Networking Course. Lesson 3. Layer 3 and Routing

Document version 0.1
This document was created, but not reviewed yet.
You should use it very carefully.

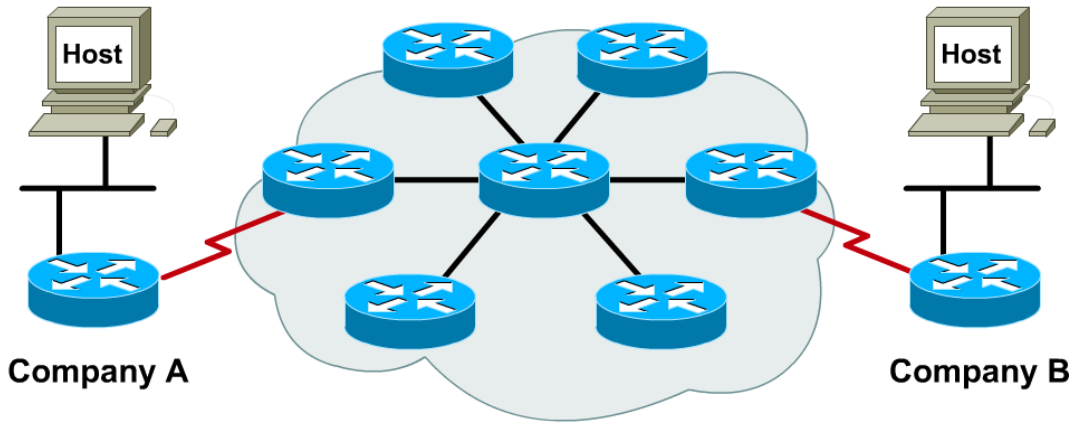
Theory

IP Addressing

IP Addressing

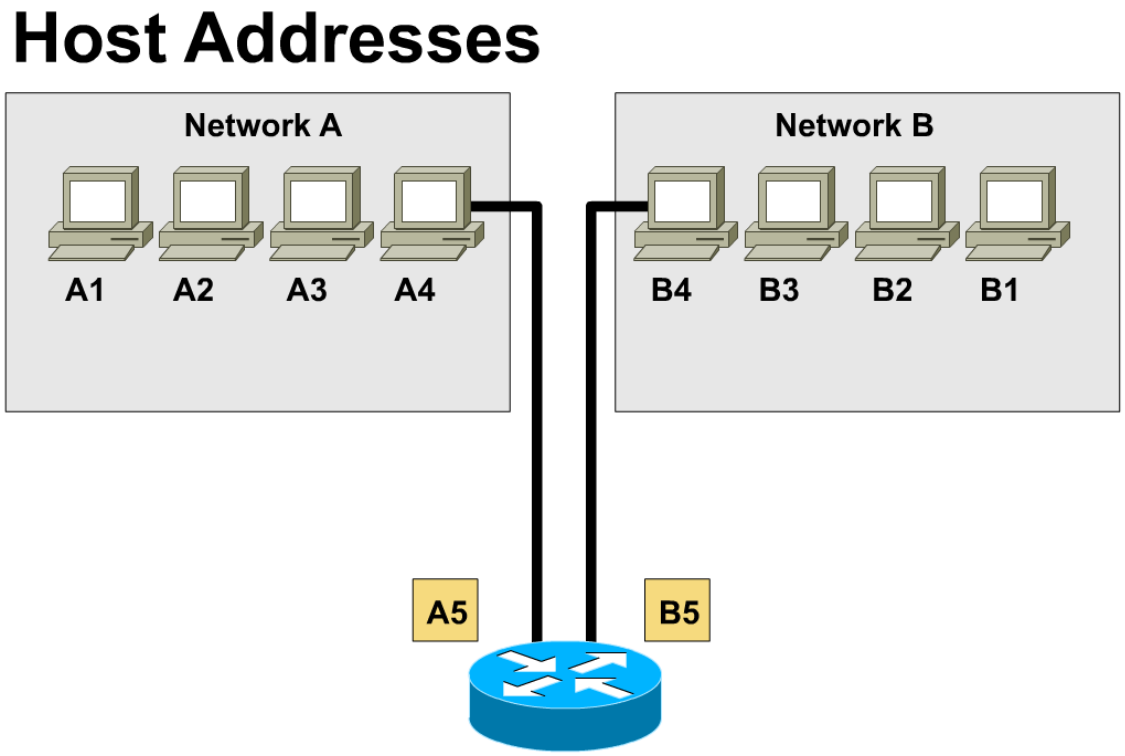
In a TCP/IP environment, end stations communicate with servers or other end stations. This can occur because each node using the TCP/IP protocol suite has a unique 32-bit logical address. This address is known as the IP address and is specified in 32-bit dotted-decimal format.

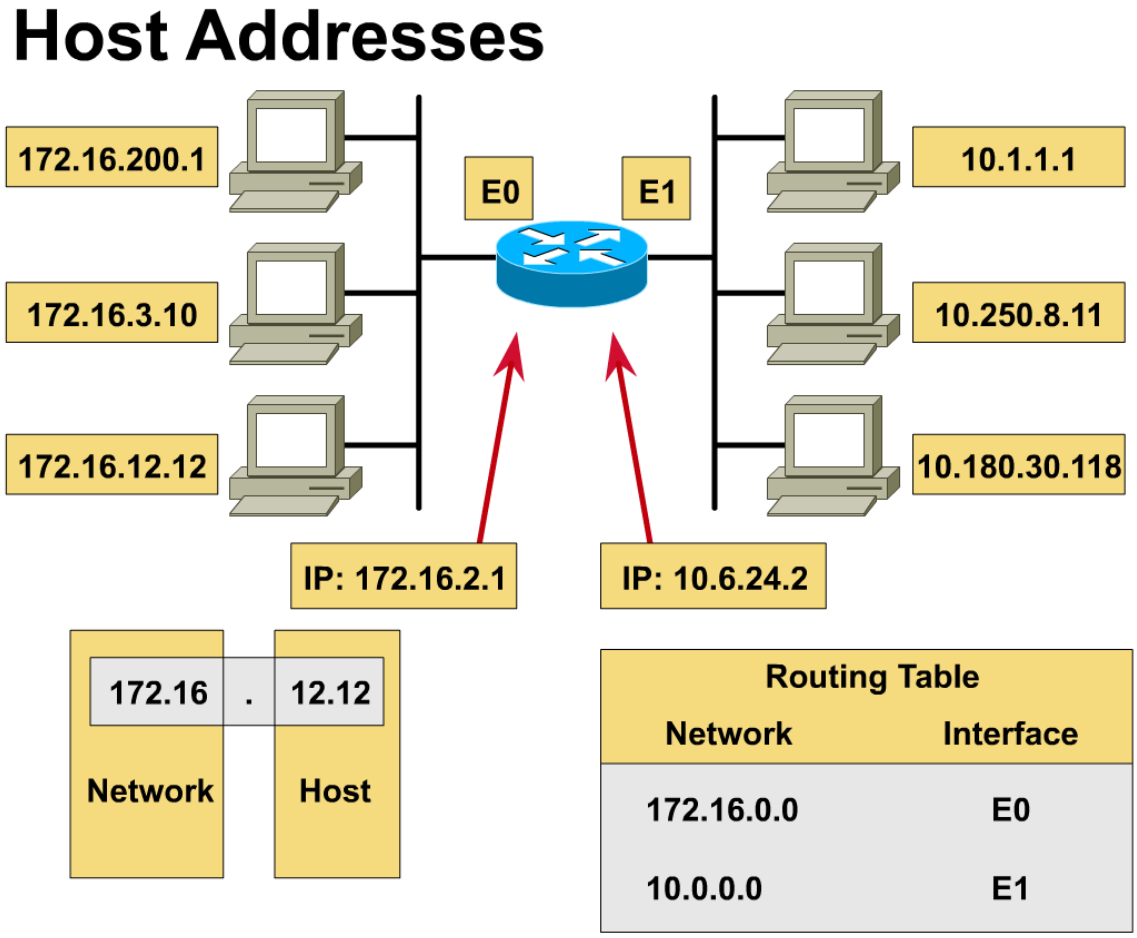
Each company or organization listed on the Internet is seen as a single unique network that must be reached before an individual host within that company can be contacted. Each company network has an address; the hosts that live on that network share that same network address, but each host is identified by the unique host address on the network.



Unique addressing allows communication between end stations.
Path choice is based on location.
Location is represented by address.

Unicats Addressing





IP Addressing Terminology

IP Addressing Terminology

Term	Definition
IP address	32-bit number, usually written in dotted decimal form, that uniquely identifies an interface of some computer.
Host address	Another term for IP address.
Network	The concept of a group of hosts.
Network number	A 32-bit number, usually written in dotted decimal form, that represents a network. This number cannot be assigned as an IP address to an interface of some computer. The host portion of the network number has a value of all binary 0s.
Network address	Another name for network number.
Broadcast address	A 32-bit number, usually written in dotted decimal form, that is used to address all hosts in the network. The host portion of the broadcast address has a value of all binary 1s. Broadcast addresses cannot be assigned as an IP address.
Subnet	The concept of a group of hosts, which is a subdivision of a network.
Subnet number	A 32-bit number, usually written in dotted decimal form, that represents all hosts in a subnet. This number cannot be used as an IP address for some computer's interface.
Subnet address	Another term for subnet number.

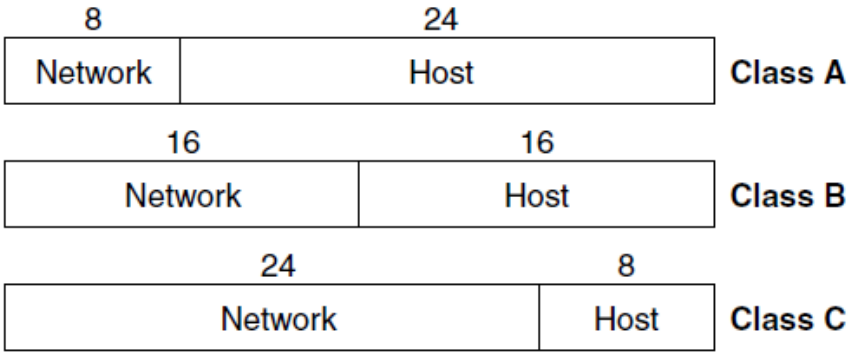
continues

IP Addressing Terminology (Continued)

Term	Definition
Subnetting	The process of subdividing networks into smaller subnets. This is jargon—for example, "Are you subnetting your network?"
Network mask	A 32-bit number, usually written in dotted decimal form. The mask is used by computers to calculate the network number of a given IP address by performing a Boolean AND of the address and mask. The mask also defines the number of host bits in an address.
Mask	A generic term for a mask, whether it is a default mask or a subnet mask.
Address mask	Another term for a mask.
Default Class A mask	The mask used for Class A networks when no subnetting is used. The value is 255.0.0.0.
Default Class B mask	The mask used for Class B networks when no subnetting is used. The value is 255.255.0.0.
Default Class C mask	The mask used for Class C networks when no subnetting is used. The value is 255.255.255.0.
Subnet mask	A non-default mask used when subnetting.
Network part or network field	Term used to describe the first part of an IP address. The network part is 8, 16, or 24 bits for Class A, B, and C networks, respectively.
Host part or host field	Term used to describe the last part of an IP address. The host part is 24, 16, or 8 bits for Class A, B, and C networks, respectively, when subnetting is not used. When subnetting, the size of the host part depends on the subnet mask chosen for that network.
Subnet part of subnet field	Term used to describe the middle part of an IP address. The subnet part is variable in size, based on how subnetting is implemented.

Subnetting

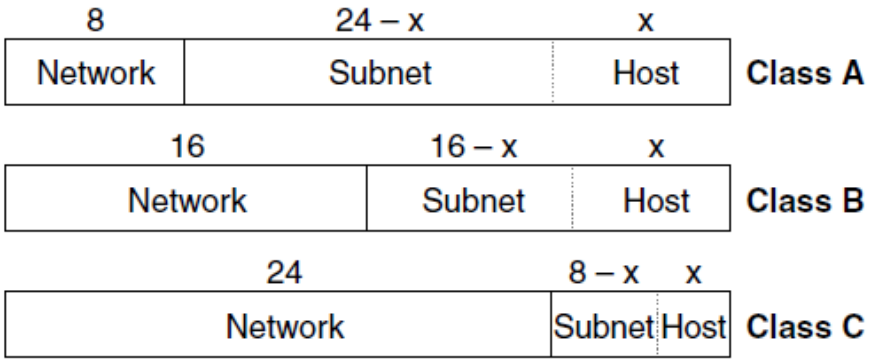
Address Formats, When No Subnetting Is Used



Class A, B, and C Networks—Network and Host Parts and Default Masks

Class of Address	Size of Network Part of Address, in Bits	Size of Host Part of Address, in Bits	Default Mask for Each Class of Network
A	8	24	255.0.0.0
B	16	16	255.255.0.0
C	24	8	255.255.255.0

Address Formats, When Subnetting Is Used



Sizes of Network and Host Parts of IP Addresses with No Subnetting

Any Network of This Class	Number of Network Bytes (Bits)	Number of Host Bytes (Bits)	Number of Addresses per Network*
A	1 (8)	3 (24)	2^{24} minus two special cases
B	2 (16)	2 (16)	2^{16} minus two special cases
C	3 (24)	1 (8)	2^{8} minus two special cases

* There are two reserved host addresses per network.

Example Network Numbers, Decimal and Binary

Network Number	Binary Representation, with Host Part Bold
8.0.0.0	0000 1000 **0000 0000 0000 0000 0000 0000**
130.4.0.0	1000 0010 0000 0100 **0000 0000 0000 0000**
199.1.1.0	1100 0111 0000 0001 0000 0001 **0000 0000**

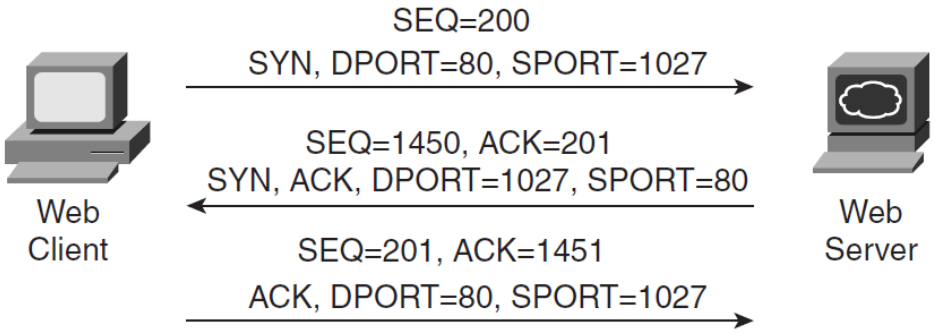
Routed Protocols

- TCP
- UDP
- ICMP

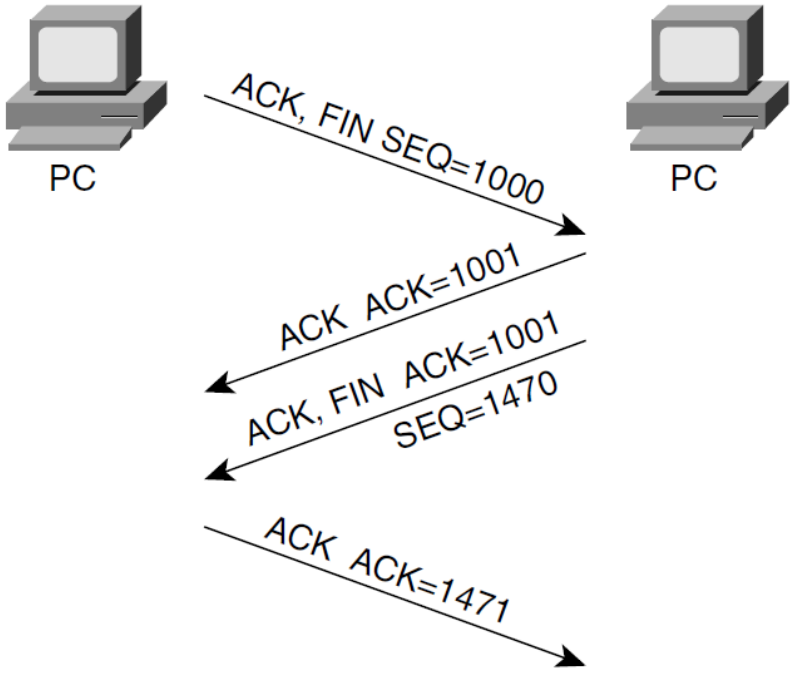
- Helper Protocol. ARP

TCP

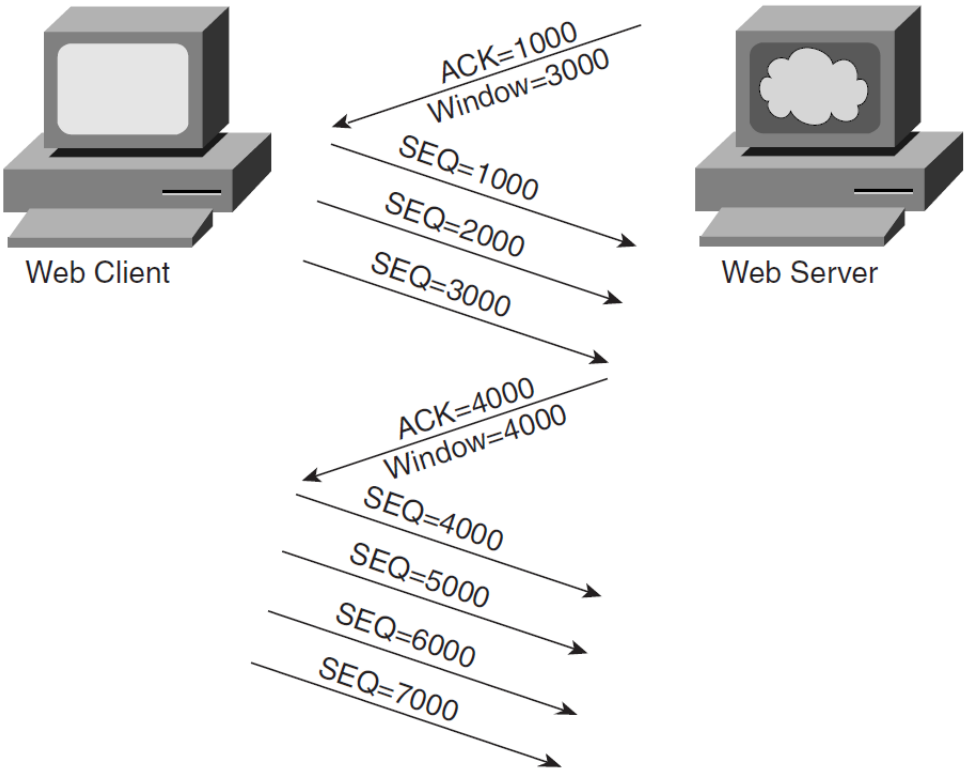
TCP Connection Establishment



TCP Connection Termination



TCP Windowing



TCP Function Summary

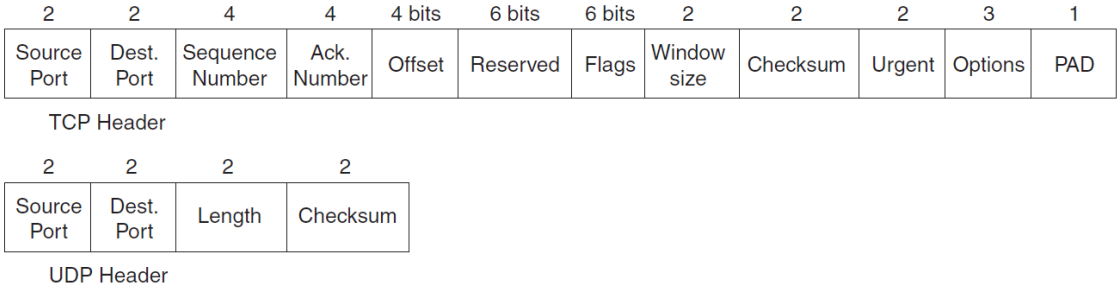
Function	Description
Data transfer	Continuous stream of ordered data.
Multiplexing	Function that allows receiving hosts to decide the correct application for which the data is destined, based on the port number.
Error recovery (reliability)	Process of numbering and acknowledging data with sequence and acknowledgment header fields.
Flow control using windowing	Process that uses window sizes to protect buffer space and routing devices.
Connection establishment and termination	Process used to initialize port numbers and sequence and acknowledgement fields.

UDP

TCP and UDP Functional Comparison

Function	Description (TCP)	Description (UDP)
Data transfer	Continuous stream of ordered data	Message (datagram) delivery
Multiplexing	Receiving hosts decide the correct application for which the data is destined, based on port number	Receiving hosts decide the correct application for which the data is destined, based on port number
Reliable transfer	Acknowledgment of data using the sequence and acknowledgment fields in the TCP header	Not a feature of UDP
Flow control	Process used to protect buffer space and routing devices	Not a feature of UDP
Connections	Process used to initialize port numbers and other TCP header fields	UDP is connectionless

Figure 5-9 *TCP and UDP Headers*



ICMP

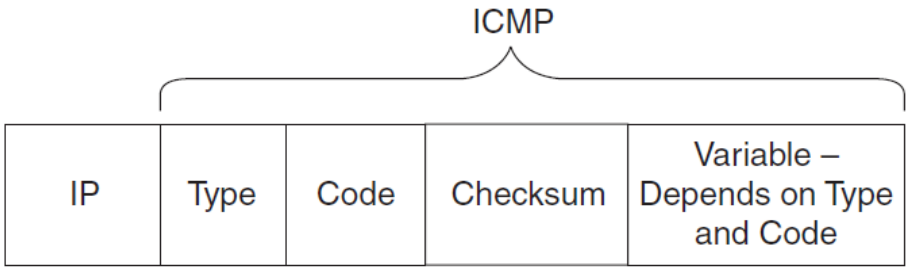
ICMP Message Types

Message	Purpose
*Destination Unreachable	This tells the source host that there is a problem delivering a packet.
*Time Exceeded	The time it takes a packet to be delivered has become too long; the packet has been discarded.
Source Quench	The source is sending data faster than it can be forwarded; this message requests that the sender slow down.

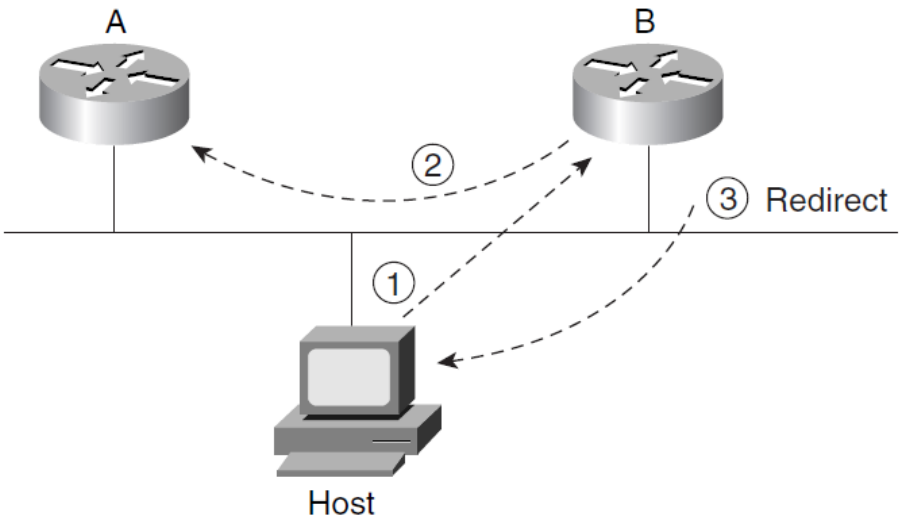
ICMP Message Types (Continued)

Message	Purpose
*Redirect	The router sending this message has received some packet for which another router would have had a better route; the message tells the sender to use the better router.
*Echo	This is used by the **ping** command to verify connectivity.
Parameter Problem	This is used to identify a parameter that is incorrect.
Timestamp	This is used to measure roundtrip time to particular hosts.
Address Mask Request/Reply	This is used to inquire about and learn the correct subnet mask to be used.
Router Advertisement and Selection	This is used to allow hosts to dynamically learn the IP addresses of the routers attached to the subnet.

ICMP Header Formats

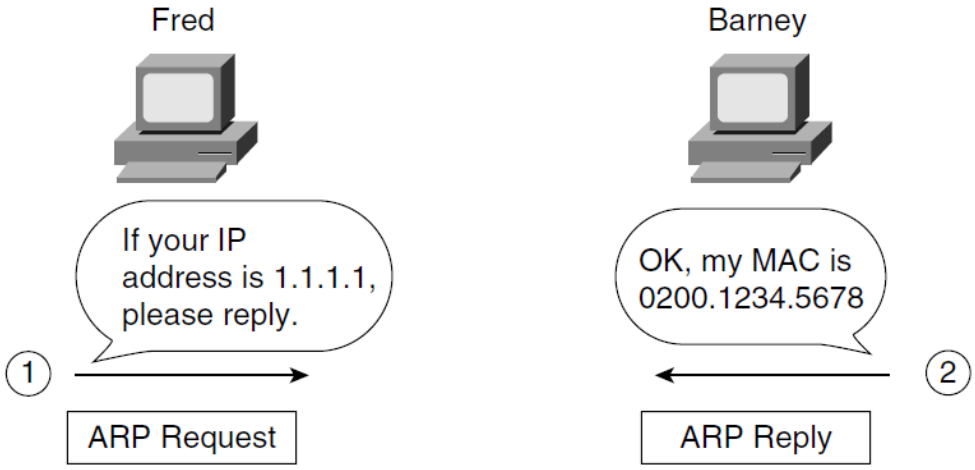


Example of an ICMP Redirect



Helper Protocol. ARP

The ARP Process



Routing Protocols

- RIP
- IGRP

Interior IP Routing Protocols and Types

Routing Protocol	Type	Loop Prevention Mechanisms	Mask Sent in Updates?
RIP-1	Distance vector	Holddown timer, split horizon	No
RIP-2	Distance vector	Holddown timer, split horizon	Yes
IGRP	Distance vector	Holddown timer, split horizon	No
EIGRP	Balanced hybrid	DUAL and feasible successors	Yes
OSPF	Link-state	Dijkstra SPF algorithm and full topology knowledge	Yes

RIP

Router A Advertising Directly Connected Routes

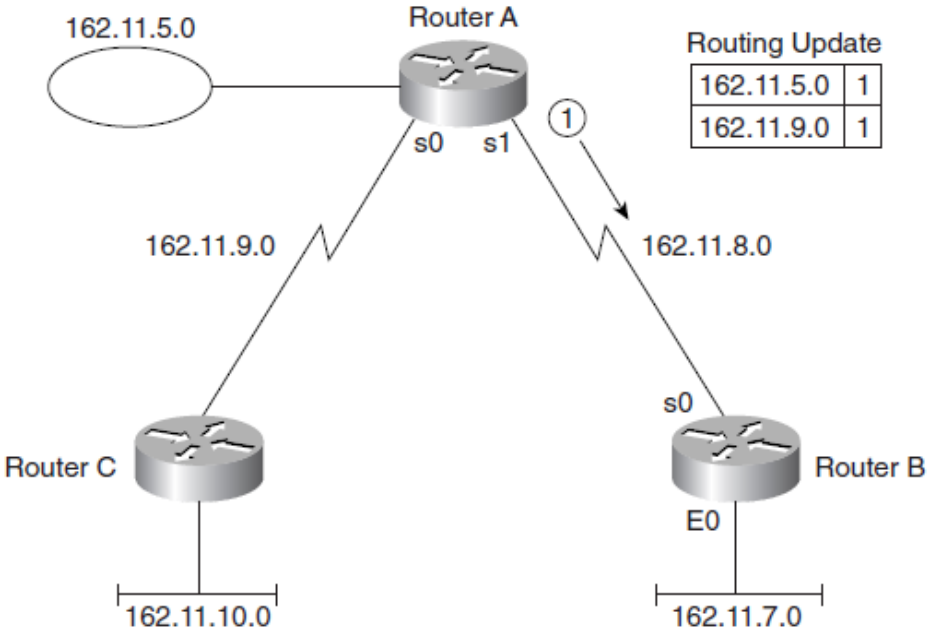
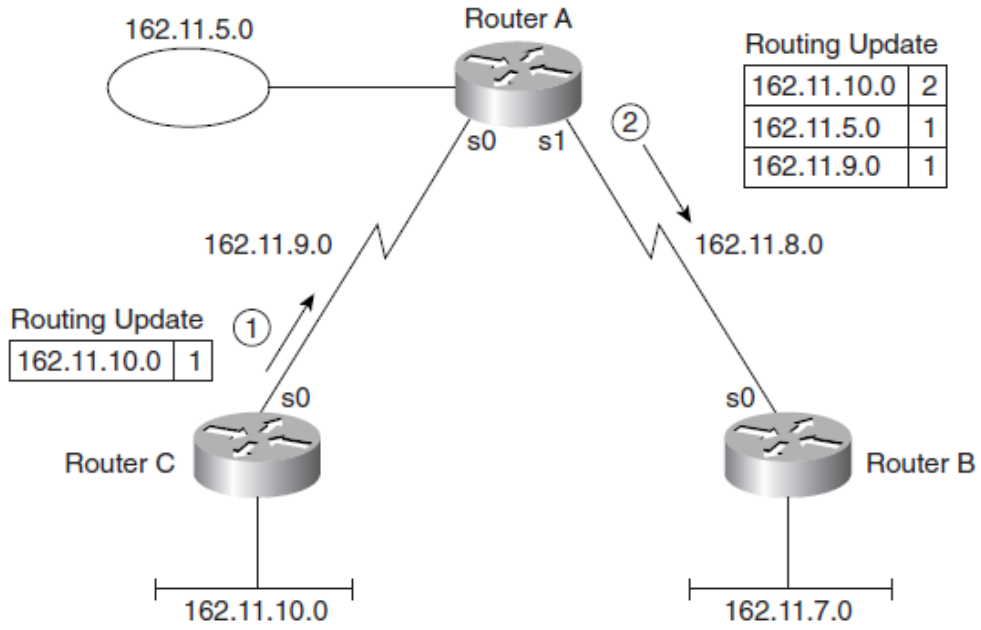


Table 6-3 shows the resulting routing table on Router B.

Router B Routing Table, After Receiving Update in Figure 6-2

Group (Mask Is 255.255.255.0)	Outgoing Interface	Next Router
162.11.5.0	S0	162.11.8.1
162.11.7.0	E0	
162.11.8.0	S0	
162.11.9.0	S0	162.11.8.1

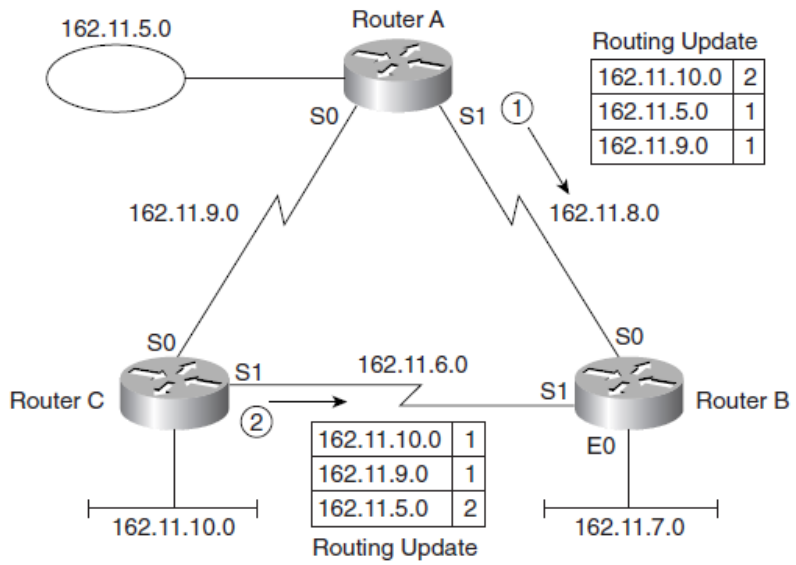
Router A Advertising Routes Learned from Router C



Router B Routing Table, After Receiving Update in Figure 6-3

Group	Outgoing Interface	Next Router
162.11.5.0	S0	162.11.8.1
162.11.7.0	E0	
162.11.8.0	S0	
162.11.9.0	S0	162.11.8.1
162.11.10.0	S0	162.11.8.1

Routers A and C Advertising to Router B



The routing updates in Figure 6-4 show only the information needed for the point being made in this example; other routes that would normally be in the routing update are omitted.

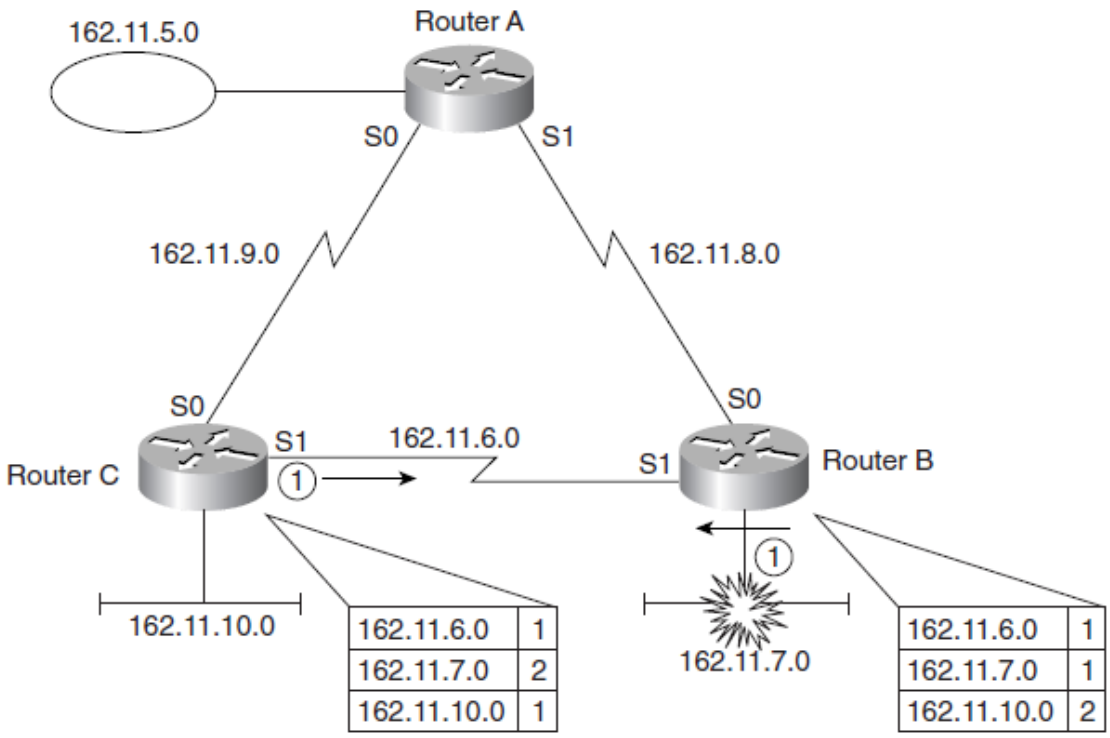
Router B Routing Table, with Two Routes to Same Subnet While Router B Serial 1 Is Down

Group	Outgoing Interface	Next Router	Metric
162.11.5.0	S0	162.11.8.1	1
162.11.7.0	E0		0
162.11.8.0	S0		0
162.11.9.0	S0	162.11.8.1	1
162.11.10.0	S0	162.11.8.1	2

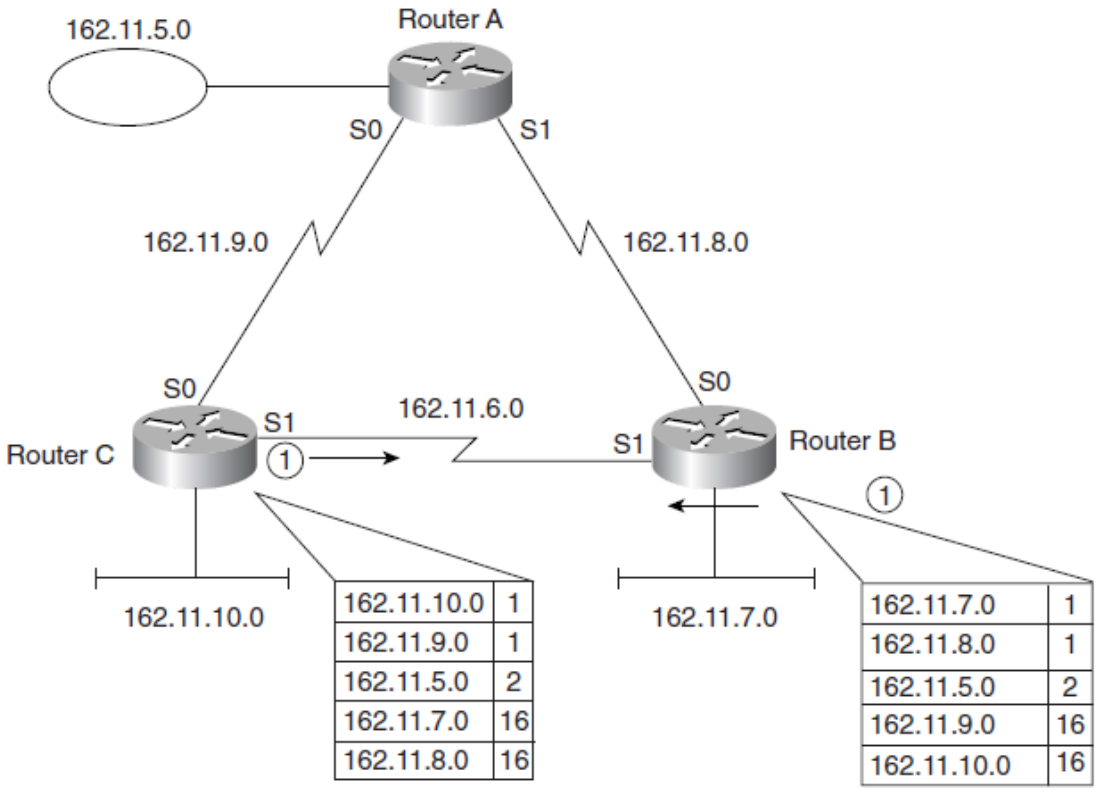
Router B Routing Table, with Two Routes to Same Subnet After Router B Serial 1 Is Up

Group	Outgoing Interface	Next Router	Metric
162.11.5.0	S0	162.11.8.1	1
162.11.6.0	S1		0
162.11.7.0	E0		0
162.11.8.0	S0		0
162.11.9.0	S0	162.11.8.1	1
162.11.10.0	S1	162.11.6.2	1

Advertisements Passing on Serial Link for Subnet 162.11.7.0



Split Horizon Enabled, with Poison Reverse



IGRP

RIP and IGRP Feature Comparison

Feature	RIP (Defaults)	IGRP (Defaults)
Update timer	30 seconds	90 seconds
Metric	Hop count	Function of bandwidth and delay (default); can include reliability, load, and MTU
Holddown timer	180	280
Flash (triggered) updates	Yes	Yes
Mask sent in update	No for RIP v1; yes for RIP v2	No
Infinity metric value	16	4,294,967,295

Practice

- Configuring Router
- Configuring Routing Protocols
- Troubleshooting Routing Process

Configuring Router

- General configuration
- Interfaces and ip addressing
- Enabling routing process

Configuring Routing Protocols

- Static routing
- RIP
- IGRP

Troubleshooting Routing Process

Case: Two PCs cannot ping each other trough router.

Hometasks

⚠️ Optional part of course. Essay.

1. Functionality of OSPF
2. Functionality of EIGRP
3. Functionality of BGP