

Chapter 1

Review: The OSI Reference Model and Classless Routing

Objectives

VLSM

RIP version 2



Chapter 1

Review: The OSI Reference Model and Routing Objectives

- Describe the overall function of the OSI reference model and the problems it solves
- Describe the characteristics of the:
 - OSI physical layer
 - OSI data link layer
 - OSI network layer
 - OSI transport layer
- Describe the function of routing in networks
- Understand the different classes of routing protocols



Benefits of the OSI Model?

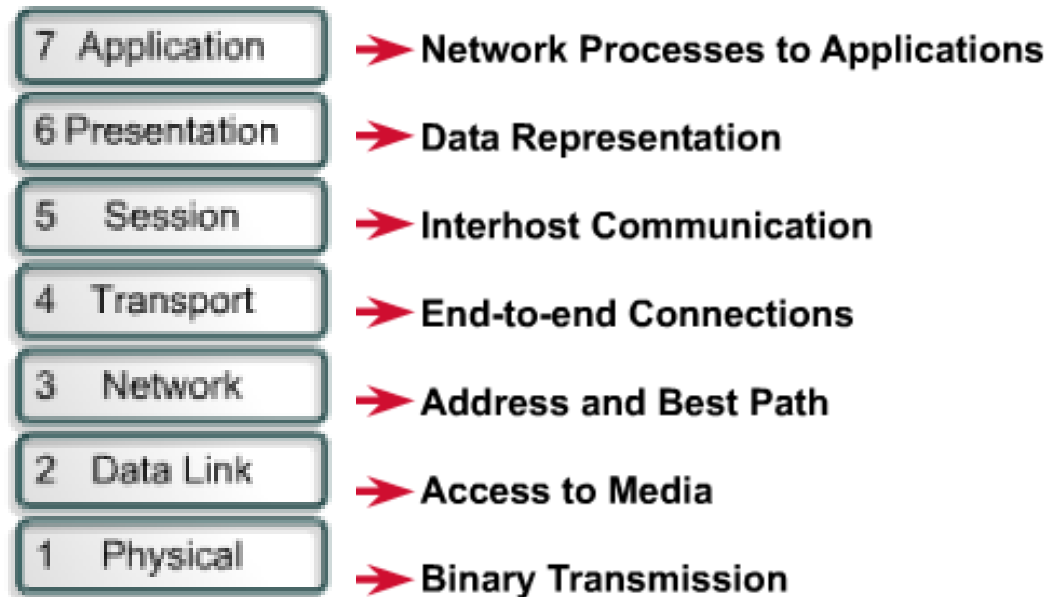


Benefits of the OSI Model:

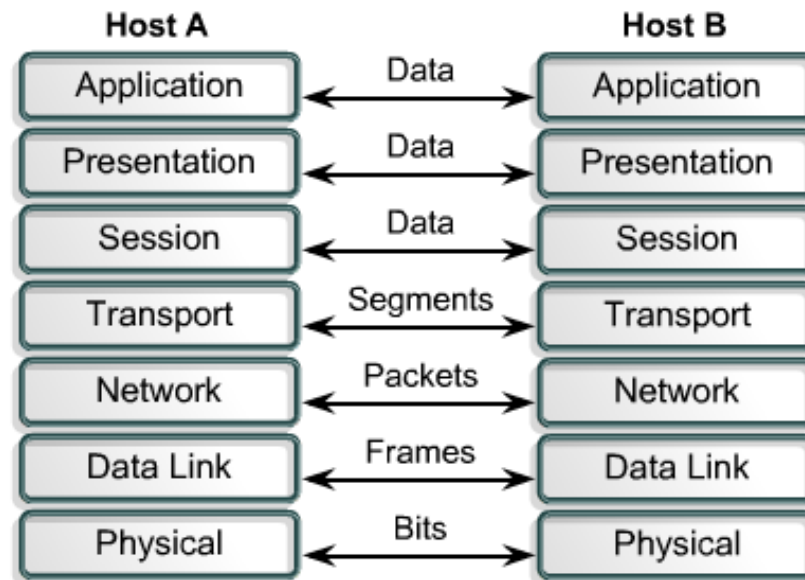
- Reduces complexity
- Standardizes interfaces
- Facilitates modular engineering
- Ensures interoperable technology
- Accelerates evolution
- Simplifies teaching and learning



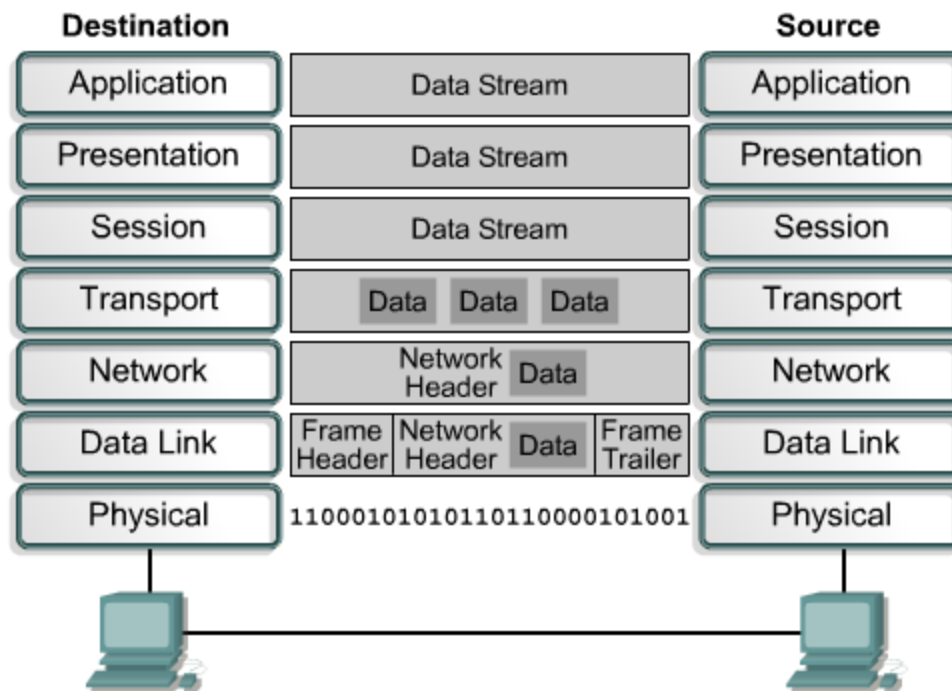
OSI Layers with Purpose



Peer-to-Peer Communication



Data Encapsulation



Types of Ethernet

- Ethernet and IEEE 802.3 — LAN specifications, which operate at 10 Mbps over coaxial and twisted-pair cable.
- 100-Mbps Ethernet — A single LAN specification, also known as Fast Ethernet, which operates at 100 Mbps over twisted-pair cable.
- 1000 Mbps Ethernet — A single LAN specification, also known as Gigabit Ethernet, which operates at 1000 Mbps (1 Gbps) over fiber and twisted-pair cables.
- 10 Gigabit Ethernet is only supported over fiber optic media.

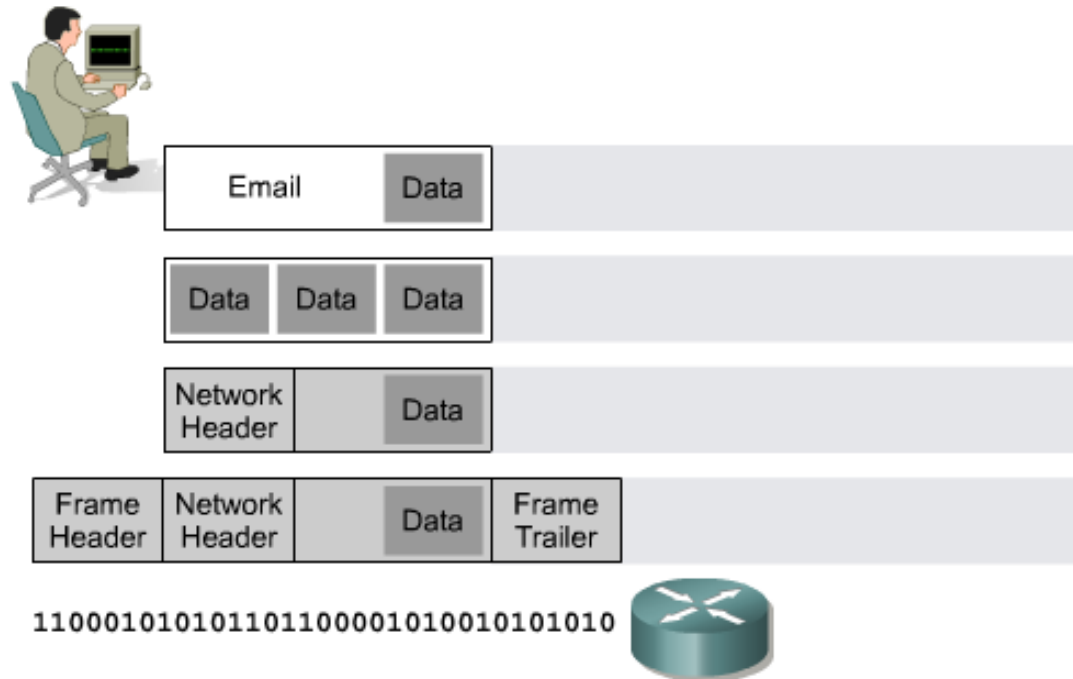


Three Varieties of 10 Mbps Ethernet

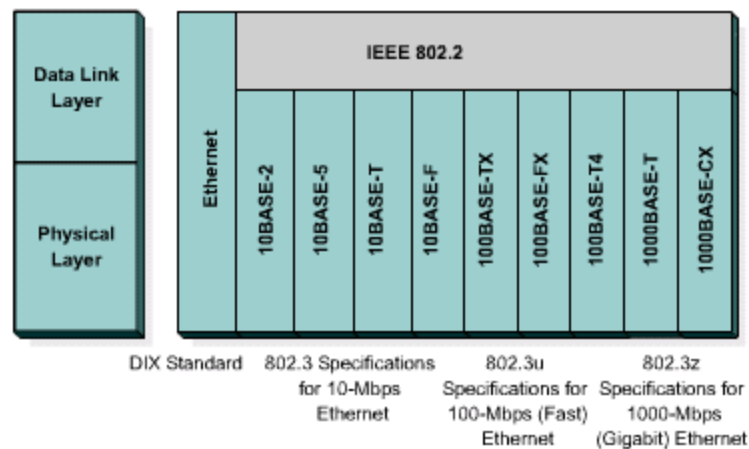
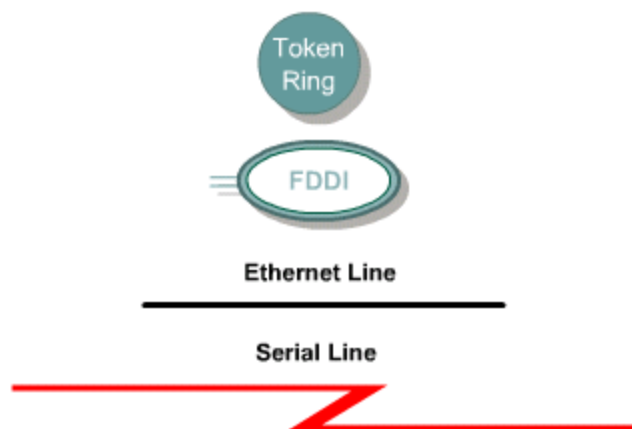
- 10BASE-2
 - Known as thin Ethernet or thinnet
 - Allows network segments up to 185 meters on coaxial cable
- 10BASE-5
 - Known as thick Ethernet or thicknet
 - Allows network segments up to 500 meters on coaxial cable
- 10BASE-T
 - Carries Ethernet frames on inexpensive twisted-pair wiring



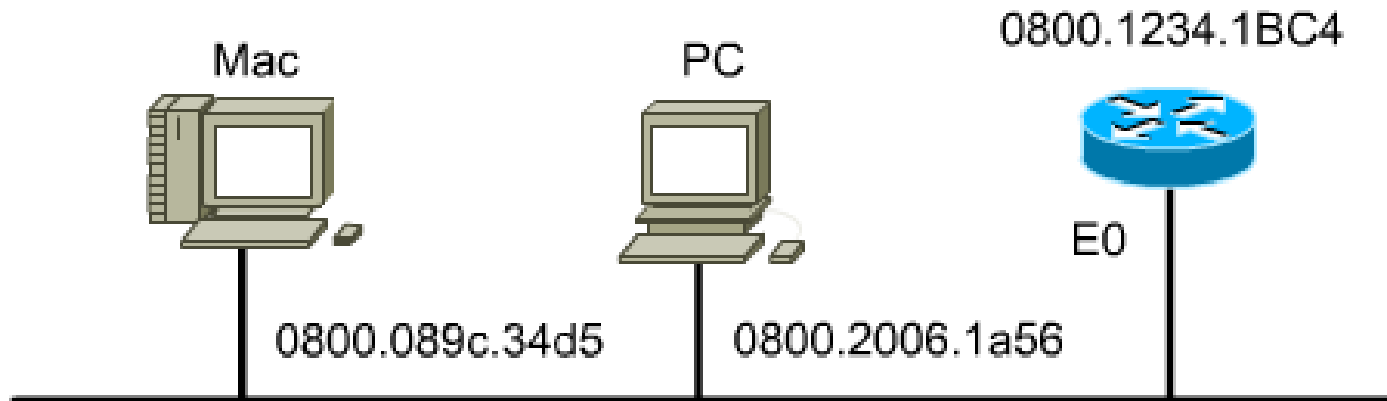
Encapsulation



The Physical Layer



The Data Link Layer

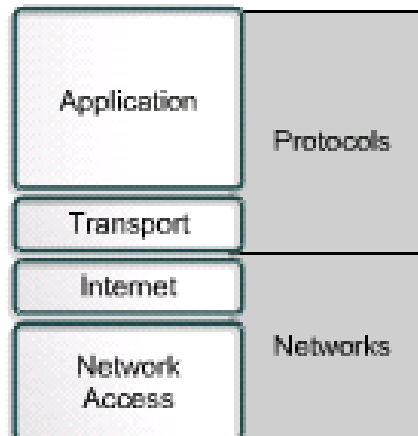


The Ethernet/802.3 Interface

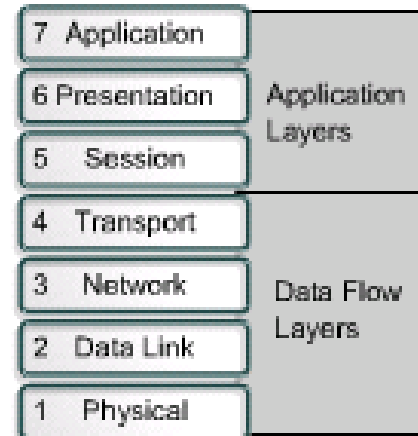


Comparing Models

TCP/IP Model



OSI Model



Address Classes

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



Address Class Prefixes

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

Class D addresses are used for multicast groups. There is no need to allocate octets or bits to separate network and host addresses. Class E addresses are reserved for research use only.



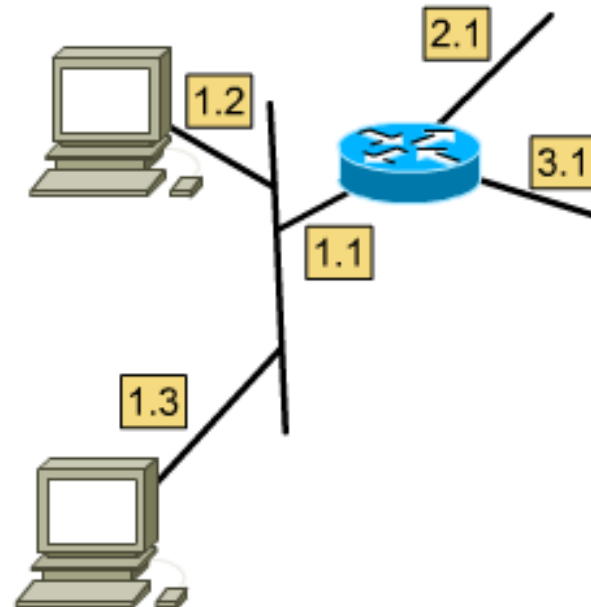
Subnetting Chart

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



Layer 3 Addresses - Path and Host Information

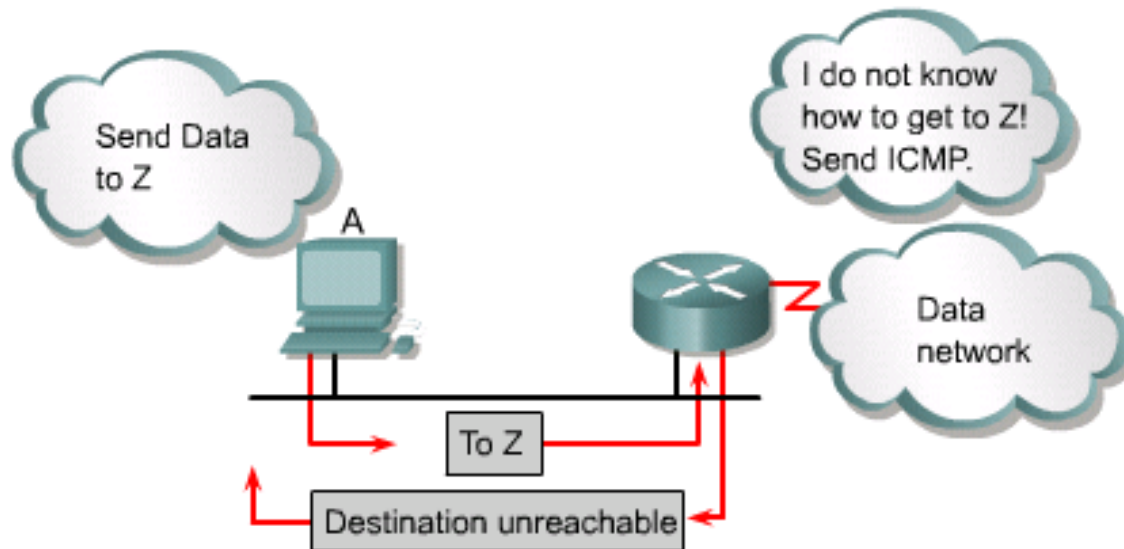
Network	Host
1	1
	2
	3
2	1
3	1



- ◆ Network Address - Location part used by the router
- ◆ Host Address - Specific port or device on the network



ICMP Testing

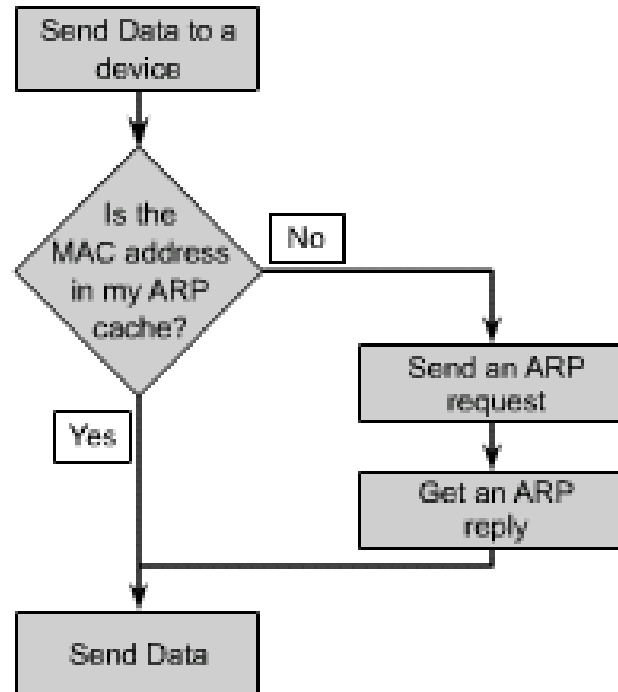


An ICMP destination unreachable message is sent if:

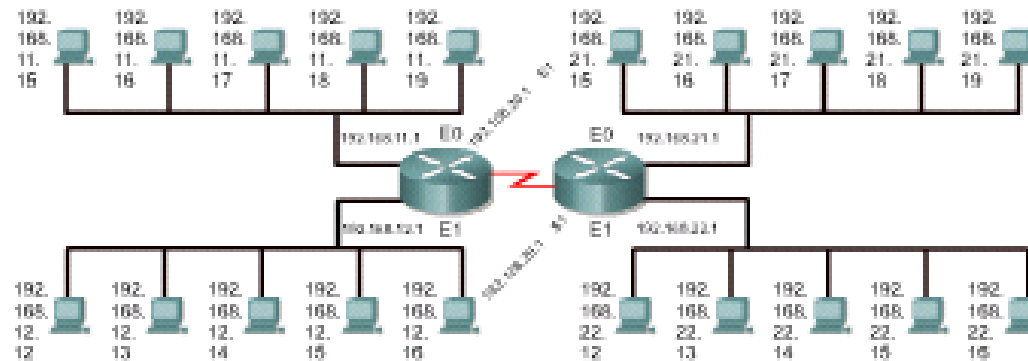
- Host or port unreachable
- Network unreachable



How ARP Works



Routing Table

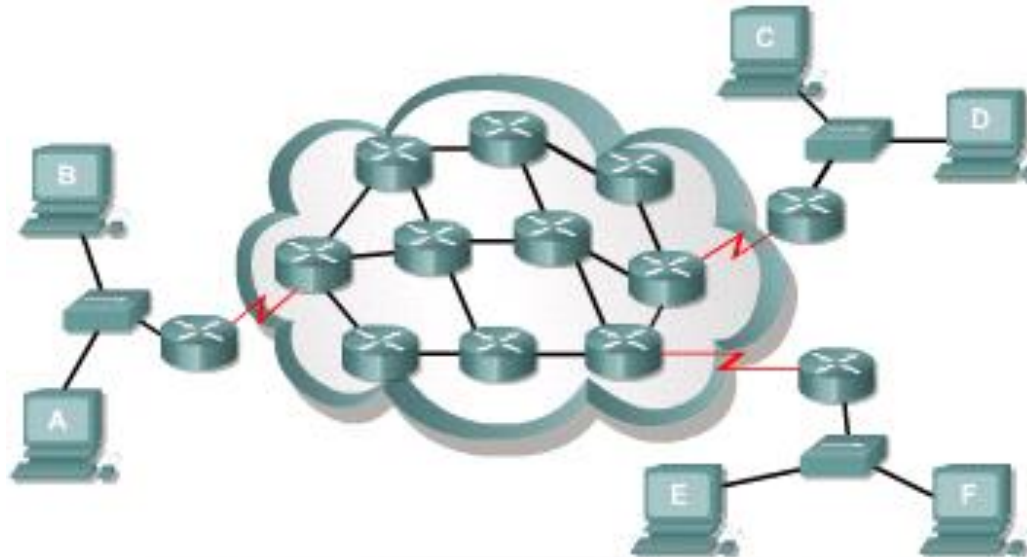


Learned	Network Address	Hop	Interface
C	192.168.11.0	0	E0
C	192.168.12.0	0	E1
C	192.168.20.0	0	S0
R	192.168.21.0	1	E0
R	192.168.22.0	1	E1

Learned	Network Address	Hop	Interface
C	192.168.21.0	0	E0
C	192.168.22.0	0	E1
C	192.168.30.0	0	S0
R	192.168.11.0	1	E0
R	192.168.12.0	1	E1



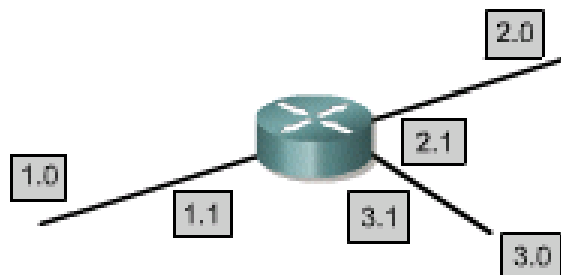
Path Determination



If computer A was sending data to computer F, what path would the data take? That is decided by their routers using routing protocols.



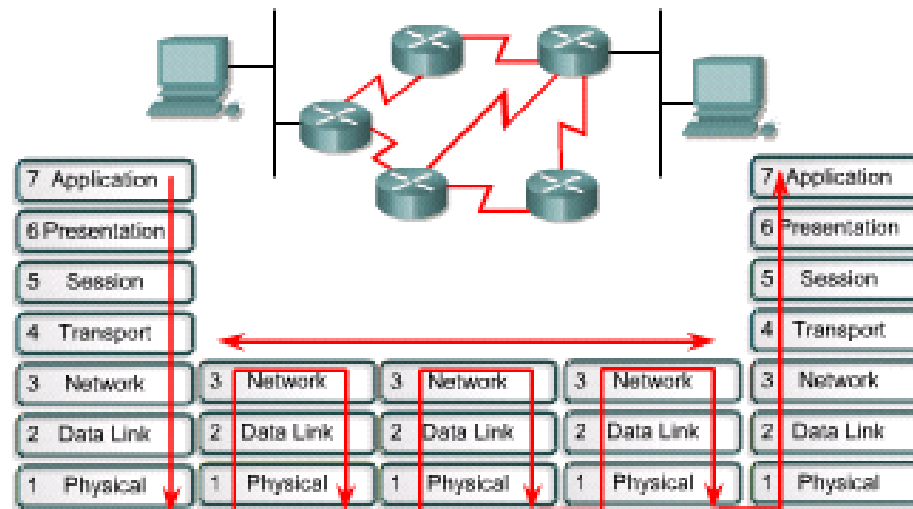
Network and Host Addressing



Destination Network	Direct and Router Port
1.0	1.1
2.0	2.1
3.0	3.1
• Network portion of address used to make path selections • Node portion of address refers to router port to the path	



Network Layer Devices in Data Flow



Each router Provides its services to support upper-layer functions

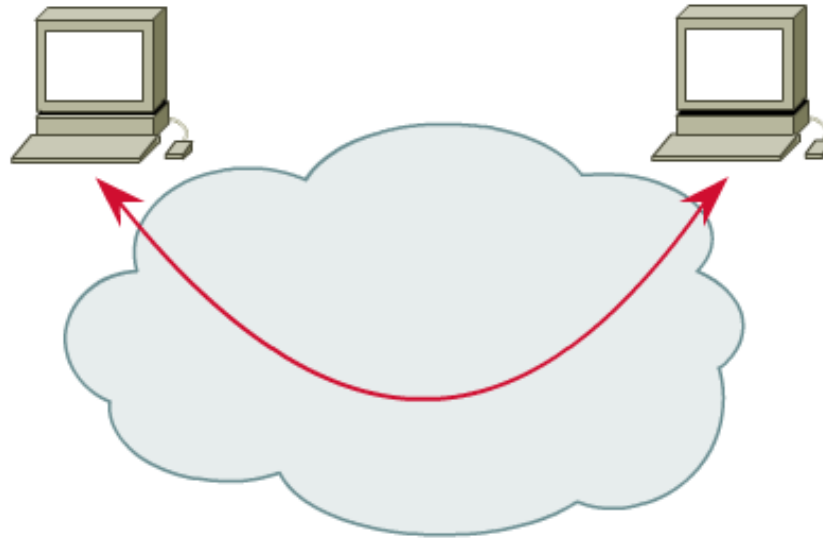


The Transport Layer

- Segmenting upper-layer applications
- Establishing a connection
- Data transfer
- Reliability with windowing
- Acknowledgment techniques



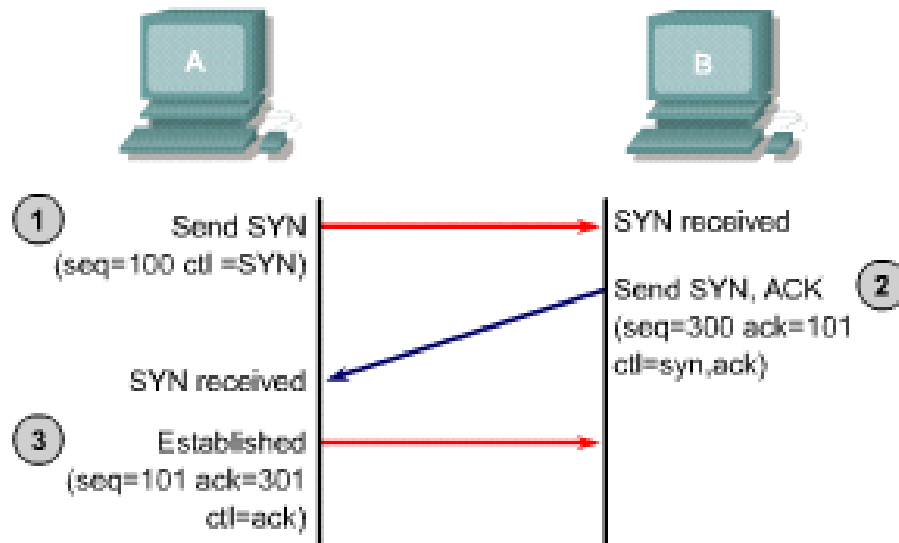
"Reliable" Transport



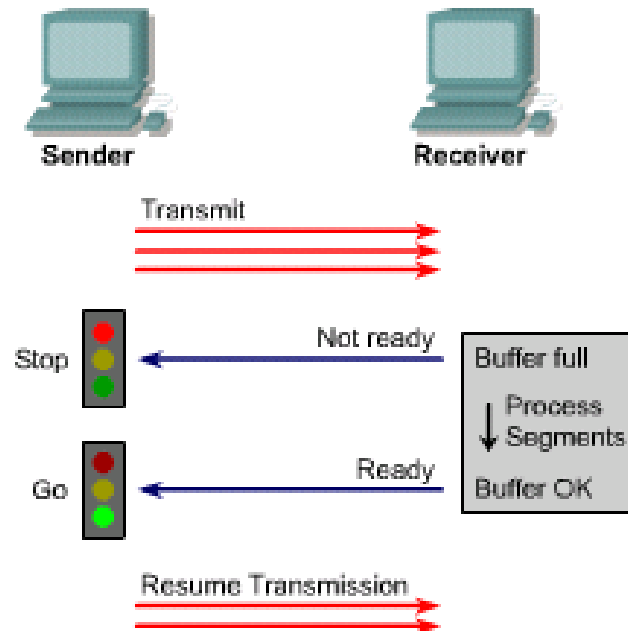
-
- ◆ Segments upper-layer applications
 - ◆ Establishes an end-to-end connection
 - ◆ Sends segments from one end host to another
 - ◆ Optionally, ensures data reliability



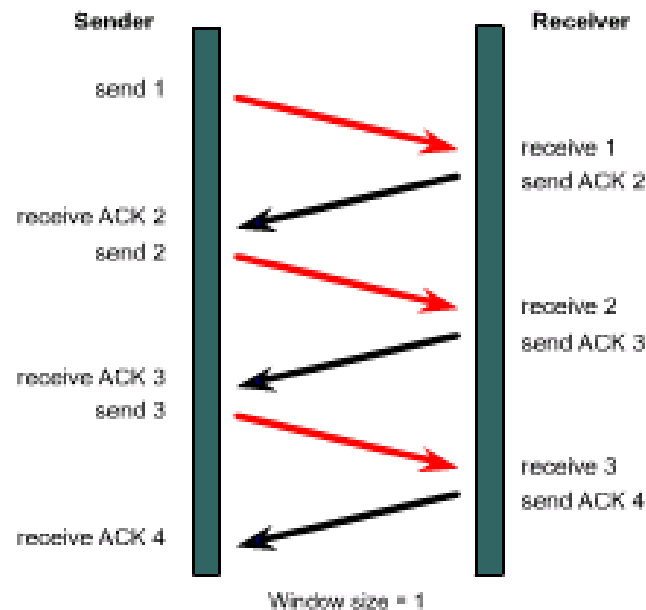
Three-Way Handshake



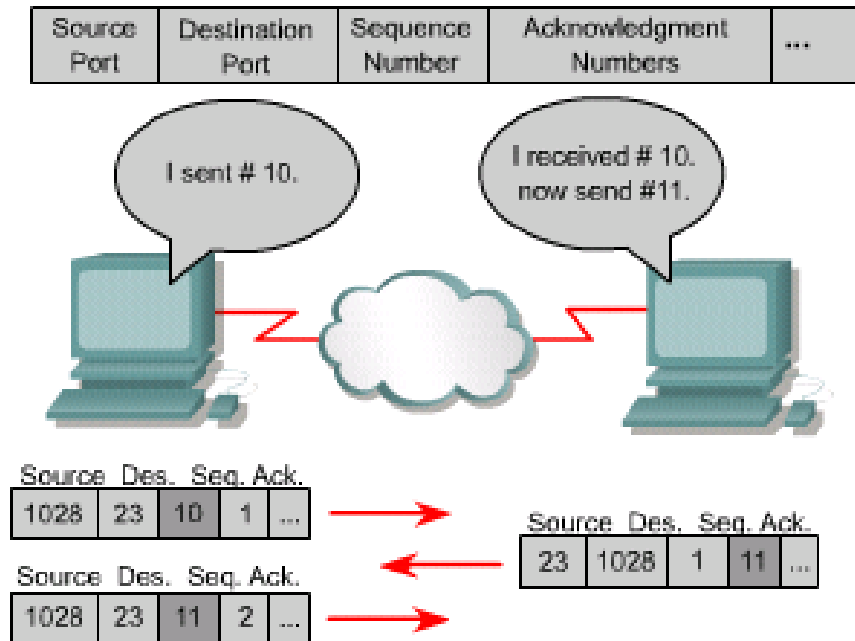
Data Transfer



Windowing – Flow Control



Positive Acknowledgment



What Is VLSM and Why Is It Used?

What is VLSM and why use it?

- Short term extensions to IPv4
- Subnetting 1985
- Variable length subnetting 1987
- Classless Interdomain Routing 1993
- Private IP addresses
- Network Address Translation (NAT)

VLSM is supported by:

- OSPF
- IS-IS
- EIGRP
- RIP v2
- Static routing

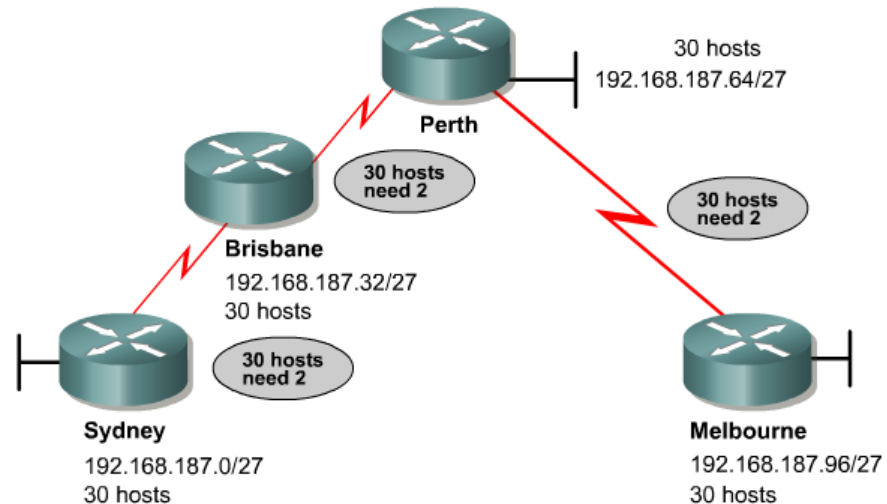
What is VLSM and why use it?

- Ultimate solution: IPv6 128 bit address space
- Allows for: 340,283, 366, 920, 938, 463, 374, 607, 431, 768, 211, 456 possibilities

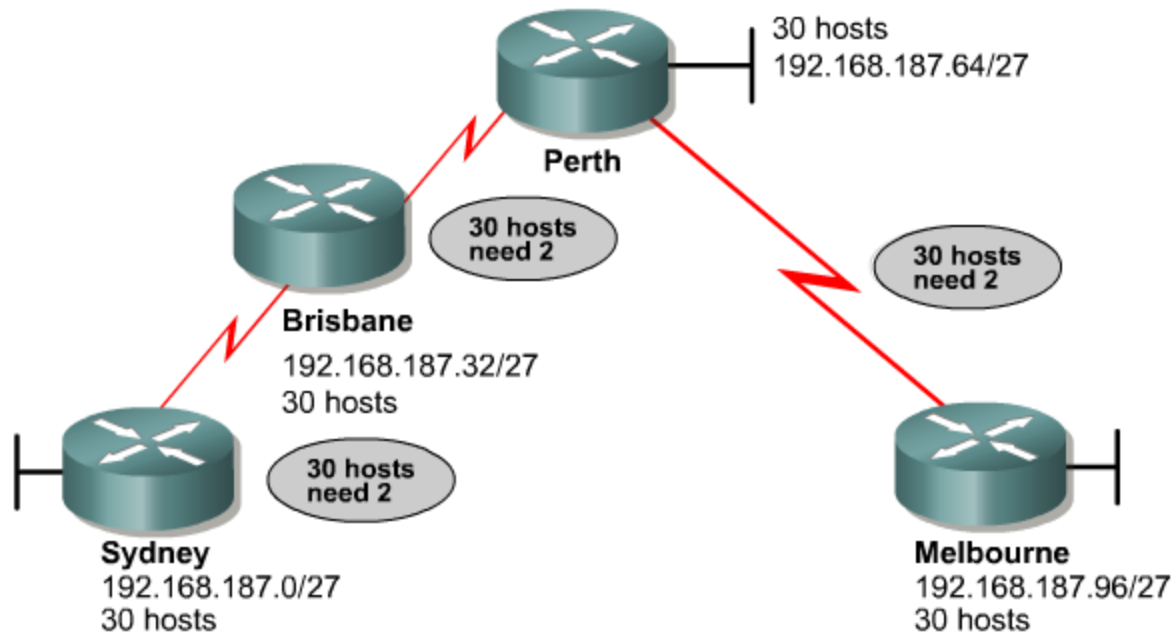


Wasting Space

Subnet Number	Subnet Address	
Subnet 0	192.168.187.0	/27
Subnet 1	192.168.187.32	/27
Subnet 2	192.168.187.64	/27
Subnet 3	192.168.187.96	/27
Subnet 4	192.168.187.128	/27
Subnet 5	192.168.187.160	/27
Subnet 6	192.168.187.192	/27
Subnet 7	192.168.187.224	/27



When to Use VLSM?



Use VLSM on the point to point links to use only 2 valid host addresses instead of wasting 30.



Calculating Subnets with VLSM

Subnetted Address: 172.16.32.0/20

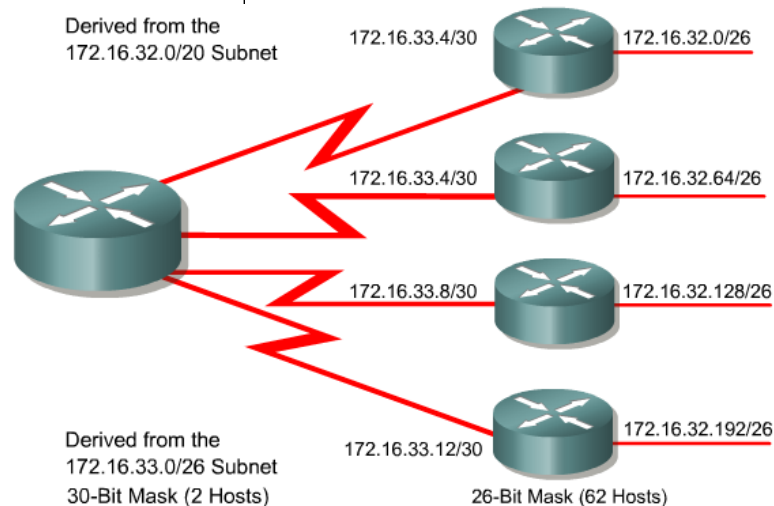
In Binary 101011100.00010000.00100000.00000000

VLSM Address: 172.16.32.0/26

In Binary 101011100.00010000.00100000.00000000

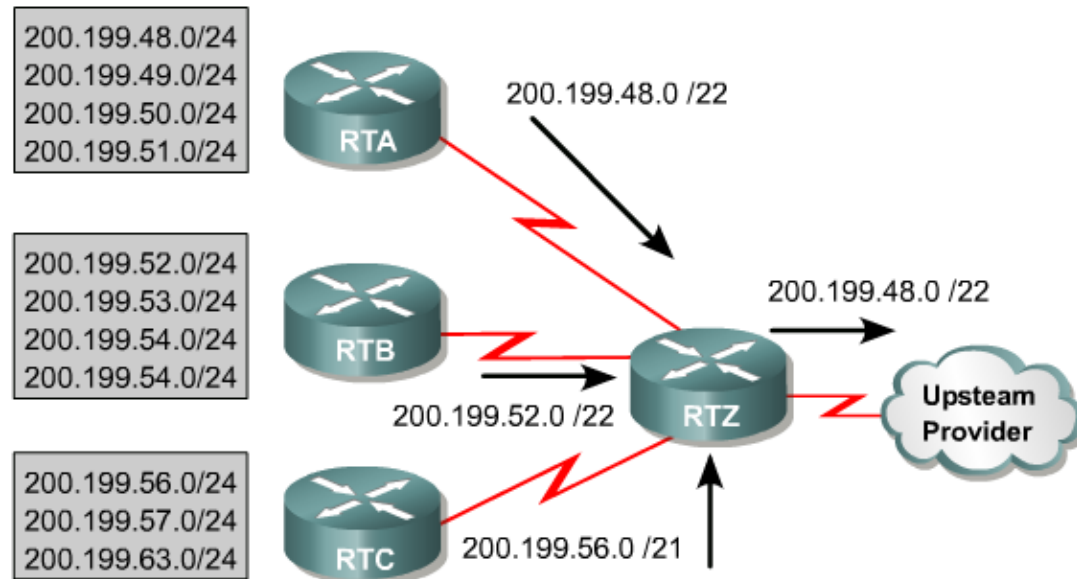
1st subnet:	172	•	16	.0010	0000.00	000000 = 172.16.32.0/26
2nd subnet:	172	•	16	.0010	0000.01	000000 = 172.16.32.64/26
3rd subnet:	172	•	16	.0010	0000.10	000000 = 172.16.32.128/26
4th subnet:	172	•	16	.0010	0000.11	000000 = 172.16.32.192/26
5th subnet:	172	•	16	.0010	0001.00	000000 = 172.16.33.0/26
	Network		Subnet	VLSM Subnet	Host	

Derived from the
172.16.32.0/20 Subnet



Route Aggregation

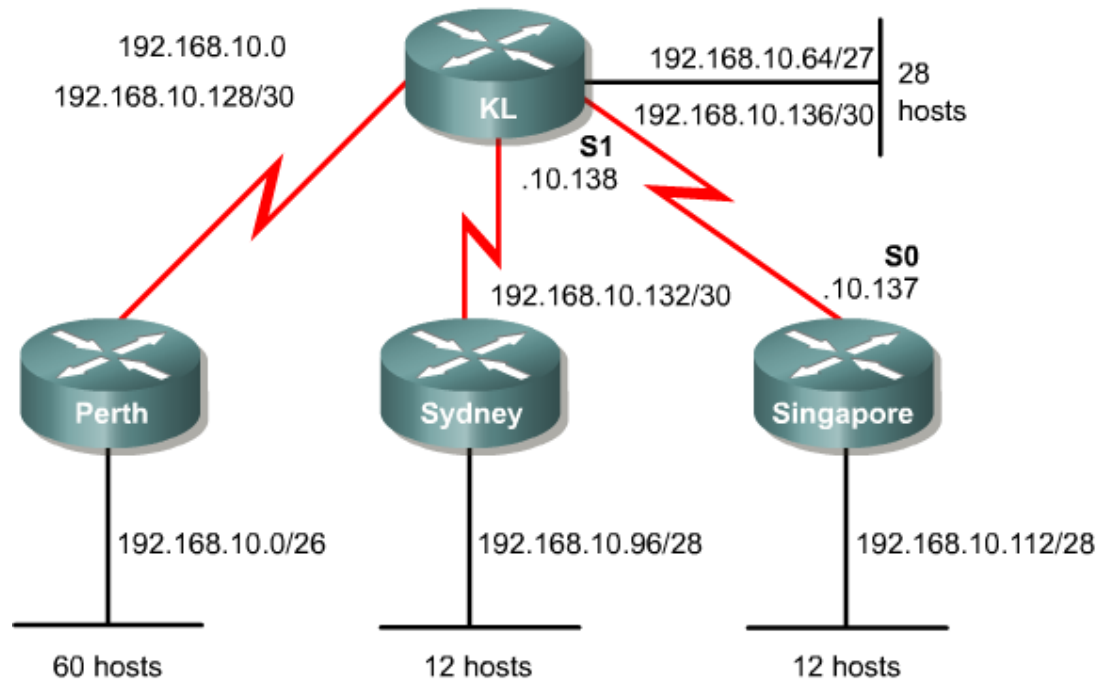
- Keeping the networks close to one another saves routing table space
- Every network needs a separate entry in the routing table
- Each subnet needs a separate entry.
- Allow for aggregation can reduce the size of the routing table.



Route summarization reduces routing table size by aggregating routes to multiple networks into one supernet.



Configuring VLSM



RIP version 2

RIP History

- RIPv1 has the following limitations:
 - It does not send subnet mask information in its updates.
 - It sends updates as broadcasts on 255.255.255.255.
 - It does not support authentication.
 - It is not able to support VLSM or classless interdomain routing (CIDR).



RIPv2 Features

Feature	Description
Transmits subnet mask with route	Enables VLSM by passing the mask along with each route so that the subnet is exactly defined.
Provides authentication	Both clear text and/or MD5
Includes a next-hop route IP address in its routing update	A router can advertise a route and direct any listeners to a different router on the same subnet (if the other router has a better route).
Uses external route tags	RIP can pass information about routes learned from an external source and redistributed into RIP. This is used to separate RIP routes from externally learned routes.
Provides multicast routing updates	Instead of sending updates to 255.255.255.255, the destination IP address is 224.0.0.9. This reduces the amount of processing required on non-RIP speaking hosts on a common subnet.

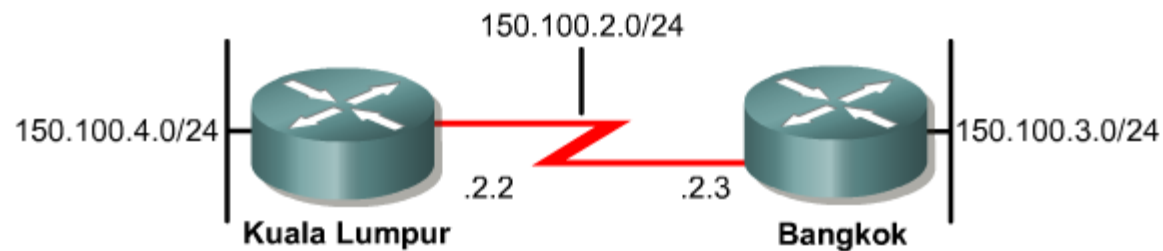


Comparing RIPv1 and RIPv2

RIP v1	RIP v2
Easy to configure	Easy to configure
Only supports classful routing protocol	Supports use of classless routing
No subnet information with the routing update	Sends subnet mask information with the routing updates
Does not support prefix routing - all the devices in the same network must use the same subnet mask.	Supports prefix routing - different subnets within the same network can have different subnet masks (VLSM)
No authentication in updates	Provides for authentication in its updates
Broadcasts over 255.255.255.255	Multicasts routing updates over the Class D address 224.0.0.9 - makes it more efficient



Configuring RIPv2

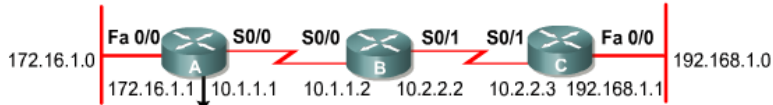


```
Kuala Lumpur (config) #router rip
Kuala Lumpur (config) #version 2
Kuala Lumpur (config) #network 150.100.4.0
Kuala Lumpur (config) #network 150.100.2.0
```

```
Bangkok (config) #router rip
Bangkok (config) #version 2
Bangkok (config) #network 150.100.2.0
Bangkok (config) #network 150.100.3.0
```



Verifying RIPv2



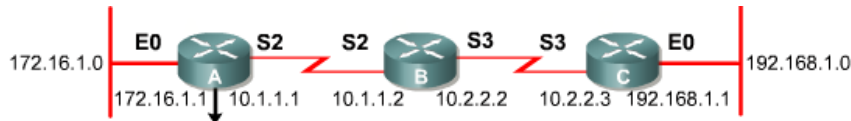
```
RouterA#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 12 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter lists for all interfaces is
  Incoming update filter lists for all interfaces is
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface    send  Recv  Triggered  RIP  Keychain
    Ethernet      1     1 2
    Serial2       1     1 2
Routing for Networks:
  10.0.0.0
  172.16.0.0
Routing Information Sources:
  Gateway         Distance      Last Update
  (this router)   120           0:2:12:15
  10.1.1.2       120           0:1:09:01
Distance: (default is 120)
```

```
RouterA#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
       N1 - OSPF external type 1, E2 - OSPF external type 2, * -
candidate
default
       U - Per-user static route, 0 = CCR
       T - Traffic engineered route

Gateway of last resort is not set
  172.16.0.0/24 is subnetted, 1 subnets
C    172.16.1.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 2 subnets
R    10.2.2.0 (120/1) via 10.1.1.2, 00:00:07, Serial 0/0
C    10.1.1.0 is directly connected, Serial 0/0
R    192.168.1.0/24 (120/2) via 10.1.1.2, 00:00:07, Serial 0/0
```



Troubleshooting RIPv2



```
RouterA#debug ip rip
RIP protocol debugging is on
RouteA#
00:06:24:RIP:received v1 update from 10.1.1.2 on Serial2
00:06:24:    10.2.2.0 in 1 hops
00:06:24:    192.168.1.0 metric 3
00:06:33:RIP sending v1 update to 255.255.255.255 via Ethernet0
(172.16.1.1.)
00:06:34:    network 10.0.0.0, metric 2
00:06:34:RIP sending v1 update to 255.255.255.255 via Serial2
(10.1.1.1)
00:06:34:    network 172.16.0.0, metric 1
```

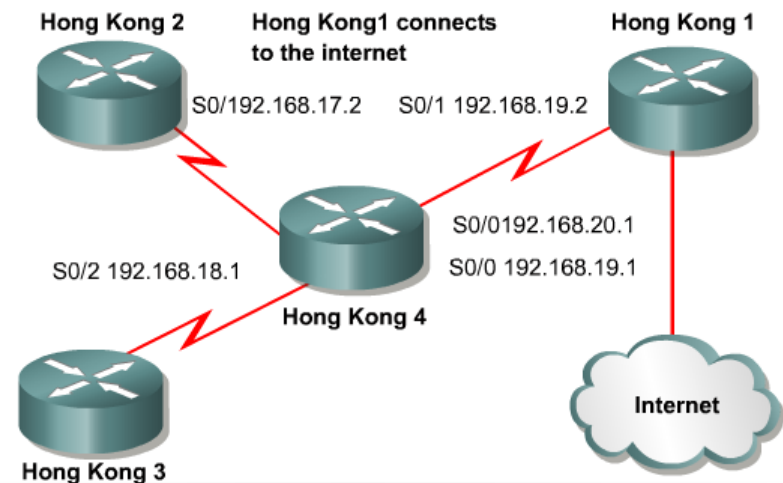
Output	Possible significance
RIP: broadcasting general request on Ethernet0	At startup Transition of interface at startup User manually clearing interface
RIP: bad version 128 from 160.89.80.43	Malformed packet from the transmitter
RIP: received v2 update from 150.100.2.3 on Serial0	Shows Version 2 RIP is receiving
RIP: sending v1 update to 255.255.255 via Serial0 (150.100.2.2)	Shows Version 1 RIP is operating
RIP: ignored v1 packet from 150.100.2.2 (illegal version)	Shows that the router is not going to deal with a RIP v1 packet
RIP: sending v2 update to 224.0.0.9 via FastEthernet0 (150.100.3.1)	Shows RIP version 2 is sending
RIP: build update entries 150.100.2.0/24 via 0.0.0.0 metric 1, tag	Shows use of default route and tag



Default Routes

- **Default routes** — The system administrator manually defines default routes as the path to take when there is no known route to the destination.
- Default routes keep routing tables shorter.

Command	Description
<code>ip default-network 192.168.20.0</code>	IP network number or subnet number defined as the default
<code>255.255.255.0</code>	Subnet mask indicates that 8 bits of subnetting are in effect
<code>172.16.2.1</code>	ip address of next-hop router in the path to the destination



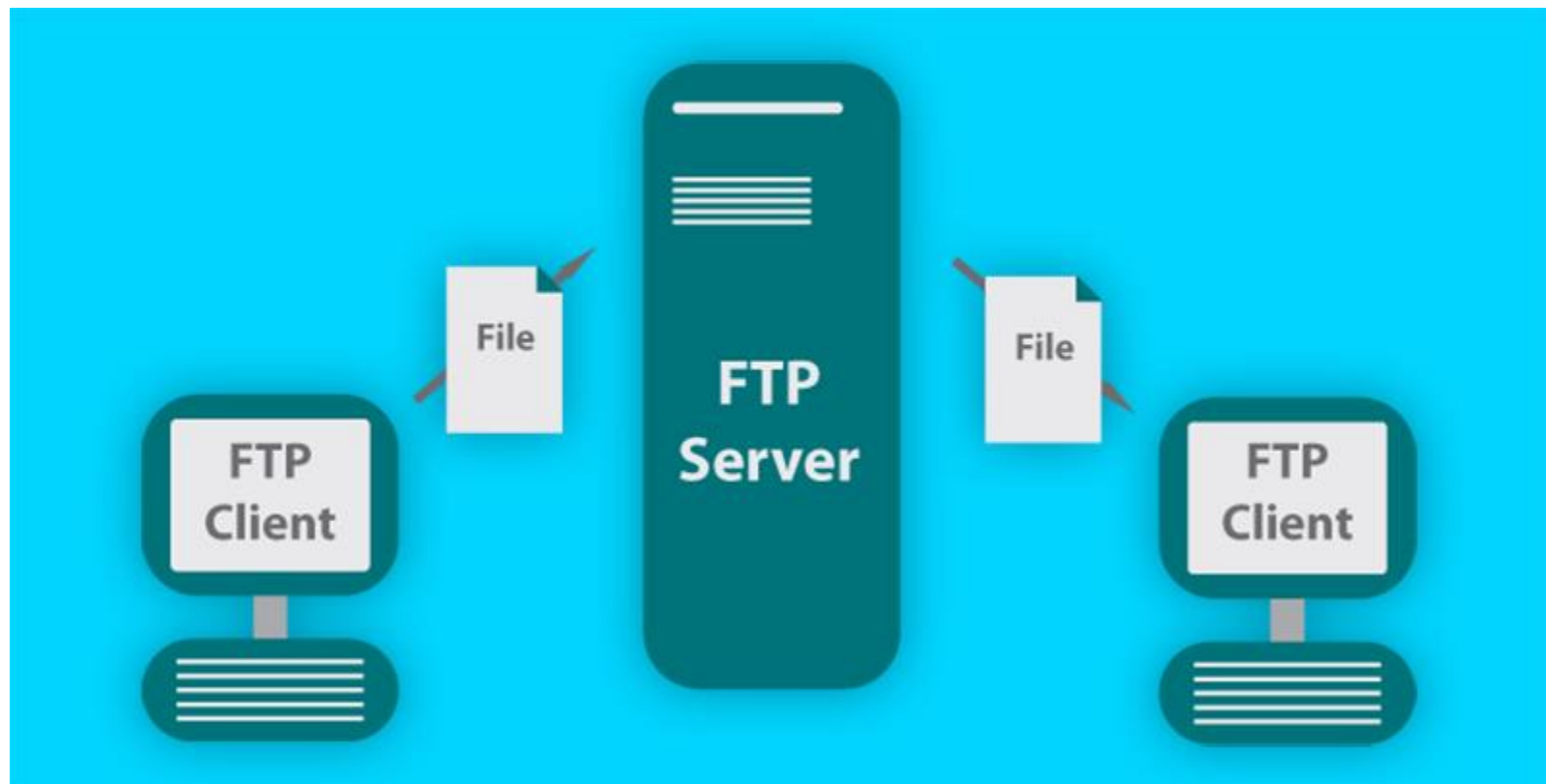
Configure HK2, HK3 & HK4 # ip default-network 192.168.20.0



File Transfer Protocol (FTP)

- The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.
- FTP is built on a client-server model architecture using separate control and data connections between the client and the server.[1] FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP).

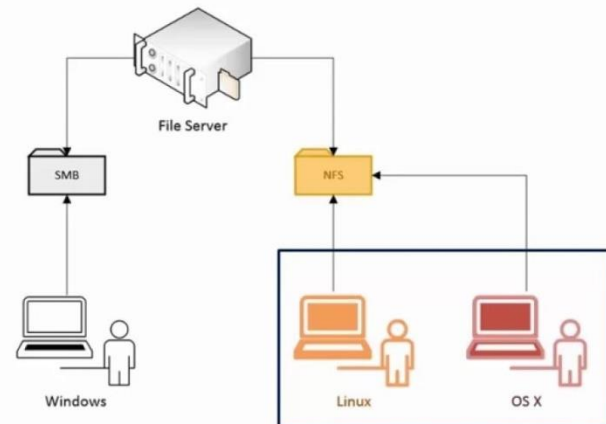




Network File System

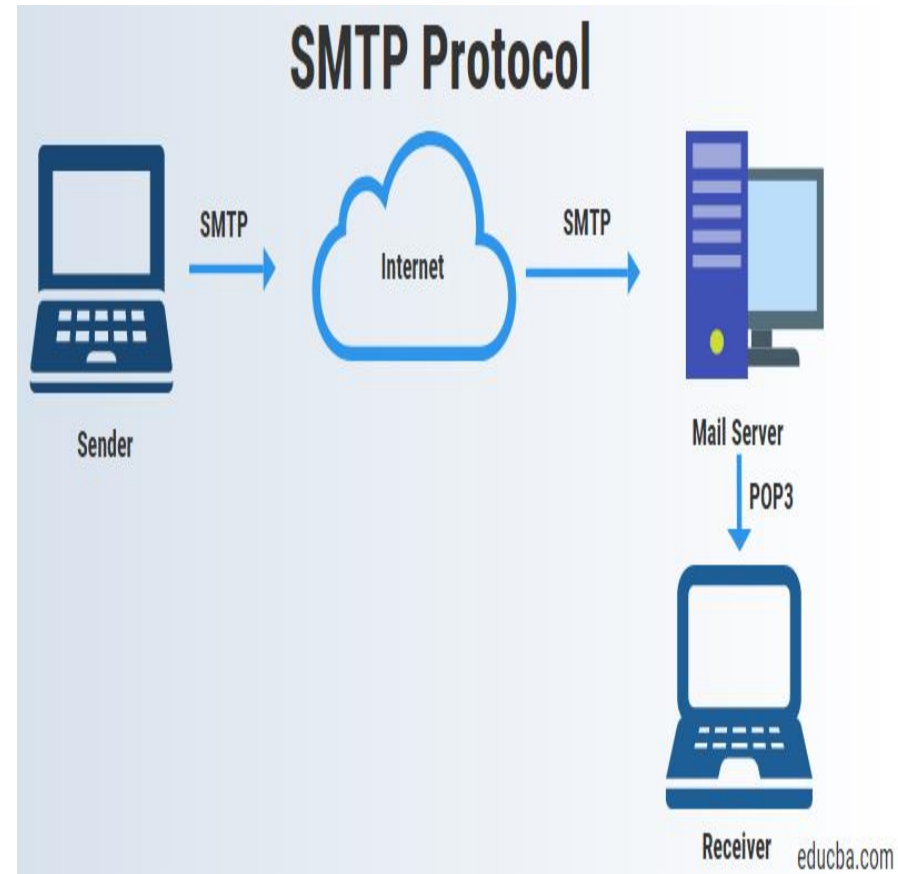
- The **Network File System** (NFS) is a client/server application that lets a computer user view and optionally store and update **files** on a remote computer as though they were on the user's own computer. The NFS protocol is one of several distributed **file system** standards for **network-attached storage** (NAS).

Network File System (NFS) Server



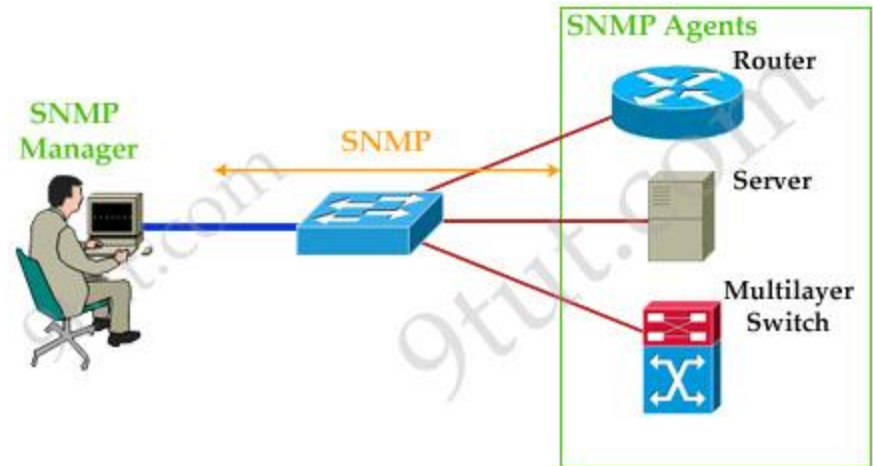
Simple Mail Transfer Protocol

- The **Simple Mail Transfer Protocol (SMTP)** is a communication **protocol** for electronic **mail** transmission. User-level email clients typically use **SMTP** only for sending messages to a **mail** server for relaying, and typically submit outgoing email to the **mail** server on port 587 or 465 as per RFC 8314.



Simple Network Management Protocol (SNMP)

- **Simple Network Management Protocol (SNMP)** is an [Internet Standard](#) protocol for collecting and organizing information about managed devices on [IP](#) networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more



Domain name system

- The **Domain Name System (DNS)** is a hierarchical and decentralized naming system for ...
This **means** that a resolving name server must issue another **DNS** request to find out the IP address of the server to which it has been referred.

