

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 Messages	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 dikonfigurasi 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 dikonfigurasi 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 scability
- Basic routing dan switching

Command-Line Internface (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:

aaa - bbb - ccc

↑ ↑ ↑

platform feature format

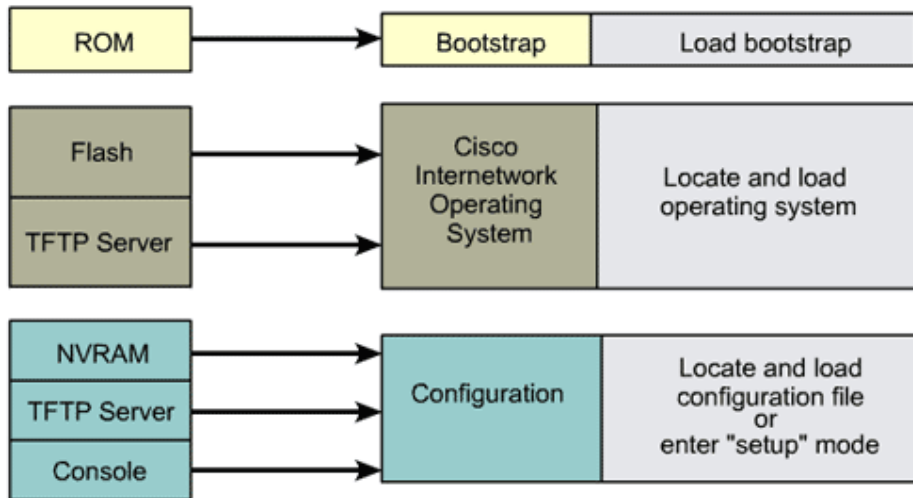
IOS mempunyai 3 environment utama, yaitu: ROMMON (Rom Monitor), Boot ROM dan IOS.

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**.

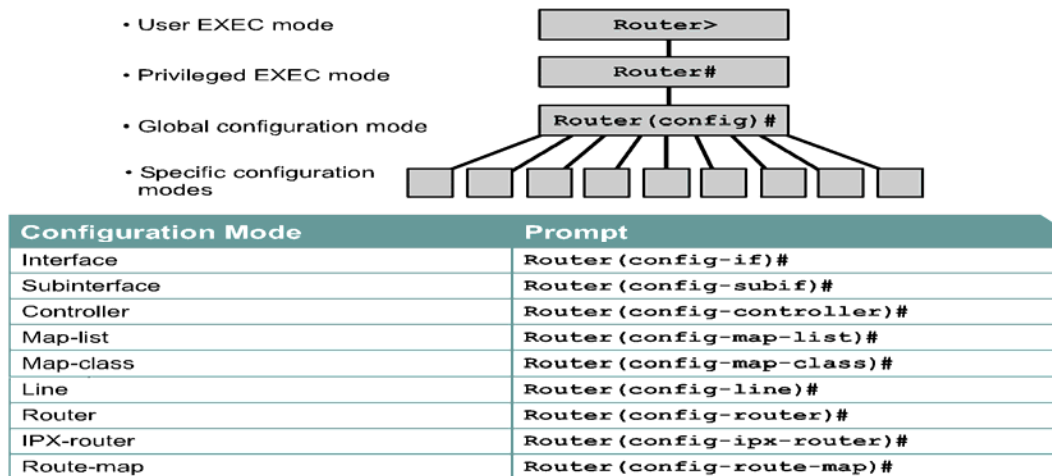
Command **show version** memunculkan informasi berikut:

- 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

Console Password

```
Router (config) #line console 0
Router (config-line) #login
Router (config-line) #password 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 privileged 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 privileged, paling aman dan sudah terenkripsi)

```
Router(config)#enable secret <password>
```

-Setting interfaces

Konfigurasi / setingan 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
```

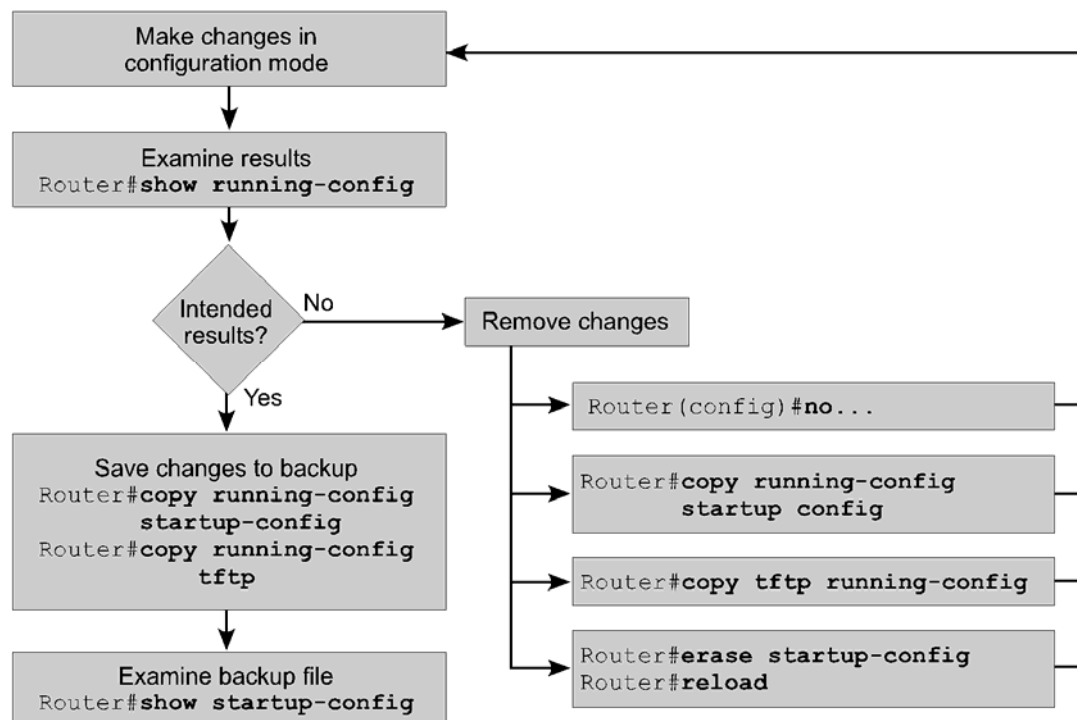
Settingan untuk save running configuration ke startup configuration file di NVRAM, masukan command di privileged mode:

```
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 memungkinkan network administrator dapat men -type apakah host name seperti Auckland atau IP address untuk Telnet ke remote host. Contoh host table.

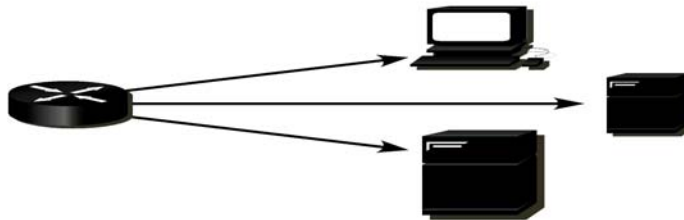
```
Router (config) #ip host Auckland 172.16.32.1
Router (config) #ip host Beirut 192.168.53.1
Router (config) #ip host Capetown 192.168.89.1
Router (config) #ip host Denver 10.202.8.1
```

Settingan host table:

1. Masuk ke global configuration mode .
2. Masukkan 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 konfigurasi 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.

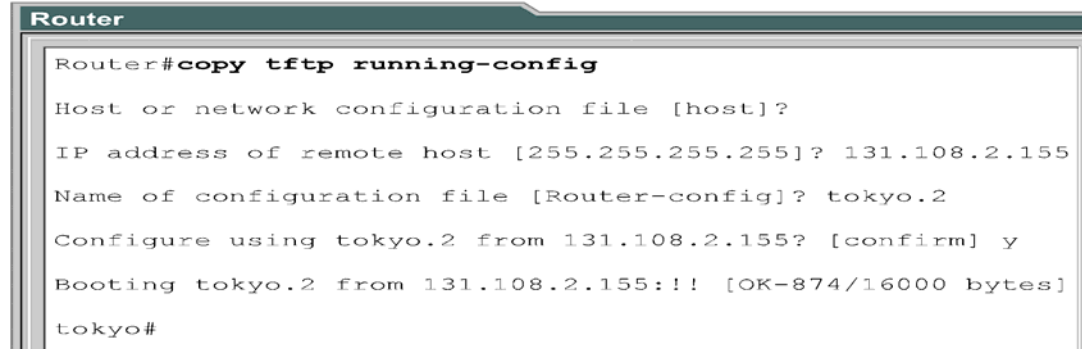
Step 3 Enter name dari configuration file.

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

Upper Layer Entry Addresses	TCP/IP	Novell IPX	AppleTalk	Others
Cisco Proprietary Data-Link Protocol	CDP discovers and shows information about directly connected Cisco devices			
Media Support SNAP	LANs	Frame Relay	ATM	Others

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 tetangganya, 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.

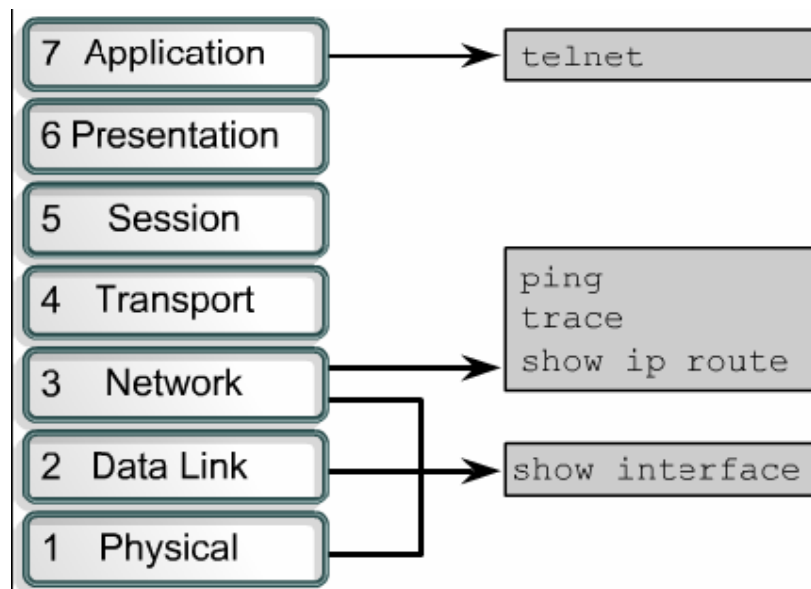
Command	Description
clear cdp table	Deletes the CDP table of information about neighbors.
clear cdp counters	Resets the traffic counters to zero.
show cdp traffic	Displays CDP counters, including the number of packets sent and received and checksum errors.
show debugging	Determines which types of debugging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

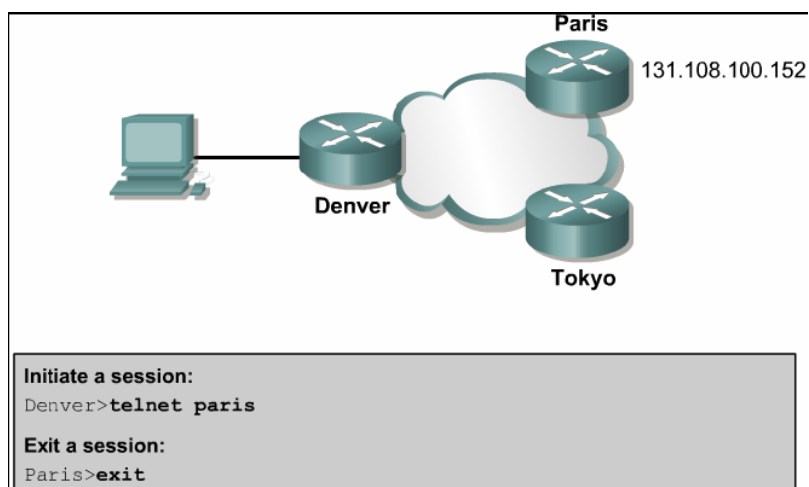
layer aplikasi antara asal dan tujuan. Fungsi telnet pada layer aplikasi OSI layer. Telnet tergantung dari TCP untuk menggaransi data antara client dan server.



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
- ☐ Diikuti 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

Initiate a session

Denver>telnet paris

End a session

Paris>exit

Suspend a session

Paris><Ctrl><Shift><6><x>

Denver>

Resume a session

Denver><Enter>

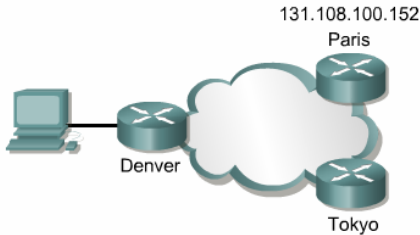
Disconnect a session

Denver>disconnect paris

Display sessions

Denver#show sessions

Conn	Host	Address	Idle	Conn Name
1	Paris	131.108.100.152	0	Paris
2	Tokyo	126.102.57.63	0	Tokyo



cara kerja telnet

Testing koneksi dengan PING

Perintah **tracert** 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 **tracert** 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 **tracert**:

- Masukkan perintah **tracert** 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

|

|

|

V

BootStarap.POST

|

|

V

Load IOS (Flash, TFTP server, ROM)

|

#1

#2

#3

|

V

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 unntuk:

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:

Sabua program daemon yg berjalan sbg service. Salah satu contoh programnya adalah 3C Daemon. TFTP server berguna untuk backup dan restore memanfaatkan Kabel LAN, karena itu sebelum melakukan 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”, arahkan 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 untuk 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 pertanyaan: “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 Ctrsl + Break sampai masuk ke rommon
2. rommon1>confreg 0x2142 [enter]
3. rommon2>i atau boot [enter]
4. copy start run
5. ganti password
6. Router(config)#config-register 0x2102 [enter]
7. copy run start
8. reload

Command untuk copy IOS ke tftp server pada computer adalah:

Router#copy flash tftp

Namun untuk 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
- memlihkan IOS pada ROMMON dengan Xmodem atau tftpdnld
- password recovery pada ROMMON:
 rommon>
 ROMMON dapat untuk password recovery, XModem, tftpdnld

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

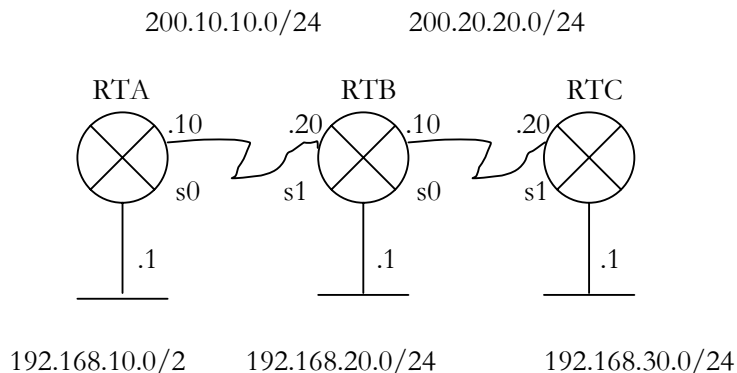
• **Melihat route :**

Router#show ip route

• **Melihat konfigurasi :**

Router#show run

Contoh :



Berdasarkan outgoing interface (gateway) :

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 distance 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 diasosiasikan 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 igmp events
- debug igmp transactions
- ping
- traceroute

Chapter 8

TCP/IP Suite Error and Control Messages

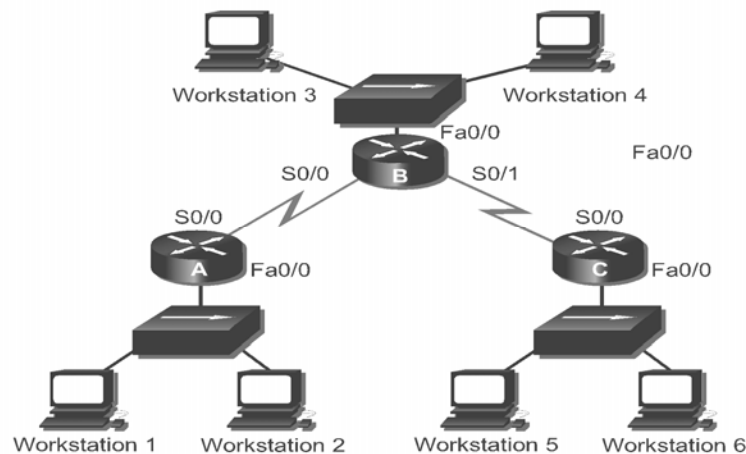
IP mempunyai keterbatasan dalam mengantar suatu data ketujuan, IP tidak mempunyai mekanisme untuk memastikan data tersebut telah sampai ke tempatnya, disebabkan hal seperti kerusakan hardware, konfigurasi yang tidak benar atau kesalahan routing informasi. Untuk mengatasi masalah diatas, IP menggunakan 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.

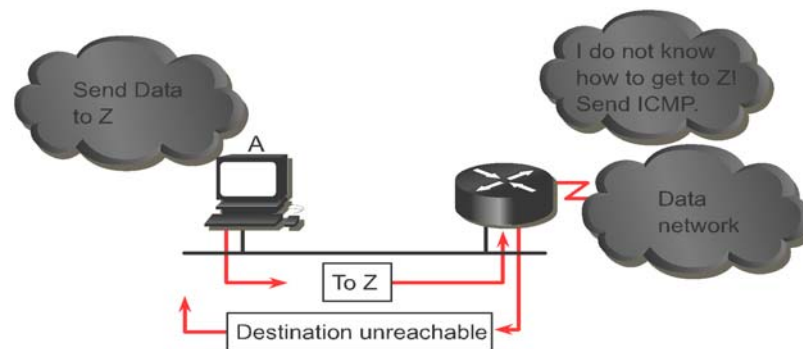
Frame Header	Datagram Header	ICMP Header	ICMP Data
Frame Header	Datagram Header	Datagram Data Area	
Frame Header	Frame Data Area		

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

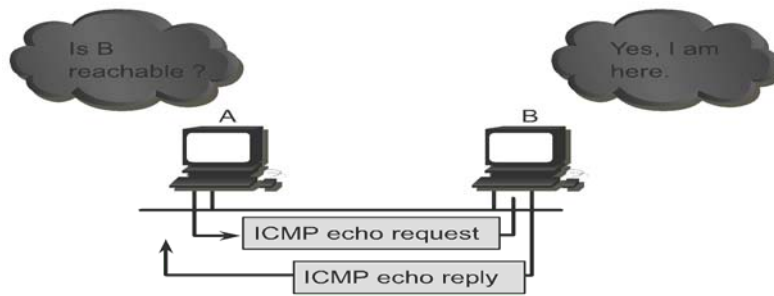
Network communication dapat terjadi jika; *Satu*, sending and receiving devices harus punya TCP/IP protocol yang di configure dengan benar. Ini meliputi peng install an TCP/IP protocol dan peng konfigurasi dari IP address and subnet mask yang tepat. Default gateway harus di konfigurasi jika datagrams 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 konfigurasi 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 mem ferifikasi 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

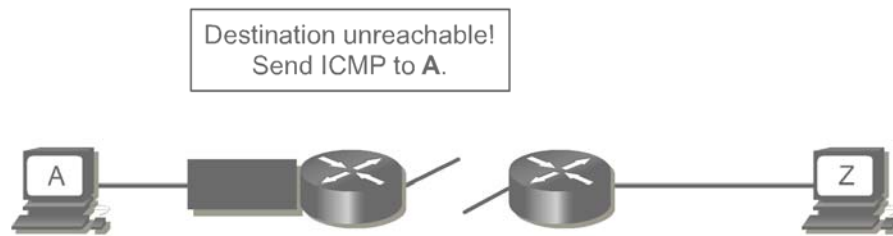
Gambar. ICMP message type.

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

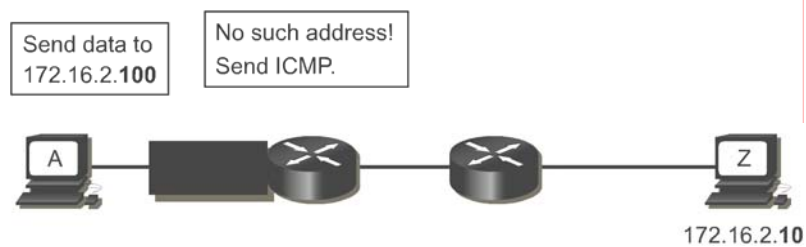
Gambar. Message format for the ICMP echo request and echo reply messages.

Jika Router tidak dapat mengirim paket ke destination, router akan mengirim ICMP "Destination Unreachable" message kembali ke sumbernya untuk menginformasikan terjadinya masalah. Router akan mengabaikan paket asli. Destination tidak terjangkau bisa disebabkan oleh host pengirim memasukkan alamat yang salah, atau router tidak mempunyai rute untuk ke destination. Jika router tidak dapat mengirim balik ICMP message dengan alasan apapun, maka undeliver ICMP message akan diabaikan.

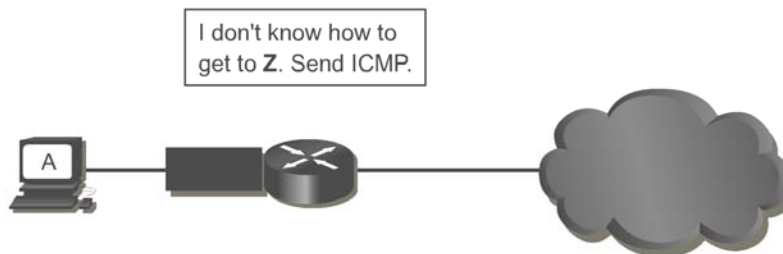
Beberapa kegagalan yang menyebabkan ICMP message terjadi:



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.

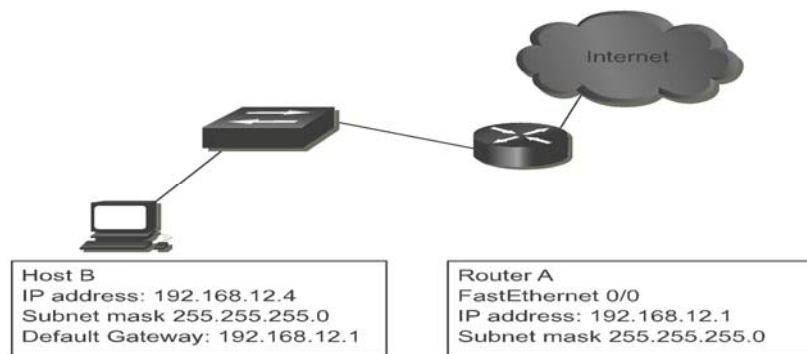
TCP/IP Suite Control Messages

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 perjalanannya 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 mengidentifikasi 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 broadcast 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	

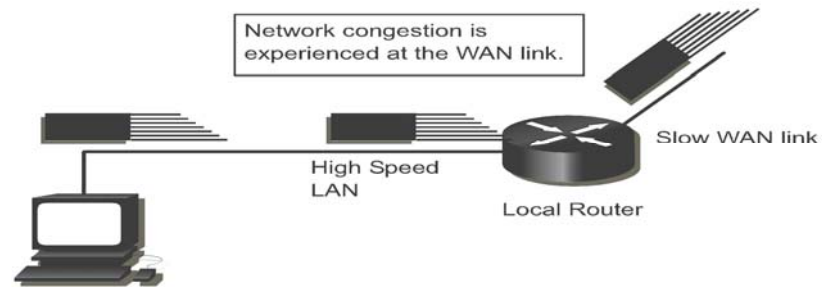
Gambar.keterangan dari tiap field.

Congestion and flow control messages

Jika multiple komputer mencoba untuk access ke destination dan waktu 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 factor untuk menghitung metric. Contohnya, RIPv1 menggunakan hop count sebagai factor menentukan metric. Protokol yang lain berdasarkan hop count, bandwidth, delay, load, reliability dan cost.

Faktor seperti bandwidth dan delay adalah statis karena mereka 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 factor statis bandwidth dan delay untuk menghitung secara manual untuk mengontrol mana jalur yang akan dipilih. IGRP juga dikonfigurasi untuk factor dinamis load dan reliability dalam perhitungan metric. Dengan menggunakan factor 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:

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

Nilai konstanta default $K1 = K3 = 1$ dan $K2 = K4 = K5 = 0$

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

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

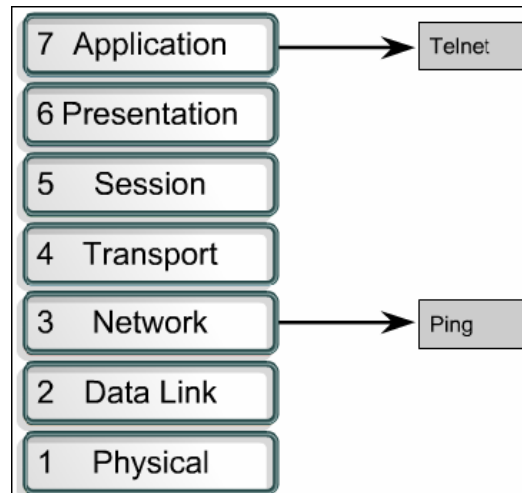
IGRP mendukung load balancing dengan cost tidak sama, yang disebut dengan variance. Perintah variance memerintahkan router supaya merutekan metric kurang dari n kali metric minimum untuk tujuan tersebut, dimana n adalah angka dari variance. Variabel n nilainya antara 1 sampai 128, dengan nilai default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

2. Testing jaringan

2.1 Pendahuluan

Dasar testing jaringan harus diproses secara sequence dari OSI layer. Dimulai dari layer 1 sampai ke layer 7, jika perlu. Pada layer 1, kelihatan 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 memungkinkan 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 konek 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 seting enkapsulasi
- Kesalahan seting 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 konektivitas. 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 keeplive
- 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

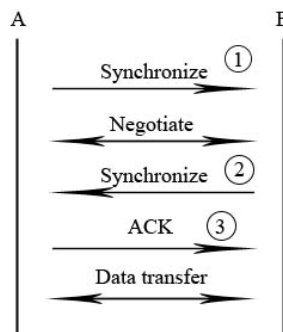
Intermediate TCP/IP

Fungsi dari transport layer :

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

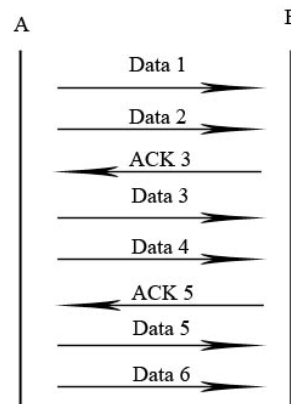
TCP / IP merupakan gabungan dari dua layer yaitu TCP pada layer 4 dan IP pada layer 3.

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 :

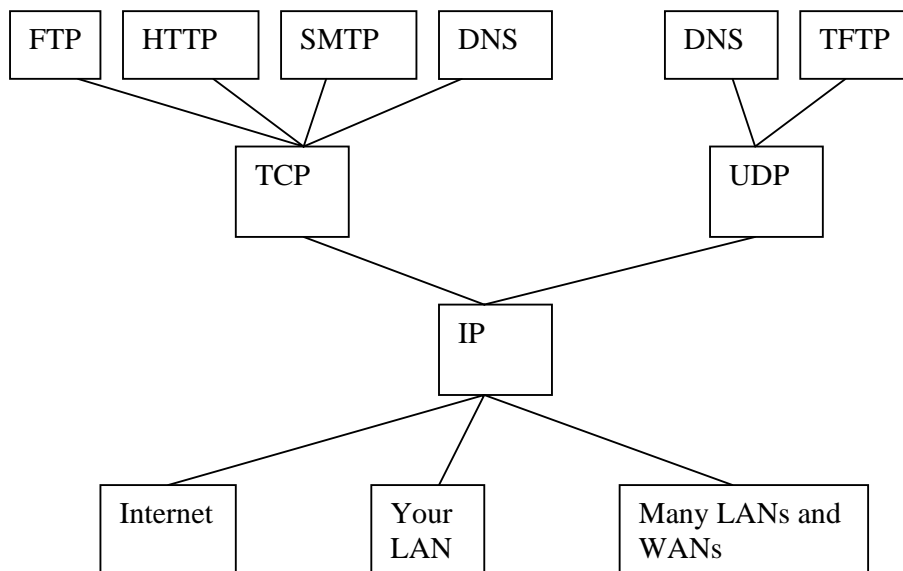


Sequence number digunakan untuk mengurutkan data agar sampai pada tujuan sesuai urutannya.

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 :

- **HTPP :**
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

Tujuannya :

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
	<hr/>	
	0000 01 00 .4	
	0000 01 11	0.0.0.3
	<hr/>	
	0000 1 000 .8	
	0000 1 111	0.0.0.7
	<hr/>	
	0001 0000 .16	
	0001 1111	0.0.0.15
	<hr/>	
	0010 0000 .32	
	0010 1111	0.0.0.15
	<hr/>	
	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 memblokir lalu lintas traffic yang tidak perlu.

Aturan-aturan dalam ACL :

- Menggunakan wildcard.
- Penulisan ACL sebaiknya dilakukan pada text editor, misalnya notepad, barulah dicopy ke Hyper Terminal.
- Standard ACL diletakkan dekat destination.
- Extended ACL diletakkan dekat source.
- Setelah dibuat pada global config, ACL harus diterapkan pada interface router.
- Perhatikan arah inbound atau outbound dalam meletakkan ACL pada interface.
- 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

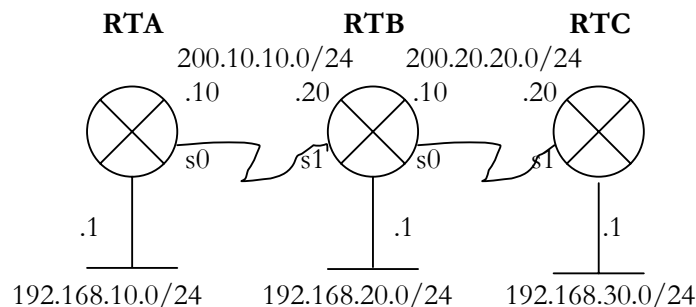
- Seluruh network dengan pernyataan :

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
```

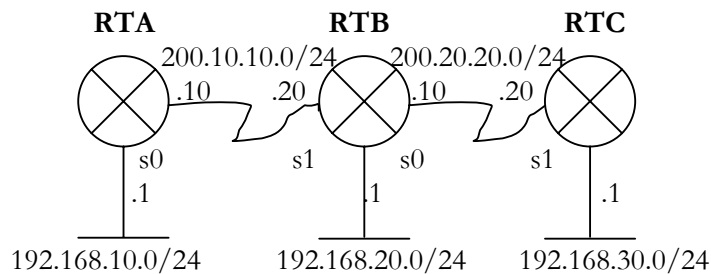
Terapkan pada interface :

```
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 eq 23
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 dan extended ACL yang telah kita pelajari merupakan numbered ACL, ada pula named ACL yang terdiri dari standard dan extended ACL

Contoh :

a) Named Standard ACL

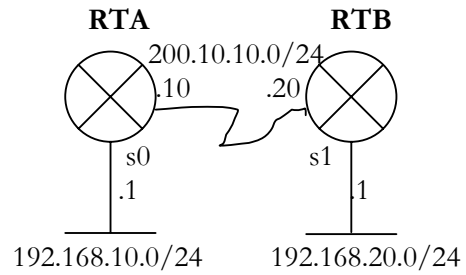
```
Router(config)# ip access-list standard namedacl
Router(config-std-nacl)# permit | deny sourcenetw wildcardsourcenetw
Router(config)#interface interface numberint
Router(config)#ip access-group namedacl in | out
```

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