E : Pindah ke akhir baris perintah

Ctrl-F atau Right Arrow : Maju 1 huruf

Esc-F : Maju 1 kata

Router command history menyimpan perintah-perintah yang pernah diberikan ke router. Default-nya router menyimpan 10 perintah terakhir, dan bisa menyimpan maksimum 256 perintah. Untuk memanggil perintah sebelumnya, tekan **Ctrl-P** atau **Up Arrow**. Untuk balik ke perintah yang lebih baru, tekan **Ctrl-N** atau **Down Arrow**.

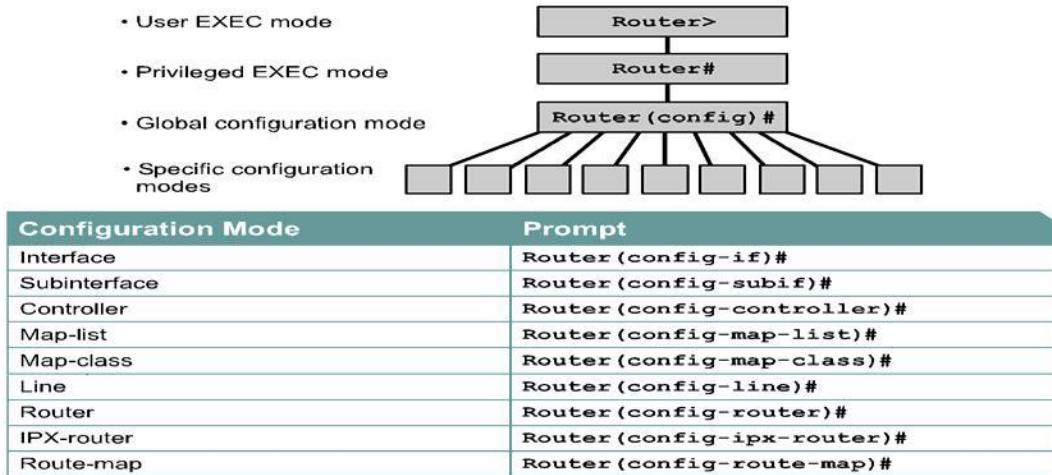
Command **show version** memunculkan informasi berikut:

- Versi IOS
- Versi Bootstrap ROM
- Versi Boot ROM
- Router uptime
- Last restart method
- Lokasi dan file System image
- Router platform
- Setting konfigurasi register

CHAPTER 3

Configuring a Router

Semua command-line interface (CLI) konfigurasi dalam Cisco router di input dalam global config mode.



Command-line interface dapat digunakan untuk merubah

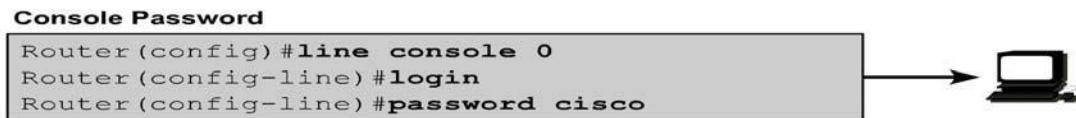
konfigurasi: -Setting hostname (memberi nama router)

Contoh: Router(config)#hostname Tokyo
Tokyo(config)#

-Setting passwords

Contoh: 1. Setting console password (masuk pertama kali ke user mode)

Pass: cisco



2. Setting password telnet (sewaktu ingin telnet) pass: cisco

Virtual Terminal Password

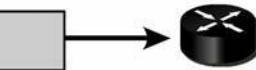
```
Router(config)#line vty 0 4  
Router(config-line)#login  
Router(config-line)#password cisco
```



3. Setting enable password (sewaktu masuk ke previledge mode) pass:san-fran

Enable Password

```
Router(config)#enable password san-fran
```



4. Setting password encryption (untuk pass, yang tidak terenkripsi)

Perform Password Encryption

```
Router(config)#service password-encryption  
(set passwords here)  
Router(config)#no service password-encryption
```

5. Setting enable secret (masuk ke previledge, paling aman dan sudah terenkripsi)

Router(config)#enable secret <password>

-Setting interfaces

Konfigurasi / settingan serial interface mengikuti beberapa steps:

1. Masuk ke global configuration mode
2. Enter interface mode
3. Specify IP address and subnet mask
4. Set clock rate jika DCE cable connected. Skip jika DTE cable connected.
5. Turn on the interface

```
Router(config)#interface serial 0/0  
Router(config-if)#ip address <ip address> <netmask>
```

Clock rates yang available (bits per second) adalah: 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000,dan 4000000.

Konfigurasi / settingan ethernet interface.

Sama dengan settingan serial interface, tanpa clock rate.

Contoh: Router (config) #interface fa0

```
Router(config-if)#ip address 192.168.10.1
```

```
255.255.255.0 Router (config-if) #no shutdown
```

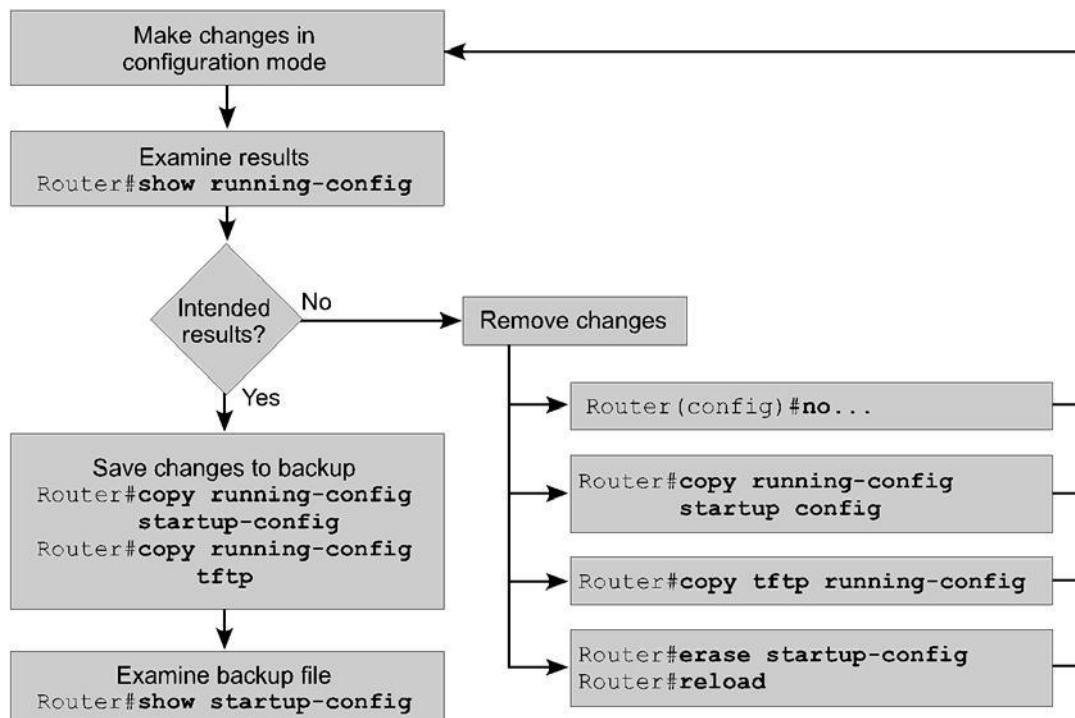
Settingan untuk save running configuration ke startup configuration file di NVRAM, masukan command di privileged mode:

```
Router#copy running-config startup-config
```

```
atau Router#copy runn start
```

-Executing adds, moves, and changes

Release 12.x (IOS) Configuration Mode



-Interface description

Interface description digunakan untuk mengidentifikasi informasi penting seperti distant router, circuit number, atau specific network segment. Description interface dapat membantu network admin mengingat specific information tentang interface.

Contoh:

```
RTA(config) #interface ethernet 0  
RTA(config-if)#description LAN Engineering, Bldg.2  
RTA (config-if) #exit  
RTA (config) #exit  
RTA# show running- config
```

Result:

```
interface Ethernet0  
  description LAN Engineering, Bldg. 2  
  ip address 192.5.5.1 255.255.255.0  
  no ip directed-broadcast!
```

-Login banner

Login banner adalah message yang di display pada saat login dan sangat berguna untuk memberikan attention/ warning. Contoh:



-Host table

Host names, tidak seperti DNS names, yang hanya significant pada router dimana dia di configured. Host table mengijinkan network administrator dapat men -type apakah host name seperti Auckland atau IP address untuk Telnet ke remote host. Contoh host table.

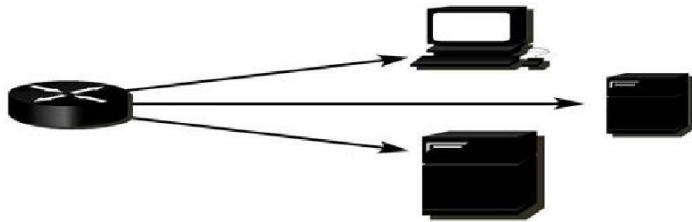
```
Router(config) #ip host Auckland 172.16.32.1  
Router(config) #ip host Beirut 192.168.53.1  
Router(config) #ip host Capetown 192.168.89.1  
Router(config) #ip host Denver 10.202.8.1
```

Settingan host table:

1. Masuk ke global configuration mode .
2. Masukan command **ip host** di ikuti dengan name router dan semua IP addresses yang ter-connected dengan interfaces di tiap router.
3. Lanjutkan dengan router-router lainnya.
4. Save configuration to NVRAM.

-Configuration backup and documentation

Penyimpanan kofigurasi sebagai backup files sangat penting jika terjadi problem, Konfigurasi files dapat disimpan pada network server, TFTP server, atau disk computer.



-Copying, editing, and pasting configurations

Proses mem backup Konfigurasi router ke TFTP server, stepnya:

Step 1 Enter **copy running-config tftp** command.

Step 2 Enter IP address dari host dimana configuration file disimpan.

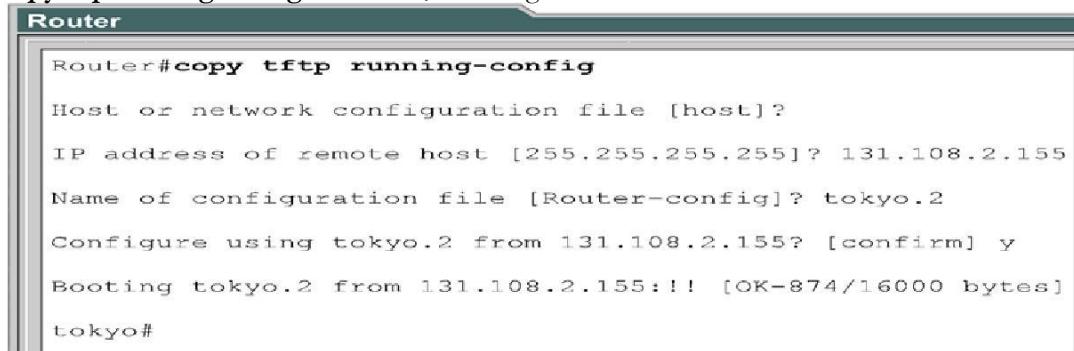
Step 3 Enter name dari configuration file.

Step 4 Confirm choices dengan answering yes each time.

Proses mengembalikan file backup di tftp server ke config router

1. Masuk configuration mode masukkan perintah

copy tftp running-config command, contoh gambar:



```
Router#copy tftp running-config
Host or network configuration file [host]?
IP address of remote host [255.255.255.255]? 131.108.2.155
Name of configuration file [Router-config]? tokyo.2
Configure using tokyo.2 from 131.108.2.155? [confirm] y
Booting tokyo.2 from 131.108.2.155:!! [OK-874/16000 bytes]
tokyo#
```

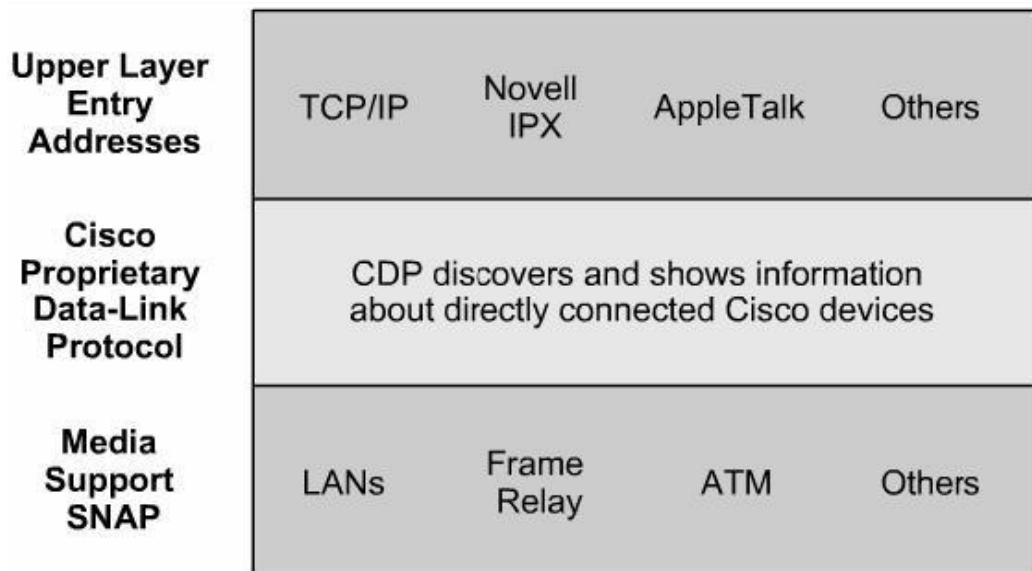
Perhatikan pada nama router, prompt berubah ke **tokyo**. Ini membuktikan bahwa reconfiguration telah berhasil.

Router configuration juga dapat di saved ke disk dengan capturing text pada router dan disimpan ke disk or hard drive. Jika file diperlukan dapat di copi kembali ke router, menggunakan perintah standard edit dari terminal emulator program (notepad,word) dan paste command file kembali ke router.

CHAPTER 4

Learning About Other Devices

1. CDP



CDP digunakan untuk mendapatkan informasi tentang cisco tetangga, seperti informasi tentang tipe device yang terhubung, interface yang terhubung, interface yang digunakan untuk koneksi dan jumlah model device. CDP adalah media dan protokol yang independen dan jalan di atas Subnetwork Access protocol (SNAP).

CDP versi 2 (CDPv2) adalah versi terbaru. Cisco IOS release 12.0(3)T atau yang lebih baru menggunakan CDPv2, sedangkan CDPv1 defaultnya enable di Cisco IOS release 10.3 sampai 12.0(3)T.

Ketika cisco device boot up, CDP secara otomatis start dan device melakukan deteksi terhadap device tetangga yang menggunakan CDP. CDP beroperasi pada data link layer dan membiarkan sistem learn ke tetangganay, meskipun menggunakan protokol layer berbeda.

Masing-masing device yang dikonfigurasi CDP mengirimkan pesan secara periodik yang dikenal dengan advertisement ke device cisco yang terhubung langsung. Masing-masing advertise paling sedikit satu address yang menerima pesan Network Management Protocol (SNMP). Advertisement juga berisi time-to-live atau informasi holdtime yang menentukan panjang waktu device menerima informasi CDP sebelum discard informasi tersebut. Setiap device listen secara periodic pesan CDP yang dikirim oleh device tetangga.

Perintah-perintah CDP

- cdp run
- cdp enable
- show cdp traffic
- clear cdp counters
- show cdp
- show cdp entry {*|device-name [*][protocol | version]}
- show cdp interface [type number]
- show cdp neighbors [type number] [detail]

Perintah cdp run digunakan untuk enable CDP secara global pada router. Secara default CDP dalam kondisi enable. Perintah cdp enable digunakan untuk men-enable-kan CDP.

Informasi dapat digunakan untuk menciptakan peta jaringan dari device yang terhubung langsung. Untuk menemukan device yang terhubung ke router tetangga, kemudian gunakan perintah show cdp neighbors.

Disable CDP

CDP dapat di-disable dengan dua level:

Menggunakan perintah no cdp run yang digunakan di global config. Perintah ini digunakan saat hanya satu device cisco dan jika CDP dijalankan tidak akan ada gunanya.

CDP dapat di-disable dari interface tertentu. Dengan menggunakan perintah no cdp enable atau no cdp advertise-v2 berdasar versi dari CDP yang digunakan.

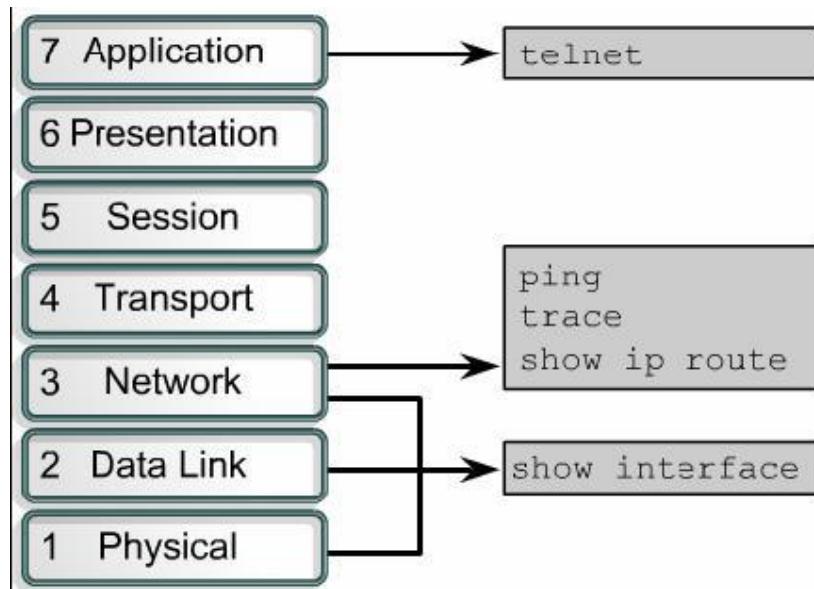
| Command | Description |
|----------------------------------|---|
| <code>clear cdp table</code> | Deletes the CDP table of information about neighbors. |
| <code>clear cdp counters</code> | Resets the traffic counters to zero. |
| <code>show cdp traffic</code> | Displays CDP counters, including the number of packets sent and received and checksum errors. |
| <code>show debugging</code> | Determines which types of debugging are enabled. |
| <code>debug cdp adjacency</code> | CDP neighbor information |
| <code>debug cdp events</code> | CDP events |
| <code>debug cdp ip</code> | CDP IP information |
| <code>debug cdp packets</code> | CDP packet-related information |
| <code>cdp timer</code> | Specifies how often the Cisco IOS software sends CDP updates. |
| <code>cdp holdtime</code> | Specifies the hold time to be sent in the CDP update packet. |
| <code>show cdp</code> | Displays global CDP information, including timer and hold-time information. |

perintah CDP troubleshooting

2. Dasar ruter dan routing Telnet

Telnet adalah suatu protokol virtual terminal yang merupakan bagian dari protokol TCP/IP. Telnet digunakan untuk remote host yang digunakan untuk verifikasi

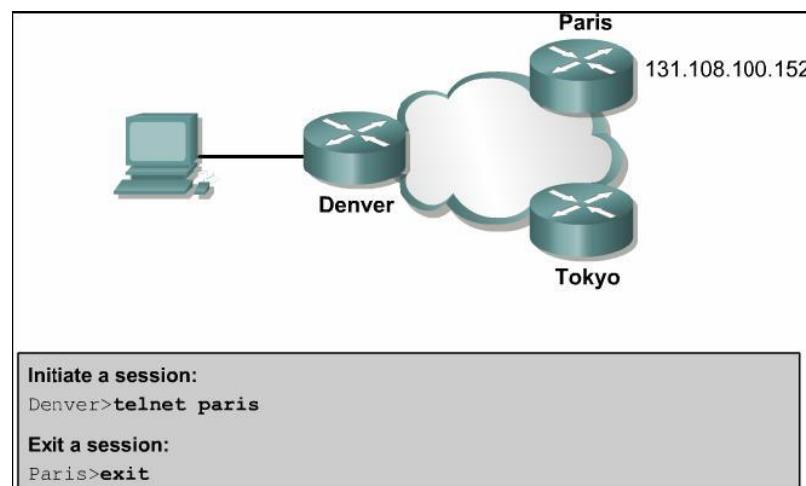
layer aplikasi antara asal dan tujuan. Fungsi telnet pada layer aplikasi OSI layer. Telnet tergantung dari TCP untuk menggaransi data antara client dan server.



telnet beroperasi pada layer aplikasi

Dengan telnet user dapat melakukan remote dari satu cisco ke cisco lainnya. Hostname atau IP address harus diketahui untuk bisa melakukan remote menggunakan telnet. Dan untuk keluar dari sesi telnet gunakan perintah exit atau logout. Untuk menginisialisasi sesi telnet dapat dilakukan dengan cara sebagai berikut:

```
Denver>connect paris  
Denver>paris  
Denver>131.108.100.152  
Denver>telnet paris
```



cara kerja telnet

Jika telnet ke satu router berhasil, gagal ke router lainnya karena kesalahan address atau masalah hak akses. Langkah selanjutnya adalah dengan menggunakan perintah ping yang berfungsi untuk melakukan testing koneksi.

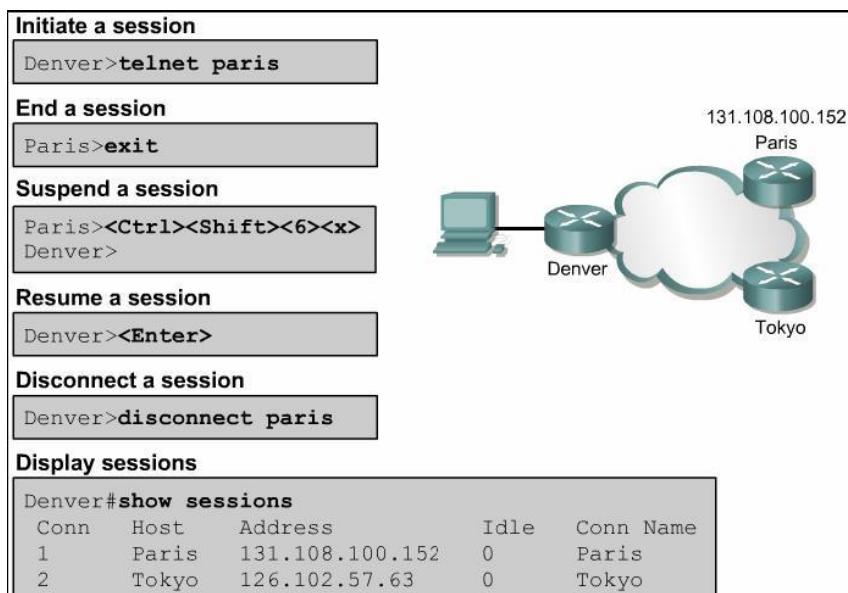
Untuk mengetahui sesi telnet mana yang sedang aktif digunakan perintah show sessions. Prosedur yang digunakan untuk diskonek sesi telnet sebagai berikut:

Masukkan perintah disconnect

Dikuti dengan hostname atau IP address,
misal: Denver>**disconnect paris**

Prosedur yang digunakan untuk keluar dari
telnet: Tekan tombol Ctrl-Shift-6, kemudian x

Masukkan hostname atau IP address



cara kerja telnet

Testing koneksi dengan PING

Perintah **traceroute** dapat digunakan untuk mencari dimana data dikirim ke jaringan. Perintah ini mirip dengan perintah **ping**. Perbedaan dasar, kalau **ping** untuk testing konektivitas dari end-to-end sedangkan **traceroute** tes konektivitas setiap step perjalanan data.

Jika satu dari router yang dilewati unreachable, maka akan muncul tanda 3 asterisk (*). Untuk melihat table routing pada router dapat digunakan perintah **show ip route**.

Di bawah ini adalah prosedur penggunaan perintah ping:

- Masukkan perintah **ping** diikuti dengan IP address atau hostname dari tujuan
- Tekan tombol **ENTER**

Sedangkan untuk menggunakan perintah traceroute:

- Masukkan perintah **traceroute** diikuti dengan IP address atau hostname dari tujuan
- Tekan tombol **ENTER**

Ping

Menggunakan protokol ICMP untuk mem-verifikasi koneksi hardware dan IP address dari layer network.

Telnet

Mem-verifikasi software layer aplikasi antara sumber dan tujuan.

Traceroute

Memberikan lokasi kegagalan antara sumber dan tujuan.

CHAPTER 5

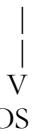
Router and Routing Basics

Pada saat inialisasi Route, yg akan dilakukan

Router on



BootStarap.POST



Load IOS (Flash, TFTP server, ROM)



| #1 #2 #3

Load Configuration File (Startup)
(NVRAM, TFTP Server, Console)

#1 #2 #3

Catatan :

#1 : prioritas pertama

#2 : jika di #1 tidak ada

#3 : jika di #2 tidak ada

Configuration Refister:

Bentuk bilangan hexadecimal yg dpt digunakan untuk melakukan perubahan terhadap cara inisialisasi Router. Nilai dari Configuration Register ada :

Ox2100 => masuk ke ROM monitor (rommon>)

Ox2101 => masuk ke boot ROM, tapi untuk IOS versi terbaru, nilai ini artinya mengambil IOS pertama yg ada di Flash

Ox2102 => normal operation

F disebut dengan boot field

Di CLI, cara setting configuration register:

Router(config)#config-register ox_ _ _ _

Di Rommon; cara setting configuration register:

Rommon1> Confreg ox_ _ _ _

Boot System :

Adalah command yg tujuan utamanya adalah unutuk:

1. mengubah inisialisasi Router dlm mencari IOS semisal kita ingin langsung load IOS dari TFTP server
2. Jika kita ingin meload IOS kedua yg berada dalam Flash Setting boot system ada 3 :
 - Router(config)#boot system flash [nama IOS]
 - Router(config)#boot_system tftp [nama IOS] [IP dari TFTP server]

```
- Router(config)#boot system rom
```

```
-
```

Command boot system baru akan berjalan bila kita sudah melakukan “copy run start” Kita dapat melihat efek dari boot system ini dengan perintah “show session” di bagian “System Image File is “.....” “

TFTP Server:

Sabuah program daemon yg berjalan sbg service. Salah satu contoh programnya adalah 3 C Daemon. TFTP server berguna untuk backup dan restore memanfaatkan Kabel LAN, karena itu sebelum melakuakan backup atau restore pastikan antar PC dengan IP fastEthernet Router berada dalam 1 subnet dan sudah terkoneksi(lakukan tes ping terlebih dahulu)

Untuk 3c Daemon yg perlu dilakukan hanya double click program tsb, lalu ada button “Configur TFTP server”, arahakan upload/ download directory ke tempat yg kita inginkan

Beberapa command untuk backup atau restore:

1. Copy run start : dari RAM ke NVRAM
2. copy run tftp : dari RAM ke TFTP
3. Copy start tftp: dari NVRAM ke TFTP
4. Copy flash tftp : backup IOS yg ada di Flash ke tftp server
5. Copy tftp run : dari tftp ke RAM
6. Copy tftp start : dari TFTP ke NVRAM
7. Copy tftp flash : restore IOS dari TFTP ke flash

Sebelum melakukan backup atau restore IOS. Terlebih dahulu pastikan nama IOS yang benar dan ukurannya(show version dan show flash)

Backup atau restore yg benar diwakili dgn tanda “!”; sementara yg tidak benar, dengan tanda “.”

Untuk Backup maupun restore Configuratio File, bias juga dilakukan dgn copy paste ataupun fitur “transfer” di Hyper Terminal

Bila kita di router sudah tidak ada IOS, maka otomatis router akan masuk rommon.

Untuk restore IOS, ada 2 cara:

1. Xmodem : menggunakan port console di router
2. tftpdnld : menggunakan port Ethernet

yg perlu diperhatikan : pastikan anda sudah punya IOS YG TEPAT unutk router anda di PC!!

Cara restore IOS menggunakan Xmodem:

1. Rommon1>confreg [enter]
2. “Do you want to change : Yes”
3. Abaikan pertanyaan2 berikutnya, kecuali pada petanyaan: “Do you want to change console baud rate?” jawab : Yes; kemudian pilih no. 7 : 115200 bps
4. setelah itu matikan HT, nyalakan lagi tapi dgn baud rate diganti jd 115200
5. rommon1>xmodem -c [nama IOS] [enter]

6. lalu di HT, di bagian Send File, pilih area dimana IOS yg baru disimpan, dan pilih protocol Xmodem

*) untuk Xmodem ini waktu restore agak lama, karena hanya 115200 bps, bandingkan dgn tftpdnld yg kecepatannya 10/100 MBps

Cara restore IOS menggunakan tftpdnld:

1. rommon1>set [enter]
2. rommon2>IP_ADDRESS = 192.168.1.1 [enter]
3. rommon3>IP_SUBNET_MASK = 255.255.255.0 [enter]
4. rommon4>DEFAULT_GATEWAY = 192.168.1.1 [enter]
5. rommon5>TFTP_SERVER = 192.168.1.1 [enter]
6. rommon6>TFTP_FILE = c2620-jk8s-mz.122-21a –bin [enter]
7. rommon7>tftpdnld [enter]
8. PAstikan semua setting sudah benar, tekan yes

PASSWORD RECOVERY

1. matikan , lalu nyalakan router, tekan Ctrl + Break sampai masuk ke rommon
2. rommon1>confreg ox2142 [enter]
3. rommon2>i atau boot [enter]
4. copy start run
5. ganti password
6. Router(config)#config-register ox2102 [enter]
7. copy run start
8. reload

Command untuk copy IOS ke tftp server pada computer adalah:

Router#copy flash tftp

Namun unutk mengembalikan IOS pada router tipe baru tidak dapat dengan:

Router#copy tftp flash

Sebab kita tidak dapat mengetikkan command ini pada ROMMON, ini hanya berlaku untuk router tipe lama.

Pada router tipe baru, pemulihan IOS dilakukan dengan:

-) XModem => pakai kabel console -)

tftpdnld =>pakai kabel fastEthernet

Kedua command router ini diketikkan pada ROMMON

Tiga environment router pada dasarnya yaitu:

-)ROMMON : rommon> -

)boot room : Router(boot)> -

)IOS Normal : Router >

Namun ada perbedaan antar router tipe lama(missal: seri 2500) dengan router tipe baru(missal:2600,1700,1800,dll) yaitu:

Tipe lama:

- ada 3 environment : ROMMON, boot room, IOS
- dapat memakai confreg: 0x2102, 0x2101, 0x2100, 0x2142
- menghapus IOS pada boot room: Router(boot)#erase flash

- memulihkan IOS pada boot room: Router(boot)#copy tftp flash
- password recovery pada ROMMON: >0/r 0x2102
>i
- Prompt pada ROMMON:
>
- ROMMON hanya untuk password recovery, tidak dapat Xmodem dan tftp dnld

Tipe baru:

- ada 2 environment : ROMMON, IOS
- dapat memakai confreg: 0x2102, 0x2100, 0x2142 (0x2101 tidak efek sebab tidak kenal boot room)
- menghapus IOS pada IOS normal: Router#erase flash
- memulihkan IOS pada ROMMON dengan Xmodem atau tftp dnld
- password recovery pada ROMMON: rommon>
ROMMON dapat untuk password recovery, XModem, tftp dnld

Command-command lainnya sama untuk keduanya, seperti:

1. Copy run start : dari RAM ke NVRAM
2. copy run tftp : dari RAM ke TFTP
3. Copy flash tftp : backup IOS yg ada di Flash ke tftp server
4. Copy tftp run : dari tftp ke RAM
5. Copy start run

CHAPTER 6

Routing and Routing Protocol

Routing yaitu proses meneruskan paket ke network tujuan based on destination IP Address.

Ada 2 jenis routing :

a) **Static Route :**

Route yang dikonfigurasi manual oleh network administrator secara satu per satu, tidak cocok untuk network skala besar.

b) **Dynamic Route :**

Route yang dikonfigurasi oleh admin, tapi memakai routing protocol yang dapat menyesuaikan route-route mana saja yang dapat dicapai, cocok untuk network skala besar.

Langkah dalam static route :

- Admin mengkonfigurasi routenya
- Route diinstall di routing table
- Paket diteruskan berdasarkan route

Command-command static route :

• **Konfigurasinya :**

Router(config)#ip route network tujuan subnetmask outgoinginterface (gateway) / next hop ip address

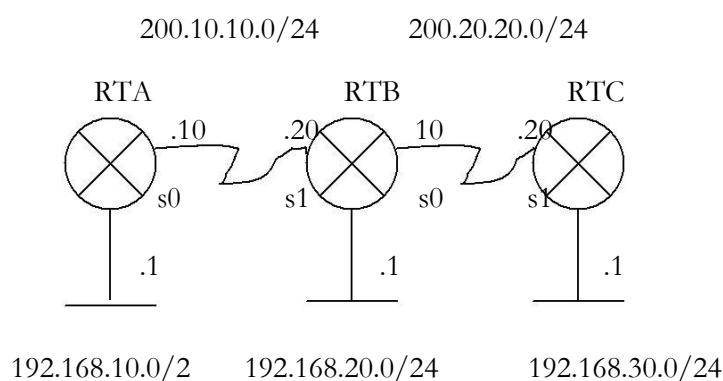
• **Melihat route :**

Router#show ip route

• **Melihat konfigurasi :**

Router#show run

Contoh :



Berdasarkan outgoing interface (gateaway) :

```
RTA(config)#ip route 192.168.20.0 255.255.255.0 s0/0  
RTA(config)#ip route 200.20.20.0 255.255.255.0 s0/0  
RTA(config)#ip route 192.168.30.0 255.255.255.0 s0/0
```

```
RTB(config)#ip route 192.168.10.0 255.255.255.0 s0/1  
RTB(config)#ip route 192.168.30.0 255.255.255.0 s0/0
```

```
RTC(config)#ip route 192.168.20.0 255.255.255.0 s0/1  
RTC(config)#ip route 200.10.10.0 255.255.255.0 s0/1  
RTC(config)#ip route 192.168.10.0 255.255.255.0 s0/1
```

Berdasarkan next hop ip address :

```
RTA(config)#ip route 192.168.20.0 255.255.255.0 200.10.10.20  
RTA(config)#ip route 200.20.20.0 255.255.255.0 200.10.10.20  
RTA(config)#ip route 192.168.30.0 255.255.255.0 200.20.20.20
```

```
RTB(config)#ip route 192.168.10.0 255.255.255.0 200.16.10.10  
RTB(config)#ip route 192.168.30.0 255.255.255.0 200.20.20.20
```

```
RTC(config)#ip route 192.168.20.0 255.255.255.0 200.20.20.10  
RTC(config)#ip route 200.20.20.10 255.255.255.0 200.20.20.10  
RTC(config)#ip route 192.168.10.0 255.255.255.0 200.10.10.10
```

CHAPTER 7

Distance Vector Routing Protocols

Pada distace vector routing protocols, routing updates muncul secara periodik dan pada saat topologi network berubah. Updates dilakukan dengan cara router mengirim routing table beserta informasi path cost kepada router-router tetangga.

Routing loop adalah keadaan di mana packet tidak dapat sampai ke tujuan dan hanya berputar di router-router yang sama. Routing loop dapat muncul apabila inconsistent routing table tidak terupdate.

Cara-cara mencegah routing loop:

- **Maximum Count**
yaitu dengan menentukan batas metric maksimum sebelum paket dibuang.
- **Split Horizon**
yaitu dengan tidak memperbolehkan router mengirimkan update balik kepada router lain yang terlebih dahulu memberikan update kepada router tersebut.
- **Route Poisoning**
yaitu dengan men-set hop count lebih dari batas maksimum untuk network yang tidak available.
- **Triggered Updates**
yaitu dengan mengirimkan update secepatnya (tidak menunggu secara periodik saja) ketika ada network yang down.
- **Holddown Timers**
yaitu dengan menunggu sesuai waktu yang di-set untuk menentukan apakah update akan digunakan atau tidak dengan membandingkan dengan update dari router lain sesuai dengan metric value-nya.

RIP

RIP adalah salah satu distance vector routing protocol. Ada 2 versi yaitu:

1. RIP version 1 (RIPv1) yang merupakan Classful Routing Protocol
2. RIP version 2 (RIPv2) yang merupakan Classless Routing Protocol

Kelebihan RIPv2:

- Dapat memuat informasi tambahan tentang routing
- Mekanisme authentication supaya table updates aman
- Mendukung variable-length subnet mask (VLSM)

RIP mengirimkan routing updates setiap 30 detik.

Untuk mencegah routing loop, RIP mengimplementasikan batas hop count maximum yaitu 15 hop, apabila lebih dari itu, maka network unreachable.

Cara konfigurasi RIP:

Ketik command **router rip** pada global config, kemudian masukkan network yang ingin diasosiasi dengan RIP. Contoh:

```
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# network 192.168.10.0
```

Ip classless membolehkan router men-forward paket yang mempunyai tujuan subnet yang tidak diketahui, untuk di-forward ke route supernet terbaik. Untuk men-set pada router, gunakan command **ip classless** (secara default sudah di-enable).

RIP menggunakan beberapa mekanisme untuk mencegah routing loop, yaitu:
Split Horizon, Poison Reverse, Holddown counters dan Triggered Updates.

Perintah-perintah untuk konfigurasinya:

Router(config-if)#no ip split-horizon ↵ untuk disable split horizon pada interface

Router(config-router)#timers basic *update/invalid/holddown/flush [sleeptime]* ↵ untuk mengubah holddown timer serta update, invalid dan flush timers

Untuk disable routing updates pada interface, gunakan command:

Router(config-router)#**passive-interface Fa0/0**

Untuk men-cek apakah konfigurasi RIP sudah benar, gunakan command:

- show ip protocols ↵ menunjukkan routing protocol mana yang membawa traffic ip
- show ip route ↵ menunjukkan route-route yang terdapat pada routing table
- show interface
- show ip interface
- show running-config

Untuk menemukan masalah yang ada pada RIP, gunakan command **debug ip rip**.

IGRP

Selain RIP, distance vector routing protocol lainnya adalah IGRP. Berbeda dengan RIP yang merupakan protocol standard, IGRP adalah protocol khusus buatan cisco. IGRP mengirim routing update setiap 90 detik dan menggunakan bandwidth dan delay sebagai metric.

3 tipe route yang di-advertise IGRP:

- Interior: Route antara subnet-subnet yang tersambung pada interface router.
- System: Route untuk network di dalam satu autonomous system. (tidak ada informasi subnet)
- Exterior: Route untuk network yang berada pada autonomous system yang berbeda.

Untuk mengkonfigurasi IGRP pada router, gunakan command
berikut: Router(config)#router igrp *as-number*

Untuk mematikan proses IGRP:

Router(config-router)#no router igrp *as-number*

Command-command untuk konfigurasi IGRP:

- show ip route
- show ip protocols ↵ menunjukkan routing protocol mana yang membawa traffic ip
- show interface
- show running-config
- show running-config interface
- show running-config | begin interface
- show running-config | begin igrp

Command-command untuk menemukan masalah pada IGRP:

- debug igrp events
- debug igrp transactions
- ping
- traceroute

Chapter 8

TCP/IP Suite Error and Control Messages

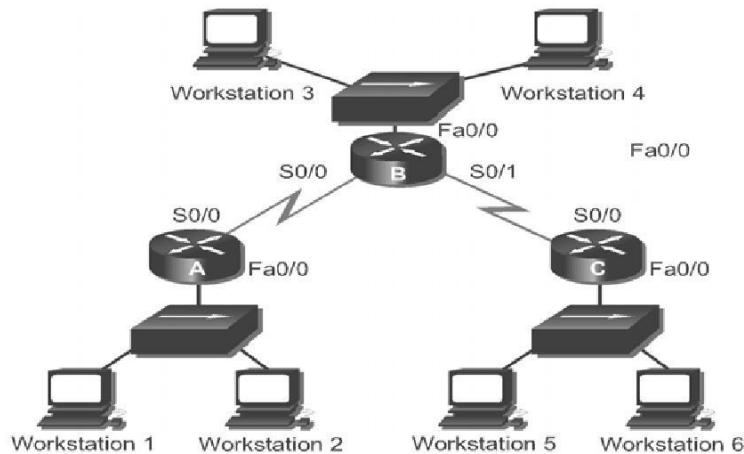
IP mempunyai keterbatasan dalam mengantar suatu data ketujuan, IP tidak mempunyai mekanisme untuk memastikan data tersebut telah sampai ke tempatnya, disebabkan hal seperti kerusakan hardware, configurasi yang tidak benar atau kesalahan routing informasi. Untuk mengatasi masalah diatas, IP menggunakan Internet Control Messages Protocol (ICMP) untuk memberi pesan ke pengirim bahwa terdapat error dalam proses pengiriman data.

Error Reporting

ICMP adalah protocol untuk memberikan pesan error. Ketika proses pengiriman data terjadi error, ICMP digunakan sebagai report yang ditujukan pada source dari data tersebut.

Contoh:

Workstation 1 mengirim data ke workstation 6, tapi interface Fa 0/0 pada Router C dalam kondisi down, Router C akan menyiapkan ICMP untuk mengirim message kembali ke Workstation 1 yang memberitahukan data tidak bisa diterima. ICMP tidak dapat mengatasi atau memperbaiki network problem, hanya melaporkan (messages) saja.



Ketika Router C menerima data dari Workstation 1, dia hanya mengetahui source dan destination IP address dari data itu. Dia tidak mengetahui apakah data tersebut melewati path lain sebelum sampai di Router C. Karena itu, Router C hanya dapat memberi pesan pada Workstation 1 bahwa telah terjadi kesalahan, dan tidak ada ICMP messages yang dikirim ke Router A dan Router B.

ICMP Messages Delivery

ICMP messages di encapsulated ke dalam datagrams dengan jalan yang sama ketika data lainnya dikirim menggunakan IP.

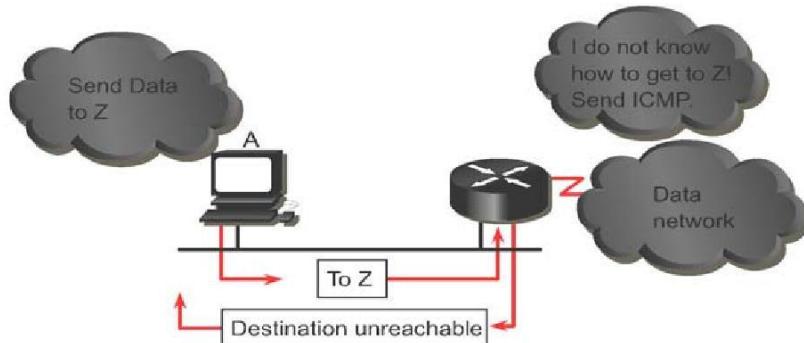
| | | | |
|--------------|-----------------|--------------------|-----------|
| Frame Header | Datagram Header | ICMP Header | ICMP Data |
| Frame Header | Datagram Header | Datagram Data Area | |
| Frame Header | Frame Data Area | | |

Gambar. displays the encapsulation of ICMP data within an IP datagram.

ICMP dalam proses pengirimannya juga bisa terjadi kesalahan/ error. Ini menyebabkan error report menimbulkan error tambahan, menjadikan peningkatan congestion pada network yang bermasalah tadi. Untuk alasan itu error yang disebabkan oleh ICMP messages tidak meng generate ICMP messagesnya sendiri.

Unreachable Networks

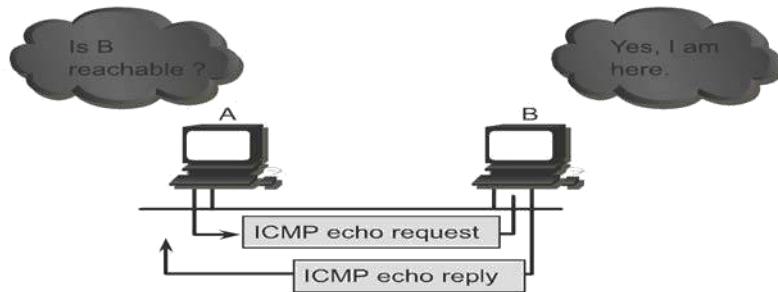
Network communication dapat terjadi jika; *Satu*, sending and receiving devices harus punya TCP/IP protocol yang di configure dengan benar. Ini meliputi peng install an TCP/IP protocol dan peng configurasian dari IP address and subnet mask yang tepat. Default gateway harus di konfigurasi jika datagrams menuju outside local network. *Dua*, intermediary devices (Router) untuk men route datagram dari source device suatu network menuju ke destination network lain. Router juga harus punya TCP/IP protocol yang di configurasi benar di interfaces nya, dan harus menggunakan routing protocol yang tepat.



An ICMP destination unreachable message is sent if:

- Host or port unreachable
- Network unreachable

ICMP protocol dapat dipakai untuk men test ketersediaan jalur ke destination. Jika destination devices menerima ICMP echo request, dia akan membalas dengan echo reply message yang dikirim kembali ke source dari echo request. Jika pengirim menerima echo reply, maka ini meng confirm bahwa destination device dapat dicapai via IP protocol.



Traffic generated by the `ping` command

Gambar. ICMP being used to issue an echo request message to the destination device

Semua ICMP message formats dimulai dengan 3 fields:

- Type
- Code
- Checksum

Type field mengindikasikan type dari ICMP message yang sedang dikirim. Code field memasukan informasi lanjutan yang spesifik ke message type. Checksum field, alias types dari packets, digunakan untuk memeriksa integritas dari data.

| ICMP Message Types | |
|--------------------|--------------------------|
| 0 | Echo Reply |
| 3 | Destination Unreachable |
| 4 | Source Quench |
| 5 | Redirect/ Change Request |
| 8 | Echo Request |
| 9 | Router Advertisement |
| 10 | Router Selection |
| 11 | Time Exceeded |
| 12 | Parameter Problem |
| 13 | Timestamp Request |
| 14 | Timestamp Reply |
| 15 | Information Request |
| 16 | Information Reply |
| 17 | Address Mask Request |
| 18 | Address Mask Reply |

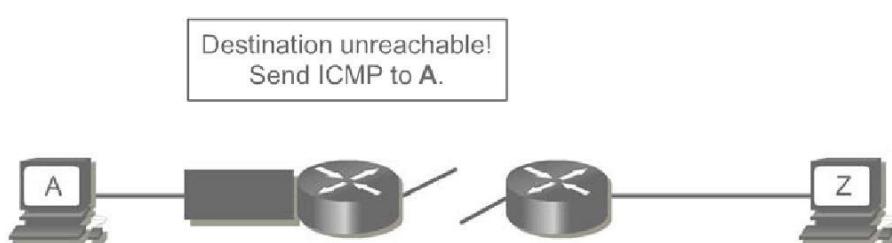
Gambar. ICMP message type.

| 0 | 8 | 16 | 31 |
|---------------|----------|----------|-----------------|
| Type (0 or 8) | Code (0) | Checksum | |
| Identifier | | | Sequence Number |
| Optional Data | | | ... |
| | | | |

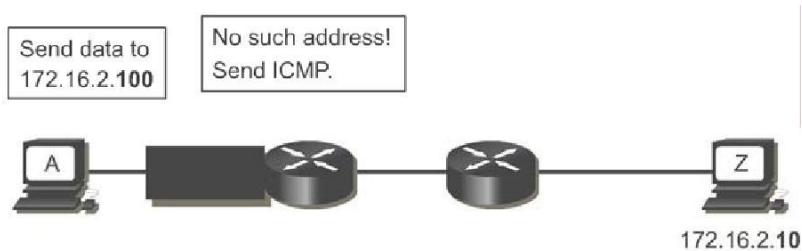
Gambar. Message format for the ICMP echo request and echo reply messages.

Jika Router tidak dapat mengirim paket ke destination, router akan mengirim ICMP “Destination Unreachable” message kembali ke sourcennya meginformasikan terjadi problem. Router akan meng discard original packet. Destination tidak terjangkau bisa disebabkan oleh host pengirim memasukan address yang salah, atau router tidak mempunyai route untuk ke destination. Jika router tidak dapat mengirim balik ICMP message dengan alasan apapun, maka undeliver ICMP message akan di discard.

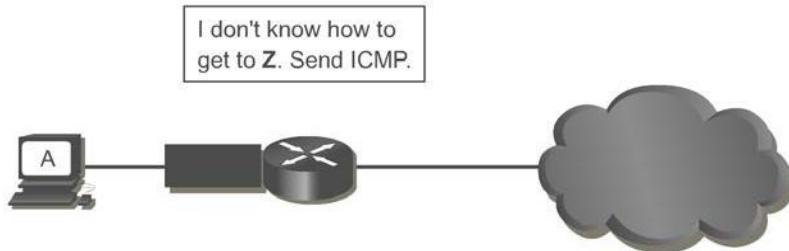
Beberapa failure yang menyebabkan ICMP message terjadi:



Gambar. Hardware failure



Gambar. Improper protocol configuration



Gambar. Incorrect routing information

A destination unreachable message dapat juga dikirimkan ketika packet fragmentation diperlukan untuk mem forward sebuah packet. Fragmentation biasanya diperlukan ketika datagram di forward dari Token-Ring network ke Ethernet network. Jika datagram tidak membolehkan fragmentation, packet tidak bisa di forward, maka destination unreachable message akan dikirim. Destination unreachable messages juga ditimbulkan oleh hal yang berhubungan dengan IP services seperti FTP or Web services are unavailable. Untuk

mengeffektif kan troubleshoot pada IP network, adalah penting untuk mengetahui the various causes of ICMP destination unreachable messages.

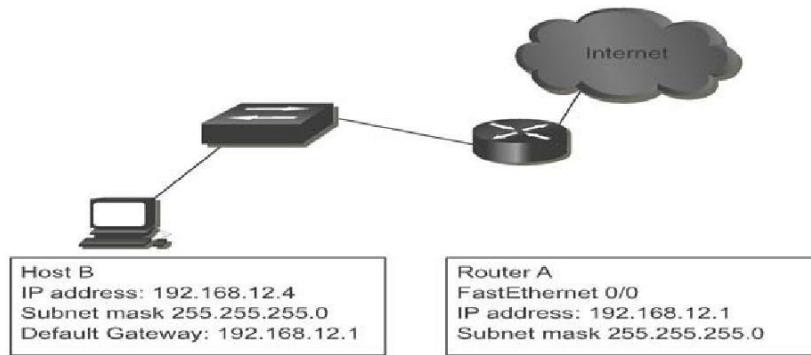
TCP/IP Suite Control Messages

Tidak seperti error message, control message tidak terjadi dikarenakan lost packet atau error kondisi yang timbul sewaktu packet transmission. Malah, digunakan untuk menginformasikan kepada host tentang kondisi seperti network congestion atau keberadaan gateway menuju remote network. Seperti semua ICMP message, ICMP control messages di encapsulated didalam IP datagram. ICMP menggunakan IP datagrams dalam perjalannya ke multiple networks

| | | | |
|--------------|-----------------|--------------------|-----------|
| Frame Header | Datagram Header | ICMP Header | ICMP Data |
| Frame Header | Datagram Header | Datagram Data Area | |
| Frame Header | Frame Data Area | | |

Paling umum dari ICMP control message adalah ICMP redirect/change request. type message ini hanya dapat di initiated oleh gateway. Semua hosts tang berkomunikasi dengan multiple IP networks harus di konfigurasi dengan default gateway. Default gateway adalah address dari suatu router port yang connected ke network yang sama sebagai host.

Gambar dibawah menunjukan host connected ke router yang menghubungkan ke Internet. Setelah di configure dengan IP address pada Fa 0/0 sebagai default gateway, Host B menggunakan IP address itu untuk menuju network luar.



Default gateways hanya mengirim ICMP redirect/change request messages jika kondisi dibawah ini terpenuhi:

- Interface dimana packet datang ke router adalah Interface yang sama dimana packet keluar.
- Subnet/network dari source IP address adalah sama dengan subnet/network dari next-hop IP address dimana packet di routekan.
- Datagram bukan source-routed.
- Bukan merupakan ICMP redirect atau default route.

- Router di konfigurasi untuk mengirim redirects. (By default, Cisco routers send ICMP redirects. The interface subcommand **no ip redirects** will disable ICMP redirects.)

Subnet mask adalah crucial dalam meng identifikasi sebuah network, subnet, and host bits dalam sebuah IP address. Jika sebuah host tidak tahu subnet mask, dia akan meminta address mask ke local router. Jika address ada di router , permintaan ini langsung dikirim oleh si router. Jika tidak, permintaan tadi di broadcast.

Contoh , misal suatu host terletak di Class B network dengan IP address of 172.16.5.2. Host ini tidak tahu subnet mask, dia akan mem broadcasts permintaan address mask :

| | |
|----------------------|----------------------------|
| Source address: | 172.16.5.2 |
| Destination address: | 255.255.255.255 |
| Protocol: | ICMP = 1 |
| Type: | Address Mask Request = AM1 |
| Code: | 0 |
| Mask: | 255.255.255.0 |

Broadcast yang diterima oleh 172.16.5.1, local router. Router merespond dengan address mask reply:

| | |
|----------------------|--------------------------|
| Source address: | 172.16.5.1 |
| Destination address: | 172.16.5.2 |
| Protocol: | ICMP = 1 |
| Type: | Address Mask Reply = AM2 |
| Code: | 0 |
| Mask: | 255.255.255.0 |

Router discovery message

Sebuah host menghasilkan permintaan ICMP router message dalam me respons hilangnya default gateway. Message ini dikirim ke semua router via multicast (address 224.0.0.2) dan ini adalah langkah pertama dari router discovery process. Local router akan me respond dengan suatu router advertisement yang mengidentifikasi default gateway untuk local host.



| 0 | 8 | 16 | 31 |
|-----------|----------|----------|----|
| Type (10) | Code (0) | Checksum | |
| Reserved | | | |

Gambar. identifikasi frame format dan Figures

| IP Fields | |
|---------------------|---|
| Source Address | An IP address belonging to the interface from which this message is sent, or 0. |
| Destination Address | The Configured solicitation address |
| Time- to - live | 1If the destination address is an IP multicast address; at least 1 otherwise |
| ICMP Fields | |
| Type | 10 |
| Code | 0 |
| Checksum | The 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP type. For computing the checksum, the checksum field is set to 0. |
| Reserved | |

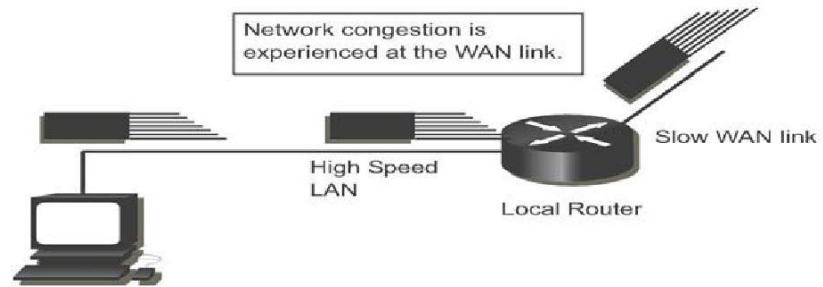
Gambar.keterangan dari tiap field.

Congestion and flow control messages

Jika multiple komputer mencoba untuk access ke destination yang sama , destination computer akan megalami traffic yang berlebih. Congestion dapat juga timbul ketika traffic dari high speed LAN sampai ke slower WAN connection. Drop packet terjadi ketika congestion sudah terlalu banyak dalam suatu network. ICMP source-quench messages digunakan untuk me reduce sejumlah data yang hilang tadi. Source-quench message meminta sender untuk me reduce jumlah dari transmit packetsatau melambatkannya.Kebanyakan Cisco routers tidak mengirim source-quench messages by default, karena source-quench message itu sendiri dapat menambah congestion network.

Sebuah small office home office (SOHO) adalah scenario dimana ICMP source-quench messages dapat digunakan secara efektif. SOHO mungkin terdiri atas empat computer network dengan CAT-5 kable dan Internet connection sharing (ICS) melalui 56K modem. Dengan mudah dapat kita lihat 10Mbps bandwidth dari SOHO LAN akan sangat melebihi dari 56K bandwidth dari WAN link, hasilnya banyak data loss dan retransmisi. Dengan ICMP messaging, host berlaku seperti gateway dalam ICS dapat me

request host lain untuk me reduce transmissi mereka pada rates yang manageable level, Hal ini akan mengurangi data loss yang berkelanjutan.



Gambar. Network congestion dalam WAN link menyebabkan communication problems

CHAPTER 9

Basic Router Troubleshooting

1. Testing table routing

1.1 Perintah show ip route

Perintah **show ip route** digunakan untuk menampilkan isi dari table routing. Table ini berisi entri semua jaringan dan subnetwork yang diketahui. Berikut ini adalah beberapa perintah tambahan yang dapat digunakan dengan perintah **show ip route**:

- **show ip route connected**
- **show ip route address**
- **show ip route rip**
- **show ip route igrp**
- **show ip route static**

```
RTA#show ip route
Codes: C - connected, S - static, I - IGRP, 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 download static route
Gateway of last resort is not set
C 192.168.4.0/24 is directly connected, Ethernet0
  10.0.0.0/16 is subnetted, 3 subnets
C 10.3.0.0 is directly connected, Serial0
C 10.4.0.0 is directly connected, Serial1
C 10.5.0.0 is directly connected, Ethernet1
```

Output perintah **show ip route**

Ketika RTA menerima paket yang ditujukan ke 192.168.4.46, tampilannya seperti prefix 192.168.4.0/24 pada table routingnya. RTA kemudian mem-forward paket keluar interface Ethernet0 berdasarkan entri table routing. Jika RTA menerima paket yang ditujukan untuk 10.3.21.5, ia mengirim paket tersebut keluar interface Serial 0.

Contoh table routing ditunjukkan oleh empat jalur jaringan yang terhubung langsung. Jalur-jalur ini diberi label "C". RTA membuang paket-paket yang ditujukan untuk jaringan yang tidak terdaftar di dalam table routing. Table routing untuk RTA akan berisi lebih jalur-jalur sebelum ia dapat mem-forward ke tujuan yang lain. Ada dua cara penambahan jalur-jalur baru:

- **Routing statis** – admin secara manual mendefinisikan jalur-jalur ke satu atau lebih jaringan tujuan
- **Routing dinamis** – router-router mengikuti aturan yang didefinisikan oleh protokol routing untuk pertukaran informasi routing dan pemilihan jalur terbaik

Secara administrasi mendefinisikan jalur-jalur dapat dikatakan statis karena mereka tidak berubah sampai admin jaringan secara manual memprogram perubahan. Jalur-jalur dipelajari dari router-router lain secara dinamis karena mereka berubah secara

otomatis sebagai update dari router-router yang terhubung langsung dengan informasi baru.

1.2 Penentuan gateway

Jalur default digunakan pada saat router tidak sesuai dengan jaringan yang dituju dengan beberapa entri yang ada dalam table routing. Router menggunakan jalur default ini untuk mencapai gateway dan mem-forward paket.

Sebelum router-router dapat secara dinamis melakukan pertukaran informasi, admin jaringan harus dikonfigurasi paling sedikit satu router dengan jalur default. Tergantung dari hasil yang didapat, admin dapat menggunakan perintah-perintah sebagai berikut:

ip default-network

Atau

ip route 0.0.0.0 0.0.0.0

1.3 Penentuan jalur asal dan tujuan

Layer network menyediakan best-effort, end-to-end dan pengiriman paket melalui jaringan interconnected. Layer network menggunakan table routing IP untuk mengirimkan paket-paket dari jaringan asal ke jaringan tujuan. Setelah router menentukan jalur mana yang digunakan, ia mem-forward paket dari satu interface ke interface lain atau port yang menuju ke jaringan tujuan.

1.4 Penentuan alamat L2 dan L3

Untuk tujuan pengiriman paket dari jaringan asal ke jaringan tujuan, menggunakan baik alamat layer 2 dan layer 3. Gambar di bawah menjelaskan proses yang terjadi paket dikirim melalui jaringan.

Alamat layer 3 digunakan untuk merutekan paket dari jaringan asal ke jaringan tujuan. Alamat-alamat IP asal dan tujuan sama. Alamat MAC berubah pada setiap hop atau router. Alamat layer data link penting karena pengiriman dalam jaringan ditentukan oleh alamat dalam header frame layer 2.

1.5 Penentuan administrative distance

Router menggunakan administrative distance di setiap jalurnya untuk menentukan jalur terbaik menuju tujuan. Administrative distance adalah nomor yang mengukur tingkat kepercayaan informasi jalur ke tujuan. Semakin kecil nilai administrative distance, semakin besar tingkat kepercayaan pemilihan jalur.

Routing protokol yang berbeda mempunyai administrative distance default yang berbeda juga. Jalur dengan administrative distance paling kecil adalah yang dimasukkan ke dalam table routing.

1.6 Penentuan jalur metric

Routing protokol menggunakan metric untuk menentukan jalur terbaik ke tujuan. Beberapa routing protokol menggunakan hanya satu faktor untuk menghitung metric. Contohnya, RIPv1 menggunakan hop count sebagai faktor menentukan metric. Protokol yang lain berdasarkan hop count, bandwidth, delay, load, reliability dan cost.

Faktor seperti bandwidth dan delay adalah statis karena sama untuk setiap interface sampai router dikonfigurasi atau jaringan di-disain ulang. Factor seperti load dan

reliability adalah dinamis karena mereka dihitung untuk setiap interface real-time oleh router.

Secara default, IGRP menggunakan faktor statis bandwidth dan delay untuk menghitung secara manual untuk mengontrol mana jalur yang akan dipilih. IGRP juga dikonfigurasi untuk faktor dinamis load dan reliability dalam perhitungan metric. Dengan menggunakan faktor default, router-router UGRP dapat membuat keputusan berdasar kondisi sekarang. Jika link menjadi berat bebannya atau unreliable, IGRP akan menaikkan metric.

IGRP menghitung metric dengan cara menambahkan nilai pembobot dari perbedaan karakteristik link. Berikut adalah perhitungan metric di IGRP:

$$\text{Metric} = [\text{K1} * \text{Bandwidth} + (\text{K2} * \text{Bandwidth}) / (256 - \text{load}) + \text{K3} * \text{Delay}] * [\text{K5}/(\text{reliability} + \text{K4})]$$

Nilai konstanta default $\text{K1} = \text{K3} = 1$ dan $\text{K2} = \text{K4} = \text{K5} = 0$

Jika $\text{K3} = 0$, maka $[\text{K5}/(\text{reliability} + \text{K4})]$ tidak digunakan. Misalkan diberikan nilai default ke K1 sampai K5, composite metric dihitung oleh IGRP untuk menurunkan Metric = Bandwidth + Delay.

1.7 Menentukan hop berikutnya

Algoritma routing mengisi table routing dengan informasi yang beragam. Hop tujuan berikutnya menentukan jalur terbaik dimana router mem-forward paket ke router berikutnya. Router ini merepresentasikan hop berikutnya ke tujuan terakhir.

Ketika router menerima paket yang datang, ia memeriksa alamat tujuan dan alamat hop berikutnya.

1.8 Menentukan update routing terakhir

Untuk mengetahui update routing terakhir dilakukan dengan cara memberikan perintah:

- show ip route
- show ip route address
- show ip protocols
- show ip rip database

1.9 Observasi beberapa jalur ke tujuan

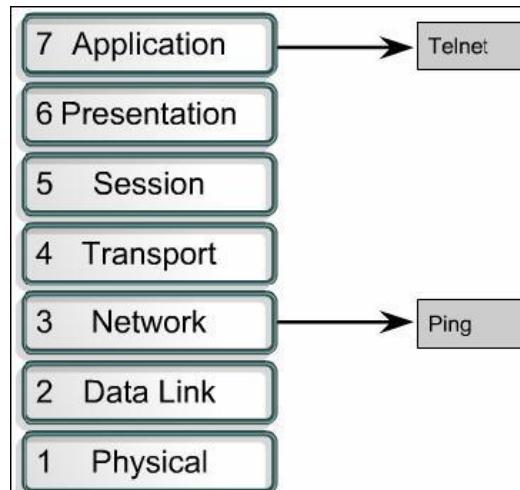
IGRP mendukung load balancing dengan cost tidak sama, yang disebut dengan variance. Perintah variance memerintahkan router supaya merutekan metric kurang dari n kali metric minimum untuk tujuan tersebut, dimana n adalah angka dari variance. Variabel n nilainya antara 1 sampai 128, dengan nilai default 1 yang artinya cost load balancing.

2. Testing jaringan

2.1 Pendahulan

Dasar testing jaringan harus diproses secara sequence dari OSI layer. Dimulai dari layer 1 sampai ke layer 7, jika perlu. Pada layer 1, kelihatannya seperti masalah sederhana

seperti power cord pada dinding dan koneksi fisik lainnya. Melakukan testing konfigurasi alamat sebelum meneruskan dengan langkah konfigurasi berikutnya.



Proses testing

Pada layer 3 test dilakukan dengan cara memberikan perintah **telnet** dan **ping** digunakan untuk test jaringan.

2.2 Langkah demi langkah proses troubleshooting

Troubleshooting adalah proses yang mengijinkan user untuk mencari masalah dalam jaringan. Langkah demi langkah adalah sebagai berikut:

Langkah 1 Mengumpulkan informasi yang ada dan menganalisa masalah. **Langkah 2** Melokalisasi masalah mulai dari jaringan, segmen, modul, unit atau user.

Langkah 3 Mengisolasi masalah ke hardware atau software dalam unit, modul atau user account jaringan.

Langkah 4 Menemukan dan memperbaiki masalah

Langkah 5 Mem-verifikasi masalah yang telah diselesaikan.

Langkah 6 Membuat dokumentasi terhadap solusi suatu masalah.

2.3 Testing dengan layer OSI

Sub bab ini menggambarkan tipe-tipe error yang terjadi pada tiga layer

OSI. Layer 1 error bisa berupa:

- Kabel putus
- Kabel tidak tersambung
- Kabel tersambung ke port yang salah
- Koneksi kabel yang tidak konsisten kadang koneksi kadang tidak
- Kesalahan dalam sambungan rollover, crossover, atau straight-through
- Masalah transceiver
- Kabel DCE bermasalah
- Kabel DTE bermasalah
- Device dalam posisi mati

Layer 2 error bisa berupa:

- Kesalahan konfigurasi interface serial
- Kesalahan konfigurasi interface Ethernet

- Kesalahan setting enkapsulasi
- Kesalahan setting clockrate pada interface serial
- Masalah pada network interface card (NIC)

Layer 3 error bisa berupa:

- Routing protokol tidak enable
- Kesalahan meng-enable-kan routing protokol
- Kesalahan alamat IP
- Kesalahan subnet mask

Jika error terlihat di jaringan, proses testing melalui layer OSI dimulai. Perintah **ping** digunakan di layer 3 untuk test koneksi. Pada layer 7 dengan perintah **telnet** untuk verifikasi aplikasi.

2.4 Troubleshooting di layer 1

Dengan cara memberikan perintah **show interfaces** tanpa argumen akan menghasilkan status dan statistik semua port router. Sedangkan **show interfaces <interface name>** menghasilkan status dan statistik pada port tertentu saja. Untuk melihat status dari serial 0/0 dengan perintah: **show interfaces serial 0/0**.

Jika banyak terjadi error di carrier transition, masalah-masalahnya bisa berasal dari:

- Pada service provider terjadi interupsi jalur
- Terjadi kerusakan pada switch, DSU atau hardware router

Jika terjadi banyak error pada output perintah show interfaces serial 0/0, ada beberapa kemungkinan sumber errornya, antara lain:

- Kesalahan pada peralatan perusahaan telepon
- Noise pada jalur serial
- Kabel salah atau panjang kabel salah
- Kabel atau koneksi rusak
- CSU atau DSU rusak
- Hardware router rusak

Sedangkan error terjadi karena reset interface penyebabnya bisa berasal dari:

- Jalur jelek sehingga menyebabkan carrier transition
- Kemungkinan masalah di hardware pada DSU, CSU atau switch

2.5 Troubleshooting di layer 2

Jika jalur putus, protokol selalu down karena tidak ada media yang digunakan di protokol layer 2. Hal ini benar karena interface down dan secara administrative down.

Jika interface up dan line protokol down, layer 2 terdapat masalah sebagai berikut:

- Tidak ada keepalive
- Tidak ada clock rate
- Tipe enkapsulasi tidak cocok

Perintah **show interfaces** digunakan setelah mengkonfigurasi interface untuk mem-verifikasi perubahan.

2.6 Perintah show cdp neighbors

Perintah ini menampilkan spesifik device secara detail seperti interface yang aktif, port ID dan device.

2.7 Perintah traceroute

Perintah ini memberikan hop yang berhasil dilewati. Jika data berhasil dilalui, kemudian output menunjukkan setiap router bahwa datagram berhasil dilewati.

2.8 Perintah-perintah lain untuk troubleshooting

- Perintah show ip route
- Perintah show controllers
- Perintah debug

CHAPTER 10

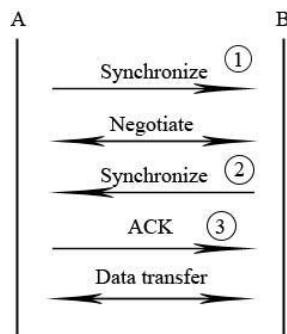
Intermediate TCP/IP

Fungsi dari transport layer :

- Meregulasikan aliran informasi secara akurat dan terpercaya dengan sliding window, sequence number, dan ACK.
- Menjamin Reliability dan melakukan flow control.

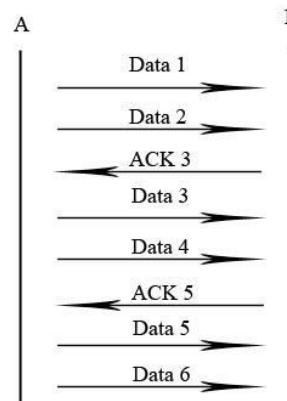
TCP / IP merupakan gabungan dari dua layer yaitu TCP pada layer 4 dan IP pada layer 3.

TCP membentuk virtual circuit, sifatnya connection oriented dan membentuk koneksi dengan three way handshake :



Flow control digunakan untuk mengatur jumlah data yang dikirim pada suatu waktu, ditentukan oleh window size.

Contoh window size 2 yang sudah membentuk sliding window :

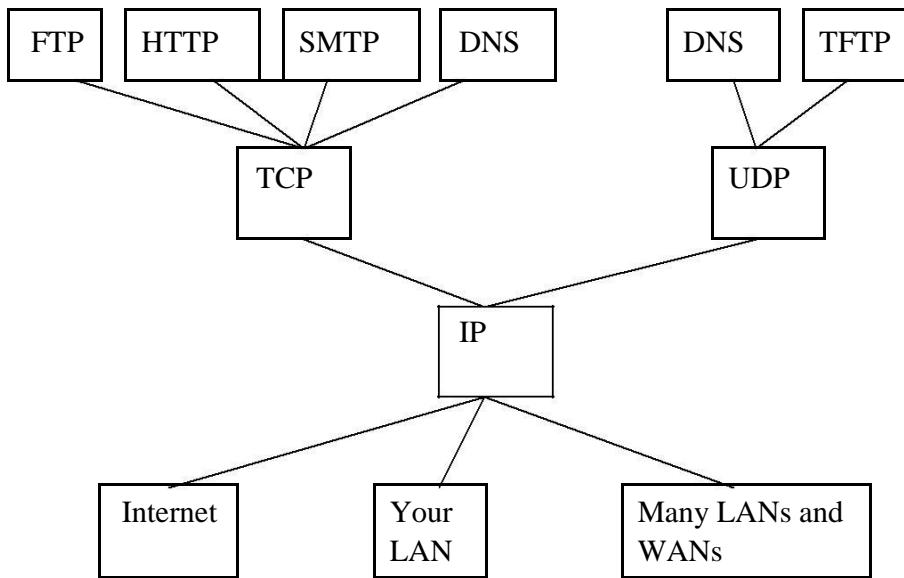


Sequence number digunakan untuk mengurutkan data agar sampai pada tujuan sesuai urutannya.

Bila pada selang waktu tertentu ACK tidak diterima oleh host sumber dari host tujuan, maka akan dilakukan *retransmission* atau pengiriman kembali ke tujuan.

Transport layer berkomunikasi dengan application layer dengan menggunakan port number.

Port dibawah 1024 disebut juga *well-known* port number.



Protocol-protocol yang memakai TCP :

- **HTTP :**
Bekerja sama dengan www digunakan untuk merequest halaman web dari web server untuk ditampilkan pada browser client.
Halaman web dapat dibuat dengan Hypertext Markup Language (HTML) yang merupakan web static ataupun dengan web dinamis seperti PHP, ASP, atau JSP
- > port 80.
- **FTP :**
Digunakan untuk melakukan transfer file dari server FTP ke client FTP (port 20 dan 21).
- **SMTP :**
Digunakan untuk email server (port 25).
- **TelNet :**
Digunakan untuk remote ke komputer lain (port 32).

User Datagram Protocol (UDP)

UDP yaitu protocol yang sifatnya connectionless, tidak membentuk koneksi atau virtual circuit, pengiriman langsung dilakukan tanpa memperdulikan data sampai pada tujuan atau tidak.

Protocol yang memakai UDP :

- **SNMP :**
Untuk manajemen network (port 161).
- **TFTP :**
Backup IOS dan configuration file pada router dan switch Cisco (port 69).

- **DHCP : (Membagi IP address)**

Membagi IP secara dinamik (port 67 dan 68).

DNS memakai TCP dan UDP sekaligus, untuk menterjemahkan nama ke IP dan sebaliknya (port 53).

Chapter 11

Access Control List

Pengenalan wildcard

Pada dasarnya, wildcard adalah kebalikan (inverse) dari subnet mask, dapat digunakan pada Access Control List (ACL) statement dan routing protocol OSPF.

Wildcard default dibagi berdasarkan class yaitu :

- a) Class A : wildcardnya 0.255.255.255
- b) Class B : wildcardnya 0.0.255.255
- c) Class C : wildcardnya 0.0.0.255

Angka-angka yang muncul pada wildcard biasanya adalah 0, 1, 3, 7, 15, 31, 63, 127, dan 255.

Secara mudah, cara untuk menentukan wildcard sebuah network yaitu dari jumlah host dikurangi satu.

Contohnya :

- A) Network 192.168.10.32/27 -> wildcard : 0.0.0.31
- B) Network 200.10.10.0/24 -> wildcard : 0.0.0.255
- C) Network 197.17.13.48/28 -> wildcard : 0.0.0.15

Wildcard digunakan pula untuk mewakili sekelompok alamat host tertentu yang dinyatakan dengan angka pada wildcard itu.

Contoh perhitungan wildcard :

1. Buatlah range wildcard alamat 192.168.10.0 – 192.168.10.20

! Jawab :

0 -> 0000 0000
20 -> 0001 0100

Tujuannnya :

Buat agar binary 0 match dengan binary 20 melalui pergerakan biner.

| | | | | |
|-------|-------|------|---------|----------|
| 0000 | | 0000 | .0 | |
| 0000 | | 1111 | | 0.0.0.15 |
| <hr/> | | | | |
| 0001 | 00 00 | .16 | | |
| 0001 | 00 11 | | 0.0.0.3 | |
| <hr/> | | | | |
| 0001 | 0100 | .20 | 0.0.0.0 | |

192.168.10.0 0.0.0.15
192.168.10.16 0.0.0.3
192.168.10.20 0.0.0.0

2. Buat range wildcard dari 192.168.10.3 – 192.168.10.51

! Jawab :

3 -> 0000 0011

51 -> 0011 0011

Tujuan :

Buat agar binary 3 match dengan binary 51 melalui pergerakan biner.

| | | | |
|---------------|-------|----------|----------|
| 0000 | 0011 | .3 | 0.0.0.0 |
| 0000 | 01 00 | .4 | |
| 0000 | 01 11 | | 0.0.0.3 |
| 0000 | 1 000 | .8 | |
| 0000 | 1 111 | | 0.0.0.7 |
| 0001 | 0000 | .16 | |
| 0001 | 1111 | | 0.0.0.15 |
| 0010 | 0000 | .32 | |
| 0010 | 1111 | | 0.0.0.15 |
| 0011 | 00 00 | .48 | |
| 0011 | 00 11 | | 0.0.0.3 |
| 192.168.10.3 | | 0.0.0.0 | |
| 192.168.10.4 | | 0.0.0.3 | |
| 192.168.10.16 | | 0.0.0.7 | |
| 192.168.10.16 | | 0.0.0.15 | |
| 192.168.10.32 | | 0.0.0.15 | |
| 192.168.10.48 | | 0.0.0.3 | |

Access Control list

Access control list digunakan untuk mengatur lalu lintas jaringan dan security sebab dapat digunakan untuk memblok lalu lintas traffic yang tidak perlu.

Aturan-aturan dalam ACL :

- a) Menggunakan wildcard.
- b) Penulisan ACL sebaiknya dilakukan pada text editor, misalnya notepad, barulah dicopy ke Hyper Terminal.
- c) Standard ACL diletakkan dekat destination.
- d) Extended ACL diletakkan dekat source.
- e) Setelah dibuat pada global config, ACL harus diterapkan pada interface router.
- f) Perhatikan arah inbound atau outbound dalam meletakkan ACL pada interface.
- g) Berlaku implicit deny (deny only) pada akhir ACL statement.

ACL terbagi dua jenis :

A) Standard ACL :

Diletakkan dekat dengan destination, nomor yang dipakai biasanya 1-99, tidak dapat memilih port atau traffic yang diatur, semua kena.

Commandnya :

```
Router(config)#access-list numberacl permit|deny sourcenetwork  
wildcardsourcenetwork
```

Terapkan pada interface :

```
Router(config)#interface interface number
```

```
Router(config-if)#ip access-group numberacl in|out
```

Pada akhir setiap ACL statement, letakkan command :

```
Router(config)#access-list numberacl permit any
```

Perhatikan :

- Host dengan wildcard 0.0.0.0 dapat digantikan dengan kata-kata “host”,

Contoh :

IP tunggal

192.168.10.1 0.0.0.0

Dapat ditulis juga :

Host 192.168.10.1

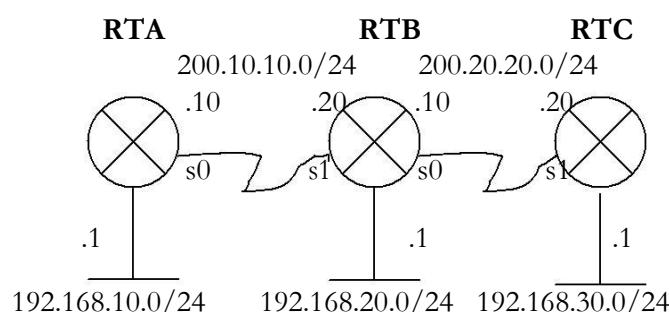
- Seluruh network dengan pernyataan :

0.0.0.0 255.255.255.255

Dapat digantikan dengan kata :

any

Contoh topologi :



a) Bloklah traffic dari RTA ke RTC !

```
RTB(config)#access-list 1 deny host 200.10.10.10
```

```
RTB(config)#access-list 1 deny 192.168.10.1
```

```
0.0.0.0 RTB(config)#access-list 1 permit any
```

```
RTB(config)#interface s0/0
```

```
RTB(config-if)#ip access-group 1 out
```

- b) Blok semua traffic ke LAN RTB kecuali default gateway RTB !

```
RTB(config)#access-list 2 deny any
RTB(config)#interface fa0/0
RTB(config-if)#ip access-group 2 out
```

NB: Access list tidak berlaku di interface dimana ia diterapkan.

B) Extended ACL :

Diletakkan dekat dengan source, nomor yang dipakai biasanya 100-199, dapat memilih protocol ataupun port yang diatur.

Commandnya :

```
Router(config)#access-list numberacl permit | deny protocol sourcenetwork
wildcard sourcenetwork destinationnetwork wilcarddestinationnetwork eq | lt |
gt | neq servicename/serviceport
```

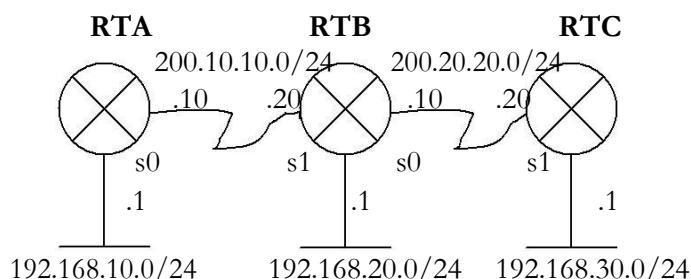
Terapkan pada interface :

```
Router(config)#interface interface number
Router(config-if)#ip access-group numberacl in | out
```

Pada akhir ACL statement, pasang command :

```
Router(config)#access-list numberacl permit ip any any
```

Contoh :



- a) Bloklah agar LAN pada RTA (network 192.168.10.0/24) tidak dapat telnet ke RTC, kecuali LAN RTA yang memiliki ip host 192.168.10.20 !

```
RTA(config)#access-list 100 permit tcp host 192.168.10.20 host 200.20.20.20 eq
23 RTA(config)#access-list 100 permit tcp host 192.168.10.20 host 192.168.30.1
eq 23 RTA(config)#access-list 100 deny tcp 192.168.10.0 0.0.255 host
200.20.20.20 eq23 RTA(config)#access-list 100 deny tcp 192.168.10.0 0.0.255 host
192.168.30.0 eq 23 RTA(config)#access-list 100 permit ip any any
RTA(config)#interface s0/0 RTA(config-
if)#ip access-group 100 out
```

- b) Bloklah agar RTB tidak dapat di ping oleh LAN RTC (network 192.168.30.0) !

```
RTC(config)#access-list 101 deny icmp 192.168.30.0 0.0.0.255 host  
200.10.10.20 RTC(config)#access-list 101 deny icmp 192.168.30.0 0.0.0.255  
host 200.20.20.10 RTC(config)#access-list 101 permit ip any any  
RTC(config)#interface s0/1 RTC(config-  
if)#ip access-group 101 out
```

- c) Bloklah agar RTA tidak dapat di-http oleh LAN RTB (network 192.168.20.0) !

```
RTB(config)#access-list 102 deny tcp 192.168.20.0 0.0.0.255 host 200.10.10.10 eq  
80 RTB(config)#access-list 102 deny tcp 192.168.20.0 0.0.0.255 host 192.168.10.1  
eq 80 RTB(config)#access-list 102 permit ip any any  
RTB(config)#interface s0/1 RTB(config-  
if)#ip access-group 102 out
```

Command-command show :

- a) Melihat statement ACL :

```
Router(config)#show access-list
```

- b) Melihat arah inbound atau outbound ACL :

```
Router(config)#show ip interface
```

- c) Melihat ACL di running-config :

```
Router(config)#show run
```

Standard dari exteded ACL yang telah kita pelajari merupakan numbered ACL, ada pula named ACL yang terdiri dari standard dan extended ACL

Contoh :

- a) Named Standard ACL

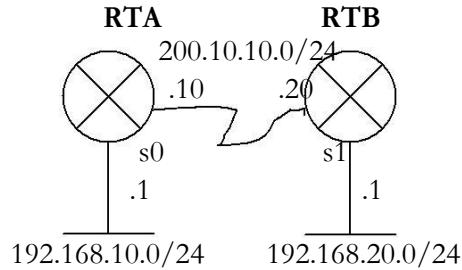
```
Router(config)# ip access-list standard namedacl Router(config-std-  
nacl)# permit | deny sourcenetw wildcardsourcenetw  
Router(config)#interface interface numberint  
Router(config)#ip access-group namedacl in|out
```

- b) Named Extended ACL

```
Router(config)# ip access-list extended namedacl  
Router(config-ext-nacl)# permit | deny protocol sourcenetw  
wildcardsourcenetw destinationnetw wildcarddestinationnetw eq | lt | gt | neq  
protocol/port Router(config)#ip access-group nameacl in|out
```

Selain access-list, juga terdapat access-class yang diterapkan pada line vty atau telnet line.

Contoh :



Buatlah agar RTA hanya dapat ditelnet oleh LAN nya sendiri yaitu 192.168.10.0/24 !

```
RTA(config)#access-list 1 permit 192.168.10.0  
0.0.0.255 RTA(config)#line vty 0 4 RTA(config-  
line)#access-class 1 in
```

Maka RTA hanya dapat ditelnet oleh LAN nya sendiri saja yaitu 192.168.10.0/24

CCNA 3

| | |
|--|-----------|
| Daftar Isi | 1 |
| Chapter 1 Introduction to Classless Routing | 2 |
| Chapter 2 Single Area OSPF | 6 |
| Chapter 3 EIGRP | 11 |
| Chapter 4 Switching Concepts | 15 |
| Chapter 5 Switches | 18 |
| Chapter 6 Switch Configuration | 20 |
| Chapter 7 Spanning-Tree Protocol | 23 |
| Chapter 8 Virtual LAN | 25 |
| Chapter 9 VLAN Trunking Protocol | 28 |

CHAPTER 1

Introduction to Classless Routing

Perbedaan classfull & classless

Classfull : Subnet mask yang digunakan adalah sama, misalkan default ataupun subnetting.

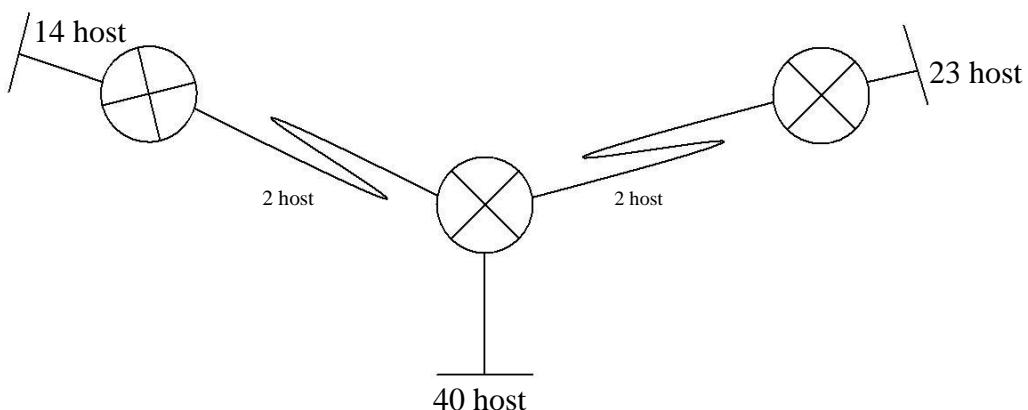
Classless : Subnet mask berbeda-beda, disesuaikan dengan kebutuhan, misalnya dilakukan VLSM.

VLSM (Variable Length Subnet Mask)

VLSM digunakan guna penghematan pembagian alamat ip agar tidak boros dalam pemakaian.

Biasanya dibagi mulai dari network yang jumlah hostnya paling banyak.

Contoh :

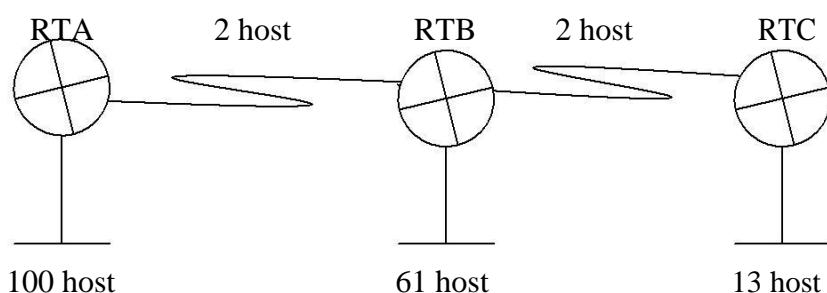


Bila diberikan ip 192.168.10.0/24, maka pembagian VLSM adalah sebagai berikut :

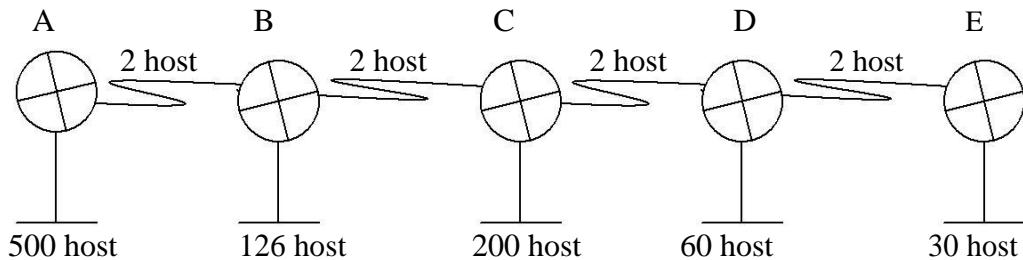
| | | |
|-------------------|----|---------|
| 192.168.10.0/26 | -> | 40 host |
| 192.168.10.64/27 | -> | 23 host |
| 192.168.10.96/28 | -> | 14 host |
| 192.168.10.112/30 | -> | 2 host |

Latihan :

1) 172.16.0.0/16



2) 10.0.0.0/8



Jawab :

- 1) 172.16.0.0/25 > 100 host
172.16.0.128/26 > 61 host
172.16.0.192/28 > 13 host
172.16.0.208/30 > 2 host
172.16.0.212/30 > 2 host

- 2) 10.0.0.0/23 > 500 host
10.0.2.0/24 > 200 host
10.0.3.0/25 > 126 host
10.0.3.128/26 > 60 host
10.0.3.192/27 > 30 host
10.0.3.224/30 > 2 host
10.0.3.228/30 > 2 host
10.0.3.232/30 > 2 host
10.0.3.236/30 > 2 host

Classless didukung oleh routing protocol :

- a) RIP v.2
- b) OSPF
- c) EIGRP

Pada VLSM maupun subnetting, terdapat istilah ip subnet zero yang aktif secara default pada router, untuk memastikannya :

Router(config)#no ip subnet-zero

Setelah dimatikan, maka tidak bisa menulis alamat ip dari subnet-zero (subnet pertama). Menghidupkan kembali dengan :

Router(config)#ip subnet-zero

Penggunaan VLSM dapat menghemat ip, contoh :

WAN link pada serial dapat ditulis /30 sebab hanya perlu 2 host untuk point-to-point, tidak mubazir seperti /24.

Routing Information Protocol Version 2

RIP v.2 mendukung classless routing, pada dasarnya sifatnya mirip dengan RIP v.1 yaitu hop count sebagai metric, maximal hop count yaitu 15 Administrative Distance 20.

Perbedaannya :

| RIP v.1 | RIP v.2 |
|--|----------------------------------|
| - Subnetting | - Subnetting & VLSM |
| - Tidak mengirim informasi subnet mask | - Mengirim informasi subnet mask |
| - Broadcast 255.255.255.255 | - Multicast 224.0.0.9 |
| - No authentication | - Support Authentication |
| - Classfull | - Classless |

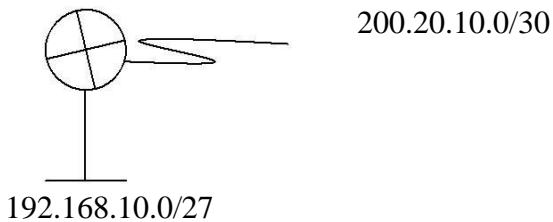
Settingan :

Router(config)#router rip

Router(config-router)#version 2

Router(config-router)#network network directly connected

Contoh :



Router(config)#router rip

Router(config-router)#version 2

Router(config-router)#network 192.168.10.0

Router(config-router)#network 200.10.10.0

Command show :

a) **Melihat routing table :**

Router#show ip route

b) **Melihat routing protocol, AD, routing update :**

Router#show ip protocol

Command debug :

a) debug ip rip

b) debug ip rip events

c) debug ip rip database

Authentication

Router(config)#key chain name

Router(config-keychain)#key key number

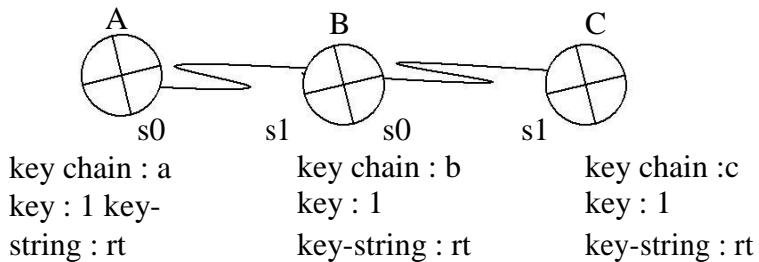
Router(config-keychain-key)#key-string keyword

```
Router(config-if)#ip rip authentication key-chain name
Router(config-if)#ip rip authentication authentication mode mode
```

NB : Mode dapat berubah : a) Text : tanpa enkripsi b)
Md5 : dengan enkripsi

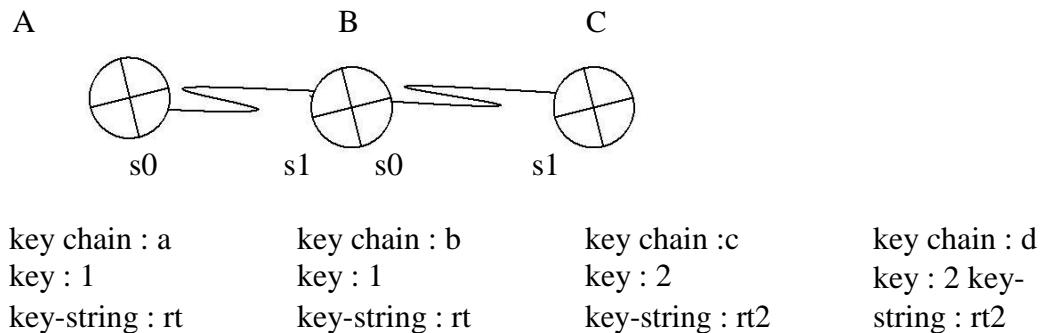
Dalam authentication, antara serial yang berpasangan harus sama key, key-string, & mode-nya.

Contoh :



Untuk nama key chain boleh berbeda.

Bisa juga disusun demikian :



Jadi pada router B diperlukan 2 key chain.

CHAPTER 2

Single Area OSPF

Routing yang umum digunakan adalah RIP, OSPF dan BGP. RIP dan OSPF dikategorikan sebagai interior gateway routing protocol (IGP) sedangkan BGP atau border gateway routing protocol termasuk kategori external routing protocol.

IGP menangani routing jaringan internal pada sebuah AS sedangkan EGP antar AS.

Single area berarti hanya mempunyai area backbone, multi area berarti mempunyai area backbone dan area lain yang terhubung dengannya

Perbandingan Link State & Distance Vector

Distance Vector

- Update frequently
- Routing loop
- Hanya tahu routing tetangga
- Mudah disetting
- Slow convergence

Link State

- trigered update
- tidak rentan routing loop
- tahu seluruh jaringan
- lebih sulit disetting
- Fast convergence

OSPF

Protocol ini termasuk dalam link -state protocol, kelebihan utama dari protocol ini adalah dapat dengan cepat mendeteksi perubahan dan mejadikan routing kembali konvergen dalam waktu singkat dengan sedikit pertukaran data.

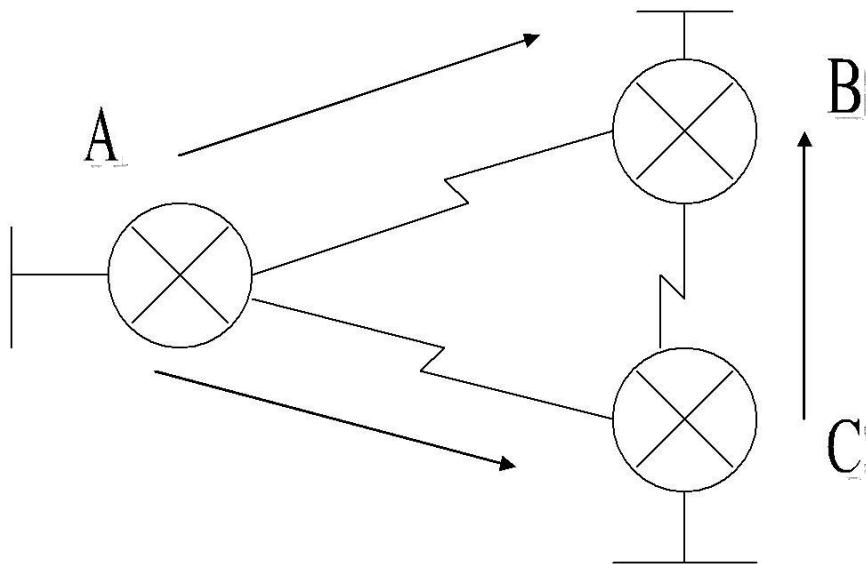
Routing ini membentuk peta jaringan dalam tiga tahap, tahap pertama setiap router mengenali seluruh tetangganya, lalu router saling bertukar informasi dan router akan menghitung jarak terpendek ke setiap tujuan. Peta jaringanya akan disimpan dalam basis data sebagai hasil dari pertukaran informasi antar router.

OSPF dapat menangani routing jaringan TCP/IP yang besar dan membuat hirarki routing dengan membagi jaringan menjadi beberapa area. Setiap paket yang dikirim dapat dibungkus dengan authentikasi, namun protocol ini membutuhkan kemampuan CPU dan memori yang besar.

Proses dasar routing OSPF adalah menghidupkan adjacency, proses flooding, dan perhitungan table routing. Router-router mengirimkan paket hello ke seluruh jaringan yang terhubung secara periodic, jika paket tidak terdengar maka jaringan dianggap down, defaultnya mengirimkan 4 kali paket hello.

Router-router selalu berusaha adjacent dengan router tetangganya berdasarkan paket hello yang diterima. Dalam jaringan multi access, router memilih Designated Router

(DR) dan Backup Designated Router (BDR) dan mencoba adjacent dengan kedua router tersebut.



Ket :

Misalkan jaringan baru terkoneksi, maka router A akan membroadcast paket hello ke semua int dengan memberikan informasi tentang router A, dan begitu juga sebaliknya A akan mengetahui informasi tentang tetangganya berdasarkan informasi yang diterima dan mengetahui berapa biaya untuk mencapai router lain. Data-data ini disimpan dalam basis data. Setelah itu setiap router mengirimkan basis data tersebut dalam satu paket LSA (link state advertisement), dan router yang menerima LSA harus mengirimkan ke semua router yang terhubung dengannya.

Karena router B telah menerima paket LSA dari router A maka jika LSA yang dikirimkan C sama dengan yang ada pada basis data B atau bukan yang baru, maka paket LSA dari C akan di drop. Antara router satu dengan yang lain akan mengirmkan paket hello dengan interval tertentu misalnya 120 detik , jika tidak terdapat hello paket dari jaringan yang terkoneksi dengannya atau tidak mendapat balasan maka jaringan tersebut dianggap down. Maka jika terjadi network down maka paket LSA akan disebarluaskan ke semua jaringan dengan menggunakan floating dan akan menyebabkan basis data LSA berubah untuk mencari jalan yang terbaik dalam paket data.

Command-command konfigurasi OSPF

Router(config)#router ospf process id

Router(config-router)#network network id wildcard mask area area number

Mengubah hello&dead message

Router(config-if)#ip ospf hello-interval time

Router(config-if)#ip ospf dead-interval time

Mengubah bandwidth

Router(config-if)#bandwidth bandwidth[1-10.000.000] -> kbps

Mengubah cost

Router(config-if)#ip ospf cost cost [1-65535]

Command-command Show

Melihat routing table

Router#show ip route

Melihat process ID,LSA authentication

Router# show ip ospf

Melihat cost,hello,dead interval,state, process ID

Router#show ip ospf interface interface

Melihat router tetangga secara OSPF

Router#show ip ospf neighbor

Melihat protocol

Router#show ip protocol

Command-command debug

Router#debug ip ospf events

Router#debug ip ospf adjacency

OSPF Authentication

Dengan MD5

Router(config-if)#ip ospf message-digest-key 1 md5 7 password

Router(config-if)#exit

Router(config)#router ospf process id Router(config-

router)#area 0 authentication message-digest

Router(config-router)#end

Dengan plain text

Router(config-if)#ip ospf authentication-key password

Router(config)#router ospf process id

Router(config-router)#area 0 authentication

Settingan untuk menyebarkan Loopback: (ip 180.10.10.1)

```
Router(config)#interface loopback 0  
Router(config-if)#ip address 180.10.10.1 255.255.0.0  
Router(config)#ip route 0.0.0.0 0.0.0.0 lo 0  
Router(config)#router ospf 10  
Router(config-router)#default-information originate
```

Pemilihan DR & BDR

OSPF sifatnya fast convergence, pada broadcast&non broadcast multi access, terdapat pemilihan DR(designed Router) & BDR(Backup designated router) ini tidak berlaku bagi point to point link, misal serial to serial.

DR digunakan sebagai pusat penyebaran informasi bagi router-router lain., alamat multicast 224.0.0.5

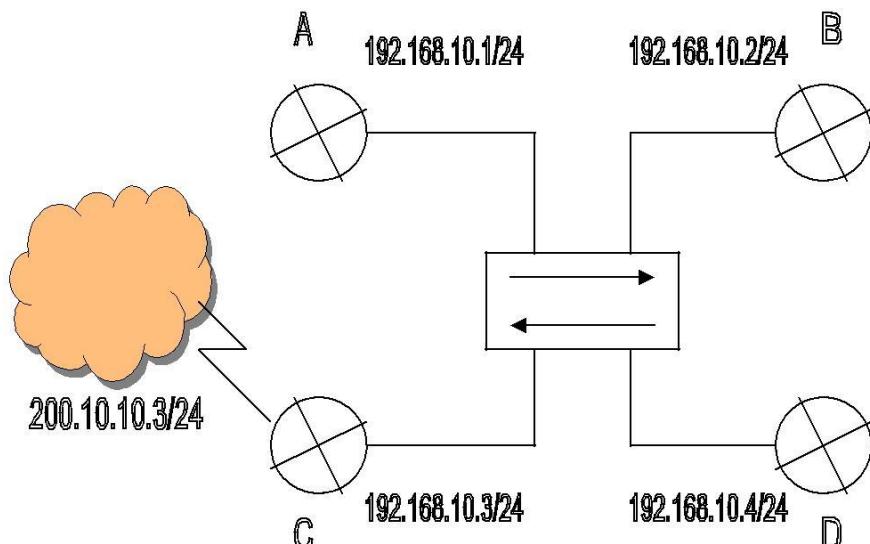
Sedangkan BDR memiliki alamat 224.0.0.6 , BDR akan menjadi DR apabila DR down, Router-router lain yang bukan DR atau BDR akan bertindak sebagai DROTHER

Penentuan DR,BDR dan DROTHER ditentukan oleh:

- **Router ID**

Yang merupakan IP tertinggi pada interface router. IP tertinggi akan menjadi DR, router id ke dua tertinggi menjadi BDR dan sisanya DROTHER

- Pemberian **Loopback address** akan membuat router tsb mempunyai router id dari alamat loopback itu.

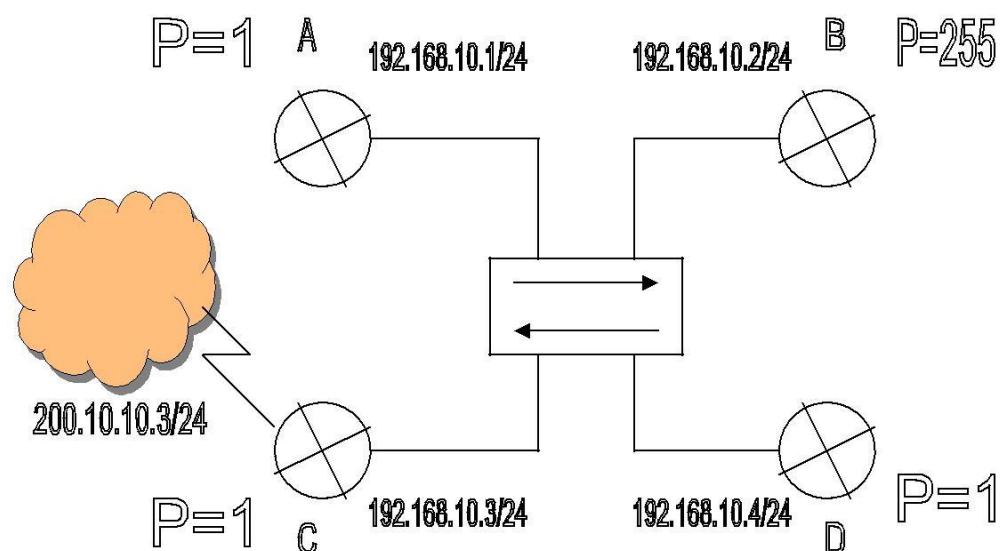


Ket: Router C skrng menjadi DR sebab router id nya menjadi 200.10.10.3/24 Router D menjadi BDR sebab memiliki router id 192.168.10.4, router A & B menjadi DROTHER

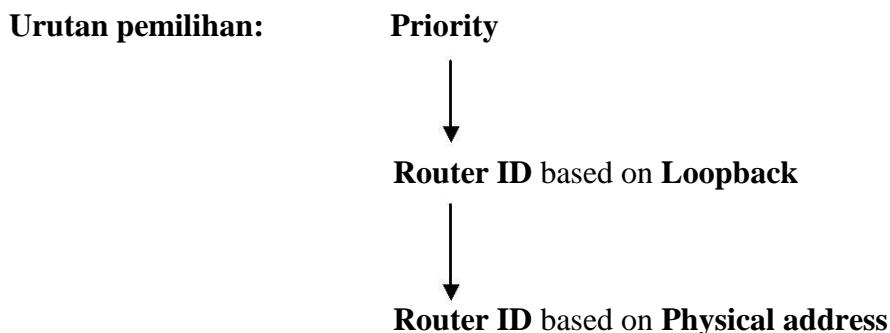
- **Router Priority**

Default nilai router priority untuk semua router adalah 1, semakin tinggi nilai priority maka semakin besar kemungkinan untuk menjadi DR

- Apabila priority router sama maka yang digunakan untuk menentukan DR/BDR adalah **Router ID**



Ket: Router B akan menjadi DR sebab prioritas nya tertinggi yaitu 255, meski router id nya 192.160.10.2. Router C akan menjadi BDR sebab memiliki Router id tertinggi dari Loopback yaitu 200.10.10.3 dalam keadaan nilai priority yang sama dngan A & D, router A & D akan menjadi DROTHER



CHAPTER 3

EIGRP

EIGRP mirip dengan IGRP sebagai Cisco Proprietary routing protocol, tetapi lebih fast convergence & dapat menangani scalability network.

- gabungan dari distance vektor & link state (tidak mengenal hop count)

Metric yang digunakan sama dengan IGRP namun dikali 256 sebab memakai metric 32 bit, sedangkan IGRP 24 bit.

Metric = BW + delay

BW $(10^7 / \text{BW}) \times 256$

Delay $(\text{delay} / 10) \times 256$

Komposisi metric seperti ini dinamakan composite metric. (path bandwidth value dan cumulative delay)

Perbandingan EIGRP dan IGRP terletak pada:

- a. compatibility mode
- b. hop count
- c. route tagging
- d. automatic protocol distribution

Route tagging

Penandaan route external yang dapat dilakukan EIGRP tapi tidak oleh IGRP.

Sama seperti IGRP, EIGRP juga memakai Autonomous System (AS) yang harus sama.

Table pada EIGRP:

- a. topology table
- b. neighbor table
- c. routing table

Info pada topology & neighbor digunakan untuk menentukan jarak ke tujuan.

Proses convergence

Router-router EIGRP membentuk adjacency dengan router tetangga melalui hello & dead message, dilakukan multicast 224.0.0.10, router lain membalas dengan ACK secara unicast.

Bila tidak membalas maka route dinyatakan down, info ini disimpan pada neighbor & topology table.

Diffusing Update Algoirthm (DUAL)

DUAL digunakan untuk menghitung jalur ke tujuan, istilah yang penting:

- feasible distance (fd)
- reported distance (rd)
- feasible successor (fs)
- successor (s)

Feasible distance jarak ke tujuan yang dilihat dari sisi diri sendiri.

Reported distance jarak ke tujuan yang dilihat dari sisi tetangga.

Pemilihan successor & feasible dilakukan berdasarkan feasible & reported distance.

Pententuan successor yaitu berdasarkan jalur yang feasible distancenya paling kecil ke tujuan.

Diffuse Update Algorithm (DUAL) pada EIGRP memiliki successor dan feasible successor ke network tujuan berdasarkan reported distance dan feasible distance.

Pada saat DUAL bekerja, status router EIGRP dalam keadaan aktif, bila route telah convergence, barulah berubah menjadi pasif kembali.

Proses lengkap pemilihan atau sampai convergence pada EIGRP:

- a. hello message dikirim dengan 224.0.0.10
- b. neighbor dan topology table didapatkan
- c. info pada topology table (feasible dan reported distance) didapat lalu digunakan untuk menghitung successor dan feasible successor.
- d. Perhitungan dilakukan oleh DUAL
- e. Convergence didapatkan

Info yang terdapat pada topology table:

- a. feasible distance
- b. reported distance
- c. route status
- d. interface information
- e. copyan dari successor

Successor yang asli disimpan dalam routing table yang menjadi metric terbaik ke destination network.

Info yang terdapat pada neighbor table:

- a. neighbor address
- b. hold time (berapa kali dikirim tidak menerima ACK)
- c. SRTT (Smooth Rand Trip Time): waktu untuk hello packet bolak balik send dan ACK
- d. sequence number
- e. queue count

Karakteristik EIGRP:

- a. Efisien dalam bandwidth
- b. Mendukung VLSM dan subnetting
- c. Independent dalam routed protocol

Independent reouted protocol berarti protocol Dependent Module (PDM), routed protocol yang digunakan tidak hanya IP, tapi dapat juga IPX, dll.

EIGRP technologies:

- a. Network discovery dan recovery
- b. DUAL
- c. Protocol Dependent Module (PDM)
- d. Reliability Transport Protocol (RTP)

EIGRP juga memiliki packet-packet sebagai berikut:

- a. hello saat membentuk koneksi awal 224.0.0.10
- b. ACK balasan dari hello packet
- c. update untuk update
- d. reply balasan query packet
- e. query bila ada perubahan topology, query packet dikirim

EIGRP adalah hybrid routing protocol, yang memiliki sisi:

- a. Distance Vector: maksimal top count 224 berbeda dengan IGRP yang maksimal top count 255
- b. Link State: mengirim hello message dan punya topology table yang menggambarkan keseluruhan network.

Administrative Distance (AD) nya:

- a. internal EIGRP: semua menjalankan EIGRP, ADnya 90
- b. eksternal EIGRP: ada router yang tidak memakai IGRP, dikenali dengan route tagging, nilai AD route ini 170

Command-command EIGRP

a. Setting routing protocol:

```
Router(config)# router eigrp AS number Router(config-
router)# network network directly connected
Router(config-router)# no auto-summary Router(config-
router)# eigrp log-neighbor-changes
```

b. Command show:

- Melihat routing table
Routing# show ip route
- Melihat routing protocol spesifik
Routing# show ip protocol
- Melihat neighbor eigrp:
Routing# show ip eigrp neighbor
- Melihat topology eigrp:
Routing# show eigrp topology

c. Command debug:

```
Router# debug eigrp fsm melihat aktivitas FUAL
Router# eigrp packet
```

Manual summary pada EIGRP

Secara default EIGRP menjalakan auto summary, ini tidak baik bagi discontiguous network network yang disubnetting atau di VLSM tapi dipisahkan oleh network lain.

CHAPTER 4

Switching Concepts

Switching adalah proses meneruskan frame ke tujuan berdasarkan destination MAC address, ini yang dilakukan oleh Switch.

Switch adalah device layer 2, memisahkan collision domain, tapi tidak memisahkan broadcast domain.

Local Area Network itu sendiri terdiri dari 3 layer pada OSI model:

1. **Layer 1** : repeater dan hub (tidak memisahkan collision domain, dan tidak memisahkan broadcast domain)
2. **Layer 2** : switch dan bridge (memisahkan collision domain, dan tidak memisahkan broadcast domain)
3. **Layer 3** : router (tidak memisahkan collision domain, dan memisahkan broadcast domain)

Memisahkan collision domain artinya melakukan microsegmentasi yang memberikan keuntungan yaitu dapat mengisolasi traffic dan meningkatkan bandwidth pada tiap host yang terhubung di port masing-masing switch.

Selain collision domain, faktor lain yang mempengaruhi perform network

- yaitu:**
- a.) multitasking :environment pada jaringan
 - b.) pemakaian aplikasi seperti browser yang melibatkan jaringan
 - c.) pengaturan client-server pada jaringan

Bentuk jaringan LAN yang umum yaitu ethernet, tujuan dan fungsi utamanya

- : a.) best effort delivery ke tujuan
- b.) memastikan semua host jaringan dapat berbagi media yang sama

Ethernet mempunyai standard IEEE 802.3 yang memiliki kelemahan:

- shared media
- bila tidak dibantu device layer 2, tidak memisahkan collision domain

CSMA/ CD digunakan oleh ethernet untuk mengatasi collision pada collision domain yang sama, tapi sifatnya mendeteksi setelah collision domain terjadi pertama kalinya, bukan mencegahnya.

Faktor-faktor lainnya yaitu:

- penggunaan bandwidth yang besar untuk multimedia, graphic, file, dll
- latency pada jaringan

Latency atau delay adalah waktu yang diperlukan oleh frame dari source menuju destination, contohnya:

- a.) **NIC delay** : berapa lama waktu sampai titik menerjemahkan data menjadi layer-layer data untuk dikirim oleh layer 1
- b.) **Propagation delay** : waktu yang diperlukan dikur dari delay media misal UTP, dll
- c.) **Network device delay** : delay yang dihasilkan network device

Perbandingan ketiga layer:

1.) Layer 1 :

Hub maupun repeater tidak melakukan microsegmentation berdasarkan apapun

2.) Layer 2 :

Switch maupun bridge melakukan microsegmentation berdasarkan MAC address, dalam mengirim data ke tujuan

3.) Layer 3 :

Router mengirim data berdasarkan destination ip address, malekukan pemisahan broadcast dan collision domain

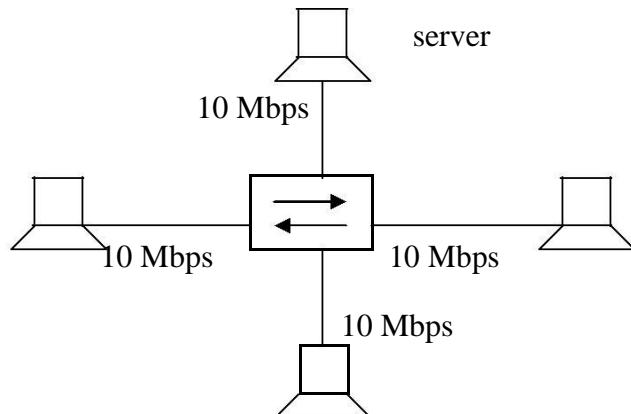
Switch terdiri dari dua jenis berdasarkan kesamaan bandwidth port-portnya:

a.) symetric switching

Switch yang semua portnya memiliki besar bandwidth yang sama misalnya bila 10 Mbps, maka semua port 10 Mbps

b.) asymmetric switching

Switch yang port-portnya tidak memiliki bandwidth yang sama besar, ada beberapa port yang uplink atau lebih besar bandwidthnya, biasanya digunakan oleh koneksi ke server



Berdasarkan sistem antrian data frame ke tujuan, switch juga dibedakan menjadi dua:

a.) port-based memory buffer

Pada saat melakukan antrian di dalam switch, maka frame dimasukkan dalam incoming port yang spesifik barulah diforward ke tujuannya. Penyimpanan dilakukan pada port

b.) shared memory buffer

Frame tidak disimpan dalam incoming port yang spesifik, tapi disimpan dalam memory switch. Besar frame data yang disimpan dipengaruhi oleh besarnya memory pada switch.

Kedua sistem penyimpanan dilakukan saat destination sibuk atau ada frame yang belum sampai ke tujuannya sehingga pengiriman berikut ke tujuan yang sama harus mengantre dibelakangnya.

Tujuan dari microsegmentation:

- a.) mengisolasi traffisc pada network
- b.) meningkatkan bandwidth

Tambahan

Bila CAM table pada switch telah lengkap maka switch setelah membentuk Virtual Circuit (VC) yang artinya dapat langsung memforward frame ke tujuan dengan membuat jalur khusus (dari MAC address dalam hal ini)

CHAPTER 5

Switches

Pedoman dalam membangun LAN :

- a) Functionality : Harus mampu memenuhi kebutuhan user
- b) Manageability : Harus dapat di manage
- c) Scalability : Dapat dikembangkan
- d) Adaptability : Mampu beradaptasi dengan teknologi baru.

Macam-macam server :

a) Enterprise Server :

Server Seperti Domain Name System (DNS) & memainkan peranan penting bagi jaringan.

b) Workgroup Server :

Server seperti file server & sifatnya tidak krusial bagi jaringan hanya pelengkap saja.

Enterprise server sebaiknya diletakkan pada Main Distribution Facilities (MDF), sedangkan Workgroup Server diletakkan pada Intermediate Distribution Facilities (IDF)

Istilah-istilah lain :

a) Horizontal Cross Connect (HCC) :

Disebut juga horizontal cabling, berfungsi menghubungkan host pada MDF maupun host pada IDF. Biasanya menggunakan UTP cable dan maksimal 100m.

b) Vertical Cross Connect (VCC) :

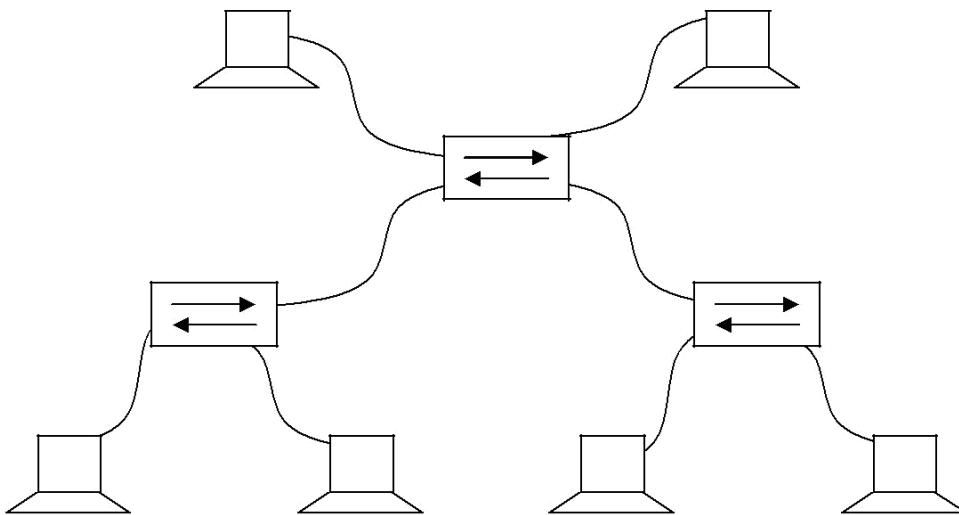
Disebut juga vertical cabling, berfungsi menghubungkan MDF & IDF biasanya memakai fiber optic.

c) Main Distribution Facilities (MDF) :

Ruang yang digunakan untuk menyimpan enterprise server, merupakan tempat penyimpanan utama.

d) Intermediate Distribution Facilities (IDF) :

Ruang penyimpanan tambahan untuk menyimpan workgroup server.



Vertical Cabling dengan fiber optic menghubungkan MDF dengan IDF, sedangkan antar MDF maupun antar IDF dihubungkan dengan Horizontal Cabling.

Switching mengenai hierachical layer yaitu :

- a) Access Layer
- b) Distribution Layer
- c) Core Layer

Masing-masing layer mempunyai fungsi tersendiri.

Access Layer

Layer yang berkaitan dengan akses ke network resources, direpresentasikan dengan penggunaan hub atau switch.

Hub untuk shared network, sedangkan switch dapat melakukan Microsegmentation.

Contoh alat :

- Catalyst 2900
- Catalyst 2950

Distribution Layer

Layer ini berkaitan dengan security, pembagian broadcast domain, dan VLAN routing, VLAN routing adalah pengelompokan network secara logical.

Contoh alat :

- Catalyst 4000
- Catalyst 5000
- Catalyst 2926

Core Layer

Core layer berkaitan dengan high-speed connection dan tidak ada paket manipulation pada layer ini.

Contoh alat :

- Switch tipe 5000 & 6000
- IGX
- Lightstream

Chapter 6

Switch Configuration

Switch tidak menggunakan shared network, tapi tiap port memiliki dedicated bandwidth sendiri, dengan dedicated bandwidth menyebabkan Switch lebih cepat dalam speed dibandingkan dengan Hub.

Sistem lampu led (indikator)pada switch berdasarkan mode dibedakan atas:

a. STAT :

| | |
|------------------------|-------------------------|
| Solid green | : link operational |
| Flashing green | : mengirim data |
| Alternated green/amber | : link fault |
| Solid amber | : port di blok oleh STP |

b. UTL:

----- 1 dari sebelah kanan, maka
bandwidth ber kurang 50%. Jika lampu mati 2 dari sebelah kanan maka
bandwidth berkurang 25%

Green : Jika semua lampu menyala hijau , switch menggunakan 50% atau lebih dari
total bandwidth

c.FDUP:

Off : mode half duplex
Green : mode full duplex.

d.100

Off : speed 10 Mbps aktif
Green : speed 100 Mbps aktif

Command-command Setting Switch:

Seting password console

```
Switch(config)#line console 0
Switch(config-line)#password password
Switch(config-line)#login
```

Seting password telnet

```
Switch(config)#line vty 0 15
Switch(config-line)#password password
Switch(config-line)#login
```

Seting password previledge

```
Switch(config)#enable password
password atau dengan enskripsi
Switch(config)#enable secret password
Pass word yang diambil yaitu password enable secret
```

Urutan langkah sebelum mereload switch:

Hapus info Vlan ;

Switch# delete flash : vlan.dat

Switch#erase startup configuration

Switch#reload

Switch menyimpan MAC Address dalam CAM table, untuk melihatnya

Switch# show mac-address-table

Syarat agar switch dapat di telnet/ping yaitu: harus dipasang IP address atau IP default gateway, caranya:

Switch (config)#interface vlan1

Switch(config-if)#ip address ip subnetmask

Switch(config-if)#no shut

Pasang default gateway

Switch(config)#ip default-gateway ip

Setting hostname

Switch(config)#hostname name

Mac address terbagi atas 3 jenis:

a. Static MAC

diseting manual pada port tertentu di switch, MAC ini tidak akan di remote oleh switch.

Cara setingnya:

Switch(config)mac-address-table static mac add interface int vlan1

Cara melihatnya:

Switch#show mac-address-table static

b.Dynamic MAC

Mac yang dimiliki oleh host yang dicolokan ke switch, dapat dilihat dengan:

Switch#show mac-address-table dynamic

c.Secure MAC

Mac yang dipasang pada port security, bila dideteksi ada Mac lain yang dipasang pada port Ini maka akan terkena violation, misal di shutdown.

Port Security

Sistem security pada port di switch, bila aturan ini dilanggar akan terkena violation,

Cara setingnya:

Switch(config)# interface int

Switch(config-if)#switch port mode access

Switch(config-if)#switch port port-security

Switch(config-if)#switch port port-security maximum max

Switch(config-if)#switch port port-security mac address mac add

Switch(config-if)#switch port port-security violation violation

Contoh penerapan:

```
Switch(config-if)#switch port port-security maximum 5
```

```
Switch(config-if)#switch port port-security mac address d5ef.1240.abcd
```

```
Switch(config-if)#switch port port-security violation shutdown
```

Bila pada port tersebut di hubungkan ke switch lain yang memiliki 5 port lebih terhubung host, maka port akan shutdown.

Port shutdown juga bila MAC address yang di hubungkan bukan d5ef.1240.abcd.

Ini yang disebut sebagai MAC address secure

Cara melihat port security:

```
Switch#show port-security
```

Command-command show lainnya:**Melihat settingan secara global**

```
Switch#show running-config
```

Melihat isi nvram

```
Switch#show startup-config
```

Melihat keterangan interface

```
Switch#show interface interface
```

Untuk mengganti IOS Switch

```
Switch# erase flash (seluruh file pada switch akan dihapus)
```

```
Switch# archive tar/xtract tftp// 10.21.22.200/namafile.tar
```

Password recovery pada switch

1. cabut kabel power switch
2. sambungkan kabel power switch sambil menekan tombol mode
3. tunggu sampai lampu system menjadi oranye (masuk ke Rommon mode)
4. ketik : flash_init (untuk inisialisasi flash)
5. ketik : dir_flash (untuk melihat isi file)
6. ketik: rename flash: config.text flash: config.old
7. ketik: boot
8. masuk ke switch seperti biasa dan jawab ‘NO’ pada setiap mode
9. masuk ke privileged mode

```
Switch#rename flash: config.old flash: config.text
```
- 10.lakukan :

```
Switch#copy flash: config.text system: running-config
```
11. ganti password (secret, enable, telnet)
12. copy run start

Settingan agar switch dapat di HTTP:

```
Switch(config)#ip http server
```

```
Switch(config)#ip http port 80
```

CHAPTER 7

Spanning-Tree Protocol

Pemasangan redundant link pada switch ke switch lain dapat meningkatkan fault tolerance, namun disisi lain, hal ini dapat menyebabkan terjadinya broadcast storm STP memblok port-port yang dapat menyebabkan broadcast storm, multiple frame transmission & MAC address database inconstancy.

Broadcast storm disebabkan oleh pengiriman frame yang berulang-ulang pada device layer 2, dalam hal ini switch. Device layer 2 tidak mempunya time to live (TTL) seperti device layer 3. Sehingga frame yang berulang-ulang tidak di discard.

Spanning tree protocol (STP) mempunyai standart IEEE 802.1d dapat mengatasi masalah ini. STP aktif secara default pada setiap switch cisco. STP memblok port-port yang dapat menyebabkan broadcast storm.

Pemilihan root bridge menjadi acuan dalam konsep ini, root bridge adalah switch yang memilih MAC address yang paling rendah dalam topologi.

Switch mengirim bridge protocol data unit (BPDU) setiap 2 detik untuk menginformasikan tentang bridge ID (BID) BID berisi MAC Address & priority, priority lebih diutamakan dibanding MAC address, defaultnya 32768.

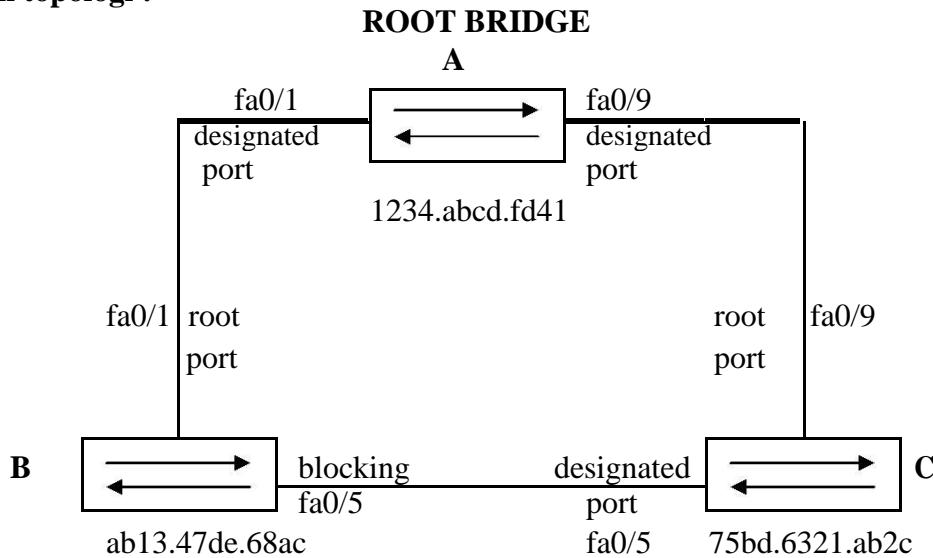
Saat switch dinyalakan proses :

- **Blocking** : tidak ada port yang dapat mengirim data, berlangsung selama 20 detik.
- **Listening** : Mencari path ke root bridge, belum mempelajari MAC address & belum memforward data, berlangsung selama 15 detik.
- **Learning** : Mempelajari MAC address, tapi belum memforward data, berlangsung selama 15 detik.

Total keadaan ini dinamakan forward delay.

- **Forward** : data telah dapat diforward, keadaan dimana topologi, switch telah selesai dipelajari.
- **Disable** : port yang tidak diijinkan mengirim data, tidak aktif karena spanning-tree protocol (STP).

Contoh topologi :



Priority yang digunakan secara default yaitu 32768 sehingga MAC address yang paling rendah digunakan dalam penentuan root bridge.

Port fa0/5 pada switch B akan diblok untuk menghindari redundant link yang menyebabkan broadcast storm.

Istilah-istilah penting :

- Bridge ID (BID)** : dikirimkan dalam BPDU, isinya adalah MAC address dan priority, BID terendah lah yang diambil.
- Bridge Protocol Data Unit (BPDU)** : dikirimkan oleh switch tiap 2 detik, isinya adalah BID.
- Designated port** : Port yang sifatnya forwarding, dapat mengirimkan data.
- Blocking port** : Port yang diblok oleh spanning-tree protocol.
- Root port** : Port pada non-root bridge yang tepat langsung mengarah ke root bridge, sifatnya selalu forwarding.
- Root bridge** : Switch pada topologi yang menjadi acuan dalam menentukan suatu port lain, dipilih berdasarkan BID yang terendah.
- Non-root bridge** : Switch yang BID-nya bukan yang terendah, non-root bridge yang BID-nya paling tinggi, salah satu portnya akan diblok.

Command-command Spanning-tree :

- Mematikan spanning-tree :**
Switch(config)#no spanning-tree vlan 1
- Mengganti priority :**
Switch(config)#spanning-tree vlan 1 priority priority
- Melihat spanning-tree :**
Switch#show spanning-tree
- Melihat MAC address switch :**
Switch#show interface vlan 1

NB : perhatikan not bridge, priority, status port pada switch, MAC address.

CHAPTER 8

Virtual LAN

Virtual LAN (VLAN) merupakan pengelompokan jaringan yang tidak tergantung dari lokasi fisik, pengelompokan dilakukan secara logikal.

Biasanya dibagi berdasarkan fungsionalitas atau department tertentu misalnya

- : a.) vlan untuk finance
 - b.) vlan untuk HRD
 - c.) vlan untuk marketing
- dan sebagainya.

Setiap vlan adalah broadcast domainnya masing-masing dan antar vlan yang berbeda tidak dapat saling berhubungan kecuali menggunakan router.

Penghubung vlan yang berbeda dengan menggunakan router disebut inter-vlan routing. Switch memiliki tabel-tabel yang terpisah untuk tiap vlan dan informasi vlan disimpan pada vlan database dalam bentuk vlan.dat.

Jenis-jenis vlan:

a.) static vlan

dikonfigurasi manual pada switch dengan perintah-perintah kemudian diassign ke dalam port.

b.) dynamic vlan

dikonfigurasi dengan menggunakan software, misalnya Ciscoworks for Switched Internetwork

Selain static dan dynamic, vlan juga dapat diassign berdasarkan port, MAC address, atau subnet (jaringan).

Assigning Based on Port

Menciptakan vlan kemudian memasukan port-port ke dalam masing-masing vlan.

Assigning Based on MAC address

Pengelompokan MAC address tertentu dimasukkan ke vlan tertentu, contoh:

Vlan 2 untuk MAC:

ff 3d : 4321 : abcd

cef4 : 5967 : 128

Assigning Based on Subnet

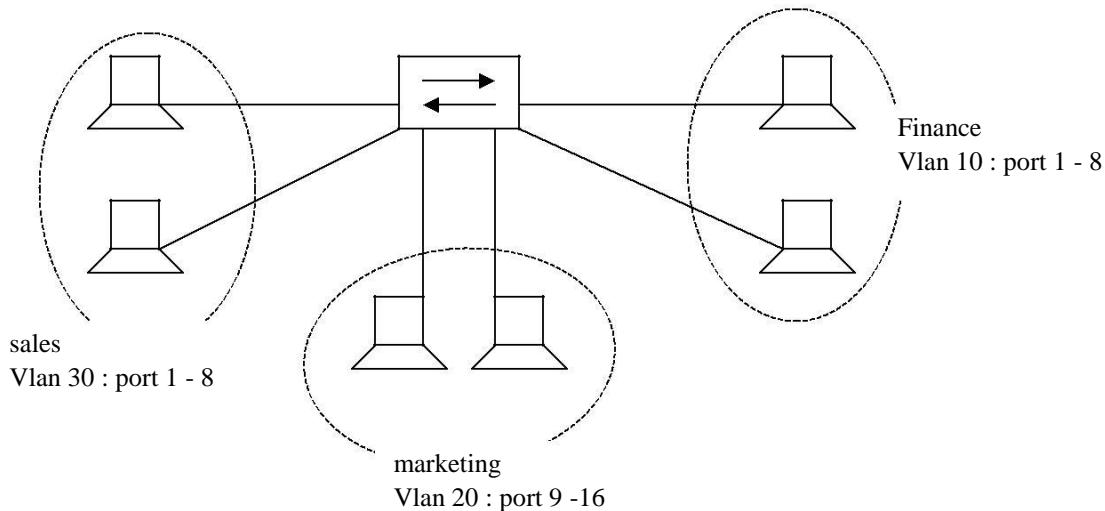
Pengelompokan berdasarkan subnet, subnet tertentu dimasukkan dalam vlan tertentu. Contoh:

192.168.10.0/24 ke vlan 3

192.168.30.0/24 ke vlan

10 dan sebagainya

VLAN yang paling umum digunakan adalah vlan assigning based on port. Biasanya dibuat per fungsionalitas, contoh:



Frame tagging digunakan oleh switch dalam mengenali suatu frame milik vlan berapa, farem tagging yang utama ada 2 yaitu:

a.) Inter Switch Link (ISL):

Proprietary cisco, menambahkan header pada frame dimana pada header terdapat vlan id.

b.) IEEE 802.1q :

Open standard, memodifikasi header frame agar dapat dikenali milik vlan berapa

Satu lagi frame tagging yaitu LANE (LAN Emulator), tapi jarang digunakan.

Biasanya ISL pada switch-switch cisco lama, switch terbaru mengikuti open standard (IEEE 802.1q)

Keuntungan-keuntungan menggunakan

- vlan:** a.) mudah menambah host
- b.) mudah mengurangi host
- c.) security

Command-command dalam membuat vlan

Membuat vlan:

Switch#vlan database

Switch(vlan)#vlan number name name

Switch(vlan)#exit

Pada akhir pembuatan vlan ada 3 perintah yang dapat digunakan:

- exit : apply + exit
- apply : apply without exit
- abort : exit without apply

contoh:

```
Switch#vlan database
Switch(vlan)#vlan 10 name finance
Switch(vlan)#vlan 20 name
marketing Switch(vlan)#exit
```

Memasukkan port pada switch ke dalam vlan :

```
Switch(config)#interface interface number
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan number
```

Contoh:

```
Switch(config)# interface fa0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

Secara default, semua port dalam switch adalah vlan 1 (default administrative vlan).

Selain satu per satu, dapat juga memasukkan vlan dalam port sekaligus banyak dengan:

```
Switch(config)#interface range interface number – number
```

Contoh:

```
Switch(config)#interface range fa0/5 – 10
```

Command-command show a.)

Melihat vlan(complete)

```
switch#show vlan
```

b.) Melihat ringkasan info vlan

```
switch#show vlan brief
```

c.) Melihat vlan berdasarkan nomor vlan

```
switch#show vlan id number
```

d.) Melihat vlan berdasarkan nama vlan

```
switch#show vlan name name
```

e.) Menghapus semua vlan

```
switch#delete flash:vlan.dat
```

CHAPTER 9

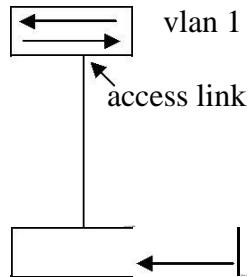
VLAN Trunking Protocol

VLAN Trunking Protocol menggunakan frame tagged untuk menandai suatu frame milik VLAN berapa.

Pada dasarnya trunking mengijinkan komunikasi antar VLAN yang sama pada switch-switch yang berbeda.

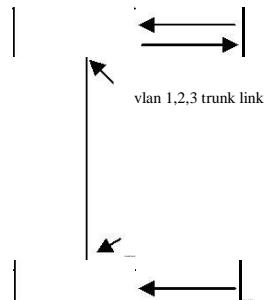
Perbedaan stocking dengan trunking

Stocking : Penghubung antar switch yang berbeda dimana hanya terdapat satu VLAN pada switch-switch tersebut.



Misalnya dua switch dihubungkan dimana switch-switch itu hanya memiliki satu VLAN, yaitu VLAN, secara default.

Trunking : penghubung antar switch yang berbeda dimana terdapat lebih dari satu VLAN pada switch-switch tersebut.



Stocking menggunakan access link sebagai penghubung, sedangkan trunking memakai trunk link.

Secara default, semua port pada switch adalah access link.

Access link : hanya dapat mengirim frame pada VLAN yang sama antar switch, untuk satu VLAN.

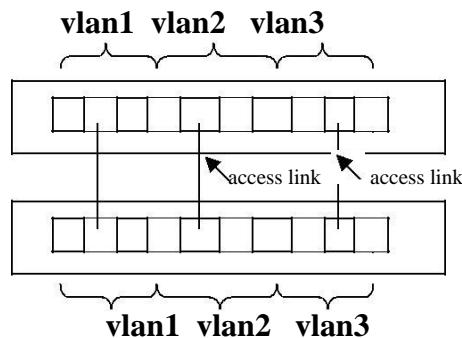
Trunk link : dapat mengirim frame yang ditujukan untuk VLAN yang sama antar switch, bila terdapat beberapa VLAN pada switch-switch itu.

Untuk menghubungkan VLAN yang berbeda tetap harus memakai inter VLAN Routing.

Perbedaan lainnya antara stocking dan trunking

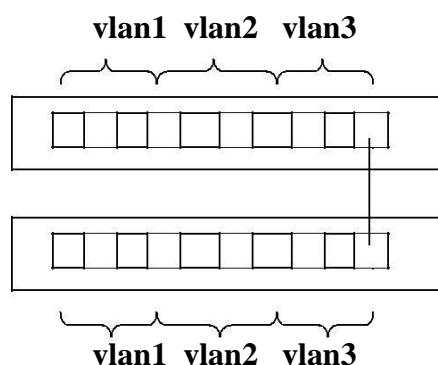
Contoh :

a) Stocking :



bisa terdapat beberapa VLAN, namun harus dihubungkan satu per satu VLAN yang ada.

b) Trunking :



Dari gambar, terlihat bahwa satu kabel, trunk link dapat membawa info banyak VLAN sekaligus.

VTP digunakan dalam mengontrol VLAN dan mengelompokkan banyak VLAN ke dalam network.

VTP dan VLAN adalah layer 2 OSI (data link).

Frame tangging juga digunakan dalam VTP, ada 2 yang utama :

a) **Interswitch-Link (ISL)**

Proprietary Cisco, memodifikasi header untuk menandai keanggotaan suatu VLAN.

b) IEEE 802.1q

Open standard, menambahkan tag berupa VLAN ID untuk menandai keanggotaan VLAN.

Keduanya untuk ethernet dan fast ethernet.

Selain ISL dan IEEE 801.1q, terdapat pula 802.10 untuk FDDI dan LANE untuk ATM.

Fungsi utama VTP yaitu menyederhanakan pembuatan VLAN pada banyak switch. Pada VTP, ada yang bertindak sebagai server, transparant, maupun client.

VTP Server

Dapat create, add, dan delete VLAN, kemudian mengirim informasi VLAN keluar dari trunk port.

VLAN Transparant

Tidak menyimpan informasi VLAN pada NVRAM, hanya meneruskan info VLAN yang diterima dari VTP server ke VTP client.

VTP Client

Menerima dan menyimpan informasi VLAN pada NVRAM, info VLAN disimpan pada NVRAM tersebut berasal dari server.

VTP server, transparant, dan client harus berada dalam domain yang sama dan memiliki password yang sama.

Langkah pemilihan VTP server, transparant, dan client, dilakukan berdasarkan configuration revision number yang saat switch dihidupkan akan bertambah jumlahnya mulai dari 0 sampai 2.147.483.648, walaupun sudah disetting ke mode VTP client, switch harus di reload dulu agar revision number kembali ke 0 sebab angka yang tinggi akan menimpa angka yang lebih rendah. Angka lebih tinggi akan menjadi VTP server.

Pengiriman info dari VTP server ke VTP client melibatkan VTP message berikut :

- a) Advertisement Request
- b) Summary advertisement
- c) Subset advertisement

Advertisement Request

Info request VLAN yang dikirim oleh VTP client pada VTP server.

Summary Advertisement

Digunakan pada saat switch dinyalakan pertama kali untuk menentukan siapa switch yang menjadi VTP server, dikirim setiap 5 menit sekali. Isinya terdapat configuration revision number dimana angka tertinggi akan menimpa angka yang lebih rendah, angka tertinggi akan menjadi server.

Subset Advertisement

Info tentang VLAN yang dikirimkan oleh VTP server kepada VTP client.

Ketiga VTP Message itu dikirimkan keluar melalui trunk port.

Command-command VTP :

Menyetting domain, mode, dan password VTP :

Switch#vlan database

Switch(vlan)#vtp domain name

Switch(vlan)#vtp mode

Switch(vlan)#vtp password password

Mengubah access link port ke trunk link port :

Switch(config)#interface interface number

Switch(config-if)#switchport mode trunk

Perintah show :

a) **Melihat domain dan mode vtp :**

Switch#show vtp start

b) **Melihat password vtp :**

Switch#show vtp password

c) **Melihat advertisement request, summary advertisement, subnet advertisement :**

Switch#show vtp counter

d) **Melihat port yang di trunk :**

Switch#sshow interface trunk

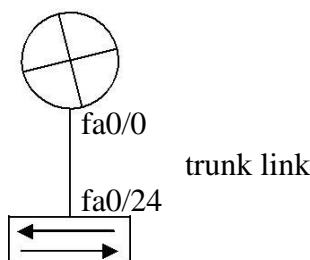
InterVLAN Routing

Konsep interVLAN Routing yaitu menghubungkan VLAN yang berbeda dengan router. Default gateway tiap VLAN disetting pada router, sering disebut juga “Router on a stick”. Command untuk default gateway tiap VLAN dipasang ke dalam subinterface.

Settingan Command

```
Router(config)#interface interface number Router(config-if)#no shutdown Router(config-if)#interface interface number sub interface Router(config-subif)#encapsulation dot1q vlan id Router(config-subif)#ip address ip subnetwork Router(config-subif)#no shutdown
```

Contoh :



vlan 1 : port 1-8
vlan 2 : port 9-16
vlan 3 : port 17-23

Pada switch, terdapat :

Vlan 1 192.168.10.0/27, Default Gateaway : 192.168.10.1
Vlan 2 192.168.10.32/27, Default Gateaway : 192.168.10.33
Vlan 3 192.168.10.64/27, Deafult Gateawat : 192.168.10.65

Pada Router, Setting :

```
Router(config)#interface fa0/0
Router(config-if)#no shutdown
Router(config-if)#interface fa0/0.1
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ip address 192.168.10.1 255.255.255.224
Router(config-subif)#no shutdown

Router(config-if)#interface fa0/0.2
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.10.33 255.255.255.224
Router(config-subif)#no shutdown

Router(config-if)#interface fa0/0.3
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.10.65 255.255.255.224
Router(config-subif)#no shutdown
```

Pada switch, port fa0/24 setting :

```
Router(config)#int fa0/24
Router(config-if)#switchport mode trunk
```

VLAN yang berbeda dapat saling berhubungan, misal host pada vlan 1 dapat connect dengan host pada vlan 10.

CCNA 4

| | |
|--|-----------|
| Daftar Isi | 1 |
| Chapter 1 | |
| Scalling IP Address | 2 |
| Chapter 2 | |
| WAN Technologies | 5 |
| Chapter 3 | |
| PPP | 11 |
| Chapter 4 | |
| ISDN and DDR | 15 |
| Chapter 5 | |
| Frame Relay | 21 |
| Chapter 6 | |
| Introduction to Network Administration | 25 |

CHAPTER 1

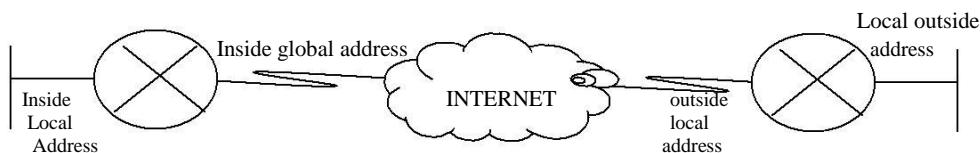
Scalling IP Address

Private IP Address

| | | | | |
|----|----------------|---|-------------------------------|-----------|
| 1. | 10.0.0.0/8 | > | 10.0.0.0 – 10.255.255.255 | 1 class |
| 2. | 172.16.0.0/12 | > | 172.16.0.0 – 172.31.255.255 | 16 class |
| 3. | 192.168.0.0/16 | > | 192.168.0.0 – 192.168.255.255 | 256 class |

Network Address Translation (NAT)

Berfungsi menterjemahkan alamat local (IP Private) menjadi alamat global (IP Public)

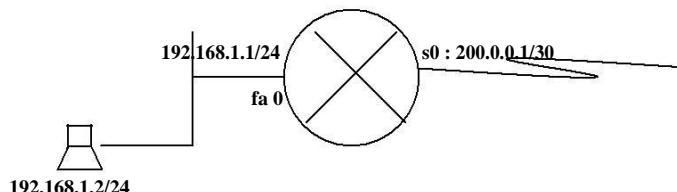


NAT Dibagi 3 :

- **NAT Static** : Ip private di map ke 1 ip public.
 - **NAT Dynamic** : 1/ beberapa ip private di map ke 1/beberapa ip public dengan lease time 24 jam.
 - **NAT Overload** : (Port Address Translation), beberapa ip private di map ke 1 ip public menggunakan port.

Konfigurasi NAT Static

Untuk web server yang disconnect ke internet, ip publicnya dedicated untuk 1 ip private.



Caranya :

1. Buat Mapping ip

Router (config)# ip nat inside source static 192.168.1.2 200.0.0.1

2. Terapkan di interface

Router(config)# int fa 0

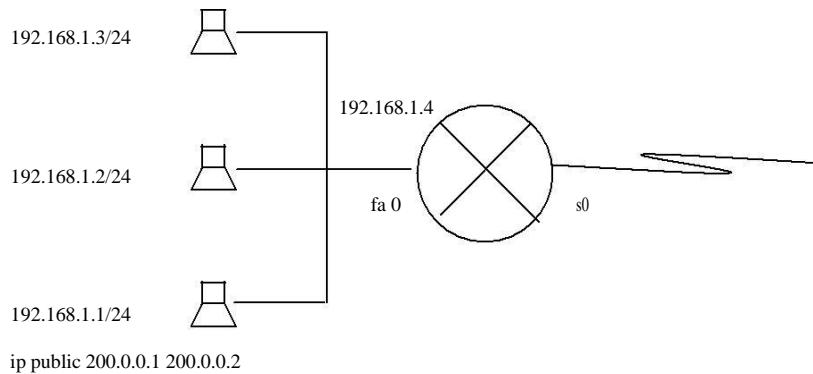
Router (config-if)# ip nat

Router (config-if)# ip nat
inside Router (config)# int s0

```
Router (config-if)# ip nat outside
```

Konfigurasi NAT Dynamic

Tetap one to one. One ip private di mapping ke one ip public. Kalau ip publicnya semuanya dipakai, maka ip private yang belum di mapping harus menunggu sampai ip public yang dipakai ip private lain dilepas (dikasih time out 24 jam, lewat dari 24 jam ip public release lagi).



Caranya :

1. Buat pool ip public

```
Router(config)# ip nat pool mypool 200.0.0.1 200.0.0.2  
          nama pool  start ip public end ip public
```

2. Buat ACL, ip private berapa aja yang boleh diakses ip public dalam pool diatas.

```
Router(config)# access list 10 permit 192.168.1.1 0.0.0.3
```

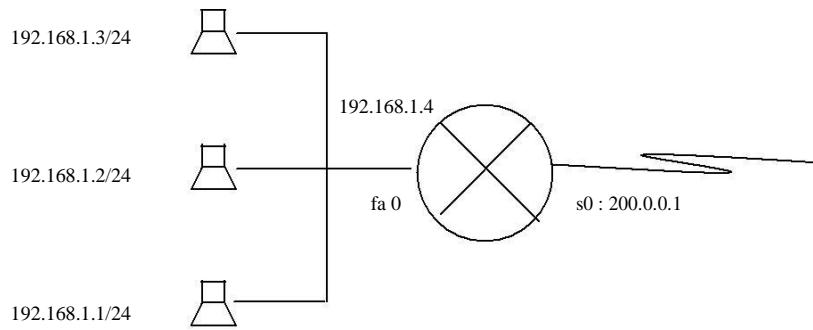
3. Terapkan ACL dalam pool

```
Router(config)# ip nat inside source list 10 pool mypool  
          no ACL      nama pool
```

4. Terapkan di interface

```
Router(config)# int fa0  
Router(config-if)# ip nat inside  
Router(config)# int s0  
Router(config-if)# ip nat outside
```

Konfigurasi NAT Overload



Caranya :

1. Buat ip Public

Dalam pool, jika ada beberapa ip public yang dimiliki kalau hanya 1, tidak perlu set ip public, cukup dengan memakai ip add serial saja.

2. Buat ACL

3. Terapkan ACL pada pool

```
Router(config)# ip nat inside source list no.ACL int s0  
overload (untuk 1 ip public yang dimiliki)
```

ATAU

```
Router(config)# ip nat inside source list no.ACL pool nama pool  
overload (untuk 2/ lebih ip public yang dimiliki)
```

4. Terapkan pada Interface

Jika sudah berhasil akses internet, ip public yang dipakai (translation) dalam table NAT akan direlease (tidak memerlukan 24 jam).

Verify NAT

```
Router# show ip nat translation  
Router# debug ip nat translation  
Router# clear ip nat translation.
```

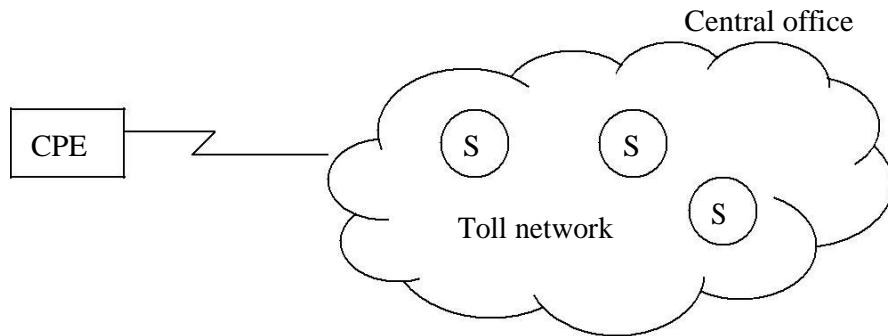
CHAPTER 2

WAN Technologies

Terdapat bermacam-macam teknologi WAN, namun berbeda dalam speed dan cost. WAN menghubungkan jaringan yang letaknya berjauhan menggunakan jasa *provider*. WAN dapat membawa video, data, dan voice, misalnya data service via WAN.

Customer Premises Equipment (CPE) pada WAN yaitu peralatan yang letaknya di sisi *customer* dan dihubungkan dengan local loop menuju Central Office. Local loop/ last mile dapat menggunakan *wired cable* dalam menghubungkan CPE dengan CO (Central Office). Contoh local loop yaitu kabel *public* yang menghubungkan PSTN dengan Telkom.

Terdapat **DTE (Data Terminal Equipment)** yang terhubung dengan CPE, biasanya Router, sedangkan DCE (Data Communication Equipment/ Data-circuit Terminating Equipment) adalah interface pada modem.



Biasanya antara CPE dan Central Office terdapat *demarcation point* yang merupakan batas antara tanggung jawab pembeli (customer) dan provider.

Device-device pada

- WAN:**
- a.) router
 - b.) modem
 - c.) communication server/
provider
 - d.) switch

Router yang digunakan

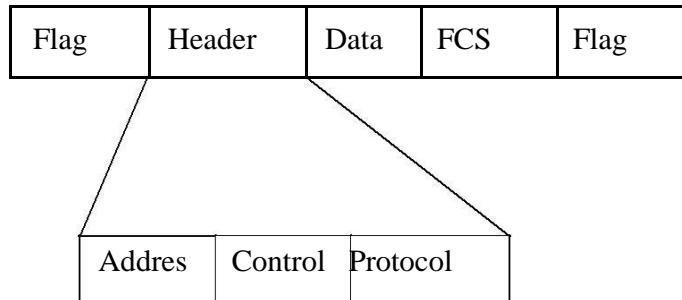
- menjanjikan:**
- a.) connectivity
 - b.) flexibility

Saat paket melewati WAN, dienkapsulasi ke dalam bentuk-bentuk:

- a.) Link Access Procedured Balanced (LAPB) : X2r
- b.) Link Access Procedured for D Channel (LAPD) : ISDN D Channel
- c.) Link Access Procedured for Frame (LAPF) : Frame Relay
- d.) High-level Data Link Control (HDLC) : ini default WAN encapsulation
- e.) Point-to-point Protocol (PPP) : untuk dial-up dan circuit switched network (ISDN)

Selain itu, paket dienkapsulasi ke bentuk yang dapat dikirimkan dalam jaringan WAN.

Bentuknya yaitu



Encapsulation yang paling banyak dipakai adalah HDLC, *field address* panjangnya 1 atau 2 bytes, tidak digunakan bila koneksi point to point.

Field Control isinya:

- a.) unnumbered frame : line setup message
- b.) Information frame : network layer data
- c.) Supervisory frame : flow information dan retransmission data bila terjadi error

WAN standard:

- a.) ITU-T (International Telecommunication Union-Telecommunication Standardization Sector), dulunya bernama CCITT
- b.) ISO (International Organization for Standardization)
- c.) IETF (Internet Engineering Task Force)
- d.) EIA dan TIA

WAN bekerja pada layer 1 dan 2 OSI layer,

perinciannya: a.) Layer 1 (physical)

- EIA/ TIA-232
- EIA/ TIA-449/ 530
- EIA/ TIA-612/ 613 : High Speed Serial Interface (HSSI)
- V.35

b.) Layer 2 (data-link)

Paket switched, leased line dan circuit switched

Lease Line

Koneksi point-to-point, biasanya menggunakan encapsulation PPP atau HDLC.

Packet Switched

Koneksi WAN dimana paket di bentuk dalam frame atau *cell*, hubungannya tidak menggunakan nomor yang *di-dial* memakai identifier untuk mengirim paket ke tujuan.

Contoh identifier : DLCI

DLCI bisa membentuk sebuah jalur yang disebut Virtual Circuit (VC), ada 2 VC, yaitu:

- Permanent Virtual Circuit (PVC) : sifatnya permanent, tetap
- Switched Virtual Circuit(SVC) : sifatnya tidak permanent, dapat hilang setelah waktu tertentu. Contoh : frame relay.

Circuit Switched

Koneksi WAN dimana pembentukan koneksi dilakukan dengan men-*dial* sebuah nomor seperti nomor telepon, setelah koneksi tercipta, barulah paket dapat dikirimkan. Contohnya: Integrated Service Digital Network (ISDN).

Teknologi-teknologi WAN

a.) Analog dial-up

Biasanya dengan sebuah modem yang digunakan untuk membentuk koneksi, kecepatannya 33 kbps-56 kbps. Analog dial-up sangat simple untuk dibentuk, dan *low implementation cost*, namun *low bandwidth rate* bila dibandingkan dengan teknologi WAN lainnya.

b.) Integrated Service Digital Network (ISDN)

ISDN terdapat dua jenis yaitu:

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)

ISDN BRI digunakan untuk jaringan skala kecil, disebut juga 2 B + D (2 B Channel + D Channel), 2 buah 64 kbps B Channel digunakan + 1 buah 16 kbps D Channel. Adapun B Channel dipakai untuk *Carrying Data*, dan D Channel untuk *call setup*.

ISDN PRI untuk jaringan yang lebih luas, ada 2 jenis:

- TI : 1544 Mbps => 23 buah 64 kbps B channel + 1 buah 64 kbps D channel => disebut 23 B + D
- EI : 2048 Mbps => 30 buah 64 kbps B channel + 1 buah 64 kbps D channel => disebut 30 B + D

Dynamic Host Configuration Protocol (DHCP)

DHCP adalah sebuah protocol untuk memberikan IP address secara dynamic, didefinisikan oleh RFC 2131.

Macam-macam pengalokasian IP:

- a.) automatic : ip diberikan secara otomatis dan permanent, dapat dengan *DHCP reservations*
- b.) manual : ip disetting secara manual oleh *network administrator*
- c.) dynamic : ip diberikan secara dynamic oleh DHCP dan sifatnya *temporary*

Pada dasarnya, DHCP memberikan ip secara system sewa atau *lease time* yang bilamana habis, client DHCP akan meminta ip kembali dari DHCP server.

Informasi yang disertakan pada DHCP, antara

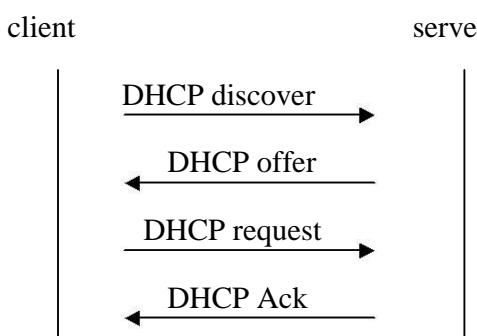
- lain: a.) ip address
- b.) subnet mask c.) default gateway
- d.) dns server

Command-command DHCP:

```
Router(config)#service dhcp  
Router(config)#ip dhcp pool poolname  
Router(dhcp-config)#network network subnetmask  
Router(dhcp-config)#default-router ip gateway  
Router(dhcp-config)#dns-server ip dns server  
Router(dhcp-config)#domain name domain  
Router(dhcp-config)#net-bios-name-server ip wins server  
Router(dhcp-config)#lease day hour minute  
Router(config)# ip dhcp excluded-address ip excluded
```

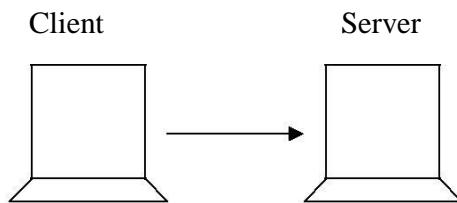
IP excluded digunakan untuk memberi pengecualian atau ip yang tidak ingin dibagikan dalam scope network DHCP

Proses Request DHCP



- a.) client melakukan discover dhcp server secara broadcast untuk menemukan dhcp server dalam jaringan
- b.) server akan menawarkan IP yang dapat digunakan oleh client, ini dilakukan secara unicast.
- c.) Client akan merequest ip yang ditawarkan oleh dhcp server, proses ini dilakukan secara broadcast
- d.) Server mengirim Acknowledgement untuk *approval sign* terhadap request client. Ini dilakukan secara unicast

DHCP menggunakan port number 67 dan 68, 67 digunakan untuk mengirim request, sedangkan 68 digunakan untuk reply dari server.



Request:

Source MAC : MAC client
Dest. MAC : FFF:FFF:FFF

Source IP: ?
Dest. IP : 255.255.255.255

Isinya:

CIADDR : ?
Mask : ?

GIADDR : ?
CHADDR : ?

Reply dari server:

Source MAC : MAC Server
Dest. MAC : MAC Client

Source IP : IP server
Dest. IP : ?

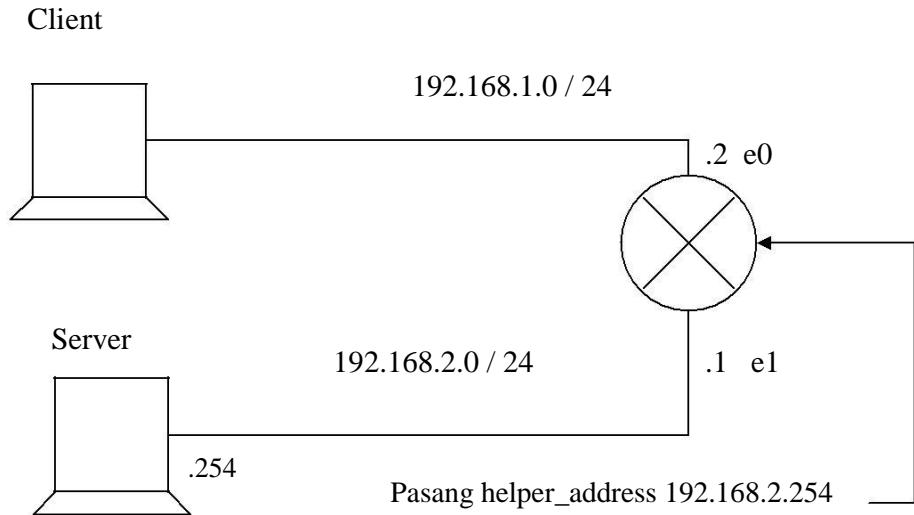
Isinya:

CIADDR : IP client
Mask : Mask Client

GIA DDR : - (tidak ada gateway di network ini)
CHADDR : MAC Client

DHCP Relay

Pada dasarnya, DHCP meneruskan request dari client secara broadcast untuk menemukan DHCP server dalam jaringan. Hal ini berarti bila DHCP server berada di luar broadcast domain, maka request tidak akan diteruskan. Untuk itulah diperlukan DHCP relay.



Client request, dating dari segmen A:

| | |
|---|----------------------------|
| Source MAC : MAC A | Source IP: ? |
| Dest. MAC : FFF:FFF:FFF | Dest. IP : 255.255.255.255 |
| Request diteruskan ke segmen dan sebelum mencapai DHCP servr: | |
| Source MAC : MAC router | Source IP: 192.168.2.1 |
| Dest. MAC : MAC Server | Dest. IP : 192.168.2.254 |
| Request dari port 67 | |

Request dari server dating dari segmen B:

| | |
|-------------------------|----------------------|
| Source MAC : MAC server | Source IP: IP server |
| Dest. MAC : MAC Router | Dest. IP : IP client |

Reply dari port 68:

Ini setelah reply (pada walanya kosong):

| | |
|-----------------------------------|--|
| CIADDR: 192.168.1.10 => ip client | GIADDR : 192.168.1.1 => gateway client |
| Mask: 255.255.255.0 | CHADDR : MAC client |

Command DHCP Relay

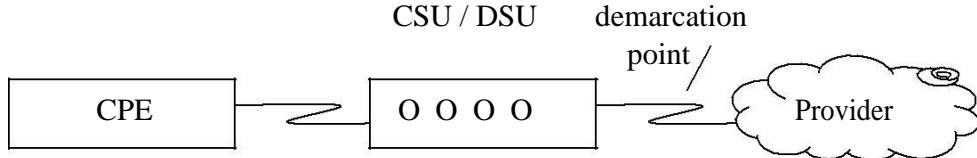
Tambahkan:

Router(config-if)#ip helper-address ipaddress pada interface

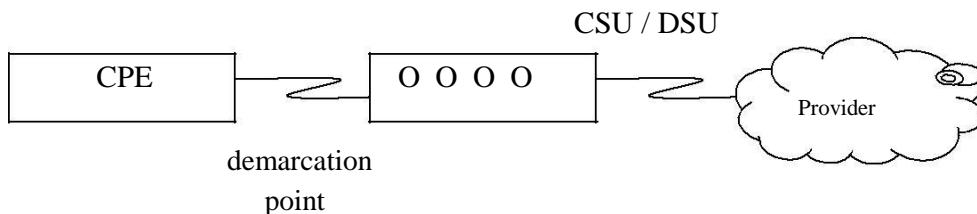
Point-to-point Protocol

PPP bekerja pada Wide Area Network (WAN) dan dapat mendukung synchronous maupun asynchronous communication. Data di encode ke dalam Non Return to Zero Inverted (NRZI), High Density Binary 3 (HDB3), dan Alternative Mark Inversion (AMI).

Pada WAN, terdapat istilah demarcation point yang merupakan batas tanggung jawab antara provider dengan customer.



Di Amerika democation point ada di antara CSU/ DSU dengan provider, sedangkan di negara lain, demorcation point ada di antara CPE dan CSU/ DSU.



Selain itu, terdapat OTE dan DCE yang membentuk koneksi WAN dimana DTE adalah sisi router dan DCE adalah sisi CSU / DSU.

Standard untuk DTE dan DCE yaitu :

- a) Mechanical/ physical : connection
- b) Electrical : voltage level 0 dan 1
- c) Functional : signalling lines pada interface
- d) Procedural : urutan event dalam mengirim data.

Pada PPP, data dienkapsulasi ke dalam :

| | | | | | |
|------|---------|---------|------|-----|------|
| Flag | Address | Control | Data | FCS | Flag |
|------|---------|---------|------|-----|------|

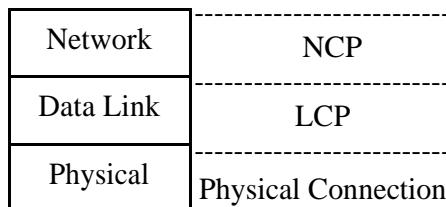
Terdapat pula frame-frame seperti I-Frame dan S-Frame secara U-frame.

Frame-frame tersebut terdapat pada Control Field :

- a) **Information Frame (I-Frame) :**
Membawa data yang ditransmit ke station.
- b) **Supervisory Frame (S-Frame) :**
Untuk request mechanism dan response mechanism.
- c) **Unnumbered Frame (U-Frame) :**
Untuk connection setup.

PPP memiliki dua sub layer yang utama yaitu :

- a) **Link Control Protocol (LCP) :**
Dapat membentuk koneksi pada PPP.
- b) **Network Control Protocol (NCP) :**
Dapat membawa network layer data.



Tiga macam LCP Frame yaitu :

- a) **Link-establishment frame :** membentuk koneksi.
- b) **Link-termination :** memutus koneksi.
- c) **Link-maintenance :** mempertahankan koneksi.

Tiga sesi pembentukan koneksi yaitu :

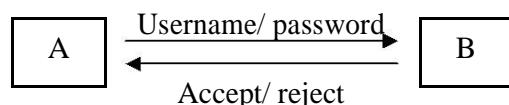
- a) Establishment phase.
- b) Authentication.
- c) Network layer phase.

LCP juga melakukan antara lain :

- a) Authentication : Password Authentication Protocol (PPP) dan Challenge Handshake Authentication Protocol (CHAP).
- b) Compress : Predictor dan Stacker.
- c) Multilink.
- d) PPP call back.

Password Authentication Protocol (PAP)

PAP adalah authentication secara two way handshake, phasenya :



PAP authentication merupakan authentication yang tidak dienkripsi maka lebih insecure daripada CHAP Authentication.

Command-command PAP :

A) One Way PAP

PAP Server :

```
Server(config)#username name password
password Server(config)#interface int number
Server(config-if)#encapsulation ppp
Server(config-if)#ppp authentication ppp
```

PAP Client

```
Client(config)#interface int number
Client(config)#encapsulation ppp
Client(config-if)#ppp pap sent-username name password password Username
```

dan passwordnya harus sesuai dengan apa yang dibuat oleh server.

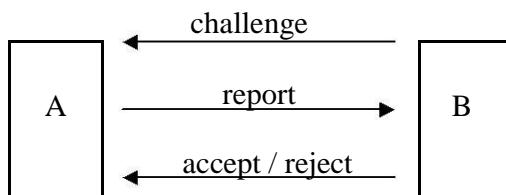
B) Two Way PAP

Dua-duanya memiliki settingan :

```
Router(config)#username name password
password Router(config)#interface int number
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication pap
Router(config-if)#ppp pap sent-username name password password
```

Challenge Handshake Authentication Protocol (CHAP)

CHAP adalah authentication secara three way handshake, phasenya :



CHAP mengenal enkripsi pada authenticationnya.

Command-command CHAP :

A) One way CHAP

CHAP Server

```
Server(config)#username name password
password Server(config)#interface int number
Server(config-if)#encapsulation ppp
Server(config-if)#ppp authentication cha
```

CHAP Client

```
Client(config)#interface int number
Client(config)#encapsulation ppp
Client(config-if)#ppp chap hostname name
Client(config-if)#ppp chap password password
```

B) Two way CHAP

Dua-duanya memiliki settingan :

```
Router(config)#username name password password
Router(config)#interface int number
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication chap
Router(config-if)# ppp chap hostname name
Router(config-if)# ppp chap password password
```

Chapter 4

ISDN and DDR

Integrated Service Digital Network menggunakan jalur atau teknologi digital dalam membangun WAN dengan jalur telepon biasa.

Dial on Demand Routing yaitu teknologi yang dikembangkan Cisco dalam membangun WAN untuk pemakaian dengan jalurtelepon biasa, sifatnya dial up dan tidak always on.

Istilah-istilah pada WAN

- Local loop = kabel atau media yang menghubungkan antara ISP dengan Costumer
- Demarcation = daerah titik pertemuan antara peralatan Costumer dan ISP
- CPE (Costumer Premises Equipment) = peralatan milik costumer dan berada di bawah tanggung jawab costumer.
- Central Office = Tempat dimana ISP menangani suatu daerah regional.

ISDN = Integrated Service Digital Network, mencoba membawa signal data dalam signal analog.

Peralatan-peralatan ISDN:

1. ISDN Switch ; terletak di provider
2. Terminal Equipment type 1 (TE1); peralatan yang kompatibel dgn ISDN
3. Terminal Equipment type 2 (TE2); peralatan yang tidak kompatibel dgn ISDN, Memerlukan Terminal Adapter
4. Terminal Adapter; peralatan yang menghubungkan ISDN dengan non ISDN
5. Network Termination type 1 (NT1); peralatan yang berfungsi mengubah 2 wire Menjadi 4 wire.
6. Network Termination type 2 (NT2); peralatan yang menghubungkan device-device yang kompatibel dengan ISDN.

Router yang built in NT1 ---- interface U

Router yang non built in NT1 ---- interface S/T

Voltase untuk interface S dan T sama, maka sering disebut interface S/T, voltase S/T dan U berbeda.

Keuntungan ISDN:

- 1.Membawa signal data,voice, video,dll
- 2.Call setup lebih cepat dibandingkan modem biasa
- 3.Pengiriman datanya lebih cepat (B channel,64 Kbps) dibandingkan modem biasa. 4.B channel untuk layer 2-nya biasanya menggunakan PPP
- 5.D channel untuk layer 2-nya menggunakan LAPD (Line Access Protocol D).

Cara kerja ISDN:

- 1.Channel D akan melakukan pen transmitan signal Call Setup
- 2.Apabila D channel ok, maka B channel baru bisa melakukan pengiriman
- 3.B channel up apabila ada pengiriman data sedangkan D channel akan selalu up

Koneksi ISDN dibagi 2:

1. BRI (Basic Rate Interface)

Digunakan pada network skala kecil

2 B----64 Kbps =128 Kbps

1 D----16 Kbps

48 Kbps untuk framing dan syncronisasi

Total 192 kbps, tapi efektif rate 144 Kbps contoh : Indonesia

2.PRI (Primary Rate Interface)

Digunakan pada network skala besar, terdapat 2

jenis: a.T1 23 B----64Kbps =1472 Kbps

1D----64 Kbps

8 Kbps untuk frame dan sinkronisasi

Total 1544 Kbps, contoh : Jepang dan North America

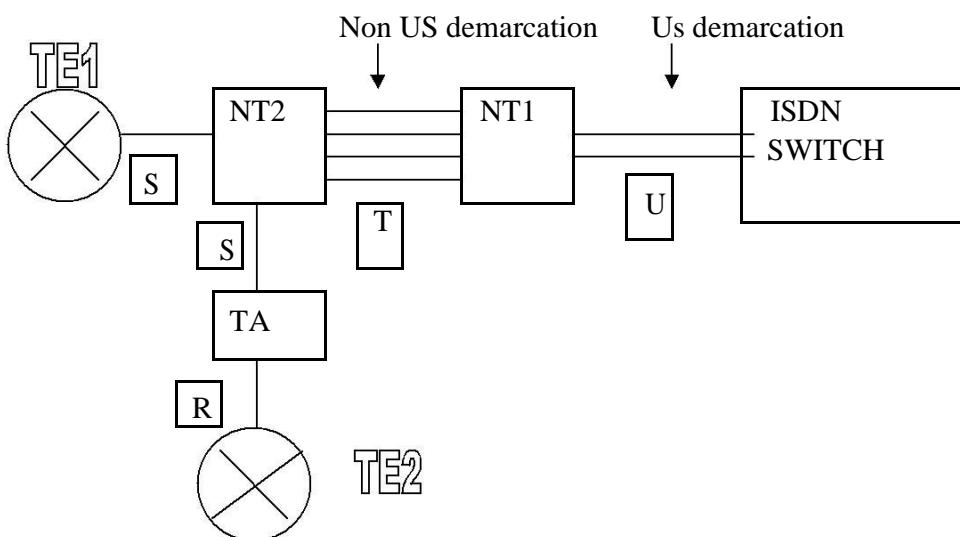
b.E1 30 B---64 Kbps =1920Kbps

1 D----64 Kbps

64 Kbps untuk frame dan sinkronisasi

Total 2048 Kbps, contoh: Eropa.

ISDN Reference Point:



Titik-titik Refrence:

R: menghubungkan TE2 ,device yg tidak kompatibel ISDN, untuk itu diperlukan TA

S: menghubungkan TE1,device kompatibel ISDN, tidak memerlukan TA.

T: menghubungkan NT2 ke NT1 yang merupakan jalan menuju costumer devices.

U: local loop yang menghubungkan antara provider dengan NT1, awal jalan/ route ke Costumer device

SPID (Service Profile Identifier)

Nomor yang digunakan untuk koneksi line ISDN (di dapat dari ISP), selain SPID terdapat pula LDN (Local Dial Number) yang menyertai SPID dalam konfigurasi .

SPID = no telepon + tambahan nomor dari ISP
LDN = no telepon yang digunakan.

Konfigurasi ISDN.

1. Interface BRI

a. tentukan switch type dari provider.

```
Router (config) # isdn switch-type switch
typenya Atau
Router (config) # int bri 0
Router (config-if) # isdn switch-type switch type
```

b. masukkan spid nya (optional)

```
Router (config) # int bri 0
Router (config-if) # isdn spid1 spid number [ldn] optional
Router (config-if) # isdn spid2 spid number [ldn] optional
```

2. Interface PRI

a. tentukan switch-type dari provider (untuk di global config)

b. tentukan controller yang digunakan

```
Router (config) # controller t1/e1
```

c. tentukan framing yang digunakan

```
T1- Router (config-controller) # framing sf/esf
E1- Router (config-controller) # framing crc4/no-crc4
```

d. tentukan line coding- untuk signaling method layer1/encoding

```
Router (config- controller) # line code ami/b8zs/hdb3
North America/T1    Eropa/E1
```

e. setting slot time

```
Router (config-controller) # pri-group timeslots
range Dimana range T1----1-24
E1----1-31
```

f. tentukan interface PRI / D channel yang digunakan. Untuk interface

PRI digunakan serial yang terhubung ke T1/E1

```
Router (config) # int serial [port/slot] :
channel Dimana channel T1----23
E1----15
```

Contoh: T1

```
Router (config) # isdn switch-type primary-
ni Router (config) # controller t1 1/0
Router (config-controller) # framing esf
Router (config-controller) # linecode b8zs
Router (config-controller) # pri-group timeslots 1-24
Router (config-controller) # interface serial 3/0 : 23
```

Contoh: E1

```
Router (config) # isdn switch-type primary-ni
Router (config) # controller e1 1/0
Router ( config-controller) # framing crc4
Router (config-controller ) # linecode hdb3
Router ( config-controller) # pri-group timeslots 1-31
Router (config-controller) # interface serial 3/0 : 15
```

Troubleshooting ISDN:

1. Router # debug isdn q921
untuk melihat layer 2 isdn switch-isdn
2. Router # debug isdn q931
untuk lihat layer 3. Call setup& tear down messageexchange
3. Router # show dialer
untuk melihat nomer siapa yang dihubungi, alas an hub, status dari hub sekarang dan lama waktu hubungan.
4. Router # show int bri
untuk menampilkan statistic int BRI + encapsulasi + LCP NCP
5. Router # show isdn status
untuk melihat status layer, pastikan layer 1=aktif, layer2=multiple frame establish
6. Router # show isdn active
untuk melihat info keseluruhan detail ISDN (nomer dial & koneksi)

DDR (Dial on Demand Routing)

DDR mirip dengan ISDN, hanya saja mengenal idle time out yang bilamana habis, koneksi akan dilakukan koneksi ulang.

Idle timeout dinyatakan dengan interesting packet/ interesting traffic.

Cara kerja Router yang DDR-enabled:

- 1.Saat paket tiba di router, akan dilihat routenya menuju ke network mana?
- 2.Bila router DDR-enabled, akan dilihat apakah paketnya interesting atau tidak.
- 3.Biasanya paket yang dikirimkan adalah interesting dan un interesting.
- 4.Un interesting paket isinya adalah data dan routing protocol.

DDR dibagi 2 jenis:

- a. Legacy DDR
- b. Dialer DDR

Legacy DDR

Digunakan saat koneksi DDR point- topoint, terdapat interface physical (BRI) dan perlu di konfigurasi juga untuk interface logical (dialer)

Interesting paket dinyatakan oleh dialerlist, perhatikan nomor-nomor konfigurasi yang harus sama;

- a.dialer list dengan dialer group
- b.dialer pool-member dengan dialer pool.

dialer pool-member biasanya pada interface physical sedangkan dialer pool pada interface logical.

Command-command Legacy DDR:

```
router (config)# isdn switch-type type
router (config)# ip route net tujuan subnetmask interface/next hop
ip router (config)# username name password password
router (config)# dialer list number* protocol protocol
permit/deny router (config)# interface bri 0 ->physical
router (config-if)# ip address ip subnetmask
router (config-if)# encapsulation ppp
router(config-if)# ppp authentication chap      ( number* = harus sama )
router (config-if)# isdn spid1 spid ldn
router (config-if)# isdn spid2 spid ldn
router (config-if)# dialer-group number*
router (config-if)# dialer idle-timeout time second & default 120
router (config-if)# dialer map ip ip tujuan name host name tujuan ldn
tujuan router (config-if)# dialer pool-member nomor member*

router( config)# interface dialer 0 & logical
router(config-if)# dialer remote-name host name
tujuan router (config-if)#dialer string ldn tujuan1
router (config-if)# dialer string ldn tujuan2 ( nomor member* = harus sama ) router
(config-if)# dialer pool nomor member*
```

Dialer Profile

Dialer profile melakukan assign ip address pada interface logical (int dialer) sehingga dapat menggunakan banyak ip pada interface physical (dimasukan secara logical). Dialer profile digunakan dalam menghubungkan router dengan router pada site lain dalam jumlah lebih dari satu. Bila hanya point to point dapat menggunakan legacy DDR.

Command command Dialer Profile

```
router (config)# isdn switch-type type
router (config)# ip route net tujuan subnet next hop ip/out going
int. router (config)# username name password password
router (config)# dialer list number* protocol protocol permit/deny
router (config)# interface dialer number
router (config-if)# ip address ip subnetmask
router (config-if)# encapsulation ppp          ( number* = harus sama )
router(config-if)# ppp authentication chap
router (config-if)# dialer idle-timeout time second & default
120 router (config-if)# dialer-group number*
router(config-if)# dialer remote-name host name
tujuan router (config-if)#dialer string ldn tujuan1
router (config-if)# dialer string ldn tujuan2
router (config-if)# dialer pool pool number*
router (config-if)# no shutdown
router (config)# interface bri number
router (config-if)# isdn spid1 spid ldn      ( pool number* = harus sama )
```

```
router (config-if)# isdn spid2 spid ldn
router (config-if)# encapsulation ppp
router(config-if)# ppp authentication chap
router (config-if)# dialer pool-member pool
number* router (config-if)# no shutdown.
```

Chapter 5

Frame Relay

Frame relay sifatnya packet switching, connection oriented, dan membentuk sebuah virtual circuit (VC).

Virtual circuit yaitu, jalur antara source dengan destination, terdapat 2 jenis,:

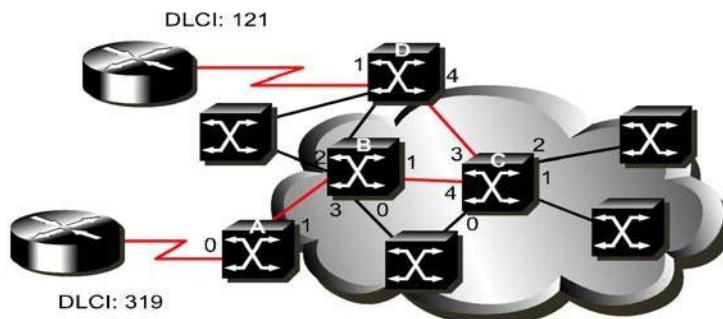
- Permanent VC / PVC sifatnya fixed
- Switched VC / SVC tidak fixed dan jalur akan dibuat ulang bila waktunya habis.

Standart untuk frame relay dibuat ITU-T dan ANSI, melalui pengiriman dengan frame, encapsulation yang digunakan adalah LAPF (Line Access Procedure for Frame).

Frame pada Frame relay

| | | | | |
|------|---------|------|-----|------|
| Flag | Address | Data | FCS | Flag |
|------|---------|------|-----|------|

Pada bagian address terdapat Data link channel identifier yang merupakan nomor identitas pada tiap site.



Virtual circuit dibuat dari tiap router /DTE ke site DTE lain dengan menggunakan nomor DLCI.

Istilah- istilah pada Frame Relay

a. Committed Information Rate (CIR)

Bandwidth pada frame relay yang di assign oleh provider, besarnya menentukan 'lebar

'pita data' yang digunakan dalam transfer data pada data frame relay switch cloud.

b. Discard Eligible (DE)

Bila data yang dikirim melebihi CIR yang ditentukan , maka ditandai sebagai DE, dan

bila data yang dikirim pada frame relay switch cloud menumpuk , maka data atau paket yang ditandai dengan DE akan di discard terlebih dulu.

c. Explicit Congestion Notification (ECN)

Bila terjadi kongesti pada jaringan frame relay switch, maka notifikasi dikirim ke router DTE sebagai pemberitahuan, ada 2 :

- **Back ward Explicit Congestion Notification (BECN)** notifikasi yang dikirimkan dari frame relay switch ke router DTE.
- **Forward Explicit Congestion Notification (FECN)** notifikasi yang dikirimkan dari router DTE ke frame relay switch sebagai reply.

d. Local Management Interface (LMI)

Hubungan yang pertama kali dibuat antara router DTE dan frame relay switch. macam- macam LMI:

- Cisco = default Cisco
- Ansi = standart ANSI
- Q 933a = standart ITU-T

e. Data Link Channel Identifier (DLCI)

Nomer- nomer pada router DTE yang digunakan sebagai patokan dalam mengirim paket ke destination, DLCI table dapat dibuat dengan Inverse ARP

f. Committed Time (Tc)

waktu yang diperlukan untuk mengirim paket sampai ke tujuan, satuan second.

g. Committed Burst (Be)

Rate yang didapat dari ; $Be = CIR \times Tc$
menentukan rate pengirim paket ke tujuan based on CIR dan Committed time.

Contoh perhitungan CIR, Be dan Tc

pengiriman paket frame relay sampai destination memerlukan waktu 0,5 second, bandwith yang disetujui provider yaitu 12.800 bps, berapa rate untuk mengirim paket ke tujuan?

$$\begin{aligned}CIR &= 12.800 \text{ bps}, Tc = 0,5 \text{ second}, Be = CIR \times \\Tc \quad Be &= 12800 \times 0,5 \rightarrow Be = 6400 \text{ bit}\end{aligned}$$

h. Virtual Circuit (VC)

Jalur pada frame relay network yang dibentuk berdasarkan nomer DLCI antara router source dan destination.

Frame relay adalah teknologi shared service dengan kecepatan ± 4 Mbps (teoritis) Frame relay baru terasa kegunaannya di multiple site interconnected dan kurang cocok untuk koneksi point to point.

Topology Frame relay

Topology wan biasanya star, dimana centralnya menyediakan primary service dan terhubung ke remote site yang membutuhkan servicenya.

1. Hub and Spoke topology

Hub (central sitenya) di letakan di leased line dengan lowest cost.

Pada topologi star frame relay, remote site terhubung ke central site dengan sebuah VC.

Hub (central sitenya) punya banyak VC, 1 VC ke 1 remote site.

Hub (central site) tidak perlu berada di tengah secara geografis, karena biaya frame relay tidak berdasar pada jarak.

Router remote = single access 1 VC Router

central = single access multiple VC

topology ini lebih sering dipakai

2. Full Mesh topology

Digunakan bila service yang ingin di akses tersebar dimana-mana secara geografis dan

butuh akses dengan tingkat reliable yang tinggi.

Tiap site saling terkoneksi 1 dengan lainnya. Bila memakai leased line butuh tambahan

hardware untuk membuat full mesh, tapi bila memakai frame relay hanya memerlukan

konfigurasi tambahan VC.

Access pada multiple VC frame relay lebih bagus dari pada single VC, karena built in

statistical multiplexing (transmit data bisa lewat 4 jalur –sejenis load balancing)

Untuk large network, full mesh kurang menguntungkan karena jumlah link yang dibentuk. tiap link dibatasi punya VC < 1000.

Frame relay ↗ Non Broadcast Multi Access (routing update tidak di broadcast) karena; kebanyakan routing protocol memakai split horizon (routing update yang diterima dari 1 interface tidak akan di broadcast melewati interface tadi) untuk menghindari routing loop.Karena frame relay memakai banyak VC dalam 1 physical interface.

Frame relay function;

1.ambil paket data dari network protocol (ip atau ipx

) 2.encapsulate jadi frame

3.lewati frame secara physical (EIA/TIA-232,449,530, V.35, X.21)
dalam framenya ada flag field, besarnya 1 byte. polanya; 01111110

Serial connection/ access link ke frame relay network biasanya: -

Leased line . access speed/port speed sekitar 64kbps-
4Mbps -PVC, tiap VC, speed dibatasi oleh CIR.

Command-command pada Frame Relay

a.Membuat encapsulation pada interface.

```
router (config) # encapsulation frame relay [ ief ]
```

b.Membuat map pada frame relay

```
router ( config-if) # frame-relay map ip ip tujuan dlci [ etf ] broadcast
```

c.Membuat route frame relay(biasanya pd frame relay switch)

```
router (config -if)# frame-relay route dlci local interface int number dlci  
tujuan
```

Command- command Show

a. Melihat permanent Virtual Circuit (PVC

```
) router # show frame-relay pvc
```

b. Melihat frame relay LMI

```
router # show frame-relay lmi c.
```

Melihat mapping- on frame relay

```
router # show frame-relay map
```

Command- command Debug

a. router # debug frame-relay packet

b. router # debug frame-relay lmi

c. router # debug frame-relay events.

Chapter 6

Introduction to Network Administration

Workstation

Workstation adalah client computer yang terhubung dengan server untuk memperoleh data yang di-share dengan komputer lain. Pada workstation, terdapat program untuk menentukan apakah commands ditujukan untuk local client atau untuk server, dan kemudian melanjutkan command-nya ke local operating system atau ke NIC untuk diproses. Nama lain yang biasa digunakan untuk workstation adalah client.

Server

Server adalah komputer yang menggunakan NOS (Network Operating System). Server biasanya mempunyai spesifikasi yang tinggi untuk men-support multiple users dan multitasking dan biasanya sudah dikonfigurasi untuk menggunakan protokol internet yaitu TCP/IP.

Server juga digunakan untuk meng-autentikasi users dan menyediakan akses ke shared resources. (seperti printer)

Aplikasi dan fungsi yang tersedia pada server:

- Web services protocols: HTTP, FTP dan DNS.
- Standard e-mail protocols: SMTP, POP3 dan IMAP.
- File sharing protocols: NFS dan SMB.
- DHCP dan NAT

NOS biasanya di-desain mengikuti model client-server untuk menyediakan network services kepada user.

Network Operating System (NOS)

NOS memungkinkan komunikasi antara beberapa devices dan sharing resources di sebuah network. Contoh NOS adalah Linux, Windows NT, Windows Server 2000, Netware.

Fitur-fitur yang perlu diperhitungkan saat memilih sebuah NOS adalah performance, management and monitoring tools, security, scalability dan fault tolerance.

NETWORK MANAGEMENT

Semakin sebuah network berkembang, maka akan menjadi semakin kompleks dan untuk me-maintain-nya akan lebih sulit. Network management diperlukan untuk mengatasi hal ini.

Tugas-tugas dalam Network Management:

- memonitor network availability
- improvisasi automation
- memonitor response time
- menyediakan security
- rerouting traffic
- kemampuan untuk restore
- mendaftarkan user

Terdapat 4 model Network Management yang dibuat oleh the International Standards Organization (ISO), yaitu:

- **Organization:** mendeskripsikan komponen-komponen dari network management seperti manager, agent, dll.
- **Information:** berhubungan dengan struktur dan penyimpanan informasi tentang network management
- **Communication:** tentang bagaimana data-data management dikomunikasikan antara agen dan manager.
- **Functional:** berhubungan dengan aplikasi network management yang terdapat pada network management station (NMS).

Terdapat 2 protocol standard, yaitu:

- **Simple Network Management Protocol (SNMP)**, oleh IETF community
- **Common Management Information Protocol (CMIP)**, oleh Telecommunications community

SNMP dipilih sebagai standard untuk internet TCP/IP, dan kemudian menjadi sangat populer sehingga kemudian di-upgrade dan menjadi SNMP version 2c. SNMPv2c menyediakan support untuk centralized dan distributed network management dan terdapat improvisasi dalam berbagai hal. Setelah itu, SNMPv3 dirilis untuk memperkuat security dengan meng-autentikasi dan mengenkripsi paket. SNMP terdapat pada layer application dan didesain untuk menfasilitasi pertukaran informasi management antara devices. SNMP adalah protocol yang paling populer untuk me-maintain berbagai network.

Model organisasional untuk SNMP ada 4 element:

- Management station
- Management agent
- Management information base

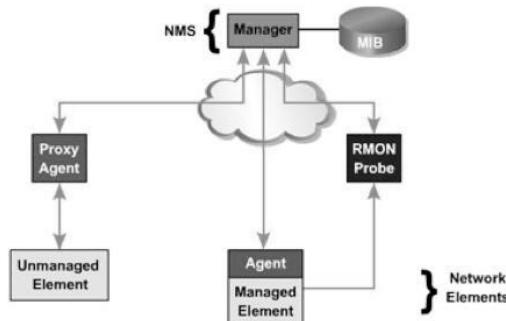
- Network management protocol

Network management station (NMS) biasanya adalah sebuah workstation dan terdapat serangkaian software yang dinamakan network management application (NMA). Pada NMA terdapat user interface agar network manager dapat mengatur network. NMA menanggapi command dari user dan meneruskan command ke management agents di network. Management agents adalah network devices seperti routers, bridges, hubs dan host lain, yang masing-masing terdapat SNMP.

Komunikasi antara NMS dan management agents menggunakan UDP di port 161 dan 162. Ada 3 message type umum:

- **Get:** Untuk management station mengambil value dari MIB object yang terdapat pada agent.
- **Set:** Untuk management station men-set value dari MIB object yang terdapat pada agent.
- **Trap:** Untuk agent memberitahukan management station apabila ada events penting.

Proxy agent digunakan untuk kebutuhan translasi antara proprietary management interface dengan manager. RMON digunakan untuk membagi fungsi network management dari NMA.



Management Information Bases (MIB)

MIB digunakan untuk menyimpan informasi tersstruktur tentang network elements dan atributnya. Struktur ini terdapat pada standard bernama SMI yang mempunyai data types yang bisa dipakai untuk menyimpan object, bagaimana menamai object dan bagaimana meng-encode object untuk transmisi.

SNMP protocol

Terdapat 3 tipe SNMP message yang dikirim NMS, yaitu GetRequest, GetNextRequest dan SetRequest. 3 message ini akan diterima agent dengan mengembalikan GetResponse message. Agent bisa mengirim Trap message untuk merespon event yang merubah MIB.

Kelebihan SNMPv3 dari SNMPv2 adalah terdapat GetBulkRequest message type dan penambahan 64-bit counter di MIB. SNMPv3 juga menggunakan autorisasi yang terenkripsi.

Configuring SNMP

Agar NMS dapat berkomunikasi dengan device lain, device-device tersebut harus memiliki SNMP yang di-enabled dan SNMP community string nya sudah dikonfigurasi.

Untuk men-set community string yang dipakai agent:

```
Router(config)#snmp-server community string ro
```

Untuk men-set read-write community string yang dipakai agent:

```
Router(config)#snmp-server community string rw
```

Beberapa string bisa dipakai untuk menentukan lokasi device dan system contact device:

```
Router(config)#snmp-server location text
```

```
Router(config)#snmp-server contact text
```

Syslog

Syslog utility adalah suatu mekanisme agar aplikasi, proses dan OS dari cisco devices dapat mencatat keadaan aktivitas dan error.

Ada 8 level security yang mengindikasi sifat error message, 0 adalah yang paling kritis dan 7 paling tidak kritis.

Untuk enable logging:

```
Router(config)#logging on
```

Untuk mengirim log messages ke syslog server host:

```
Router(config)#logging hostname | ip address
```

Untuk men-set logging severity level ke level 6, informational:

```
Router(config)#logging trap informational
```

Untuk memasukkan timestamp di message syslog:

```
Router(config)#service timestamps log datetime
```