Top-Down Network Design

Chapter Six

Designing Models for Addressing and Naming

Guidelines for Addressing and Naming

- Use a structured model for addressing and naming
- Assign addresses and names hierarchically
- Decide in advance if you will use
  - Central or distributed authority for addressing and naming
  - Public or private addressing
  - Static or dynamic addressing and naming

Advantages of Structured Models for Addressing & Naming

- It makes it easier to
  - Read network maps
  - Operate network management software
  - Recognize devices in protocol analyzer traces
  - Meet goals for usability
  - Design filters on firewalls and routers
  - Implement route summarization

Public IP Addresses

- Managed by the Internet Assigned Numbers Authority (IANA)
- ISPs obtain allocations of IP addresses from their appropriate Regional Internet Registry (RIR)
- Users are assigned IP addresses by Internet service providers (ISPs).

Private Addressing

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255.

- These are addresses assigned by internal networks and hosts without any coordination from an ISP or the Internet Assigned Numbers Authority (IANA)
- An advantage is security. Private numbers are not advertised on the Internet
- Can reserve scarce Internet addresses for public servers

Private and Public IPv4 Address Selection Criteria

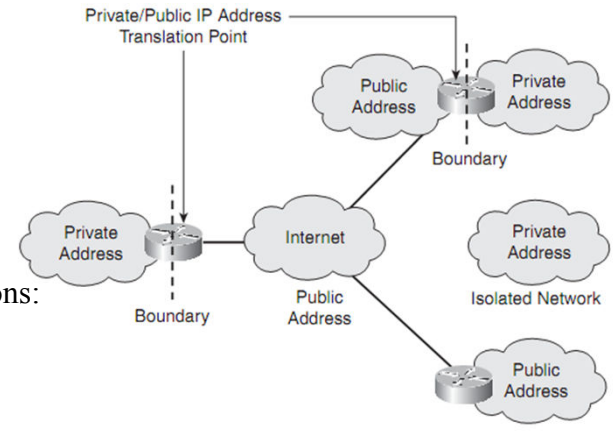
Cisco.com

- Are private, public, or both IPv4 address types required?
- How many end systems only need access to the public network?
- How many of the end systems need to be visible to the public network?
- How are the boundaries between private and public addresses crossed?

Network Address Translation (NAT)

- An IP mechanism that is used for converting addresses from an inside network to addresses that are appropriate for an outside network and vice-versa
- NAT administrator configures a pool of outside addresses that can be used for translation
- Some NAT products offer port translation for mapping several addresses to the same address
- When using NAT all traffic must go through a NAT gateway
- Must also modify IP addresses that occur inside the data part of a packet

Private and Public IPv4 Address Options



Three combinations:

- Private only
- Public only
- Combination

Public IPv4 addresses are used for external communication, and private IP addresses are used for internal communication.

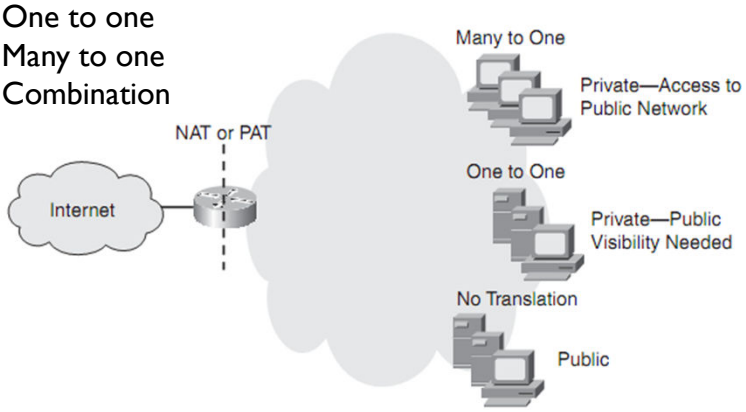
Private and Public IPv4 Address Decision Table

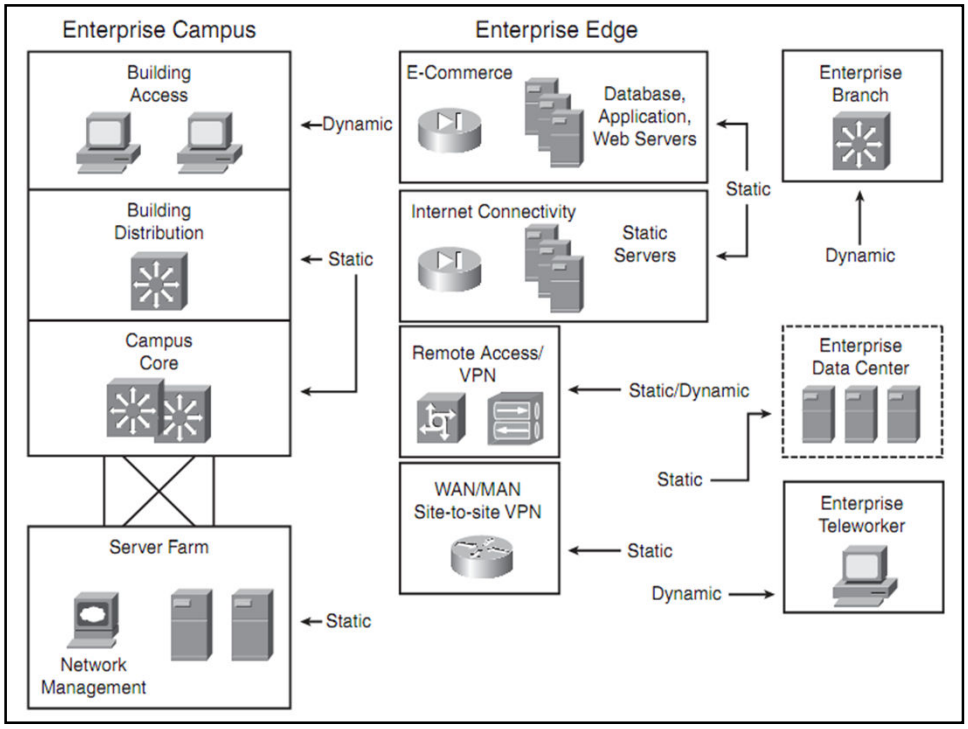
Cisco.com

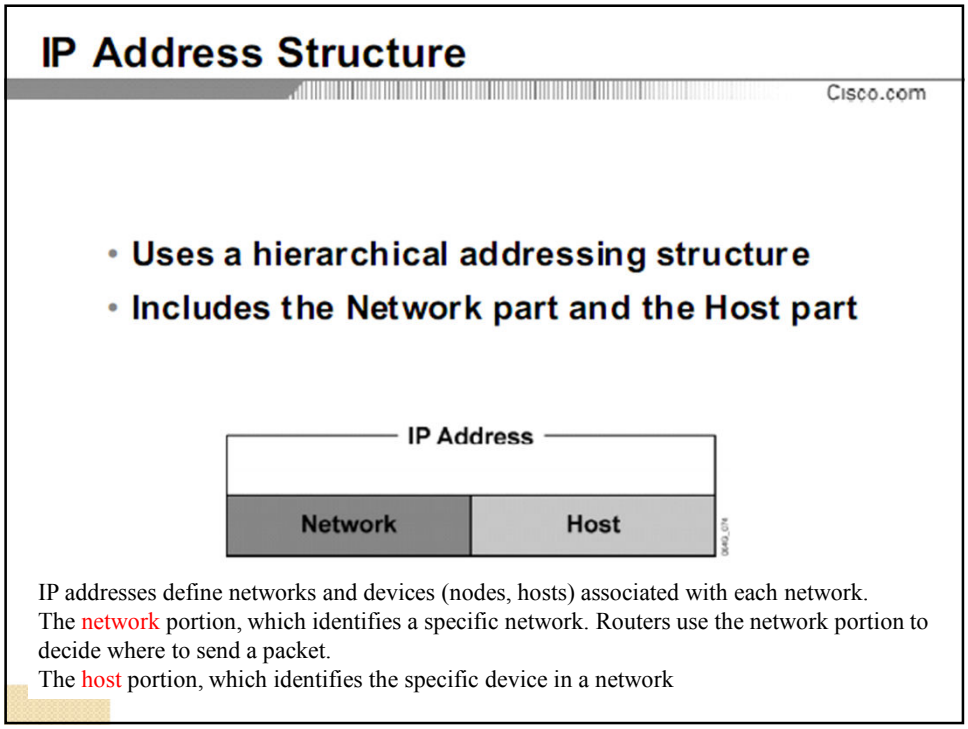
	Private IP Address Space	Public IP Address Space
No Internet connectivity	Used for the whole network	Not needed
Internet connectivity, no public servers	Used for internal numbering	Required only for connections to Internet
Internet connectivity, publicly accessible servers	Used for internal numbering	Required for connections to Internet and public accessible servers
All end systems publicly accessible	Not needed	Used for the whole network

Private and Public Translation

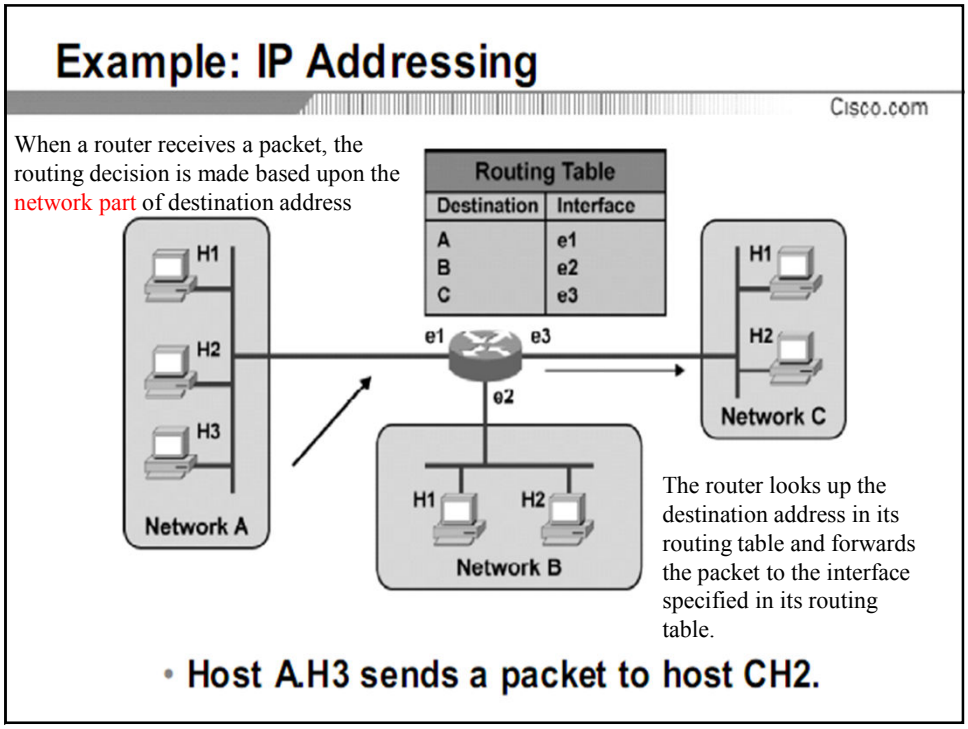
- Used for end systems that need access to the public network and do not need to be visible to the outside world.
- Translation options:
  - One to one
  - Many to one
  - Combination

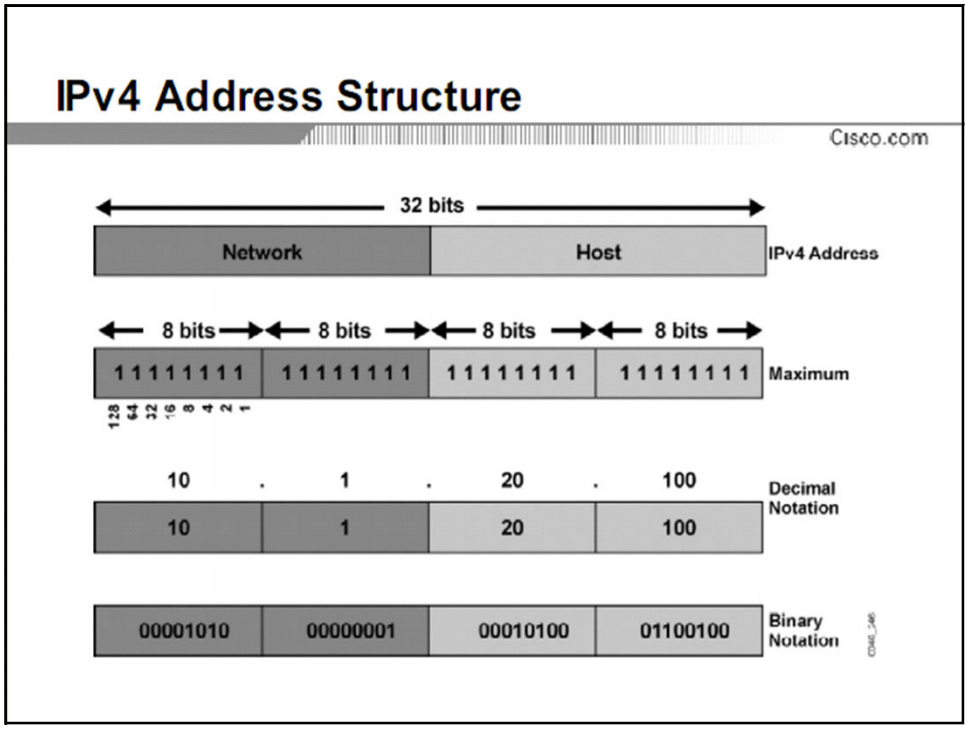


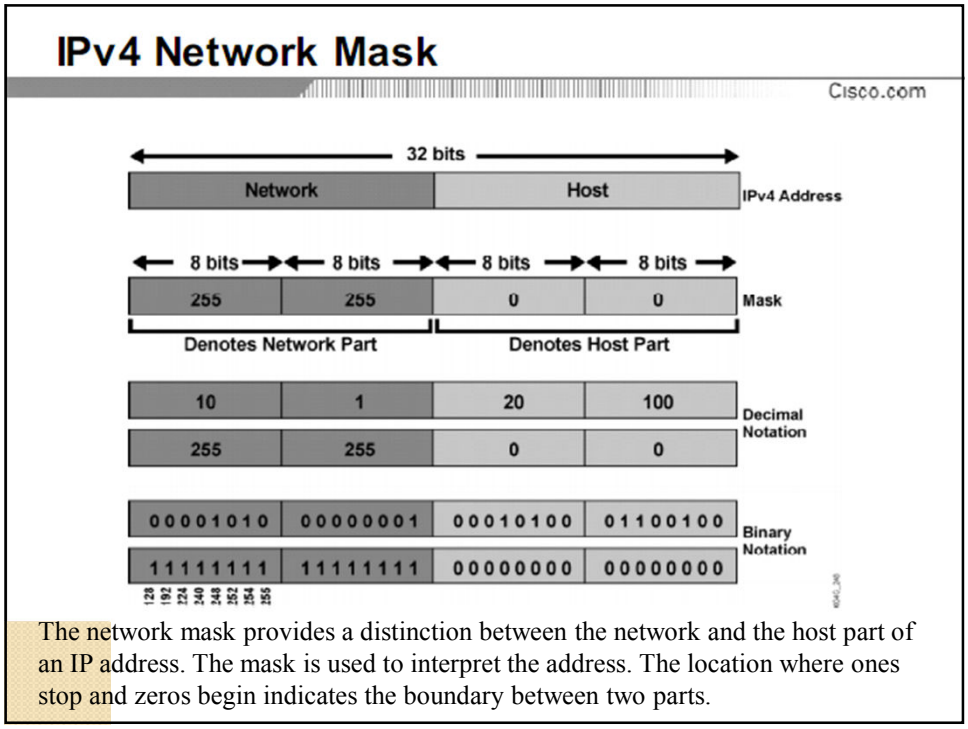




IP addresses define networks and devices (nodes, hosts) associated with each network.
The network portion, which identifies a specific network. Routers use the network portion to decide where to send a packet.
The host portion, which identifies the specific device in a network



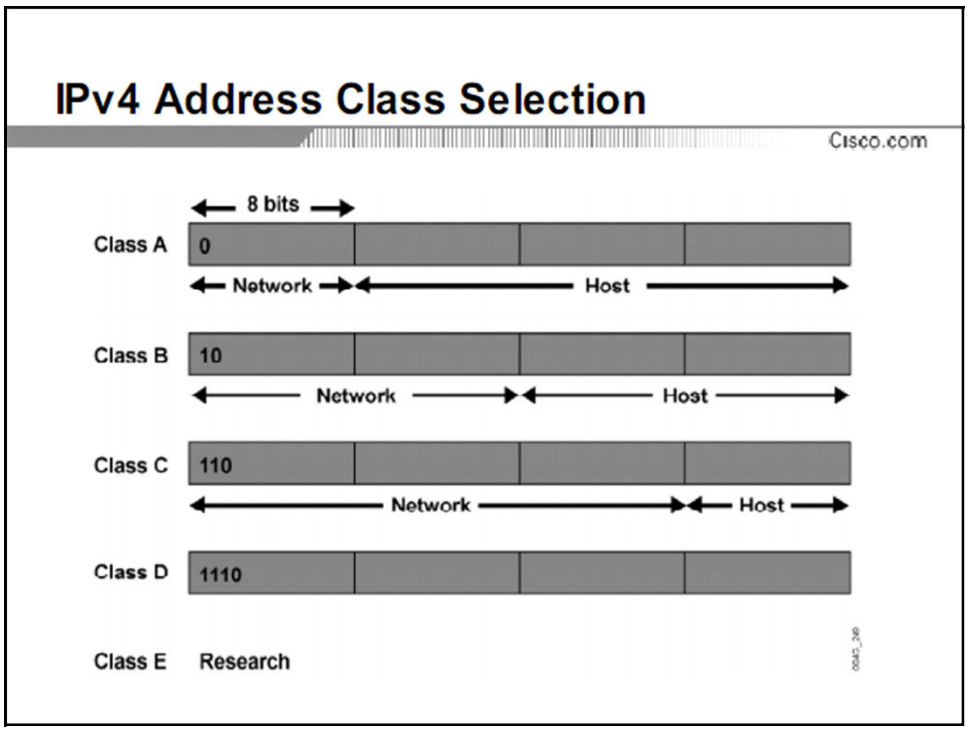




The network mask provides a distinction between the network and the host part of an IP address. The mask is used to interpret the address. The location where ones stop and zeros begin indicates the boundary between two parts.

Prefix Length

- An IP address is accompanied by an indication network mask either in decimal notation (255.255.255.0) or in prefix notation (/24), which indicates the number of consecutive ones.
- Examples
  - 192.168.10.1 255.255.255.0
  - 192.168.10.1/24



Subnet Mask Example

- 11111111 11111111 00000000 00000000
- What is this in slash notation?
- What is this in dotted-decimal notation?

Another Subnet Mask Example

- 11111111 11111111 11110000 00000000
- What is this in slash notation?
- What is this in dotted-decimal notation?

- 11111111 11111111 11111000 00000000
- What is this in slash notation?
- What is this in dotted-decimal notation?

Designing Networks with Subnets

- Determining subnet size
- Computing subnet mask
- Computing IP addresses

Addresses to Avoid When Subnetting

- A node address of all ones (broadcast)
- A node address of all zeros (network)
- A subnet address of all ones (all subnets)
- A subnet address of all zeros (confusing)

Practice

- Network is 172.16.0.0
- You want to divide the network into subnets.
- You will allow 600 nodes per subnet.
- What subnet mask should you use?
- What is the address of the first node on the first subnet?
- What address would this node use to send to all devices on its subnet?

More Practice

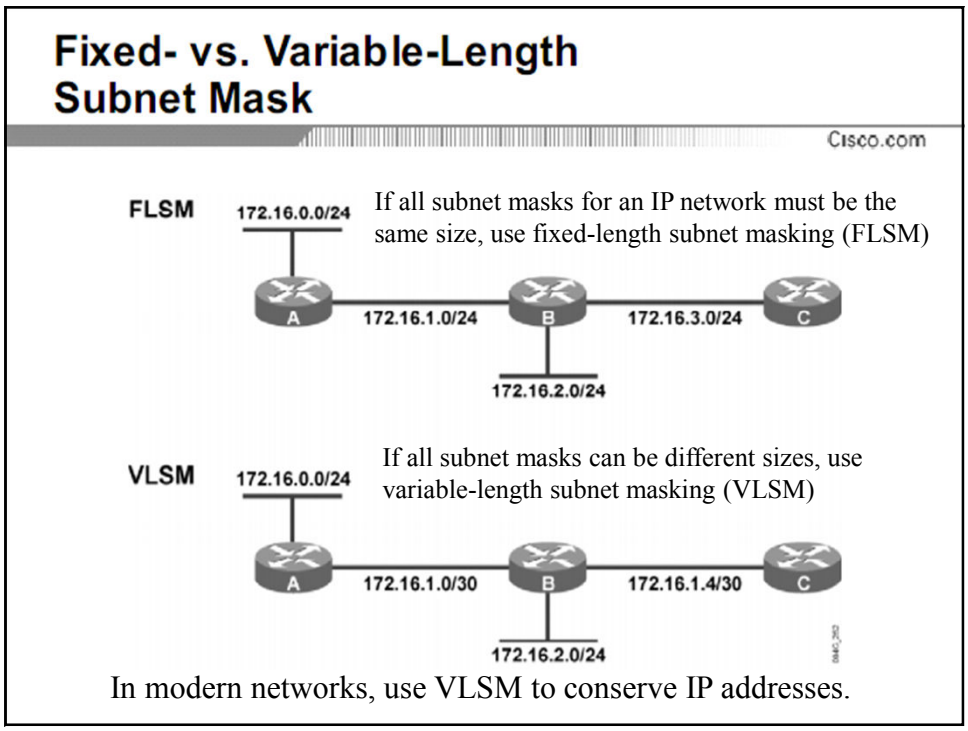
- Network is 172.16.0.0
- You have eight LANs, each of which will be its own subnet.
- What subnet mask should you use?
- What is the address of the first node on the first subnet?
- What address would this node use to send to all devices on its subnet?

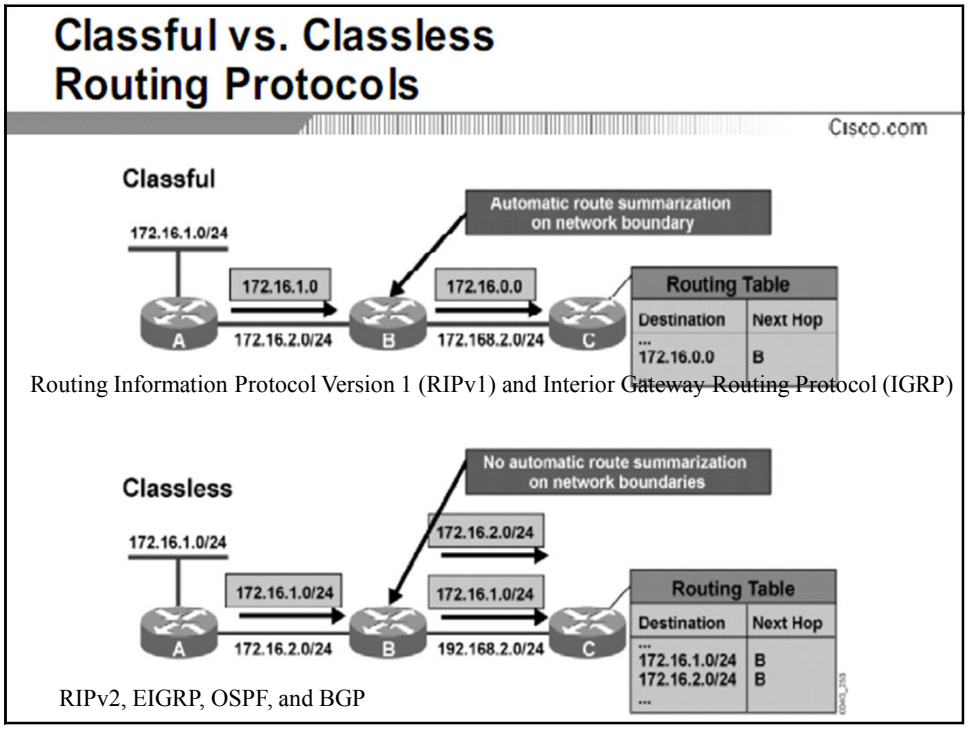
One More

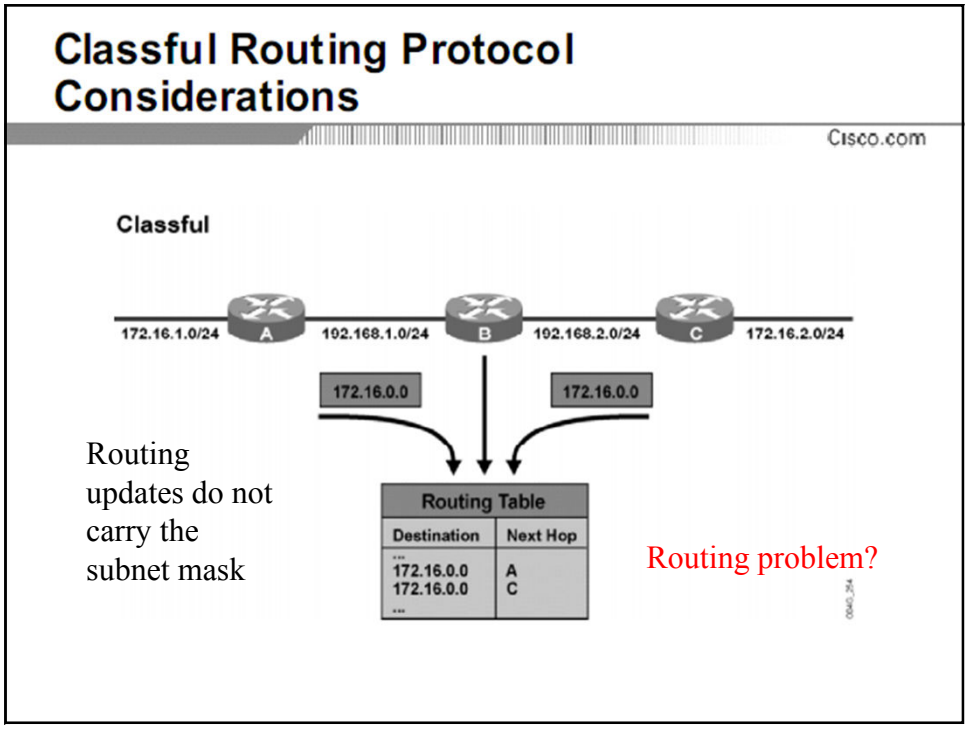
- Network is 192.168.55.0
- You want to divide the network into subnets.
- You will have approximately 25 nodes per subnet.
- What subnet mask should you use?
- What is the address of the last node on the last subnet?
- What address would this node use to send to all devices on its subnet?

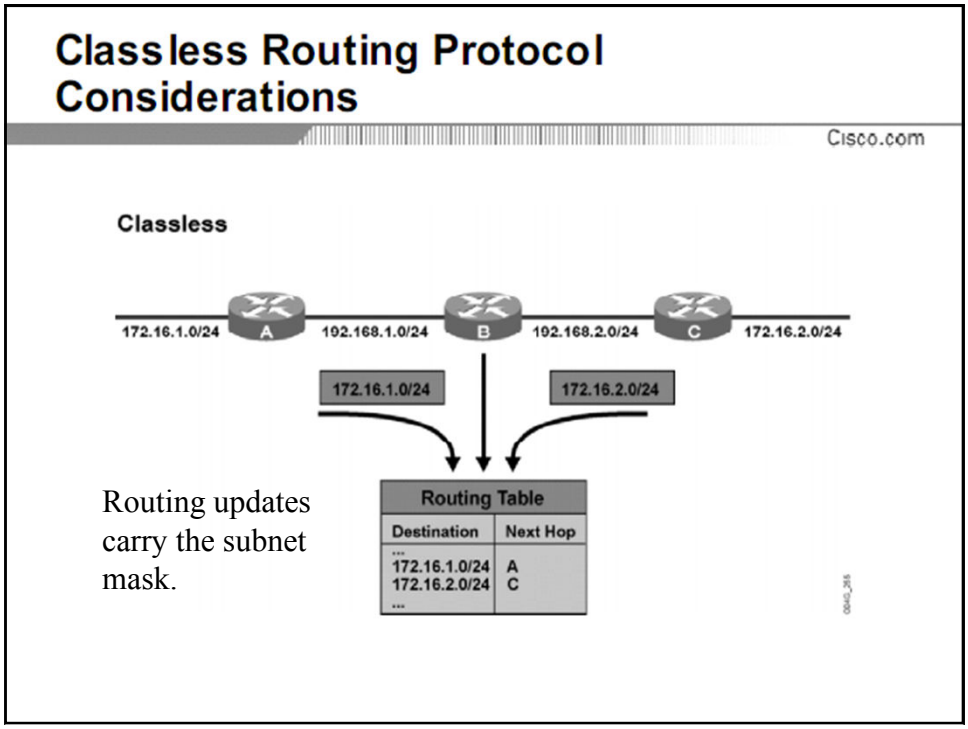
Classless Addressing

- Prefix/host boundary can be anywhere
- Less wasteful
- Supports route summarization
  - Also known as
    - Aggregation
    - Supernetting
    - Classless routing
    - Classless inter-domain routing (CIDR)
    - Prefix routing


Fixed- vs. Variable-Length Subnet Mask
Cisco.com
FLSM
172.16.0.0/24
If all subnet masks for an IP network must be the same size, use fixed-length subnet masking (FLSM)
A
172.16.1.0/24
B
172.16.3.0/24
C
172.16.2.0/24
VLSM
172.16.0.0/24
If all subnet masks can be different sizes, use variable-length subnet masking (VLSM)
A
172.16.1.0/30
B
172.16.1.4/30
C
172.16.2.0/24
In modern networks, use VLSM to conserve IP addresses.

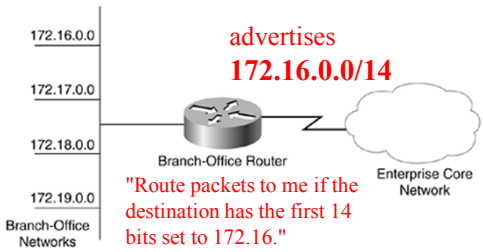

Classful vs. Classless Routing Protocols
Cisco.com
Classful
Automatic route summarization on network boundary
172.16.1.0/24
172.16.1.0
172.16.0.0
Routing Table
Destination
Next Hop
...
172.16.0.0
B
A
172.16.2.0/24
B
172.168.2.0/24
C
Routing Information Protocol Version 1 (RIPv1) and Interior Gateway Routing Protocol (IGRP)
Classless
No automatic route summarization on network boundaries
172.16.1.0/24
172.16.2.0/24
172.16.1.0/24
172.16.1.0/24
Routing Table
Destination
Next Hop
...
172.16.1.0/24
B
172.16.2.0/24
B
...
A
172.16.2.0/24
B
192.168.2.0/24
C
RIPv2, EIGRP, OSPF, and BGP





Route Summarization (Aggregation)

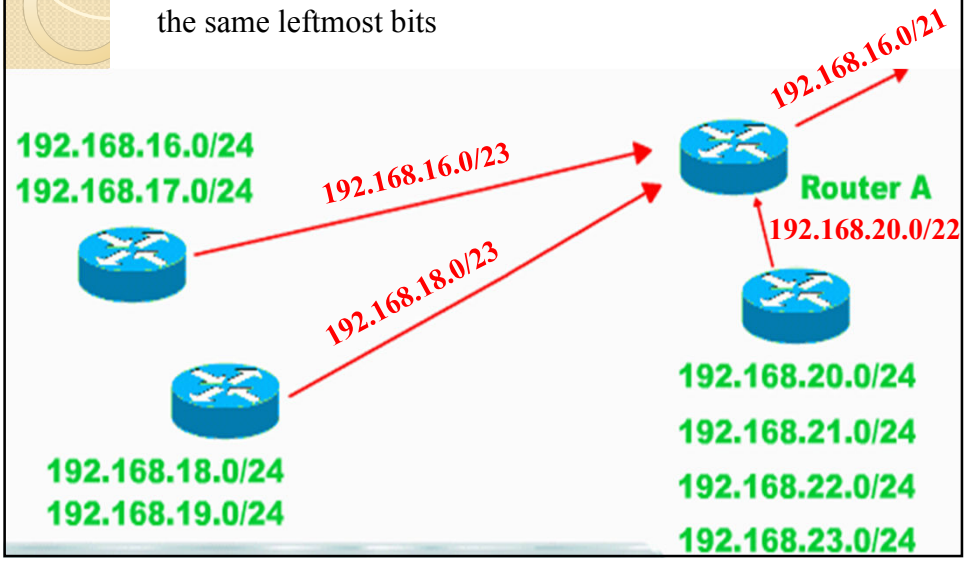
- When advertising routes into another major network classful routing protocols automatically summarize subnets



- Only advertise route to a Class A, B, or C network instead of routes to subnets
- Discontiguous subnets are not supported
- Classless routing protocols advertise a route and a prefix length

Route Summarization Example

Multiple IP addresses must share the same leftmost bits



Network Size and IP Addressing Plan

Cisco.com

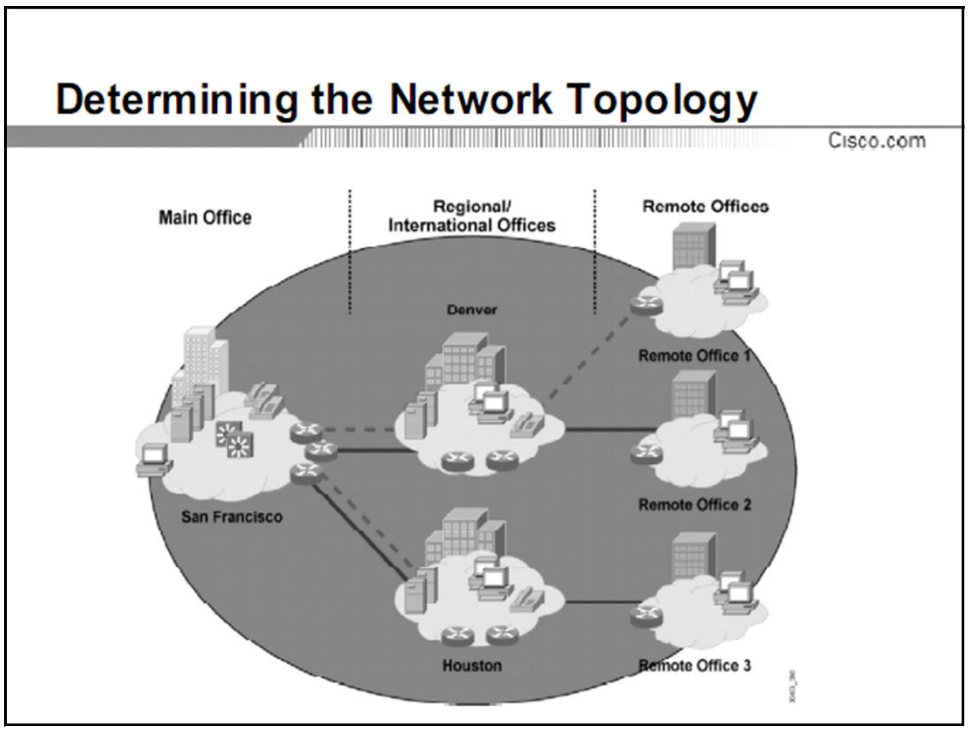
- How big is the internetwork?
- How many locations are in the network?
- What are the IP addressing requirements for individual locations?
- What class of addresses and how many networks are available from the public number authority?

Network Size Data Analysis

Cisco.com

Device Type	Number	Comments
Workstations	1000	Mobile and fixed workstations
Servers	50	Internal and public servers
IP phones	1000	IP telephony replaces POTS
Router interfaces	45	Physical and virtual interfaces
Switch management interfaces	37	
Firewall interfaces	12	
Total	2144	Add 20% for future growth

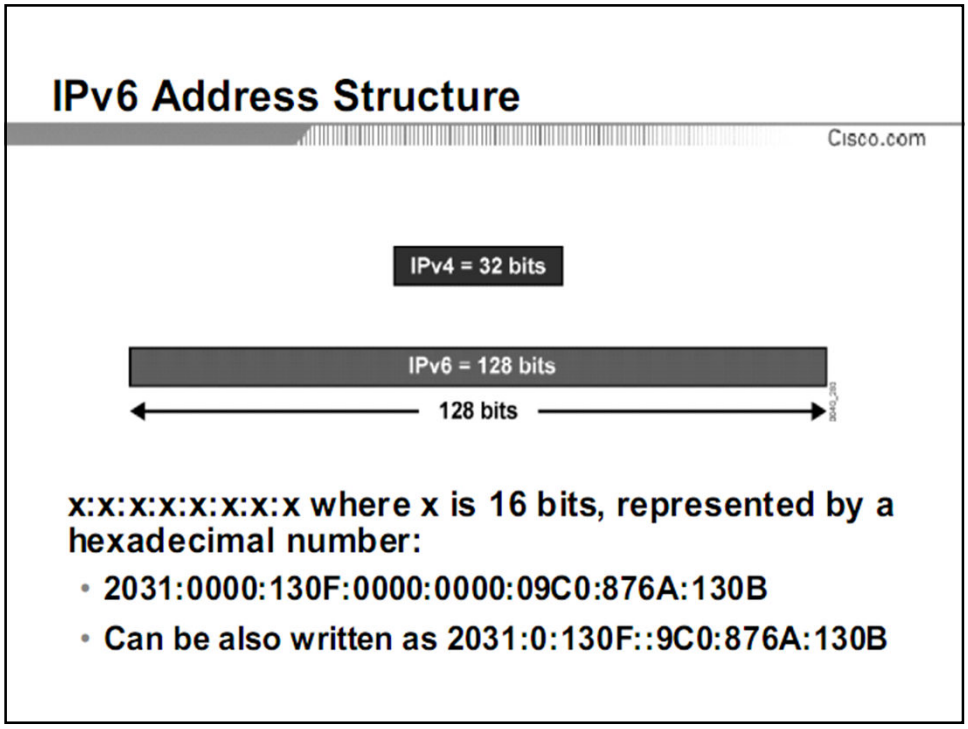
The network size, in terms of the IP addressing plan, relates to the number of devices and interfaces that need an IP address.

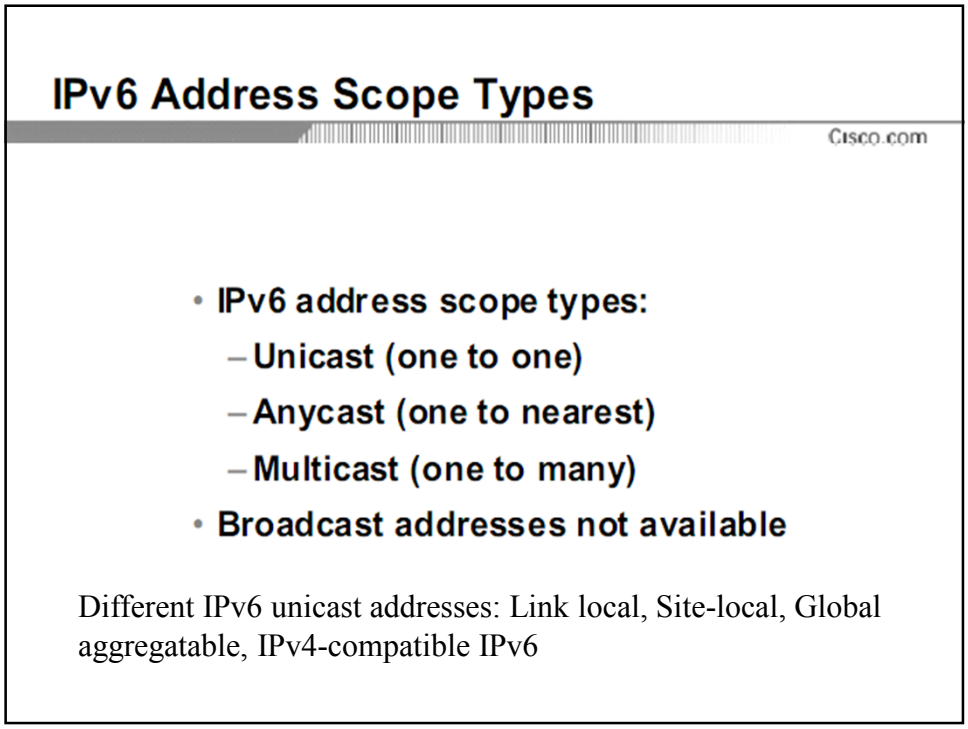


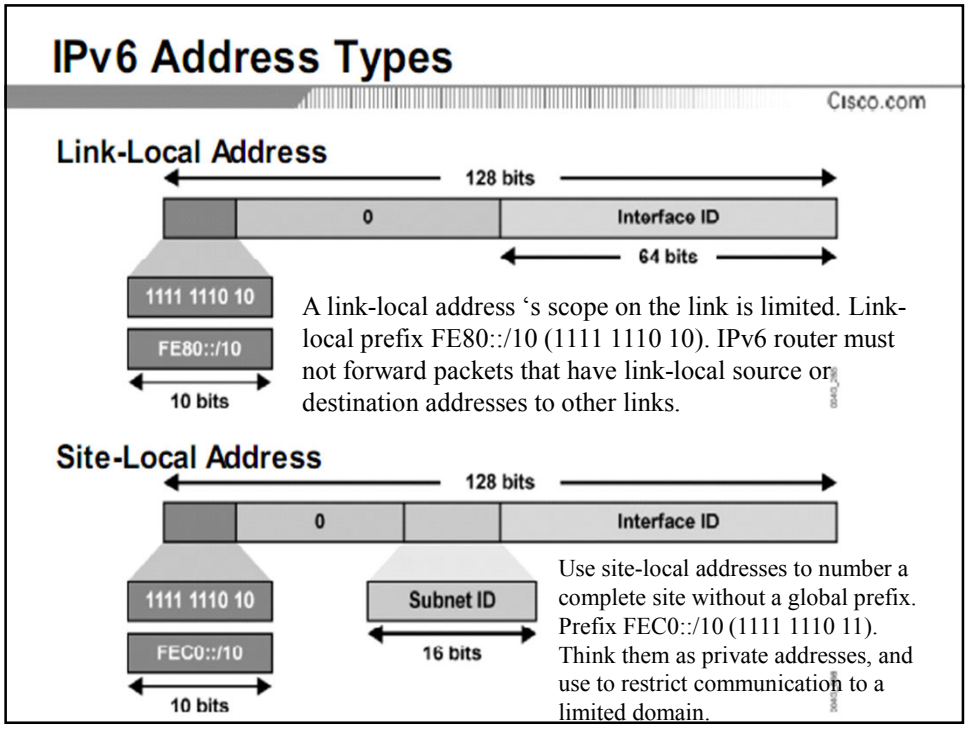
IP Address Requirements by Location

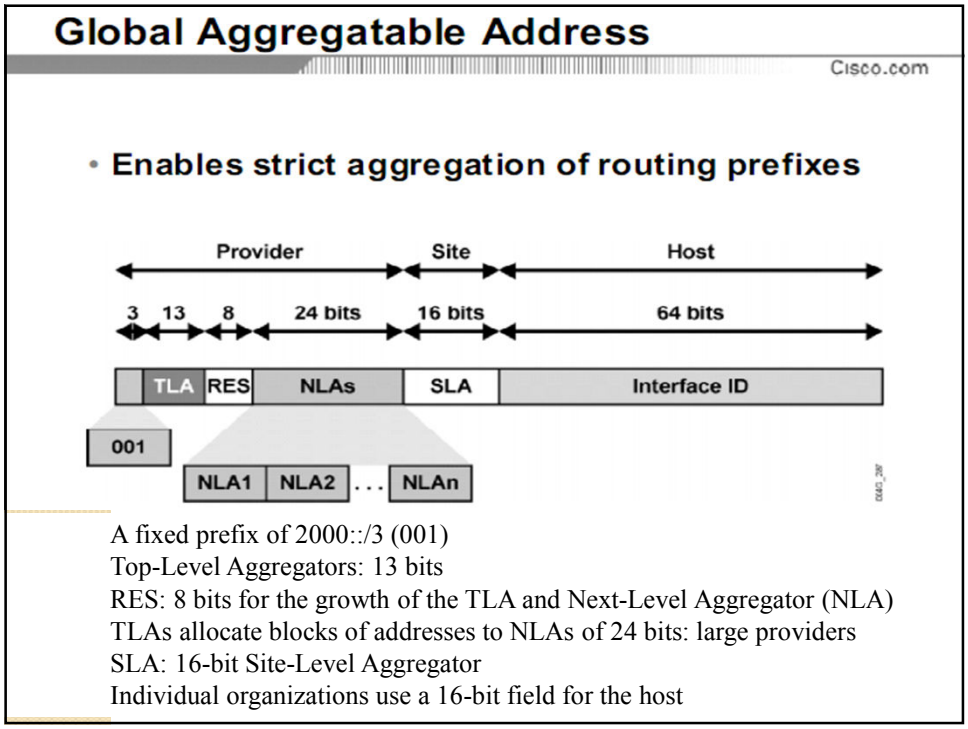
Cisco.com

Location	Office Type	Workstations	Servers	IP Phones	Router Interfaces	Switches	Firewall Interfaces	Reserve	Total
San Francisco	Main	600	35	600	17	26	12	20%	1290
Denver	Regional	210	7	210	10	4	0	20%	441
Houston	Regional	155	5	155	10	4	0	20%	329
Remote Office 1	Remote	12	1	12	2	1	0	10%	28
Remote Office 2	Remote	15	1	15	3	1	0	10%	35
Remote Office 3	Remote	8	1	8	3	1	0	10%	21
Total		1000	50	1000	45	37	12		2144









IPv4 to IPv6 Transition Strategies

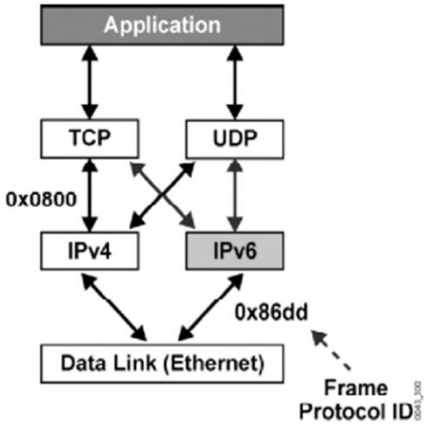
Cisco.com

Three major transition strategies are available:

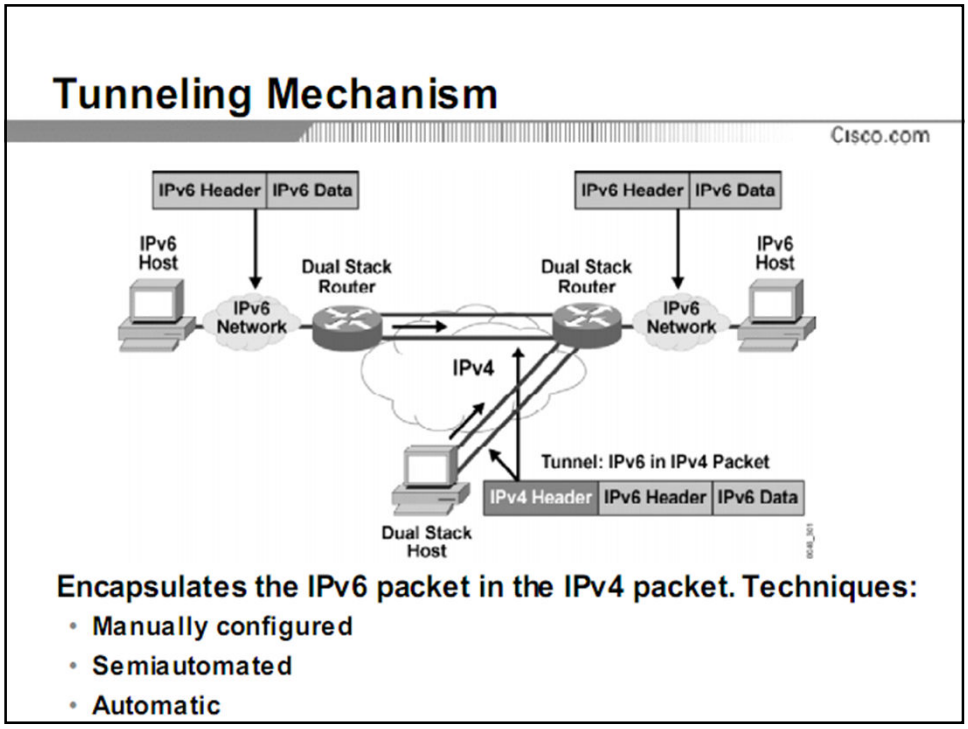
- Dual stack (IPv4 and IPv6 coexist in the same device and networks)
- Tunneling (IPv6 packets are encapsulated into IPv4 packets)
- Translation (IPv6-only devices can talk to IPv4 devices)

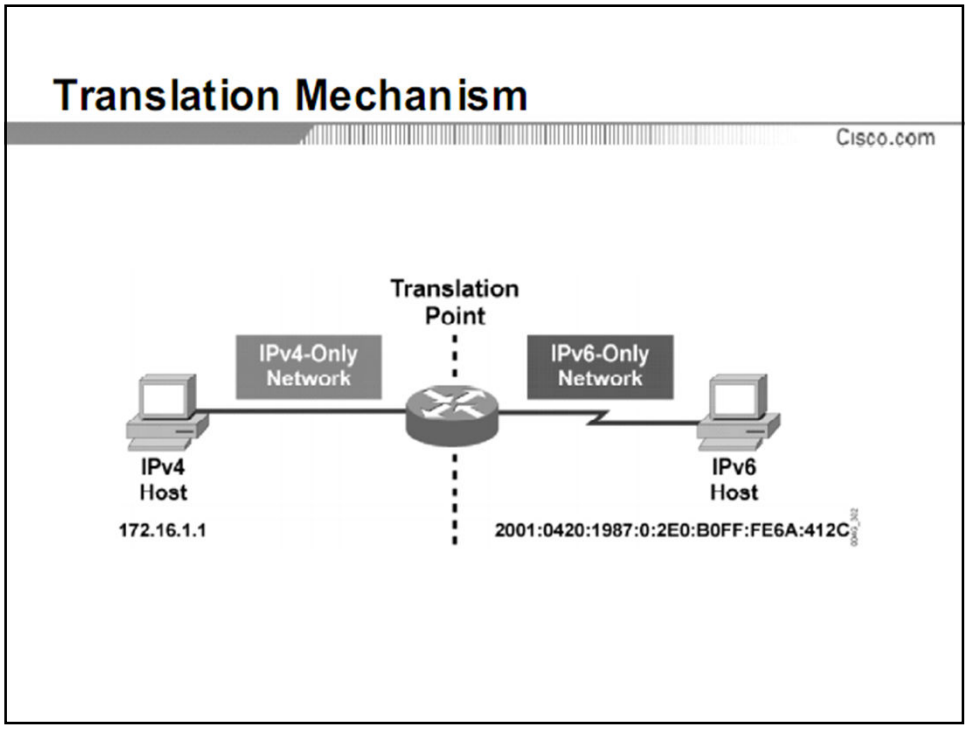
Dual-Stack Mechanism

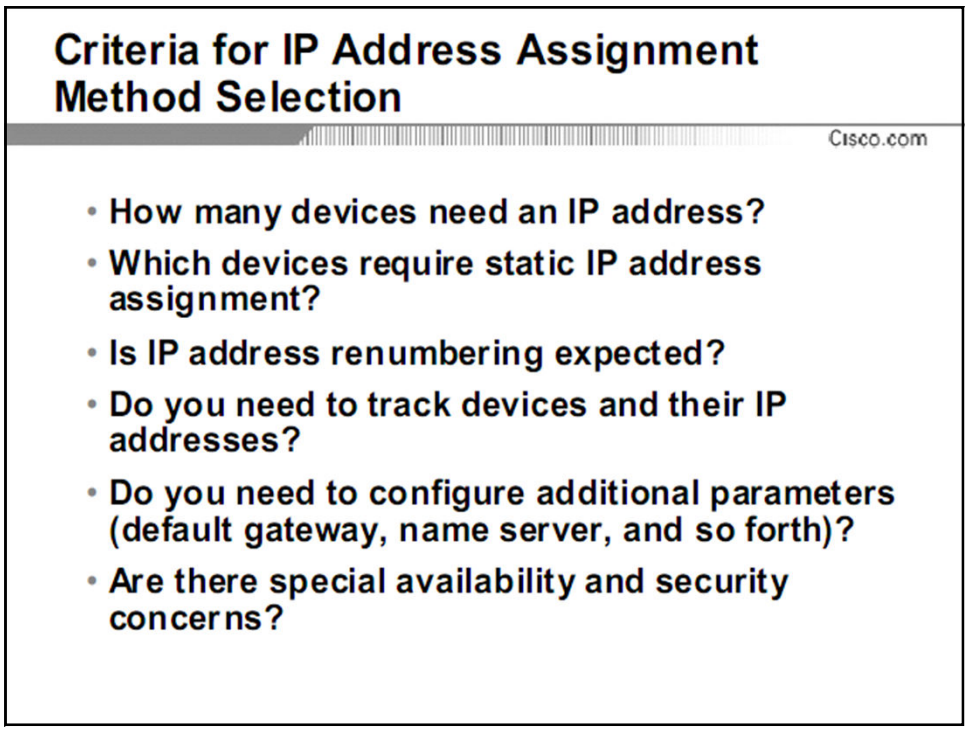
Cisco.com

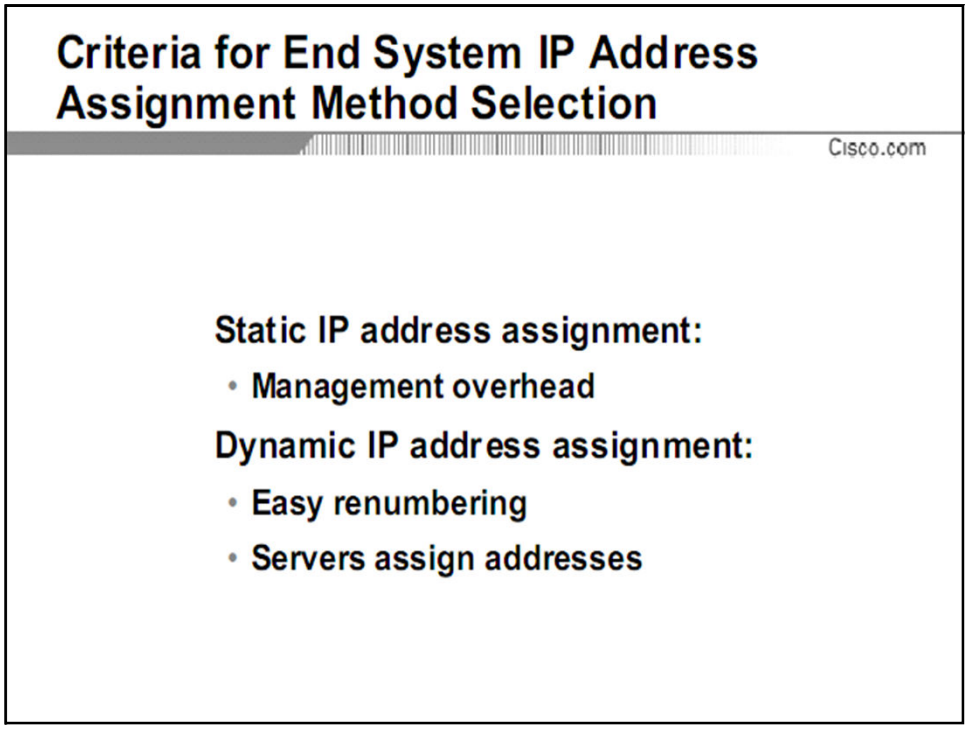


- Both IPv4 and IPv6 stacks are enabled.
- Applications can talk to both stacks.
- IP version choice is based on name lookup and application preference.
- Popular operating systems support IPv6.


Tunneling Mechanism
Cisco.com
IPv6 Header
IPv6 Data
IPv6 Header
IPv6 Data
IPv6 Host
Dual Stack Router
Dual Stack Router
IPv6 Host
IPv6 Network
IPv6 Network
IPv4
Tunnel: IPv6 in IPv4 Packet
IPv4 Header
IPv6 Header
IPv6 Data
Dual Stack Host
Encapsulates the IPv6 packet in the IPv4 packet. Techniques:
Manually configured
Semiautomated
Automatic


Translation Mechanism
Cisco.com
Translation Point
IPv4-Only Network
IPv6-Only Network
IPv4 Host
172.16.1.1
IPv6 Host
2001:0420:1987:0:2E0:B0FF:FE6A:412C





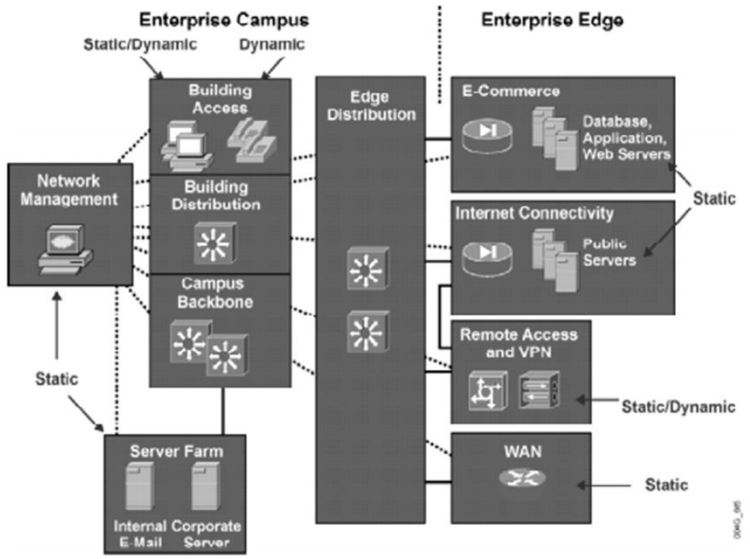
End System IP Address Assignment Method Decision Table

Cisco.com

Criteria \ Method	Static Address Assignment	Dynamic Address Assignment with DHCP
Number of hosts	Up to 30 hosts	More than 30 hosts
Renumbering	Requires manual reconfiguration of all hosts	Only DHCP server reconfiguration is needed
Address tracking	Easy address tracking	Requires additional DHCP server configuration
Additional parameters	Manual configuration of all hosts required	Only DHCP server needs to be configured
High availability	IP addresses are available at any time	Redundant DHCP server is required
Security	Minor security risk	Any device gets IP address

Example: IP Address Assignment Methods in an Enterprise Network

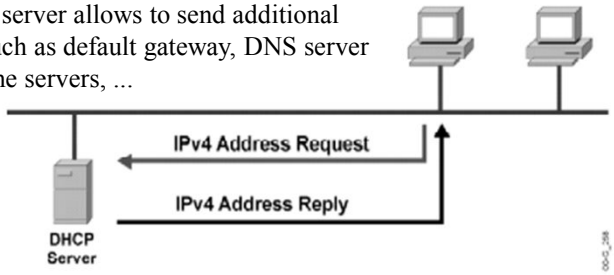
Cisco.com



IPv4 Address Assignment with DHCP

Cisco.com

In addition to the IPv4 address and the subnet mask, DHCP server allows to send additional parameters such as default gateway, DNS server addresses, time servers, ...



DHCP address allocation mechanisms:

- **Manual** IPv4 address to a specific MAC address
- **Automatic** The IPv4 address is permanently assigned to a host
- **Dynamic** The IPv4 address to a host for a limited time

Criteria for Selecting Name Resolution

Cisco.com

- How many hosts require name resolution?
- Are applications that depend on name resolution present?
- Is the network isolated or is it connected to the Internet?
- If the network is isolated, how frequently are new hosts added and how frequently do names change?

Static vs. Dynamic Name Resolution

Cisco.com

- Names used to ease computer-human interaction
- Names resolved into IP addresses
- Different name resolution strategies:

Static: The network administrator manually defined name-to-IP-address resolutions in a special file by entering the name and IP address pairs.
Dynamic: The administrator needs only to enter the name-to-IP-address resolutions on a special server and is relieved of repeating the task on every host

Name Resolution Method Decision Table

Cisco.com

Criteria \ Method	Static Name Resolution	Dynamic Name Resolution
Number of hosts	Up to 30 hosts	More than 30 hosts
Isolated network	Applicable	Applicable
Internet connectivity	Not applicable	Mandatory
Frequent changes and addition of names	Not recommended	Recommended
Application depending on name resoltuion	Not recommended	Recommended

Guidelines for Assigning Names

- Names should be
  - Short
  - Meaningful
  - Unambiguous
  - Distinct
  - Case insensitive
- Avoid names with unusual characters
  - Hyphens, underscores, asterisks, and so on

Domain Name System (DNS)

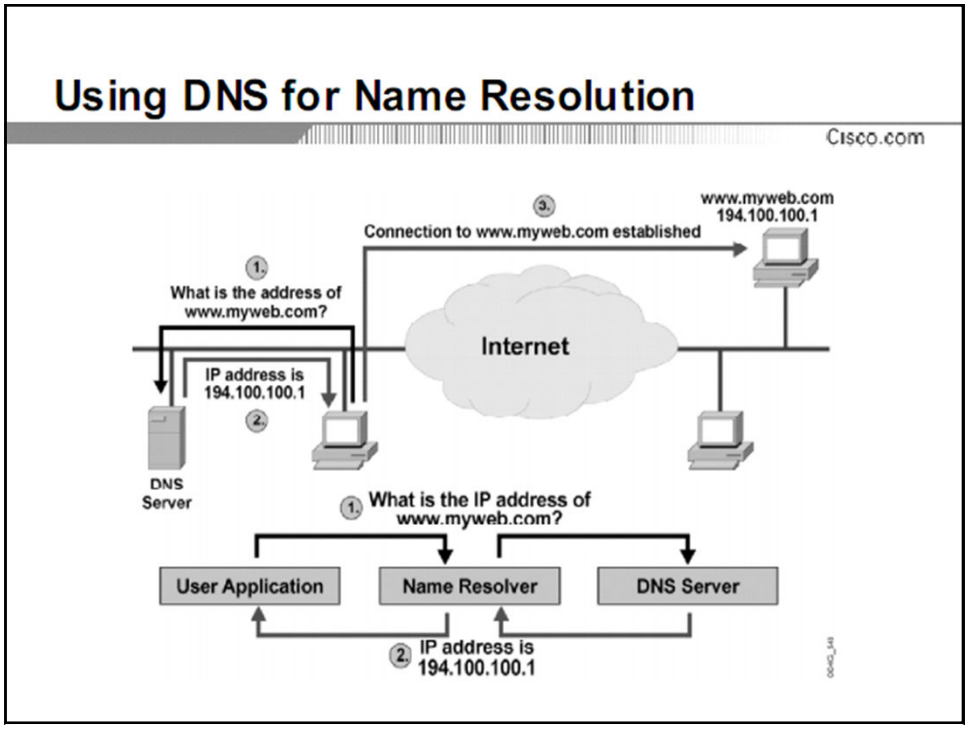
- Maps names to IP addresses
- Supports hierarchical naming
  - example: csehui.wordpress.com
- A DNS server has a database of resource records (RRs) that maps names to addresses in the server's "zone of authority"
- Client queries server
  - Uses UDP port 53 for name queries and replies
  - Uses TCP port 53 for zone transfers

DNS Details

- Client/server model
- Client is configured with the IP address of a DNS server
  - Manually or DHCP can provide the address
- DNS *resolver software* on the client machine sends a query to the DNS server. Client may ask for *recursive lookup*.

DNS Recursion

- A DNS server may offer *recursion*, which allows the server to ask other servers
  - Each server is configured with the IP address of one or more root DNS servers.
- When a DNS server receives a response from another server, it replies to the resolver client software. The server also caches the information for future requests.
  - The network administrator of the authoritative DNS server for a name defines the length of time that a non-authoritative server may cache information.



Summary

- Use a systematic, structured, top-down approach to addressing and naming
- Assign addresses in a hierarchical fashion
- Distribute authority for addressing and naming where appropriate
- IPv6 emerges in our future

Review Questions

- Why is it important to use a structured model for addressing and naming?
- When is it appropriate to use IP private addressing versus public addressing?
- When is it appropriate to use static versus dynamic addressing?
- What are some approaches to upgrading to IPv6?

