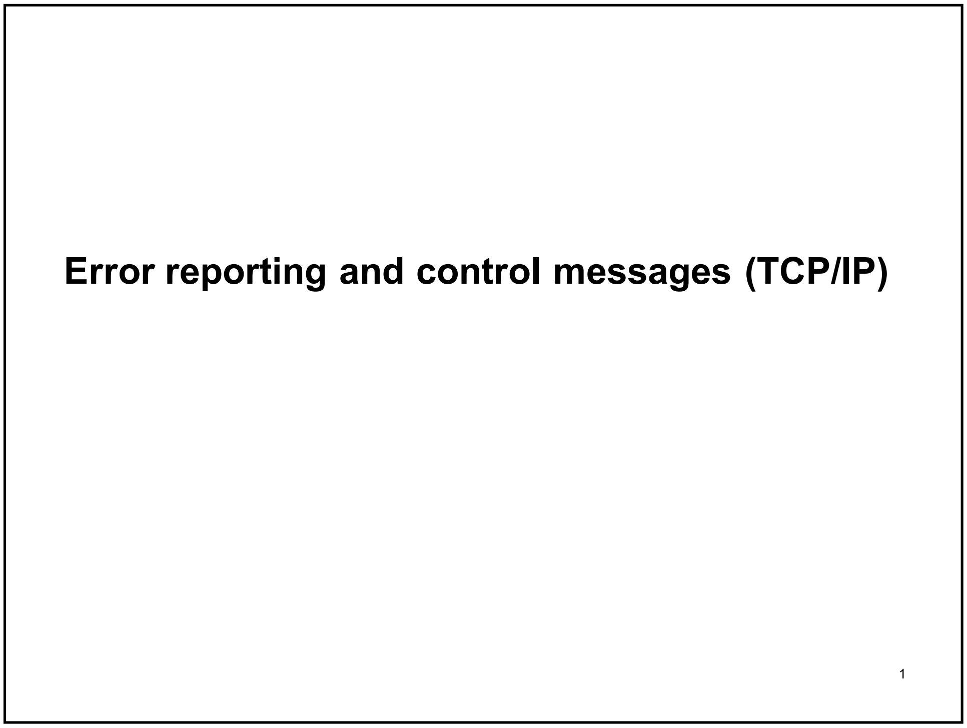
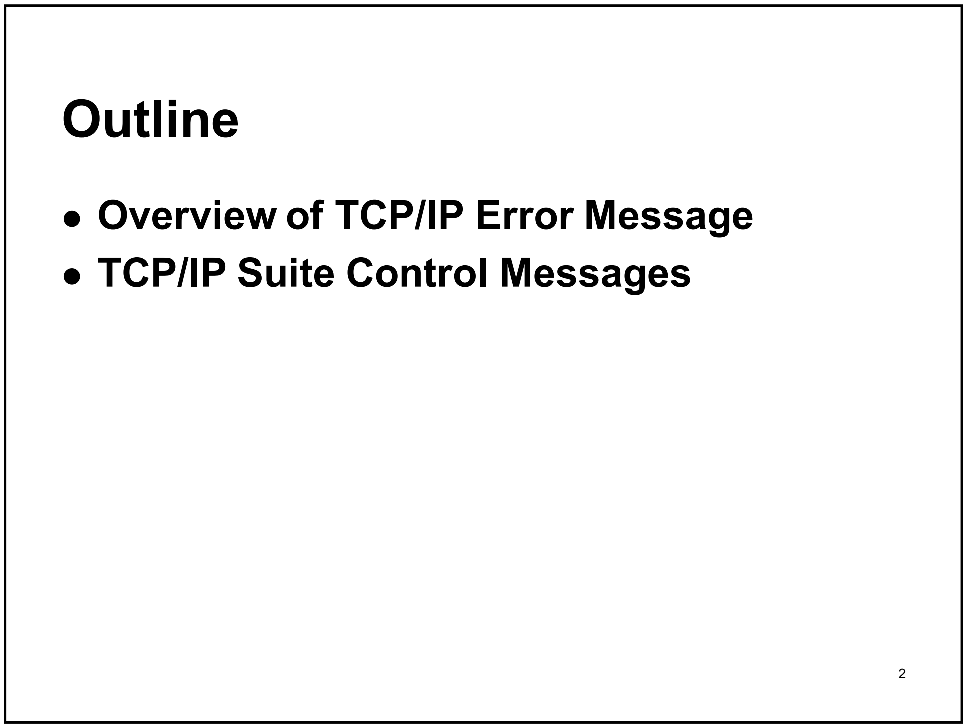


Error reporting and control messages (TCP/IP)



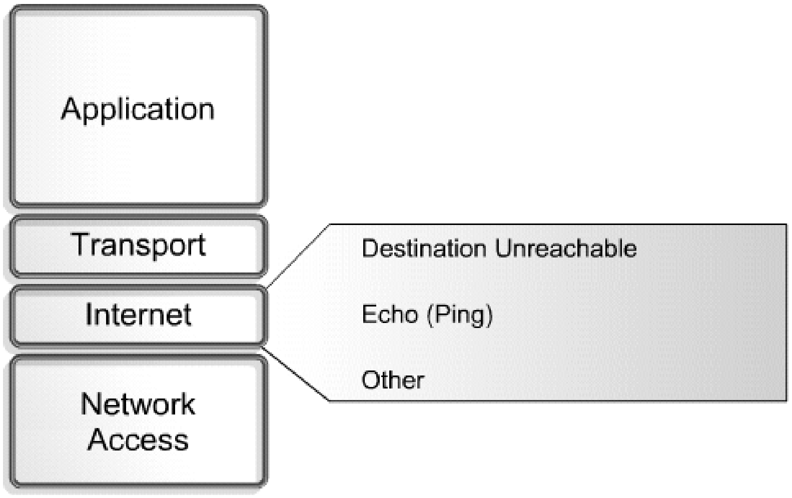
Outline

- Overview of TCP/IP Error Message
- TCP/IP Suite Control Messages

Internet Control Message Protocol (ICMP)

- IP is an unreliable method for delivery of network data.
- It has no built-in processes to ensure that data is delivered in the event that problems exist with network communication.
- If an intermediary device such as a router fails, or if a destination device is disconnected from the network, data cannot be delivered.
- Additionally, nothing in its basic design allows IP to notify the sender that a data transmission has failed.

- Internet Control Message Protocol (ICMP) is the component of the TCP/IP protocol stack that addresses this basic limitation of IP.
- ICMP does not overcome the unreliability issues in IP.
- Reliability must be provided by upper layer protocols if it is needed.

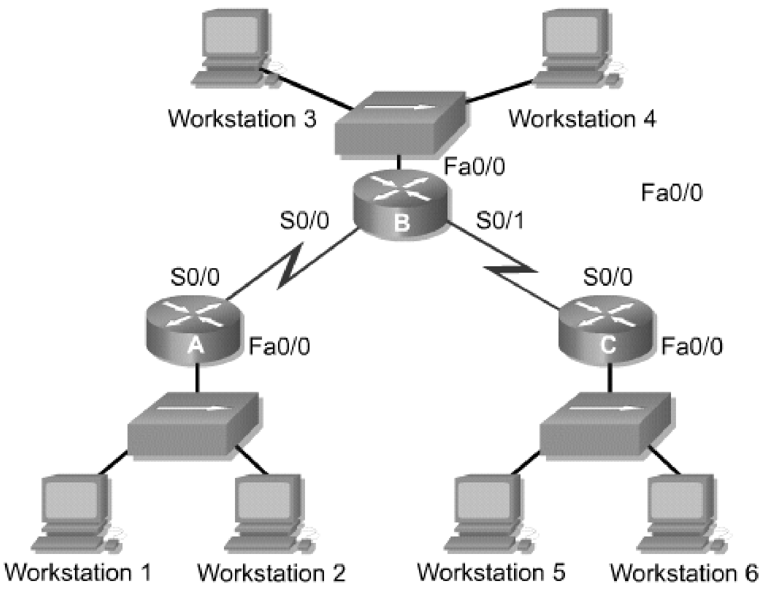


5

Error reporting and error correction

- ICMP is an error reporting protocol for IP.
- When datagram delivery errors occur, ICMP is used to report these errors back to the source of the datagram.
- ICMP does not correct the encountered network problem; it merely reports the problem.
- ICMP reports on the status of the delivered packet only to the source device.
- It does not propagate information about network changes to routers.

6



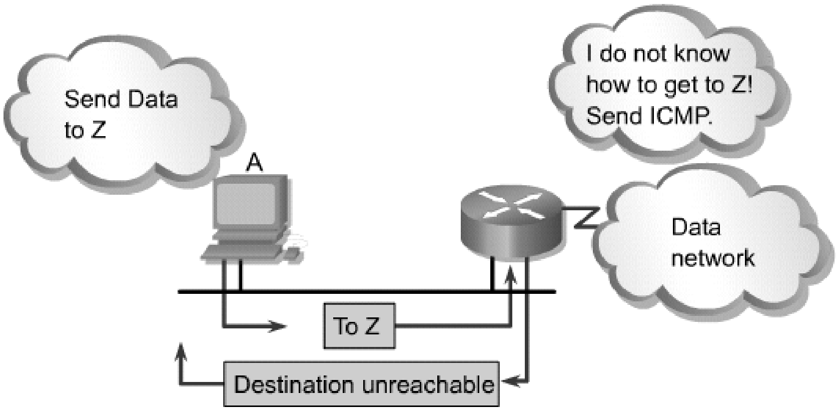
ICMP message delivery

- ICMP messages are encapsulated into datagrams in the same way any other data is delivered using IP.
- This creates a scenario where error reports could generate more error reports, causing increased congestion on an already ailing network.
- For this reason, errors created by ICMP messages do not generate their own ICMP messages.
- It is thus possible to have a datagram delivery error that is never reported back to the sender of the data.

Unreachable networks

- Network communication depends upon certain basic conditions being met.
  - First, the sending and receiving devices must have the TCP/IP protocol stack properly configured.
  - Second, intermediary devices must be in place to route the datagram from the source device and its network to the destination network.

- For instance, the sending device may address the datagram to a non-existent IP address or to a destination device that is disconnected from its network.
- Routers can also be points of failure if a connecting interface is down or if the router does not have the information necessary to find the destination network.
- If a destination network is not accessible, it is said to be an unreachable network.

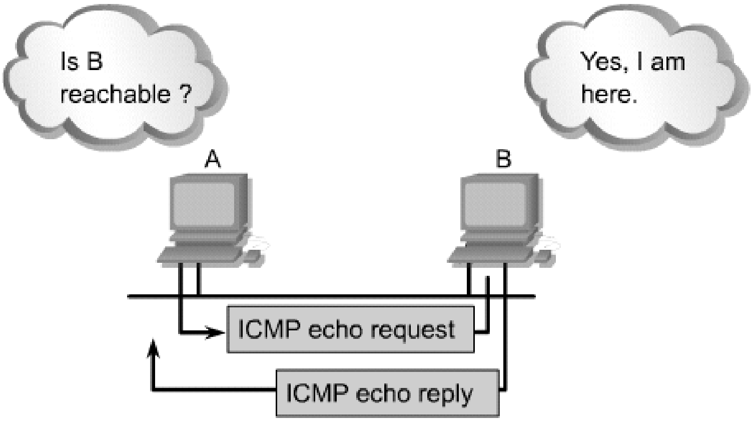


An ICMP destination unreachable meassage is sent if:

- Host or port unreachable
- Network unreachable

Using ping to test destination reachability

- The ICMP protocol can be used to test the availability of a particular destination.
- Figure shows ICMP being used to issue an echo request message to the destination device.
- If the destination device receives the ICMP echo request, it formulates an echo reply message to send back to the source of the echo request.
- The echo request message is typically initiated using the **ping** command.



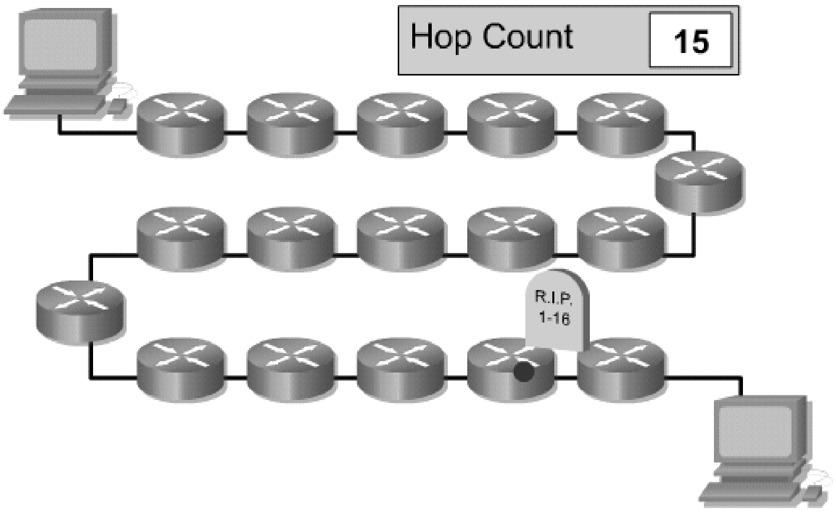
Traffic generated by the `ping` command

Detecting excessively long routes

- The limitations of the routing protocol can result in destinations being unreachable.
- For example, RIP has a limit on the distance a certain routing information is allowed to travel.
- The hop limit of RIP is 15, which means that the packet will only be allowed to pass through 15 routers.

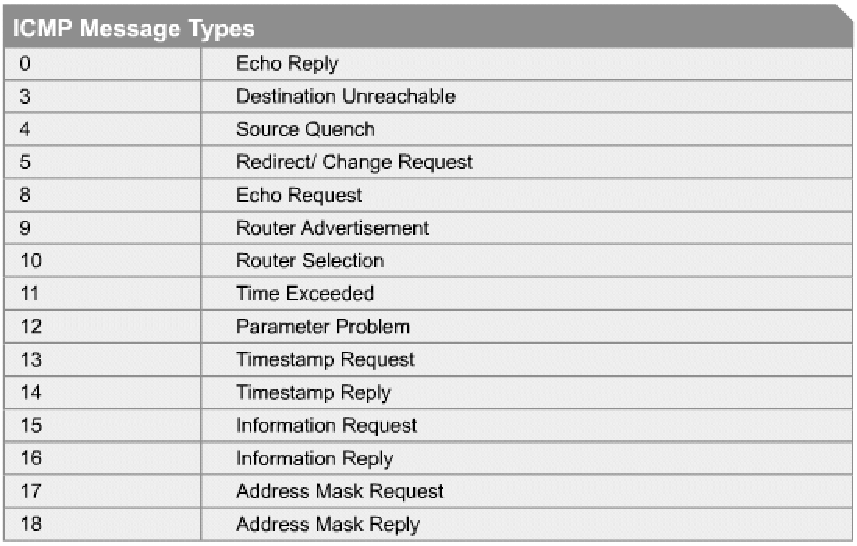
- Whether the actual path includes a circular routing path or too many hops, the packet will eventually exceed the maximum hop count.
- This is also known as reaching its time-to-live (TTL), because the TTL value typically matches the maximum hop count defined by the routing protocol.
- As each router processes the datagram, it decreases the TTL value by one.
- When the TTL of the datagram value reaches zero, the packet is discarded.
- ICMP uses a time exceeded message to notify the source device that the TTL of the datagram has been exceeded.

15



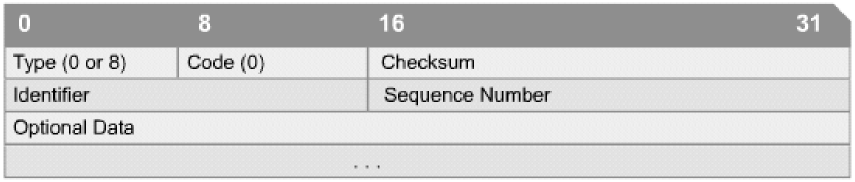
Echo messages

- ICMP message formats start with these three fields:
  - Type
  - Code
  - Checksum
- The type field indicates the type of ICMP message being sent.
- The code field includes further information specific to the message type.
- The checksum field, as in other types of packets, is used to verify the integrity of the 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

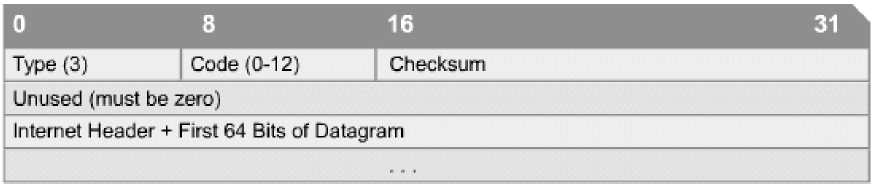
- Figure shows the message format for the ICMP echo request and echo reply messages.
- The identifier and sequence fields are used to match the echo replies to the corresponding echo request.
- The data field contains additional information that may be a part of the echo reply or echo request message.



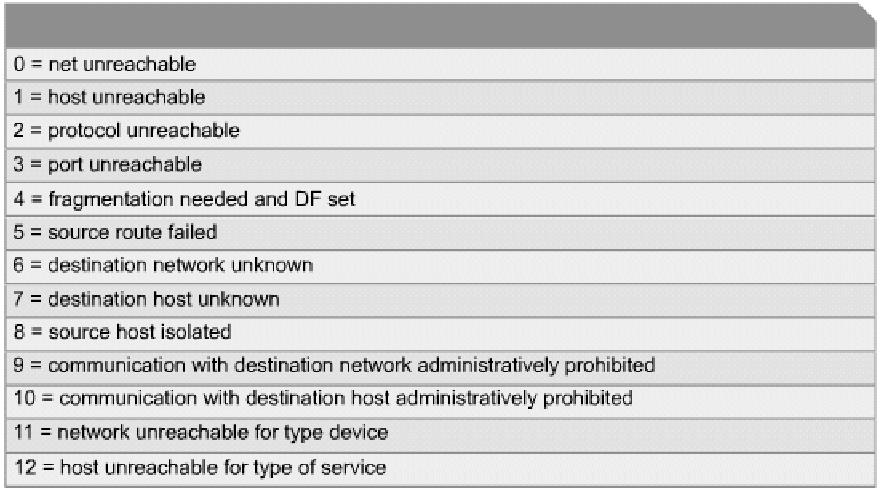
0	8	16	31
Type (0 or 8)	Code (0)	Checksum	
Identifier		Sequence Number	
Optional Data			
. . .			

Destination unreachable message

- Figure shows an ICMP destination unreachable message header.
- The value of 3 in the type field indicates it is a destination unreachable message.
- The code value indicates the reason the packet could not be delivered.



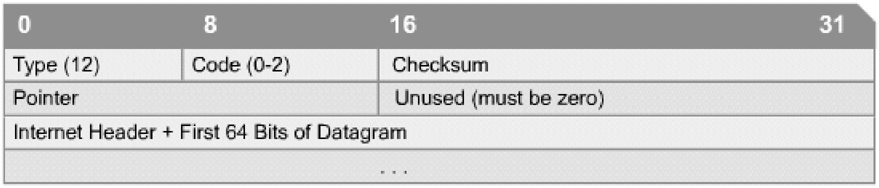
0	8	16	31
Type (3)	Code (0-12)	Checksum	
Unused (must be zero)			
Internet Header + First 64 Bits of Datagram			
. . .			



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 device
12 = host unreachable for type of service

Miscellaneous error reporting

- Devices that process datagrams may not be able to forward a datagram due to some type of error in the header.
- This error does not relate to the state of the destination host or network but still prevents the datagram from being processed and delivered.
- In this case, an ICMP type 12 parameter problem message is sent to the source of the datagram.



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

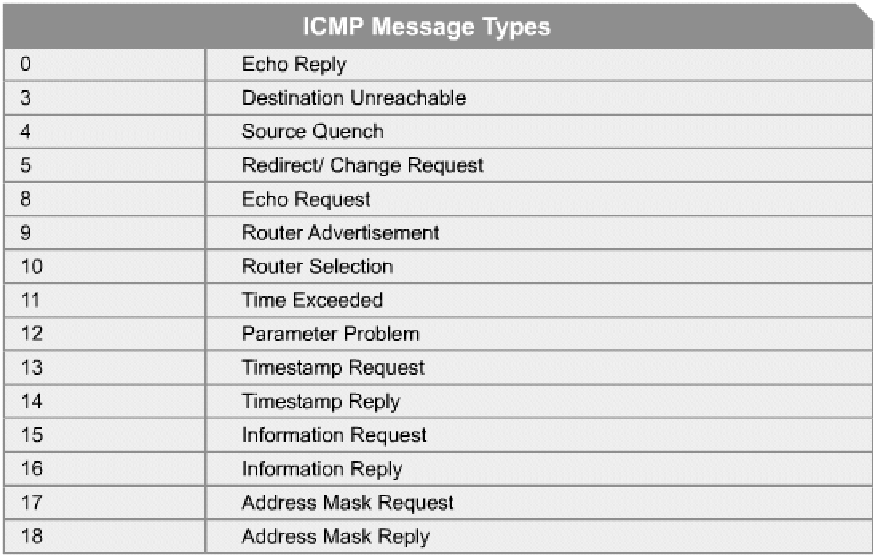
Outline

- Overview of TCP/IP Error Message
- TCP/IP Suite Control Messages

Introduction to control messages

- The Internet Control Message Protocol (ICMP) is an integral part of the TCP/IP protocol suite.
- Unlike error messages, control messages are not the results of lost packets or error conditions which occur during packet transmission.
- Instead, they are used to inform hosts of conditions such as network congestion or the existence of a better gateway to a remote network.

- Like all ICMP messages, ICMP control messages are encapsulated within an IP datagram.
- ICMP uses IP datagrams in order to traverse multiple networks.
- Multiple types of control messages are used by ICMP.



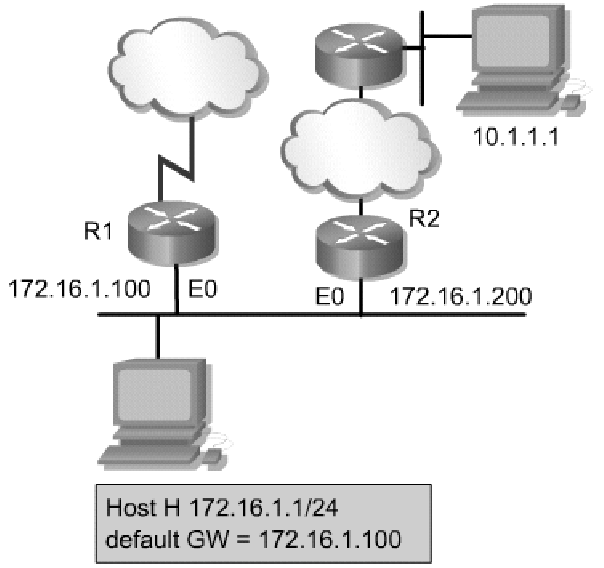
ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request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

29

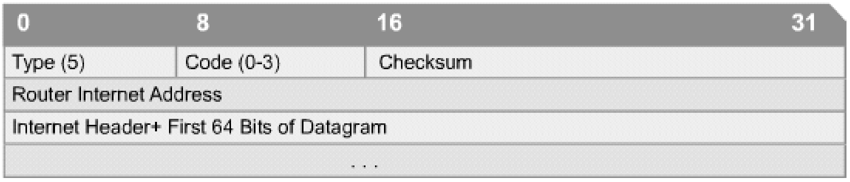
ICMP redirect/change requests

- This type of message can only be initiated by a gateway.
- However, in some circumstances, a host connects to a segment that has two or more directly connected routers.
- In this case, the default gateway of the host may need to use a redirect/change request to inform the host of the best path to a certain network.

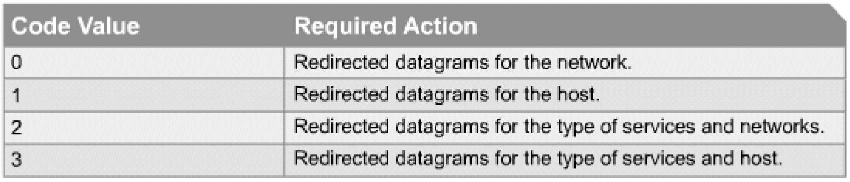
30



- Default gateways only send ICMP redirect/change request messages if the following conditions are met:
  - The interface on which the packet comes into the router is the same interface on which the packet gets routed out.
  - The subnet/network of the source IP address is the same subnet/network of the next-hop IP address of the routed packet.
  - The datagram is not source-routed.
  - The route for the redirect is not another ICMP redirect or a default route.
  - The router is configured to send redirects. (By default, Cisco routers send ICMP redirects. The interface subcommand **no ip redirects** will disable ICMP redirects.)



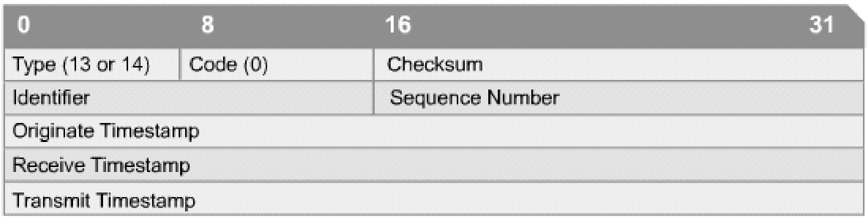
0	8	16	31
Type (5)	Code (0-3)	Checksum	
Router Internet Address			
Internet Header+ First 64 Bits of Datagram			
. . .			



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.

Clock synchronization and transit time estimation

- Hosts on different networks who are trying to communicate using software that requires time synchronization can sometimes encounter problems.
- The ICMP timestamp message type is designed to help alleviate this problem.
- The ICMP timestamp request message allows a host to ask for the current time according to the remote host.
- The remote host uses an ICMP timestamp reply message to respond to the request.

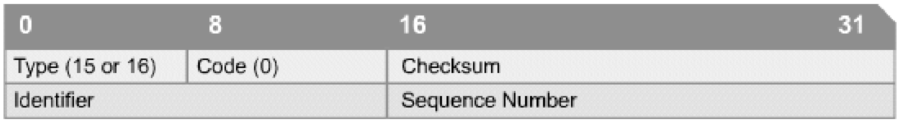


0	8	16	31
Type (13 or 14)	Code (0)	Checksum	
Identifier		Sequence Number	
Originate Timestamp			
Receive Timestamp			
Transmit Timestamp			

- More robust protocols such as Network Time Protocol (NTP) at the upper layers of the TCP/IP protocol stack perform clock synchronization in a more reliable manner.

Information requests and reply message formats

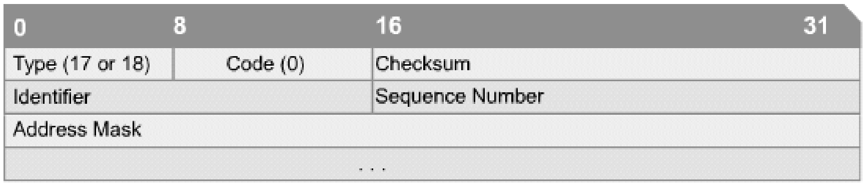
- The ICMP information requests and reply messages were originally intended to allow a host to determine its network number.
- Type 15 signifies an information request message, and type 16 identifies an information reply message.
- This particular ICMP message type is considered obsolete.
- Other protocols such as BOOTP and Dynamic Host Configuration Protocol (DHCP) are now used to allow hosts to obtain their network numbers.



0	8	16	31
Type (15 or 16)	Code (0)	Checksum	
Identifier		Sequence Number	

Address mask requirements

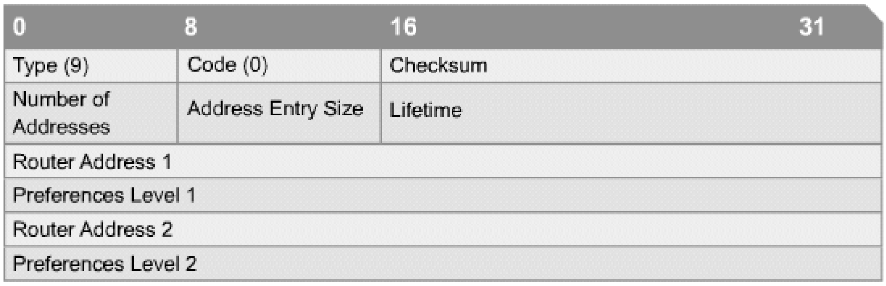
- If a host does not know the subnet mask, it may send an address mask request to the local router.
- If the address of the router is known, this request may be sent directly to the router. Otherwise, the request will be broadcast.
- When the router receives the request, it will respond with an address mask reply.



0	8	16	31
Type (17 or 18)	Code (0)	Checksum	
Identifier		Sequence Number	
Address Mask			
. . .			

Router discovery message

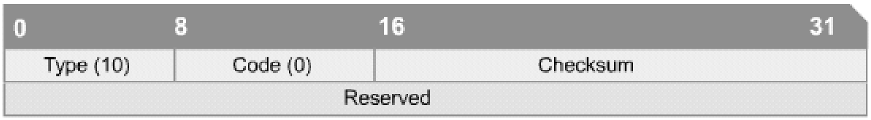
- When a host on the network boots, and the host has not been manually configured with a default gateway, it can learn of available routers through the process of router discovery.
- This process begins with the host sending a router solicitation message to all routers, using the multicast address 224.0.0.2 as the destination address.
- When a router that supports the discovery process receives the router discovery message , a router advertisement is sent in return.



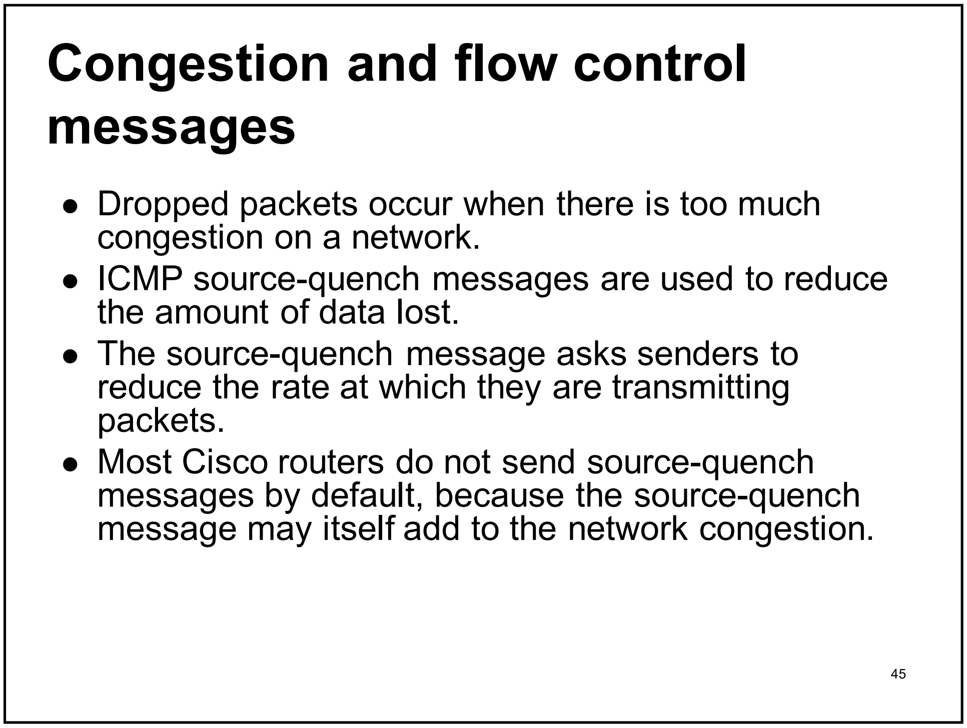
0	8	16	31
Type (9)	Code (0)	Checksum	
Number of Addresses	Address Entry Size	Lifetime	
Router Address 1			
Preferences Level 1			
Router Address 2			
Preferences Level 2			

Router solicitation message

- A host generates an ICMP router solicitation message in response to a missing default gateway.
- This message is sent via multicast and it is the first step in the router discovery process.
- A local router will respond with a router advertisement identifying the default gateway for the local host.



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



Congestion and flow control messages

- Dropped packets occur when there is too much congestion on a network.
- ICMP source-quench messages are used to reduce the amount of data lost.
- The source-quench message asks senders to reduce the rate at which they are transmitting packets.
- Most Cisco routers do not send source-quench messages by default, because the source-quench message may itself add to the network congestion.