# Modul 11 TCP/IP Suite Error dan Control Messages

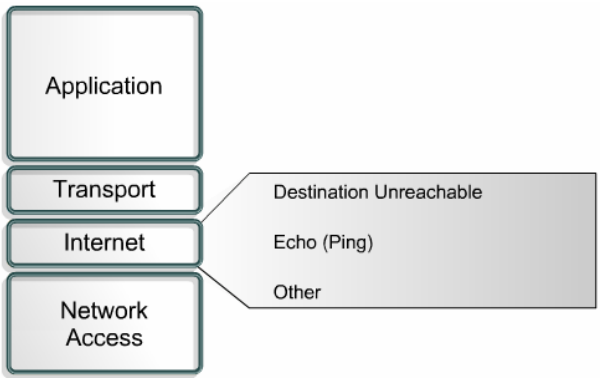
**Pendahuluan**
Tidak ada mekanisme untuk menjamin bahwa data yang dikirim melalui jaringan berhasil. Data mungkin gagal mencapai tujuan dengan berbagai macam alas an seperti kerusakan pada hardware, kesalahan konfigurasi, atau informasi routing yang salah. Untuk membantu mengidentifikasi kesalahan-kesalahan itu, IP menggunakan Internet Control Message Protocol (ICMP) untuk memberikan pesan ke pengirim data yang mengalami error pengiriman tersebut.

Karena IP tidak mempunyai mekanisme untuk pengiriman error dan control messages, ia menggunakan ICMP untuk mengirim dan menerima error dan control message ke host-host dalam jaringan.

Diharapkan setelah melalui modul ini, Anda dapat melakukan:

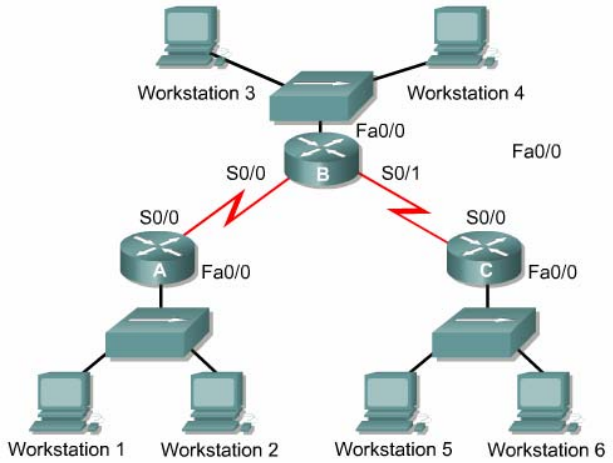
- Menggambarkan cara kerja ICMP
- Menggambarkan format pesan ICMP
- Mengidentifikasi tipe-tipe pesan error ICMP
- Mengidentifikasi sebab-sebab yang potensial pesan error ICMP
- Menggambarkan control messages ICMP
- Mengidentifikasi control messages yang digunakan di jaringan
- Menentukan pentebab untuk control messages ICMP

**1. ICMP**
IP menggunakan metode unreliable pada saat pengiriman data ke jaringan. Tidak ada proses untuk menentukan masalah saat pengiriman data ke jaringan. Jika terdapat kegagalan seperti router mati, atau jika device tujuan tidak terhubung ke jaringan, maka data tidak dapat terkirim. ICMP merupakan komponen dari protokol TCP/IP yang membantu IP untuk mengidentifikasi kesalahan-kesalahan itu.




**Gambar 1.1** Internet Control Message Protocol (ICMP)

1.1 Error reporting dan error correction
ICMP digunakan untuk report error yang dikembalikan ke datagram asal. Seperti yang digambarkan di bawah ini.




**Gambar 1.1.1** Error Reporting dan Error correction

Workstation 1 mencoba mengirimkan datagram ke workstation 6, tapi interface Fa0/0 pada router C mati. Router C menggunakan ICMP untuk mengirimkan pesan balik ke workstation 1. Pesan ini menunjukkan bahwa datagram tidak dapat terkirim. ICMP tidak dapat memperbaiki jaringan yang bermasalah, ia hanya memberikan report saja.

Pada saat router C menerima datagram workstation 1, ia mengetahui hanya alamat IP asal dan tujuan dari datagram. Ia tidak tahu jalur mana pastinya yang nanti akan diambil. Oleh karena itu router C hanya bisa memberi informasi ke workstation 1 tentang masalah yang terjadi dan tidak ada pesan ICMP yang dikirim ke router A dan router B. ICMP melaporkan status dari pengiriman paket hanya ke peralatan asal. Ia tidak mengirim informasi tentang perubahan jaringan ke router-router yang lain.

1.2 Pengiriman pesan ICMP

Pesan ICMP dienkapsulasi menjadi datagram dengan cara yang sama ke data yang dikirim ketika IP digunakan. Gambar di bawah ini menampilkan enkapsulasi data ICMP dalam datagram IP.

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

**Gambar 1.2.1** enkapsulasi pesan ICMP dalam paket IP

Ketika pesan ICMP ditransmisikan dengan cara sama dengan pengiriman data lain, maka mereka menjadi subjek ke masalah pengiriman yang sama. Untuk alas an ini, error diciptakan oleh pesan ICMP tidak membentuk pesan ICMP sendiri. Oleh karenanya, kemungkinan pengiriman error datagram yang tidak pernah dilaporkan balik ke pengirim data.

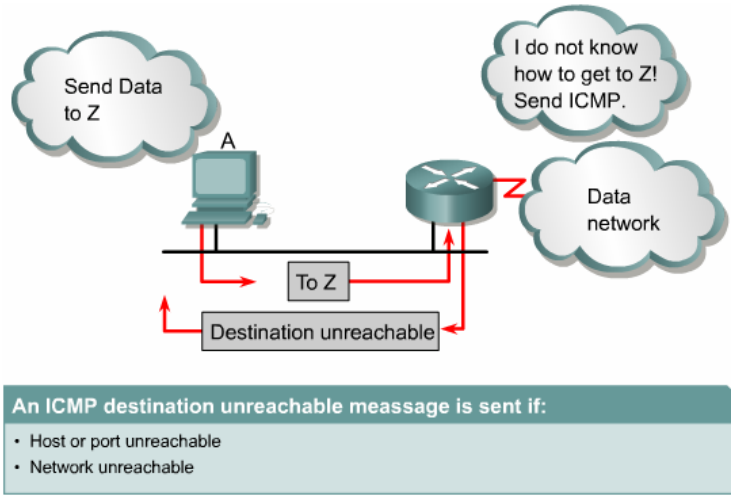
1.3 Network unreachable

Komunikasi di jaringan tergantung dari beberapa kondisi yang ditemui. Pertama, protokol TCP/IP harus dikonfigurasi untuk device yang mengirim dan menerima data. Termasuk pemasangan protokol TCP/IP dan konfigurasi alamat IP dan subnet mask. Default gateway juga harus dikonfigurasi jika

datagram keluar jaringan local. Kedua, device harus ditempatkan untuk melewatkan datagram dari device asal dan jaringannya ke device tujuan. Router juga harus mempunyai protokol TCP/IP yang dikonfigurasi di interface-interfacenya dan harus menggunakan protokol routing tertentu.

Jika kondisi tidak ditemukan, kemudian komunikasi jaringan tidak dapat dilakukan. Device pengirim mengalamatkan datagram ke IP address yang tidak ada atau ke device tujuan yang tidak terhubung ke jaringan. Router dapat juga sebagai titik kesalahan jika koneksi interface putus atau jika router tidak memiliki informasi yang berguna untuk menemukan jaringan tujuan. Jika jaringan tujuan tidak dapat diakses, hal seperti ini disebut dengan unreachable network.

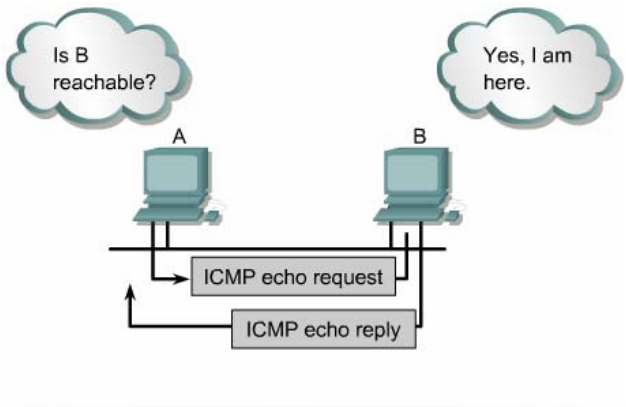
Gambar berikut ini menunjukkan router yang menerima paket yang tidak dapat dikirim. Paket tidak terkirim karena tidak mengetahui jalur ke tujuan. Oleh sebab itu, router mengirimkan pesan ICMP host unreachable ke asal.




**Gambar 1.3.1** Destination unreachable

1.4 Echo reply

Protokol ICMP dapqat digunakan untuk melakukan testing ke tujuan. Gambar di bawah menunjukkan pesan echo request ke device tujuan. Jika tujuan menerima echo request ICMP, ia memformulasikan pesan echo reply mengirim balik ke asal. Jika pengirim menerima echo reply, ini berarti bahwa tujuan dapat dicapai menggunakan protokol IP.




**Gambar 1.4.1** echo reply

Pesan echo request secara tipikal dihasilkan oleh perintah **ping** seperti yang ditunjukkan gambar berikut. Perintah ping digunakan dengan alamat IP dari device tujuan. Perintah dapat juga dimasukkan dengan alamat IP dari tujuan seperti yang ditunjukkan gambar.

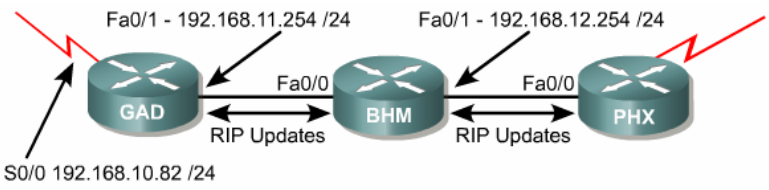
```
Microsoft Windows 2000 [Version 5.00.2195]
<C> Copyright 1985-2000 Microsoft Corp.

C:\> ping 198.133.219.25

Pinging 198.133.219.25 with 32 bytes of data:

Reply from 198.133.219.25: bytes= 32 time= 16ms TTL=247
Reply from 198.133.219.25: bytes= 32 time= 16ms TTL=247
Reply from 198.133.219.25: bytes= 32 time= 16ms TTL=247
Reply from 198.133.219.25: bytes= 32 time= 16ms TTL=247

Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 16ms, Average = 16ms
C:\>
```

**Gambar 1.4.2** Perintah ping

Pada gambar tampilan perintah ping, terdapat nilai time-to-live (TTL). TTL adalah field dalam paket header IP yang digunakan oleh IP untuk mem-forward paket. Ketika router menerima paket dengan TTL = 1, ia akan menurunkan nilai TTL ke 0 dan paket tidak dapat di-forward. Pesan ICMP dibangkitkan dan dikirim balik ke mesin asal dan undeliverable paket dibuang.

1.5 Hop count

Rute yang panjang dapat terjadi dalam jaringan dimana datagram tidak pernah mencapai tujuan. Hal ini terjadi jika dua router secara kontinu melewatkan datagram balik diantara router-router, yang mengasumsikan router yang lain sebagai hop berikutnya ke tujuan. Seperti yang dijelaskan pada gambar di bawah ini:




| Destination Address | Hop Count | Next Hop Address | Port |
|---|---|---|---|
| GAD Partial Route Table Entries | | | |
| 192.168.50.0 /24 | 14 | 192.168.10.83 | S0/0 |
| 192.168.10.0 /24 | 0 | --- | S0/0 |
| 192.168.11.0 /24 | 0 | --- | Fa0/1 |
| 192.168.12.0 /24 | 1 | 192.168.11.253 | Fa0/1 |
| BHM Partial Route Table Entries | | | |
| 192.168.50.0 /24 | 15 | 192.168.11.254 | Fa0/0 |
| 192.168.10.0 /24 | 1 | 192.168.11.254 | Fa0/0 |
| 192.168.11.0 /24 | 0 | --- | Fa0/0 |
| 192.168.12.0 /24 | 0 | --- | Fa0/1 |

**Gambar 1.5.1** hop count

Keterbatasan protokol routing dapat menyebabkan unreachable detination. Batas hop RIP adalah 15 artinya jaringan jumlah hop lebih dari 15 tidak akan mampu mempelajari melalui RIP.

1.6 Tipe-tipe pesan ICMP

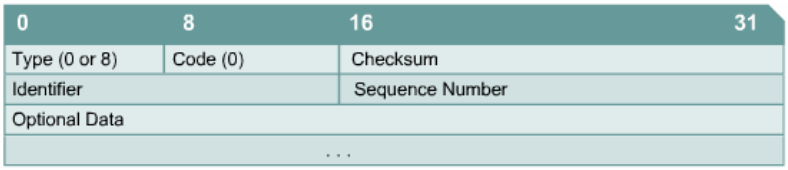
Pesan iCMP memiliki format khusus. Masing-masing tipe pesan ICMP ditunjukkan oleh gambar. Semua format pesan ICMP dimulai dengan tiga field yang sama:

- Type
- Code
- Checksum

| 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 1.6.1** Tipe-tipe pesan ICMP

Field tipe menunjukkan tipe dari pesan ICMP yang dikirim. Field code menunjukkan informasi yang khusus untuk tipe pesan. Checksum field sebagai tipe lain dari paket yang digunakan untuk mem-verifikasi integritas data.

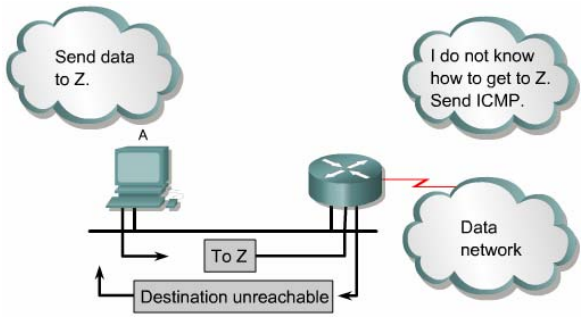



**Gambar 1.6.2** pesan echo request dan echo reply ICMP

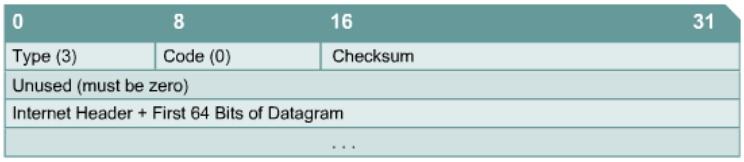
Gambar di atas menunjukkan format pesan echo request ICMP dan echo reply. Tipe yang cocok dan nomor kode ditunjukkan di tiap-tiap tipe pesan. Field identitas dan field sequence number sifatnya unik untuk pesan echo request dan echo reply. Field-field itu digunakan mencocokkan echo reply dengan echo request. Field data berisi informasi tambahan yang mungkin bagian dari echo reply atau echo request.

1.7 Pesan Destination Unreachable

Datagram tidak selalu dapat di-forward ke tujuannya. Masalah di hardware, konfigurasi protokol yang salah, interface mati dan informasi routing yang salah adalah factor-faktor penyebabnya. Dalam hal ini, ICMP mengirimkan pesan ke pengirim pesan destination unreachable dimana datagram tidak dapat di-forward ke tujuan.




**Gambar 1.7.1** Destination Unreachable




**Gambar 1.7.2** Pesan destination unreachable

Gambar di atas menunjukkan header pesan destination unreachable. Nilai 3 dari field tipe menunjukkan pesan destination unreachable. Nilai kode menunjukkan alasan paket dapat dikirim. Nilai kode 0 berarti jaringan unreachable.

| |
|---|
| 0 = net unreachable |
| 1 = host unreachable |
| 2 = protocol unreachable |
| 3 = port unreachable |
| 4 = fragmentation needed and DF set |
| 5 = source route failed |
| 6 = destination network unknown |
| 7 = destination host unknown |
| 8 = source host isolated |
| 9 = communication with destination network administratively prohibited |
| 10 = communication with destination host administratively prohibited |
| 11 = network unreachable for type of service |
| 12 = host unreachable for type of service |

**Gambar 1.7.3** nilai kode untuk pesan destination unreachable

Pesan destination unreachable juga mungkin dikirim ketika fragmentasi paket dibutuhkan untuk mem-forward paket. Fragmentasi selalu dibutuhkan saat datagram di-forward dari jaringan token ring ke jaringan Ethernet. Jika datagram tidak mengijinkan fragmentasi datagram, maka paket tidak dapat di-forward sehingga pesan destination unreachable dikirim. Pesan destination unreachable juga dibangkitkan jika layanan IP seperti FTP atau Web tidak ada.

1.8 Error reporting lainnya

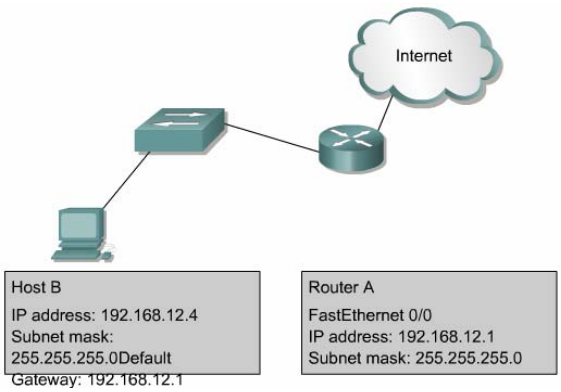
Device yang memproses datagram mungkin tidak dapat mem-forward datagram sesuai dengan error dalam parameter header. Error ini tidak berhubungan untuk host tujuan atau jaringan tapi masih mencegah datagram dari proses dan pengiriman, dank arena itu datagram dibuang. Dalam hal ini, pesan masalah parameter ICMP tipe 12 dikirim ke asal datagram.

Parameter pesan masalah meliputi pointer field dalam header. Ketika nilai kode 0, pointer field menunjukkan octet datagram yang menghasilkan error.

| 0 | 8 | 16 | 31 |
|---|---|---|---|
| Type (12) | Code (0-2) | Checksum | |
| Pointer | | Unused (must be zero) | |
| Internet Header + First 64 Bits of Datagram | | | |
| . . . | | | |

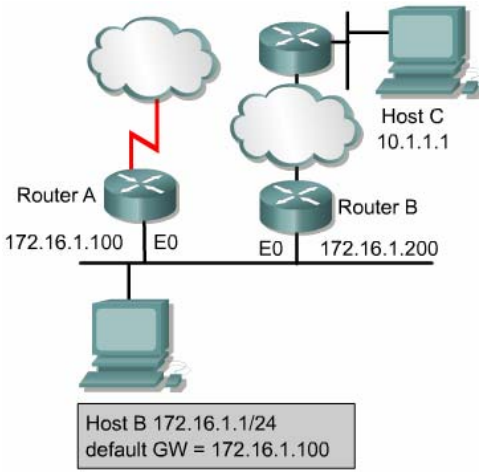
**Gambar 1.8.1** Parameter pesan masalah

1.9 ICMP redirect/change request




**Gambar 1.9.1** Sebuah host dengan koneksi ke internet

Gambar di atas terdapat suatu host yang terhubung ke internet melalui router. Setelah host B dikonfigurasi dengan alamat IP pada interface FastEthernet 0/0 sebagai default gateway dan digunakan untuk menuju ke jaringan mana saja yang tidak terhubung langsung. Secara normal, host B terhubung ke single gateway. Bagaimanapun, host mungkin terhubung ke segmen yang memiliki dua atau lebih router yang terhubung langsung. Dalam hal ini, default gateway dari host membutuhkan redirect/change request untuk menginformasikan host jalur terbaik di jaringan.

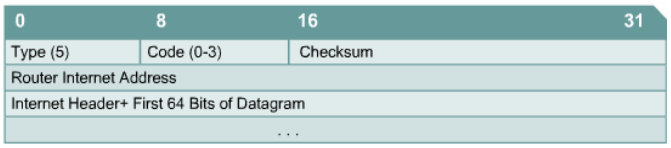



**Gambar 1.9.2** ICMP redirect

Host B mengirimkan paket ke host C dalam jaringan 10.0.0.0/8. Host B tidak terhubung langsung ke jaringan yang sama, ia mem-forward paket ke default gatewaynya, router A. Router A mencari rute yang benar untuk menuju ke jaringan 10.0.0.0/8 dengan cara melihat isi table routingnya. Ia menentukan jalur ke jaringan adalah kembali ke interface yang sama, permintaan untuk mem-forward paket kembali. Ia mem-forward paket dan mengirimkan ICMP redirect/change request ke host B. Request itu memrintahkan host B supaya menggunakan router B sebagai gateway ke forward semua request ke jaringan 10.0.0.0/8.

Default gateway hanya mengirim pesan ICMP redirect/change request jika mengalami kondisi-kondisi berikut ini:

- Interface dimana paket itu datang ke router adalah interface yang sama saat paket di-rute keluar
- Subnet/jaringan alamat IP asal adalah subnet/jaringan yang sama dari alamat IP hop berikutnya dari paket yang di-rutekan
- Datagram bukan source-routed
- Jalur untuk redirect adalah bukan ICMP redirect atau default route
- Router yang dikonfigurasi untuk mengirim redirect. Secara default, router Cisco mengirim pesan ICMP redirect. Perintah yang digunakan adalah **no ip redirects** akan men-disable ICMP redirect



| 0 | 8 | 16 | 31 |
|---|---|---|---|
| Type (5) | Code (0-3) | Checksum | |
| Router Internet Address | | | |
| Internet Header+ First 64 Bits of Datagram | | | |
| . . . | | | |

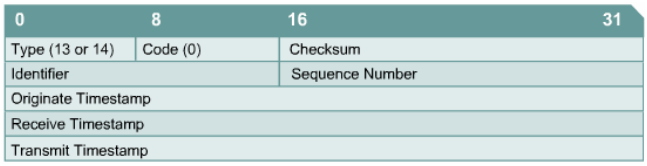
**Gambar 1.9.3** Pesan redirect/change request

| Code Value | Required Action |
|---|---|
| 0 | Redirected datagrams for the network. |
| 1 | Redirected datagrams for the host. |
| 2 | Redirected datagrams for the type of services and networks. |
| 3 | Redirected datagrams for the type of services and host. |

**Gambar 1.9.4** tipe kode ICMP

Field alamat internetrouter dalam ICMP redirect adalah berupa alamat IP yang seharusnya digunakan sebagai default gateway untuk suatu jaringan. Contoh, ICMP redirect dikirim dari router A ke host B yang mempunyai nilai field alamat internet router 172.16.1.200 yaitu alamat IP dari E0 pada router B.

1.10 Sinkronisasi clock dan estimasi waktu transit
ICMP timestamp meminta pesan dari suatu host untuk menanyakan waktu sekarang untuk menuju ke remote host. Remote host menggunakan pesan ICMP timestamp reply untuk respond an untuk request.



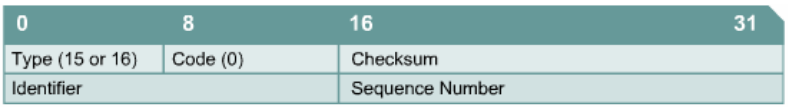
| 0 | 8 | 16 | 31 |
|---|---|---|---|
| Type (13 or 14) | Code (0) | Checksum | |
| Identifier | | Sequence Number | |
| Originate Timestamp | | | |
| Receive Timestamp | | | |
| Transmit Timestamp | | | |

**Gambar 1.10.1** Pesan timestamp reply

Semua pesan ICMP timestamp reply berisi originate, receive dan timestamp transit. Dengan menggunakan tiga timestamp ini, host dapat menentukan waktu transit ke jaringan dengan cara subtract waktu originate dari waktu receive. Atau dapat menentukan waktu transit arah kembali dengan cara subtract waktu transmit dari waktu sekarang. Host yang meminta timestamp originate dapat juga mengestimasi waktu local pada komputer remote.

Sedangkan pesan ICMP timestamp menyediakan cara yang mudah untuk mengestimasi waktu pada host remote dan waktu transmit total jaringan, hal ini bukan merupakan cara terbaik untuk mendapatkan informasi. Protokol yang khusus untuk menangani masalah ini adalah Network Time Protocol (NTP) pada layer atas TCP/IP yang digunakan untuk sinkronisasi waktu.

1.11 Pesan information request atau information reply
Ada dua kode pada pesan tipe ini. Tipe 15 memberikan information request dan tipe 16 memberikan pesan information reply. Protokol lain seperti BOOTP, Reverse Adress Resolution Protocol (RARP) dan Dynamic Host Configuration Protocol (DHCP) sekarang digunakan untuk melewatkan host-host ke jaringan.




**Gambar 1.11.1** pesan information request atau information reply

1.12 Pesan Adress Mask

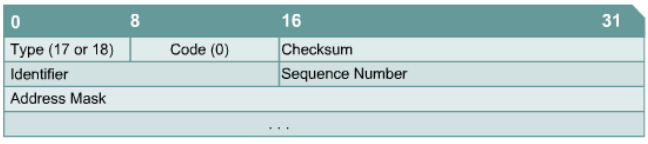
Digunakan pada saat admin menggunakan proses subnetting untuk membagi alamat IP menjadi beberapa subnet, maka akan tercipta subnet mask baru. Sebagai contoh, diasumsikan bahwa host yang terletak dalam jaringan kelas B dan mempunyai alamat IP 172.16.5.2. host ini tidak mengenal subnet mask sehingga ia broadcast dengan request:

```
Source address: 172.16.5.2

Destination address: 255.255.255.255

Protocol: ICMP = 1

Type: Adress Mask Request = AM1

Code: 0

Mask: 255.255.255.0
```

Broadcast pesan ini akan diterima oleh 172.16.5.1, sebagai router local. Kemudian router membalasnya dengan mengirimkan:

```
Source address: 172.16.5.1

Destination address: 172.16.5.2

Protocol: ICMP = 1

Type: Adress Mask Request = AM2

Code: 0

Mask: 255.255.255.0
```

Format frame untuk address mask request dan reply ditunjukkan oleh gambar di bawah ini. Catatan bahwa format frame yang sama digunakan untuk kedua address mask request dan reply. ICMP tipe 17 digunakan untuk request dan tipe 18 untuk reply.




**Gambar 1.12.1** Pesan address mask

| IP Fields | |
|---|---|
| Addresses | The address of the source in an address mask request message will be the destination of the address mask reply message. To form an address mask reply message, the source address of the request becomes the destination address of the reply and the source address of the reply is set to the replier's address. The type code is changed to AM2, the address mask value is inserted into the address mask field, and the checksum is recomputed. However, if the source address in the request message is zero, then the destination address for the reply message should denote a broadcast. |

| | |
|---|---|
| Type 17 | Address mask request message |
| Type 18 | Address mask reply message |
| Code 0 | Address mask request message |
| Code 0 | Address mask reply message |
| Checksum | The checksum is the 16-bit ones complement of the ones complement sum of the ICMP message starting with the ICMP Type. For computing the checksum, the checksum field should be zero. This checksum may be replaced in the future. |
| Identifier | An identifier to aid in matching requests and replies, may be zero |

**Gambar 1.12.2** Diskripsi field pesan address mask

1.13 Pesan router discovery

| 0 | 8 | 16 | 31 |
|---|---|---|---|
| Type (9) | Code (0) | Checksum | |
| Number of Addresses | Address Entry Size | Lifetime | |
| Router Address 1 | | | |
| Preferences Level 1 | | | |
| Router Address 2 | | | |
| Preferences Level 2 | | | |

**Gambar 1.13.1** Pesan router discovery

Pesan router discovery juga dapat di-broadcast ke router-router yang tidak dikonfigurasi untuk multicast. Jika pesan ini dikirim ke router yang tidak mendukung proses discovery, maka router tersebut tidak akan menjawab, sebaliknya jika router mendukung proses discovery dan menerima pesan discovery, maka router akan membalasnya dengan format khusus.

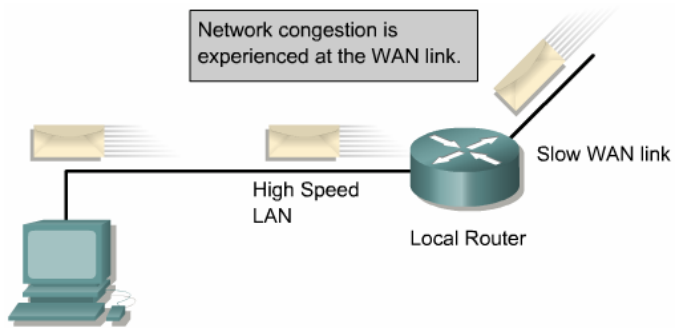
| IP Fields | |
|---|---|
| Source Address | An IP address belonging to the interface from which this message is sent. |
| Destination Address | The configured advertisement address or IP address of a neighboring host. |
| Time To Live | Set to 1 if the destination address is an IP multicast address. Otherwise, set to at least 1. |

| ICMP | |
|---|---|
| Type | 9 |
| Code | 0 |
| Checksum | The 16-bit ones complement of the ones complement sum of the ICMP message, starting with the ICMP type. For computing the checksum, the checksum field is set to 0. |
| Num Addrs | The number of router addresses advertised in this message. |
| Addr Entry Size | The number of 32-bit words of information per each router address. This is 2 in the version of the protocol described here. |
| Lifetime | The maximum number of seconds that the router addresses may be |

**Gambar 1.13.2** deskripsi field-field pesan ICMP router discovery

1.14 Masalah komunikasi dari link WAN

Pada kantor kecil, small office home office (SOHO) dimana pesan ICMP mungkin digunakan efisien. SOHO yang terdiri atas empat computer dengan jaringan menggunakan kabel CAT-5 dan mempunyai jalur internet lewat 56K modem. Dan LAN dengan bandwidth 10Mbps. Host gateway seharusnya dapat menggunakan pesan ICMP untuk request host-host lainnya seperti yang digambarkan di bawah ini:




**Gambar 1.14.1** masalah komunikasi dari link WAN

**Kesimpulan**

- IP menggunakan Internet Control Message Protocol (ICMP) untuk memberitahu pengirim bahwa terjadi error data pada proses pengiriman.
- Pesan ICMP ditransmisikan menggunakan protokol IP dengan metode pengiriman unreliable.
- Pesan ICMP echo request dan reply membantu admin jaringan untuk melakukan tes konektivitas IP yang digunakan dalam proses troubleshooting.