CSET 150

NETWORK DESIGN AND MANAGEMENT

EVENING MASTERS EDITION

DR. MAHBOOB QAOSAR

ASSOCIATE PROFESSOR, CSE, RU

Chapter 3: IPv4 Routing Design

Network Design: Design Principles, Determining Requirements, Analyzing the Existing Network, Preparing the Preliminary Design, Completing the Final Design Development, Deploying the Network, Monitoring and Redesigning, Maintaining, Design Documentation, Modular Network Design, Hierarchical Network Design, The Cisco Enterprise Composite Network Model.

Technologies - Switching Design: Switching Types, Spanning, Tree Protocol, Redundancy in Layer 2 Switched Networks, STP Terminology and Operation, Virtual LANs, Trunks, Inter VLAN Routing, Multilayer Switching, Switching Security and Design Considerations. IPv4 Address Design, Private and Public Addresses, NAT, Subnet Masks, Hierarchical IP Address Design, IPv4 Routing Protocols, Classification, Metrics, Routing Protocol Selection.

Network Security Design: Hacking, Vulnerabilities, Design Issues, Human Issues, Implementation Issues, Threats, Reconnaissance Attacks, Access Attacks, Information Disclosure Attacks, Denial of Service Attacks, Threat Defense, Secure Communication, Network Security Best Practices, SAFE Campus Design.

Wireless LAN Design: Wireless Standards, Wireless Components, Wireless Security, Wireless Security Issues, Wireless Threat Mitigation, Wireless Management, Wireless Design Considerations, Site Survey, WLAN Roaming, Wireless IP Phones, Quality of Service Design, QoS Models, Congestion Avoidance, Congestion Management.

Network Management: ISO Network Management Standard, Protocols and Tools, SNMP, MIB, RMON NetFlow, Syslog, Network Management Strategy, SLCs and SLAs, IP Service-Level Agreements, Content Networking Design, Case Study, Venti Systems.

How Routers Use Subnet Masks

- When you configure the IP address of a router's interface, you include the **address** and the **subnet mask.**
  - The router uses this information not only to address the interface but also to determine the address of the subnet to which the interface is connected.
- The router then puts this subnet address in its routing table, as a connected network on that interface.

How Routers Use Subnet Masks

To determine the network or subnet address to which a router is connected, the router performs a logical AND of the interface address and the subnet mask. Logically "ANDing" a binary 1 with any number yields that number; logically "ANDing" a binary 0 with any number yields 0.

Table 3-1 *Example Calculation of Subnet Address*

	Network	**Subnet**	**Subnet**	**Host**
Interface IP Address 10.5.23.19	00001010	00000101	00010111	00010011
Subnet Mask 255.255.255.0	11111111	11111111	11111111	00000000
Subnet Address 10.5.23.0	00001010	00000101	00010111	00000000

How Routers Use Subnet Masks

- **When a packet arrives at the router,**
  - the router analyzes the destination address of the packet to determine which network or subnet it is on.
  - The router looks up this network or subnet in its routing table to determine the interface through which it can best be reached;
  - the packet is then sent out of the appropriate router interface.
  - [If the router does not have a route to the destination subnet, the packet is rejected and an **Internet Control Message Protocol (ICMP)** error message is sent to the source of the packet.]

Subnet Mask to Use

- **Determining the Subnet Mask to Use**
  - … depends on the number of **subnets required** and
  - the number of **host addresses** required on each of these subnets

Determining the Subnet Mask to Use

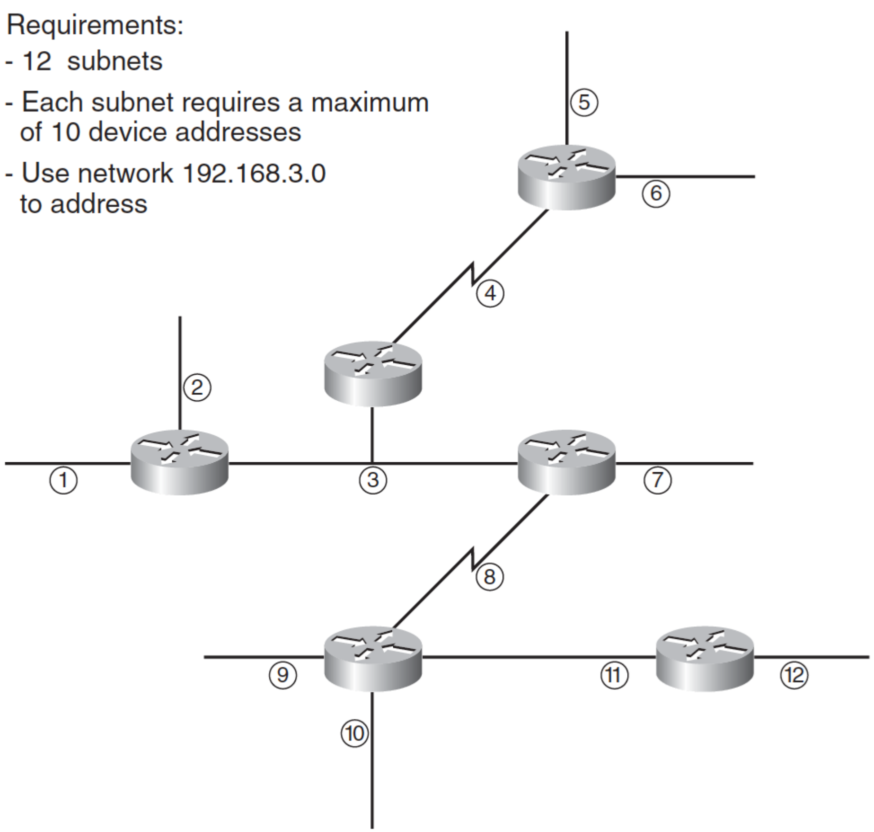


Figure 3-2 *The Number of Subnets and Hosts Required Determines the Subnet Mask to Use*

- A total of 12 subnets exist in this network;
- Each has a maximum of 10 device addresses.
- Some of the addresses are for router interfaces and some are for hosts (not shown in the figure);
- each device on each subnet needs to have its own IP address.

- Select a series : say 192.168.3…

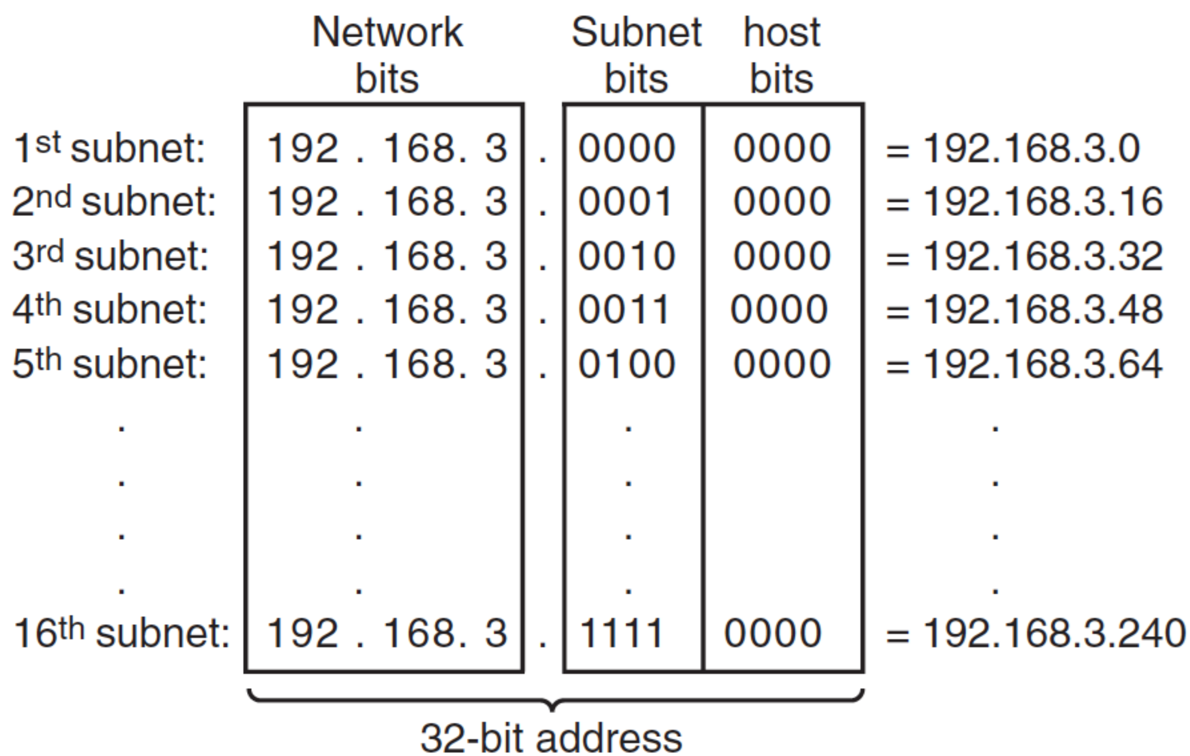
Determining the Subnet Mask to Use

- Number of subnet required 12 2^4 4 bits needed
- Number of host address required 10 2^4 4bit needed

- IPv4 32 bit – 8 bit . 8 bit . 8 bit . **8 bit**
- 8 bit . 8 bit . 8 bit . **4 bit (Subnet) + 4 bit (Host)**
- **255. 255 . 255. 1111000 255.255.255.240 –** network mask or subnet mask

Determining the Subnet Mask to Use

Figure 3-3 *Calculating Subnet Addresses*



Thus, the first subnet address that can be used with a mask of 255.255.255.240 is 192.168.3.0; this can also be written as 192.168.3.0/28. The second subnet is 192.168.3.16/28, and so on.

Determining the Subnet Mask to Use

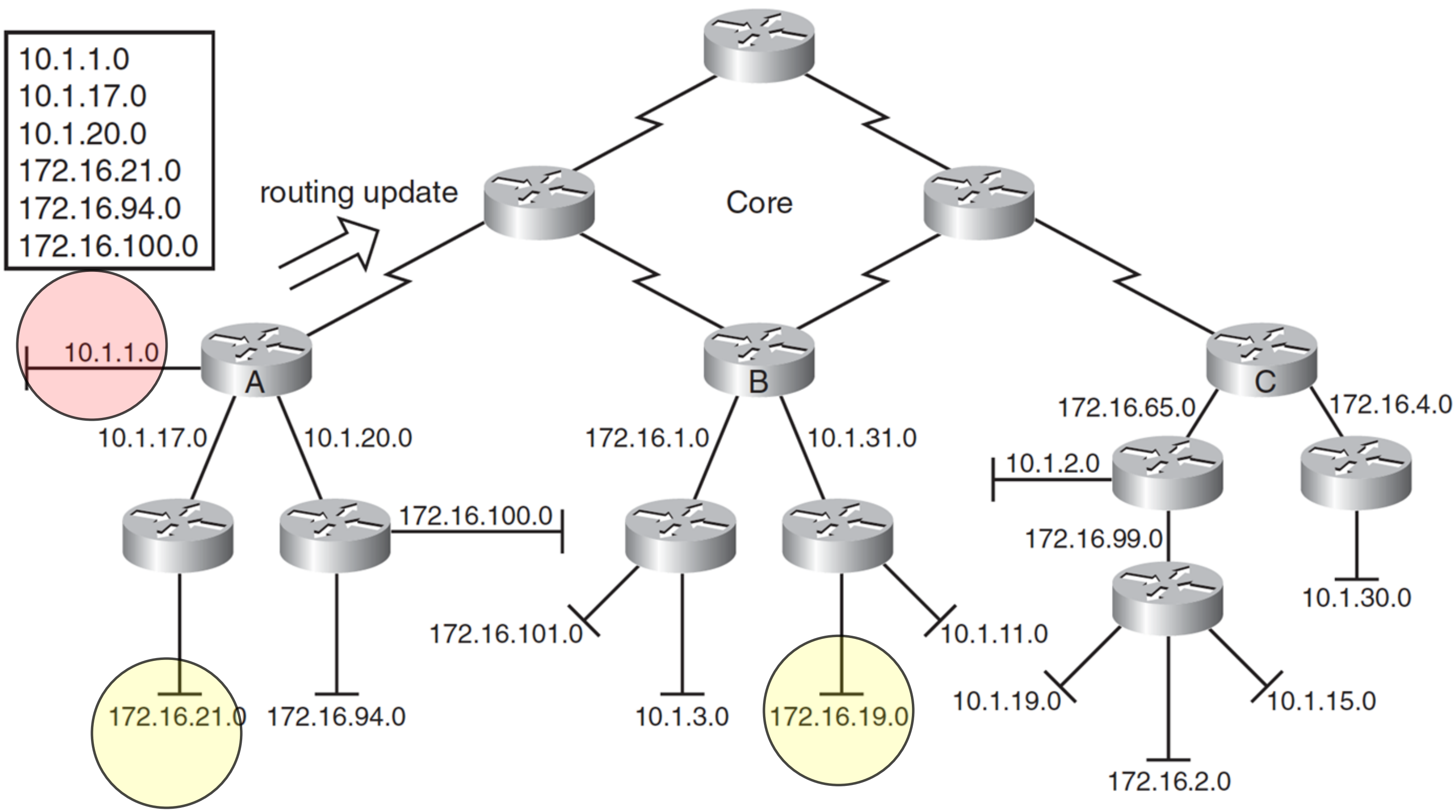
Figure 3-4 *Calculating Device Addresses*

	Network bits		Subnet bits	host bits	
Subnet address	192 . 168. 3	.	0010	0000	= 192.168.3.32
1st host address	192 . 168. 3	.	0010	0001	= 192.168.3.33
2nd host address	192 . 168. 3	.	0010	0010	= 192.168.3.34
.	.		.	.	.
.	.		.	.	.
.	.		.	.	.
.	.		.	.	.
Last host address	192 . 168. 3	.	0010	1110	= 192.168.3.46
Broadcast address	192 . 168. 3	.	0010	1111	= 192.168.3.47

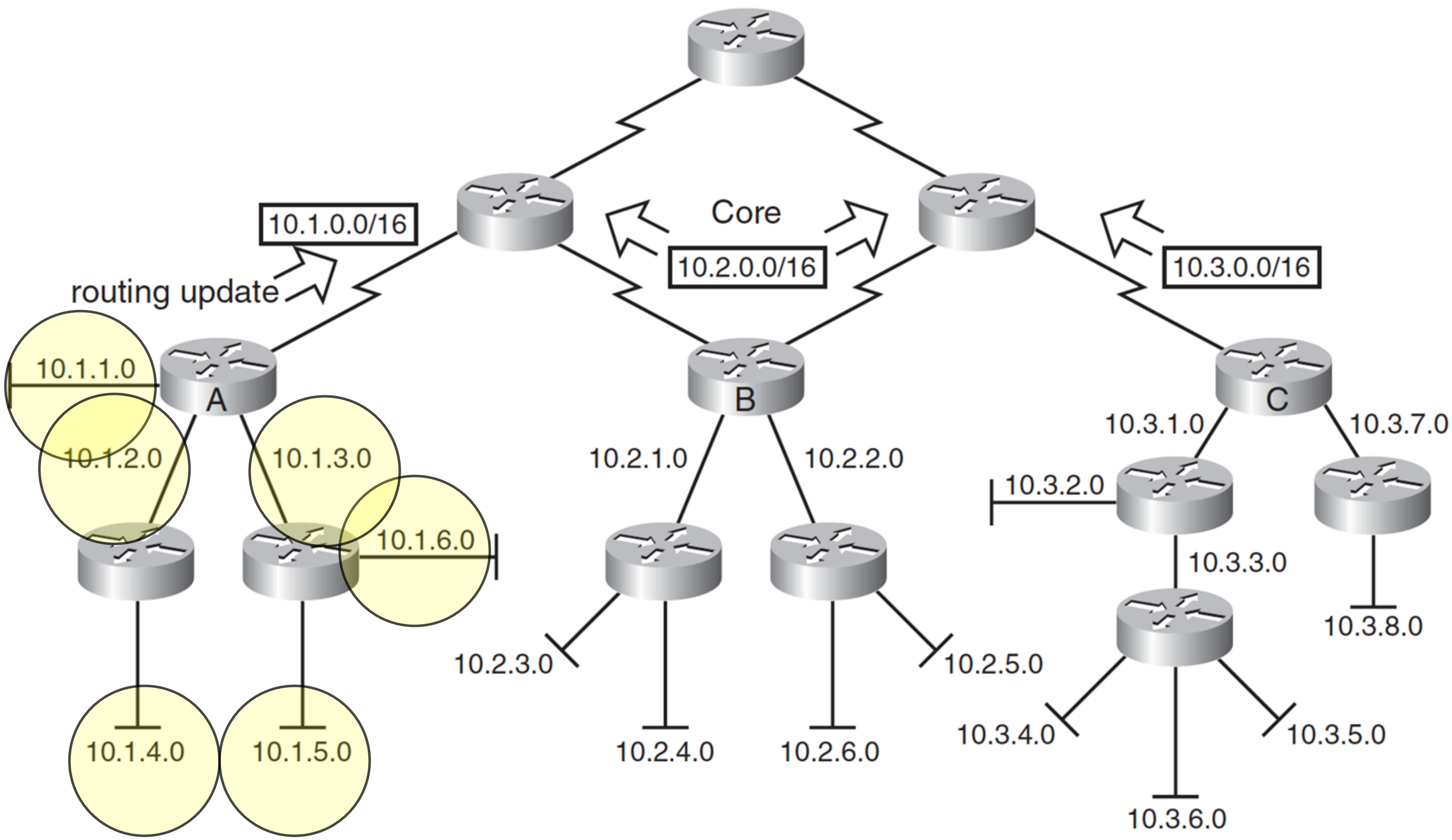
32-bit address

Remember that the address in which all host bits are 0 is the subnet address, and the address in which all host bits are 1 is the broadcast address

Hierarchical IP Address Design



Hierarchical IP Address Design

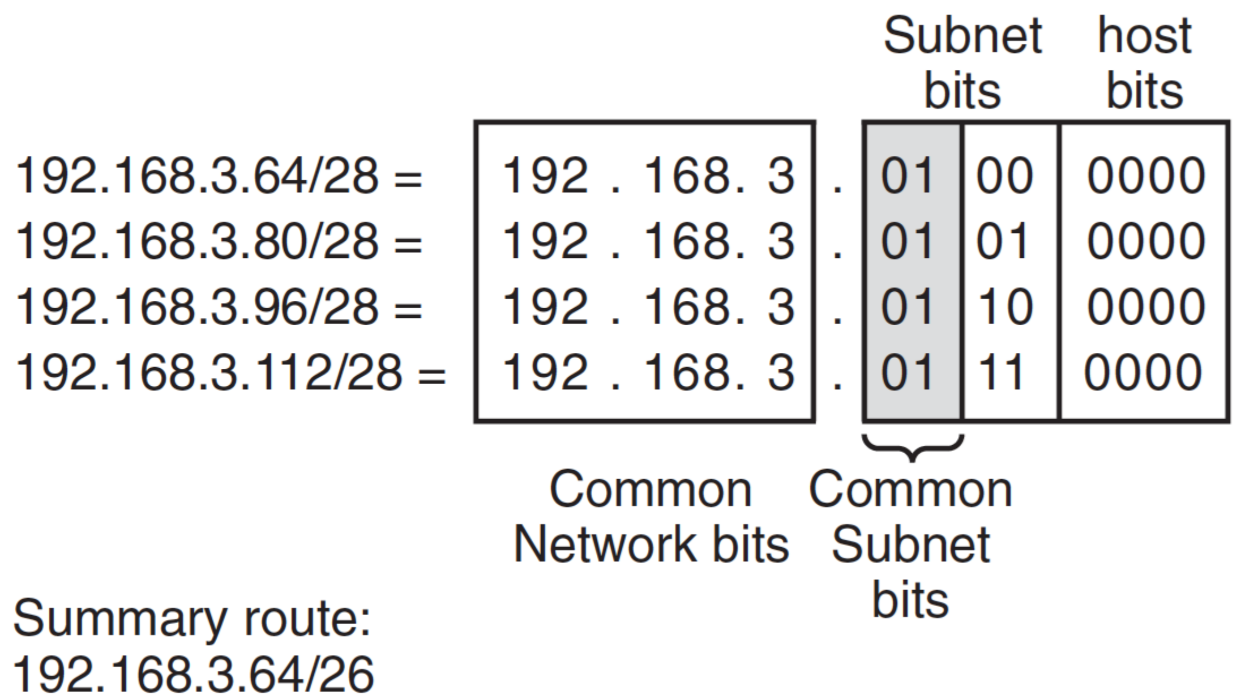


Hierarchical IP Address Design

- **Router A**
  - 192.168.3.64/28
  - 192.168.3.80/28
  - 192.168.3.96/28
  - 192.168.3.112/28
- **Router B**
  - 192.168.3.0/28
  - 192.168.3.16/28
  - 192.168.3.32/28
  - 192.168.3.48/28.

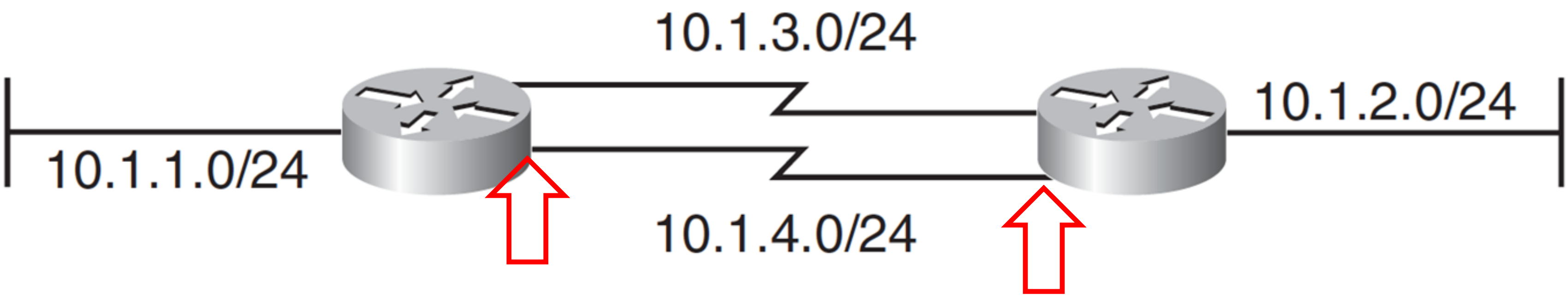
Hierarchical IP Address Design

Figure 3-7 *Route Summarization on a Nonoctet Boundary*



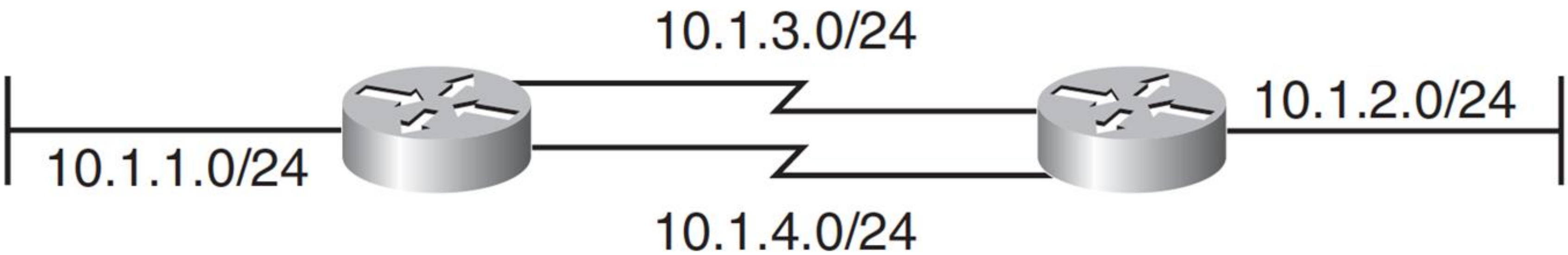
Variable-Length Subnet Masks

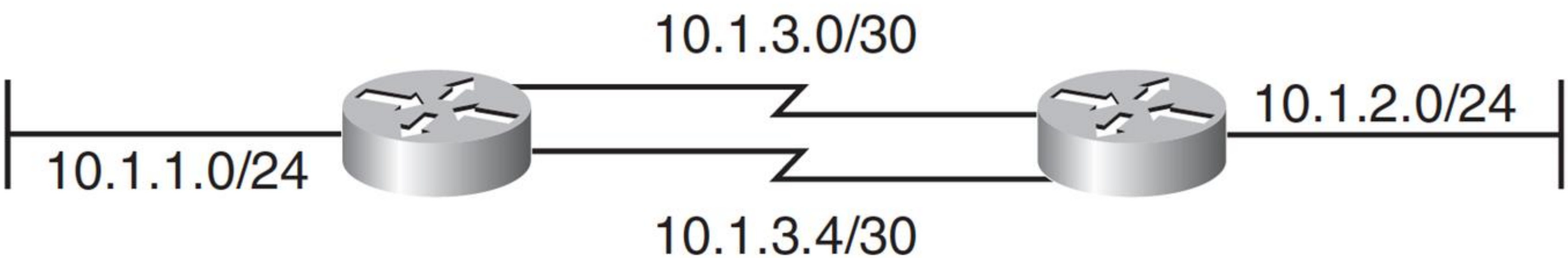
- Variable-Length Subnet Masks –VLSM



up to $2^8 - 2 = 254$ hosts can be addressed.

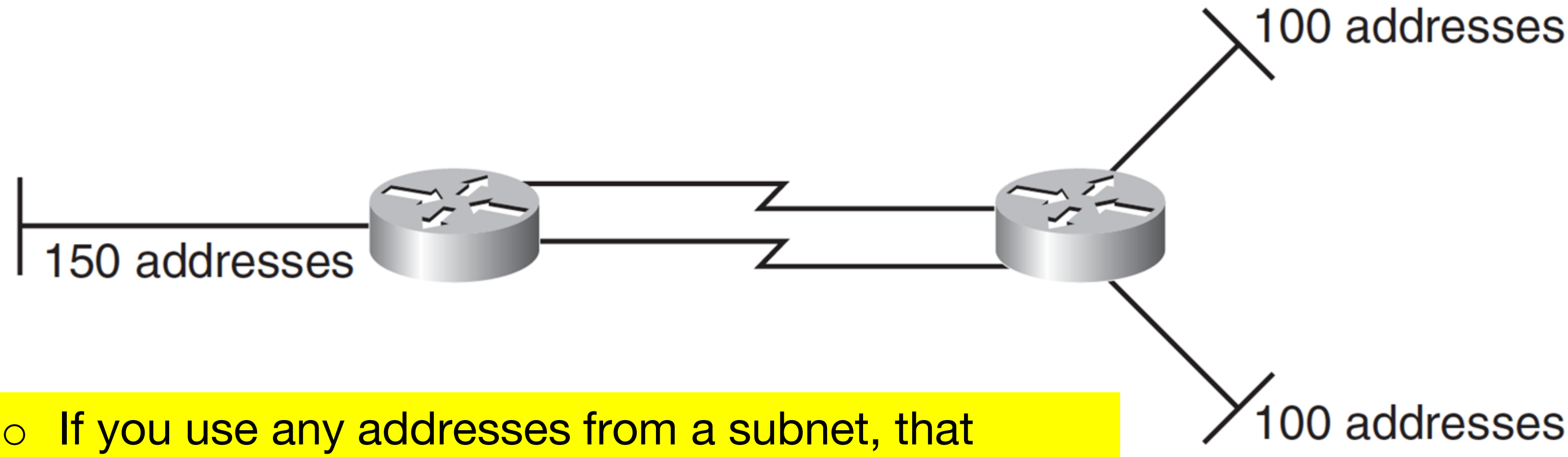
Variable-Length Subnet Masks





Variable-Length Subnet Masks

Use 10.5.16.0/20 to address this network,
conserving as many addresses as possible.

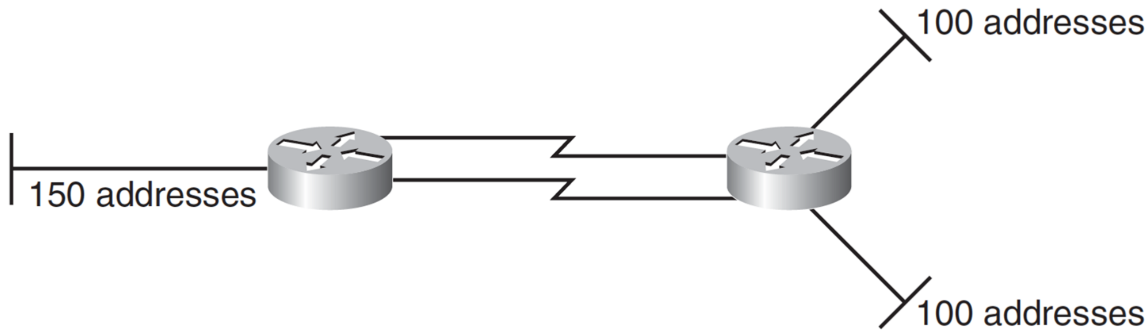


- If you use any addresses from a subnet, that subnet should not be further subnetted.

10.5.16.0/20

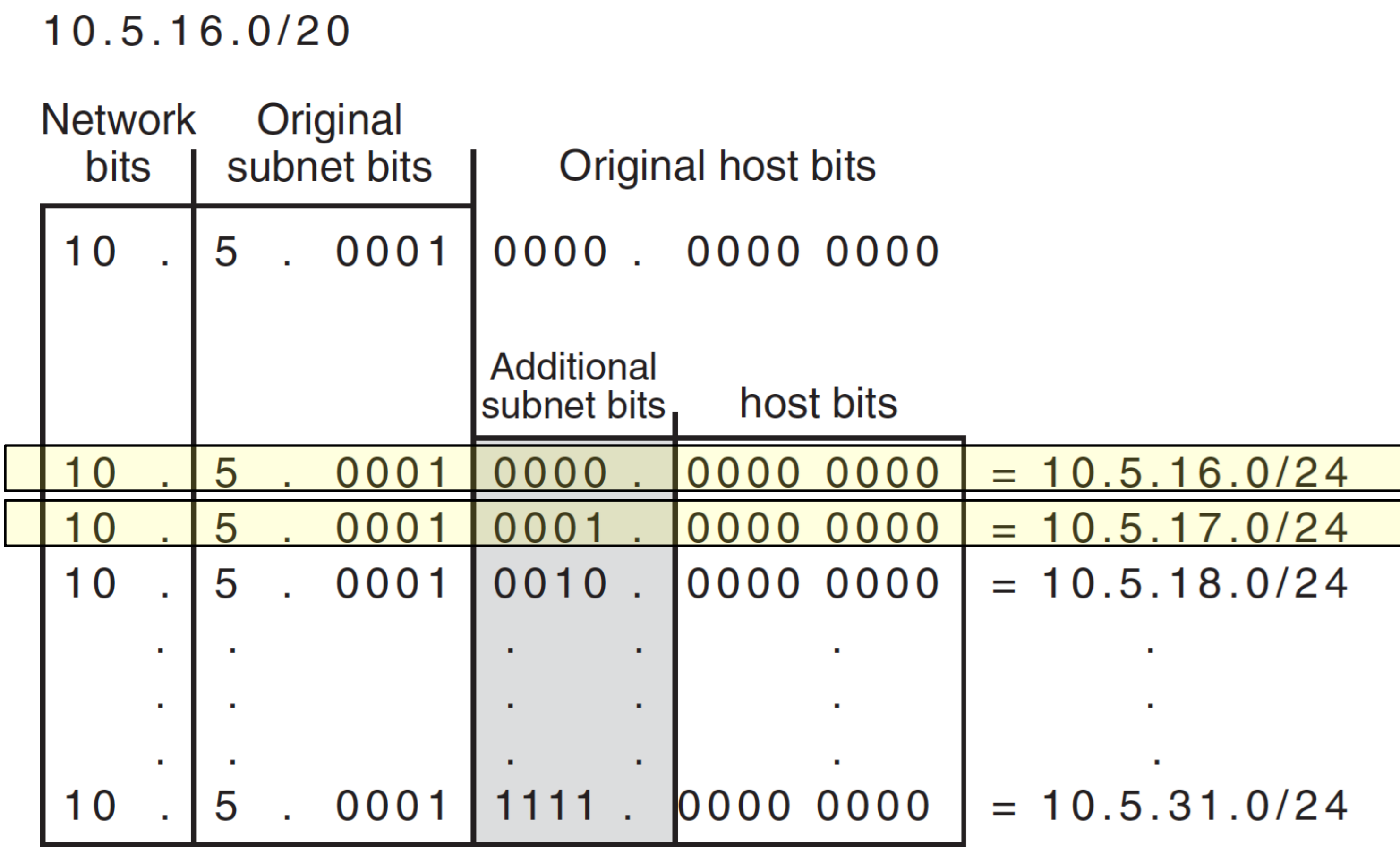
Network bits	Original subnet bits	Original host bits
10 .	5 . 0001	0000 . 0000 0000

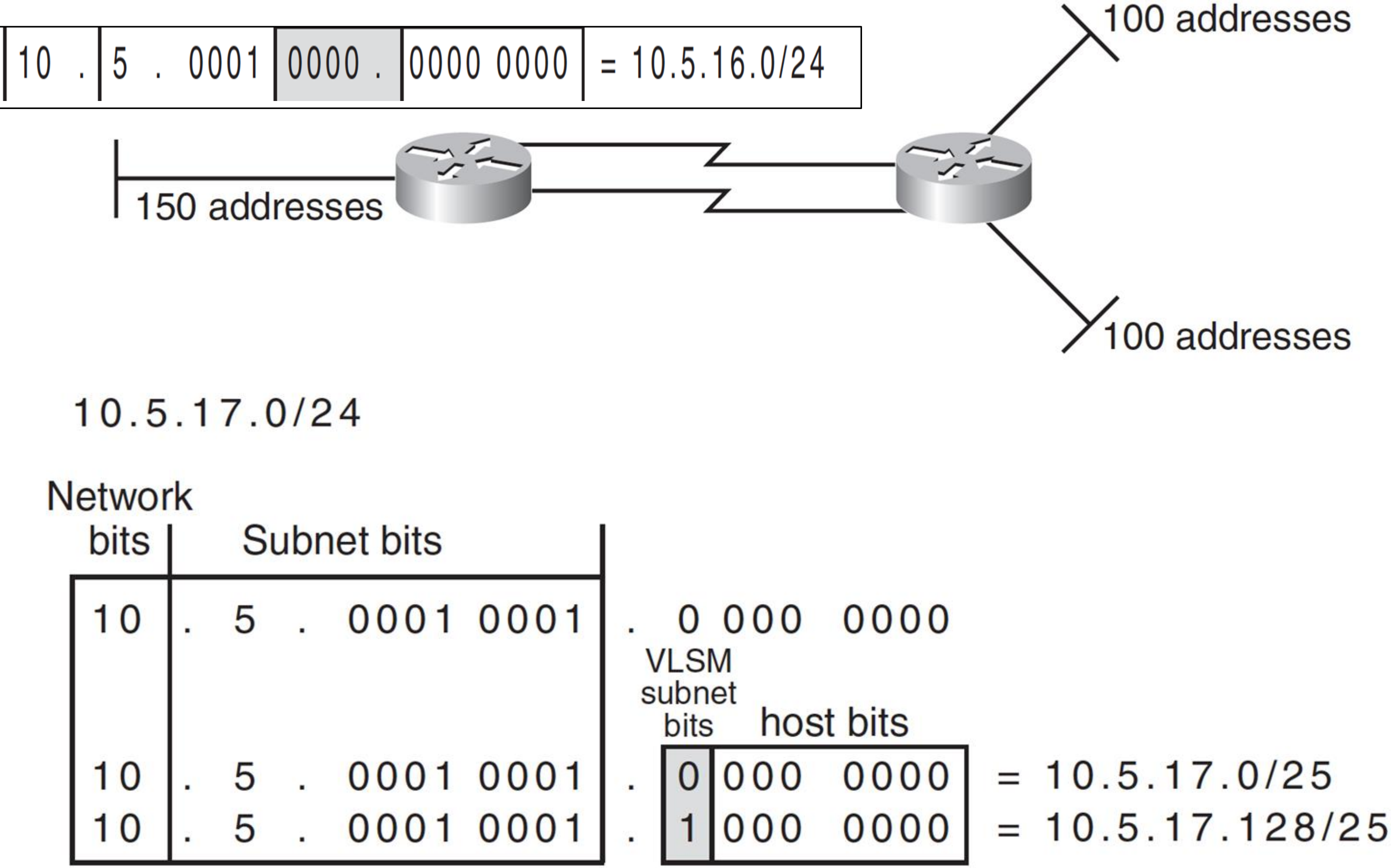
Use 10.5.16.0/20 to address this network, conserving as many addresses as possible.

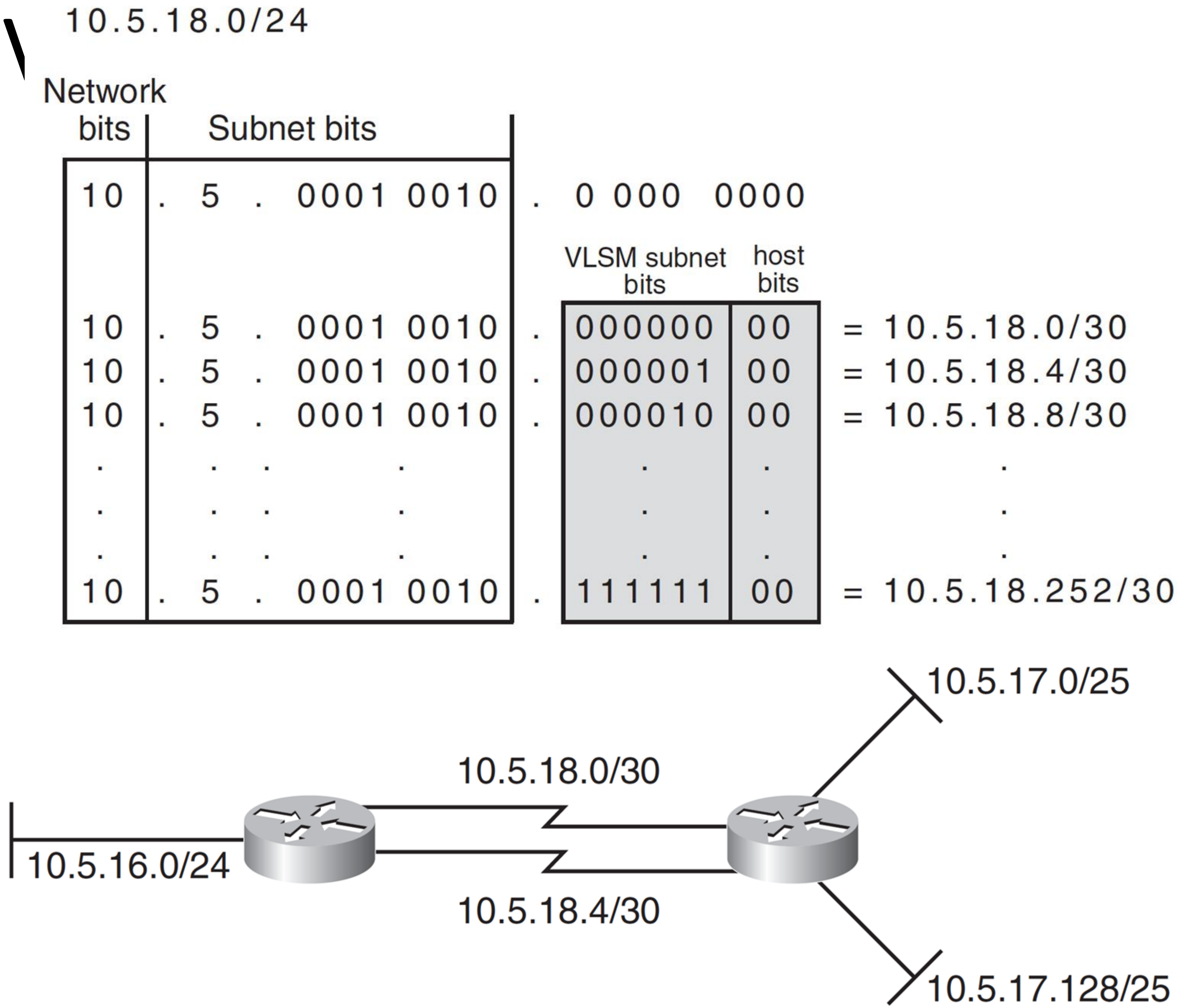


- For the left LAN, **150** addresses are needed;
  - rounding up to the next power of 2 gives 256.
  - Because $2^8 = 256$, 8 host bits are needed.
- For the other two LANs, 100 addresses are needed;
  - rounding up to the next power of 2 gives 128.
  - Because $2^7 = 128$, 7 host bits are needed for each LAN.
- The WANs require 2 host bits each.

- Because at most 8 host bits are needed, the 10.5.16.0/20 address can be further subnetted into sixteen /24 subnets (leaving 8 host bits)

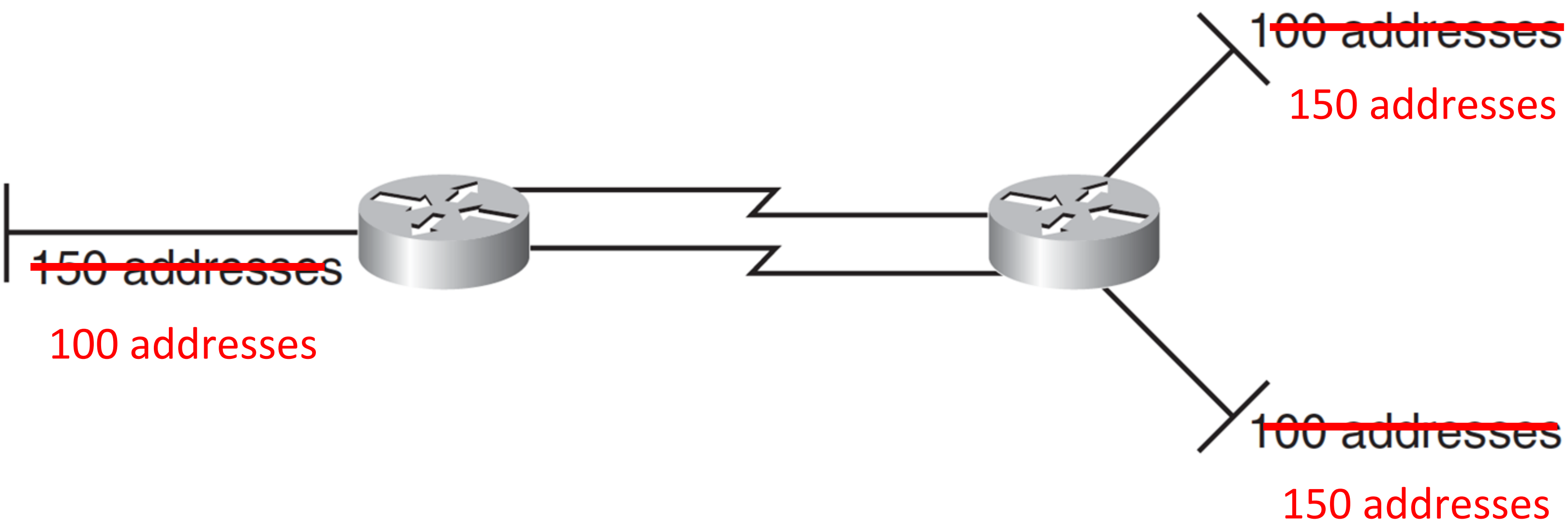



10 . 5 . 0001 0000 . 0000 0000 = 10.5.16.0/24
100 addresses
150 addresses
100 addresses
10.5.17.0/24
Network bits
Subnet bits
10 . 5 . 0001 0001 . 0 000 0000
VLSM subnet bits
host bits
10 . 5 . 0001 0001 . 0 000 0000 = 10.5.17.0/25
10 . 5 . 0001 0001 . 1 000 0000 = 10.5.17.128/25


10.5.18.0/24
Network bits
Subnet bits
10 . 5 . 0001 0010 . 0 000 0000
VLSM subnet bits
host bits
10 . 5 . 0001 0010 . 000000 00 = 10.5.18.0/30
10 . 5 . 0001 0010 . 000001 00 = 10.5.18.4/30
10 . 5 . 0001 0010 . 000010 00 = 10.5.18.8/30
10 . 5 . 0001 0010 . 111111 00 = 10.5.18.252/30
10.5.17.0/25
10.5.18.0/30
10.5.16.0/24
10.5.18.4/30
10.5.17.128/25

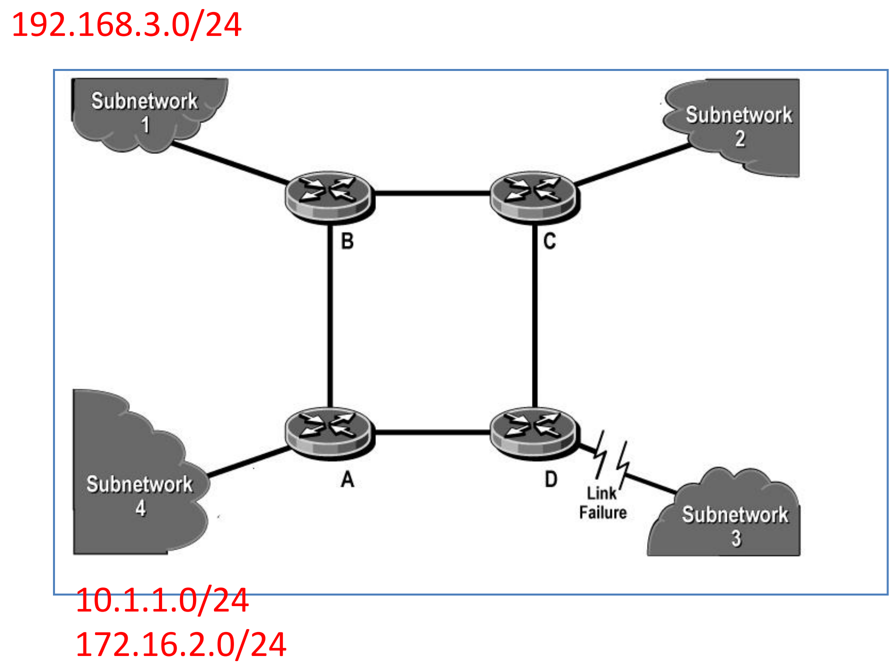
Report Submission

Use 10.5.16.0/20 to address this network, conserving as many addresses as possible.



IPv4 Routing Protocols

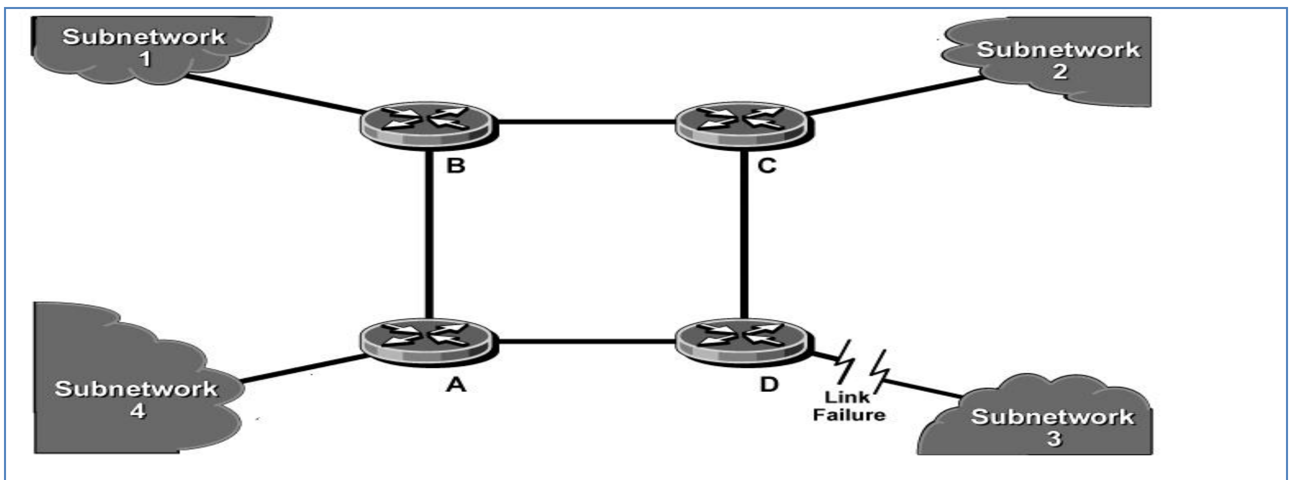
- The main functions of a router are:
  - first to determine the best path that each packet should take to get to its destination, and
  - second to send the packet on its way



- To determine the best path on which to send a packet,
  - a router must know where the packet's destination network is.

IPv4 Routing Protocols

- It can be mentioned by **network administrator**
- Routes configured by network administrators are known as **static routes**
- Routes to which a router is physically connected are known as **directly connected routes**.
- Routers learn routes from other routers by using a **routing protocol**.



Classifying Routing Protocols

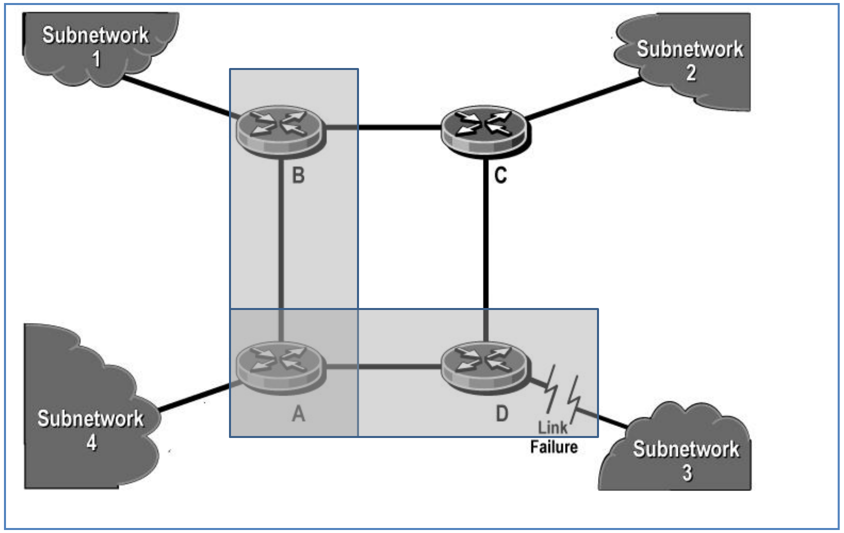
- Can be classified in various ways
  - Interior and Exterior Routing Protocols
  - Distance Vector, Link-State and Hybrid Routing Protocols
  - Flat and Hierarchical Routing Protocols
  - Classful and Classless Routing Protocols

Interior and Exterior Routing Protocols

- Autonomous - independent
- An **autonomous system** (AS) is a network controlled by **one organization**;
- it uses **interior routing protocols**, called **interior gateway protocols (IGPs)** within it, and
- **exterior routing protocols**, called **exterior gateway protocols (EGPs)**, to communicate with other autonomous systems.

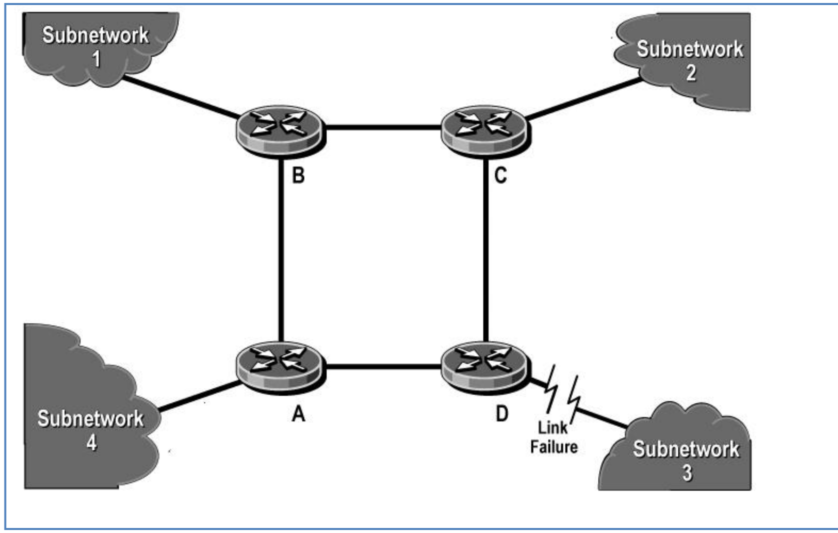
Distance Vector, Link-State, and Hybrid Routing Protocols

- Distance vector routing protocol
  - All the routers send their routing tables to only their **neighboring routers**.
  - The routers then use the received information to determine whether any changes need to be made to their own routing table
  - The process **repeats periodically**.



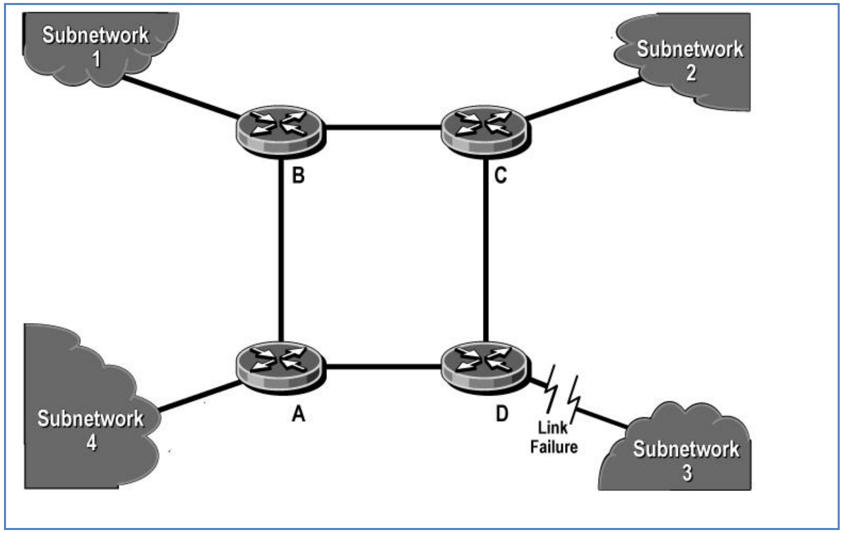
Distance Vector, Link-State, and Hybrid Routing Protocols

- In a link-state routing protocol,
  - each of the routers sends the **state** of its **own interfaces** (its links) to **all other routers** (*) only when there is a change to report.
    - (or to all routers in a part of the network, known as an area)
  - Each router uses the received information to recalculate the best path to each network and then saves this information in its routing table.



Distance Vector, Link-State, and Hybrid Routing Protocols

- **A Hybrid protocol**
- As its name suggests, a hybrid protocol borrows from both distance vector and link-state protocols.
- Hybrid protocols send only changed information (similar to link-state) but only to neighboring routers (similar to distance vector).

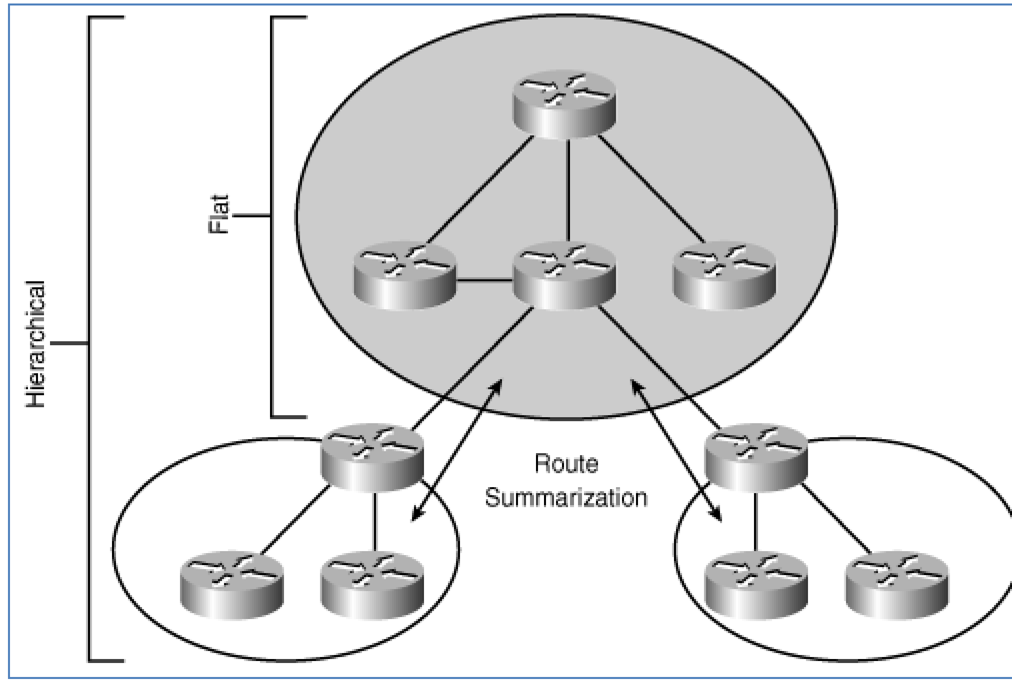


Distance Vector, Link-State, and Hybrid Routing Protocols

- Link-state routers have knowledge of **the entire network**, while distance vector routers only know what their neighbors tell them.
- Routers running **distance vector** routing protocols typically send updates in **broadcast packets**, while those running link-state and hybrid routing protocols send the updates in **multicast packets**

Flat and Hierarchical Routing Protocols

- Flat routing protocols have **no way to restrict routes from being propagated** within a major network (a Class A, B, or C network).
- In contrast, hierarchical routing protocols allow the network administrator to separate the network into areas and limit how routes are propagated between areas.
- This in turn reduces the routing table size and amount of routing protocol traffic in the network.



Classful and Classless Routing Protocols

- Classful addressing is obsolete and has not been used in the Internet since the implementation of Classless Inter-Domain Routing (CIDR) starting in 1993.

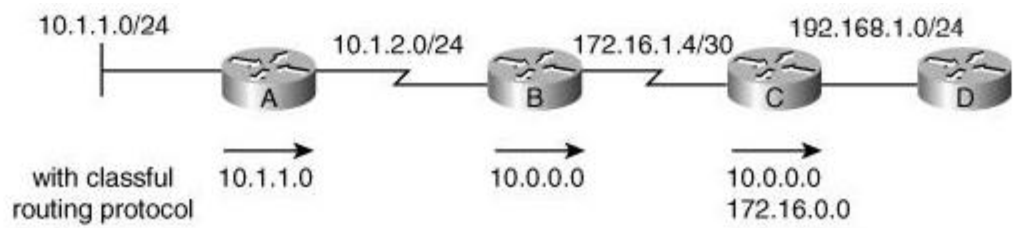
- Routing updates sent by a Classful routing protocol do not include the subnet mask.
- Routing updates sent by a classless routing protocol include the subnet mask.

Classful and Classless Routing Protocols

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

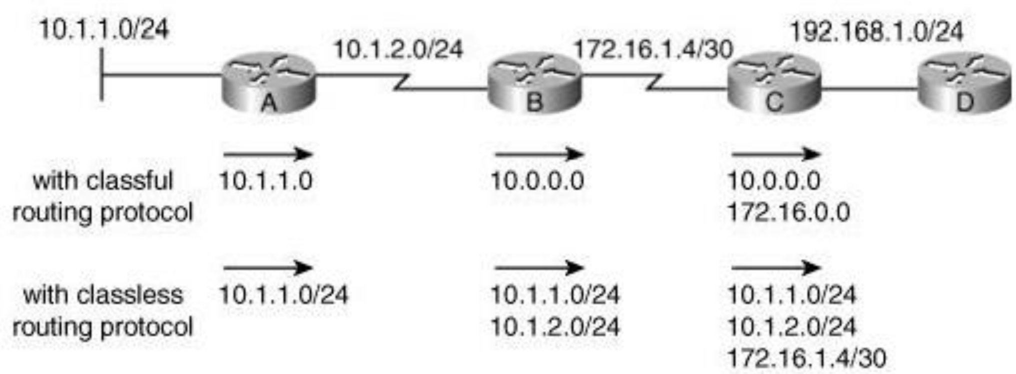
```
Class A
  0.  0.  0.  0 = 00000000.00000000.00000000.00000000
127.255.255.255 = 01111111.11111111.11111111.11111111
                  0nnnnnnn.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B
128.  0.  0.  0 = 10000000.00000000.00000000.00000000
191.255.255.255 = 10111111.11111111.11111111.11111111
                  10nnnnnn.nnnnnnnn.HHHHHHHH.HHHHHHHH

Class C
192.  0.  0.  0 = 11000000.00000000.00000000.00000000
223.255.255.255 = 11011111.11111111.11111111.11111111
                  110nnnnn.nnnnnnnn.nnnnnnnn.HHHHHHHH
```

Classful and Classless Routing Protocols

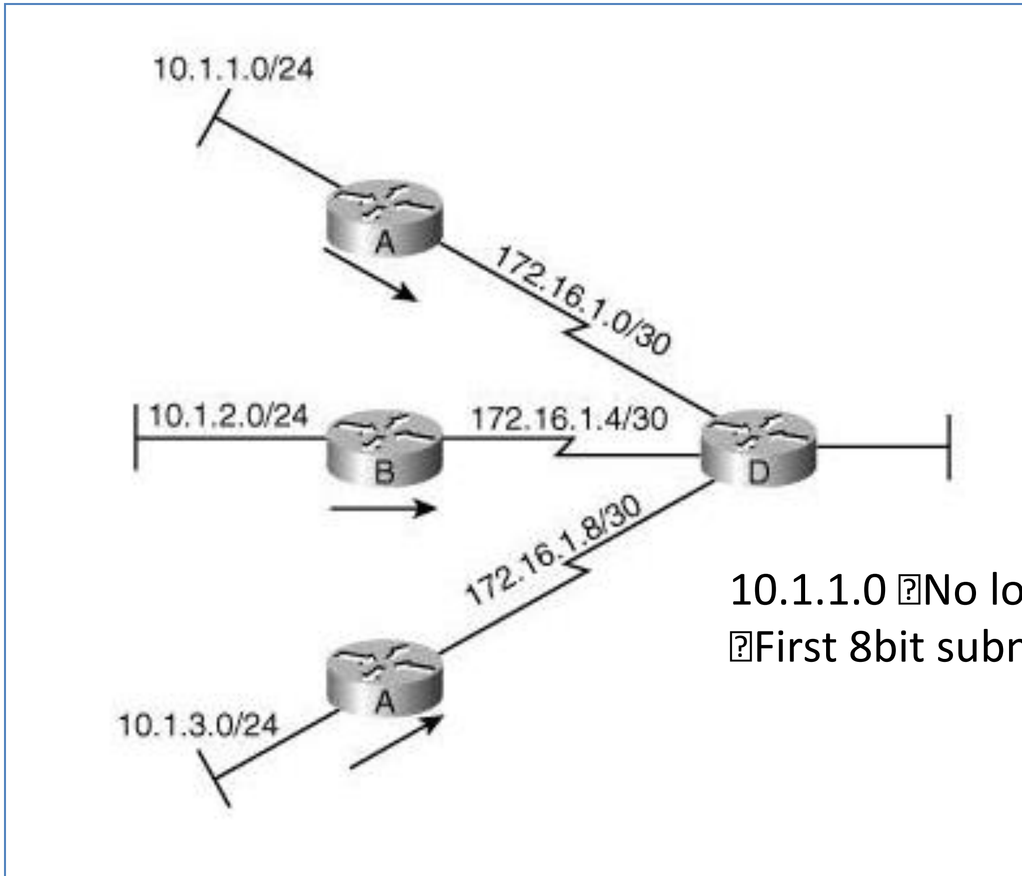


- Router B assumes that the mask of the 10.1.1.0 route sent by Router A must be the same as the mask on the 10.1.2.0 subnet to which it is connected, because the mask is not sent along with the route.
- Router B **summarizes** all subnets of network 10.0.0.0 when it sends routing information to Router C because it is sending the route on an interface that is in a different major network.
- For the same reason, Router C summarizes network 172.16.0.0 when it sends routing information to Router D.

Classful and Classless Routing Protocols



Classful and Classless Routing Protocols



- ❑ Classful Routing Protocols Do Not Support Discontiguous Networks;
- ❑ Classless Routing Protocols Do

10.1.1.0 ⍰No local interface ⍰ Class A Network ⍰First 8bit subnet mask ⍰routing table 10.0.0.0

Classful and Classless Routing Protocols

- The IP address design implications of using a classful routing protocol are as follows:
  - All subnets of the same major network must use the same subnet mask.
  - All subnets of the same major network must be contiguous;
    - in other words, all subnets of the same major network must be reachable from each other without going through a part of any other major network.
  - Classful routing protocols automatically summarize routes on the major network boundary.

Metrics

- One of a router's jobs is to determine the **best path to each destination** network.
- The routing **protocol metric is** the value that the routing protocol uses to evaluate which path is best.
- Metrics can include the following factors:
    1. Hop count
    2. Bandwidth
    3. Delay
    4. Cost
    5. Load
    6. Reliability

Metrics

- Hop count
  - The number of hops, or other routers, to the destination network; the path with the least number of hops is preferred.
- Bandwidth
  - The path with the lowest bandwidth segment is the least preferred path.
- Delay
  - The path with the lowest accumulated delay (also called latency) is the preferred path.
- Cost
  - Usually inversely related to bandwidth; in other words, the path with the slowest links has the highest cost and is the least preferred path.

Metrics

- Load
  - The utilization of the path (in other words, how much of the bandwidth is currently being used).
  - For example, in the Cisco Interior Gateway Routing Protocol (IGRP) and Enhanced Interior Gateway Routing Protocol (EIGRP) metrics, load can be included as a number from 0 to 255, representing a 5-minute exponentially weighted average load. Load is not included by default in these calculations because it can be constantly changing.
- Reliability
  - The likelihood of successful packet transmission.
  - For example, in IGRP and EIGRP metrics, reliability can be included as a number from 0 to 255, with 255 meaning 100 percent reliability and 0 meaning no reliability. Reliability is not included by default in these calculations because it can change often (for example, with heavy traffic load).

Convergence Time

- A network is **converged** when the routing tables in all the routers are synchronized so that they all contain a usable route to every available network.
- Convergence time is the time it takes all the routers in a network to agree on the network's topology, after that topology has changed.

- Network design impacts convergence time significantly; in fact, proper network design is a must, or else the network might never converge.