# CCNA Discovery 4.0 Designing and Supporting Computer Networks

## Using IP Addressing in Network Design– Chapter 6

Cisco | Networking Academy®
Mind Wide Open™

# Objectives

- Select the appropriate hierarchical IP addressing scheme to meet the physical and logical network requirements.
- Choose a routing protocol and design a route summarization strategy.
- Create a logical naming structure for networking devices.
- Describe IPv6 and the methods to implement it on a network.
- Implement IPv6 on a Cisco device.

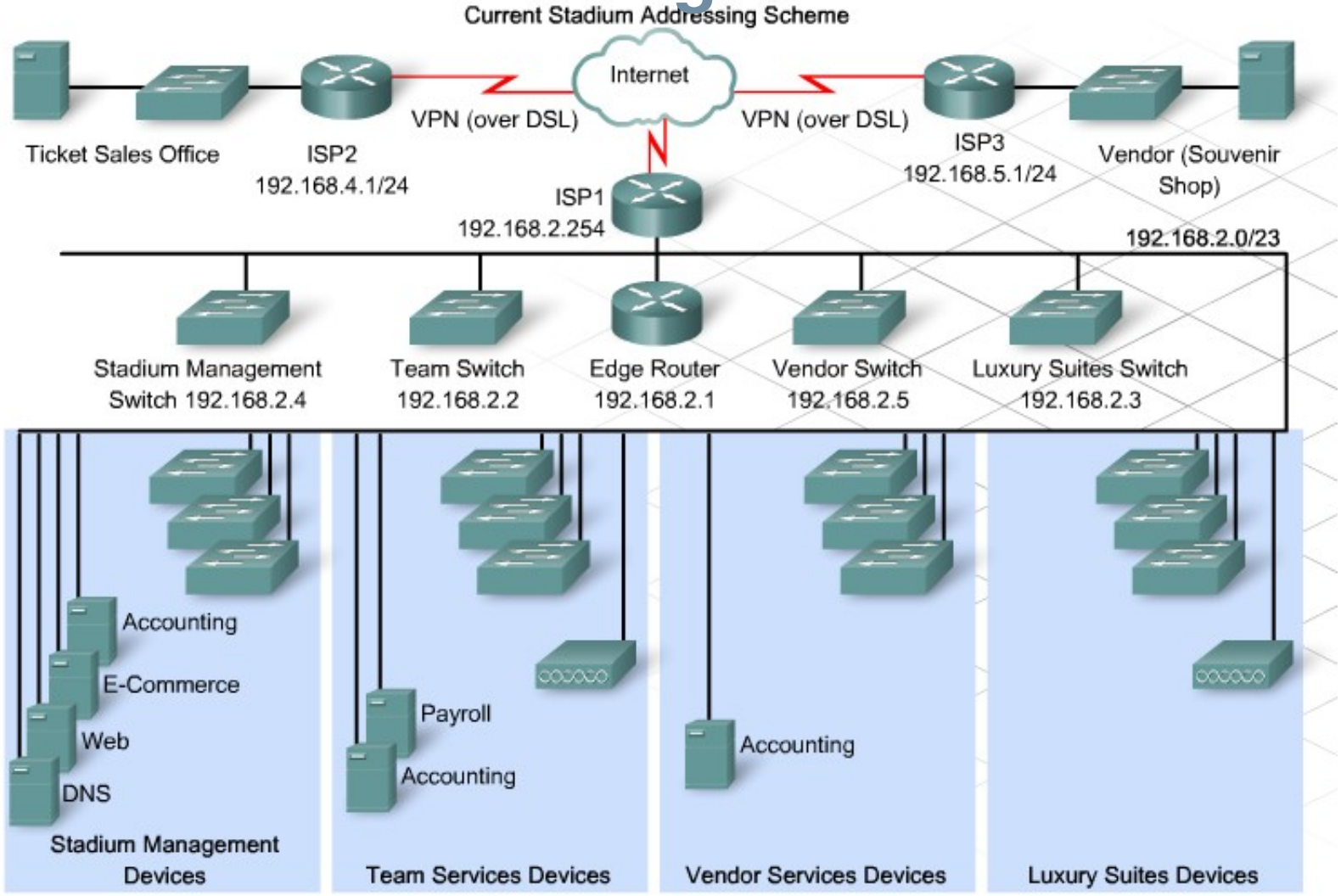
# Using Hierarchical Routing and addressing Schemes

- The IP Addressing Scheme
- In the existing IP addressing scheme for the stadium network, the network administrator chose the private IP network address of 192.168.2.0/23. Two additional subnets, 192.168.4.0/24 and 192.168.5.0/24, were used for addressing the two remote locations. The administrator assigned unique client IP addresses, using DHCP and static addresses. to each of the various network devices.

# Using Hierarchical Routing and addressing Schemes

- The current addressing scheme used for the stadium is not adequate because it cannot support the planned expansion of the network. In addition, the two wireless APs are assigning IP addresses that overlap with the existing StadiumCompany addresses.
- The new design needs to use an IP addressing scheme that ensures that each network device is assigned a unique IP address.

# Using Hierarchical Routing and addressing Schemes



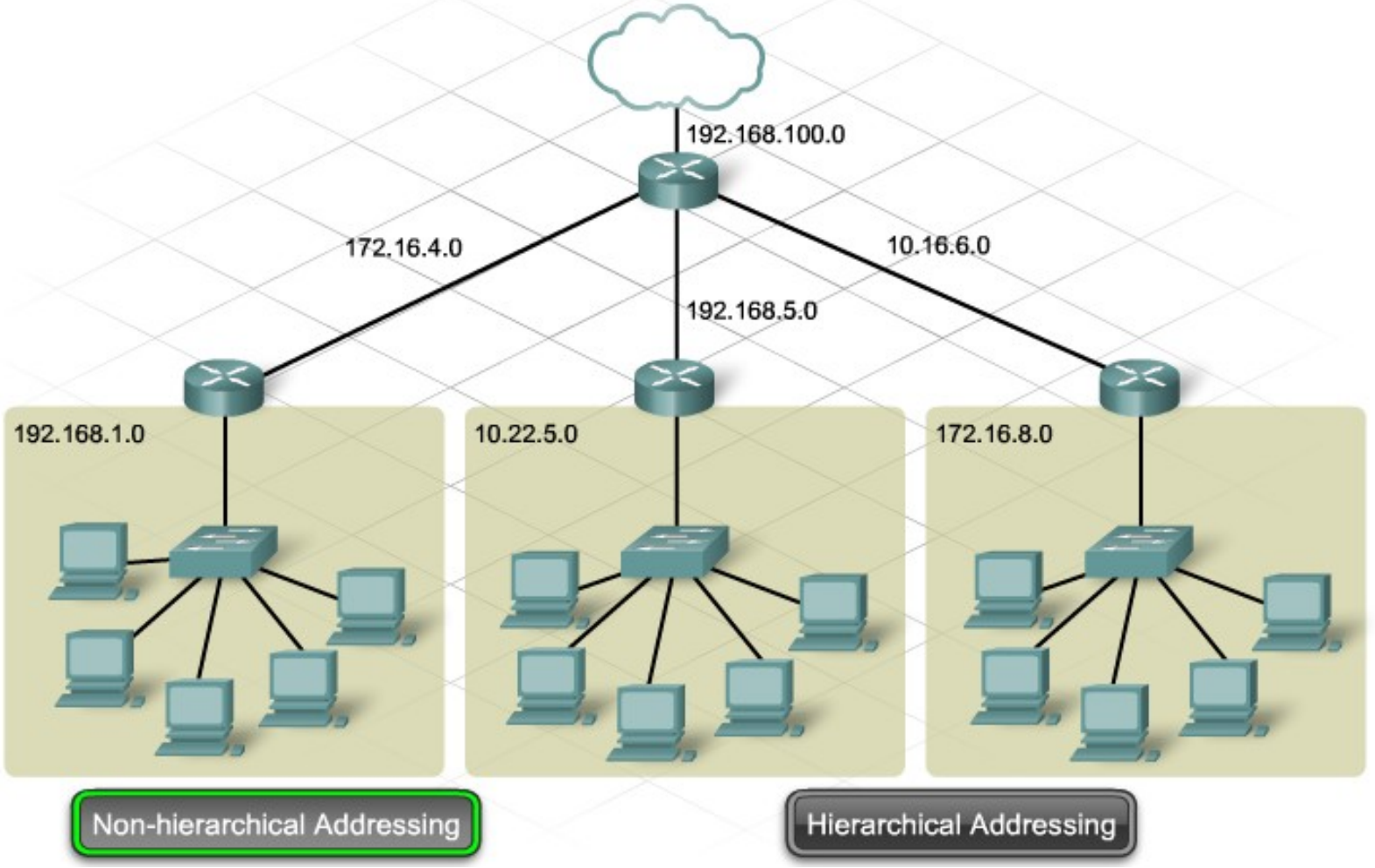
# Using Hierarchical Routing and addressing Schemes

- If the same IP address is assigned to more than one device on a network, an IP conflict occurs. An IP conflict on the network means that packets are not reliably delivered to the devices with the same IP address.
- With proper network planning, a new IP addressing scheme can support hierarchical routing and provide an efficient Layer 3 structure.

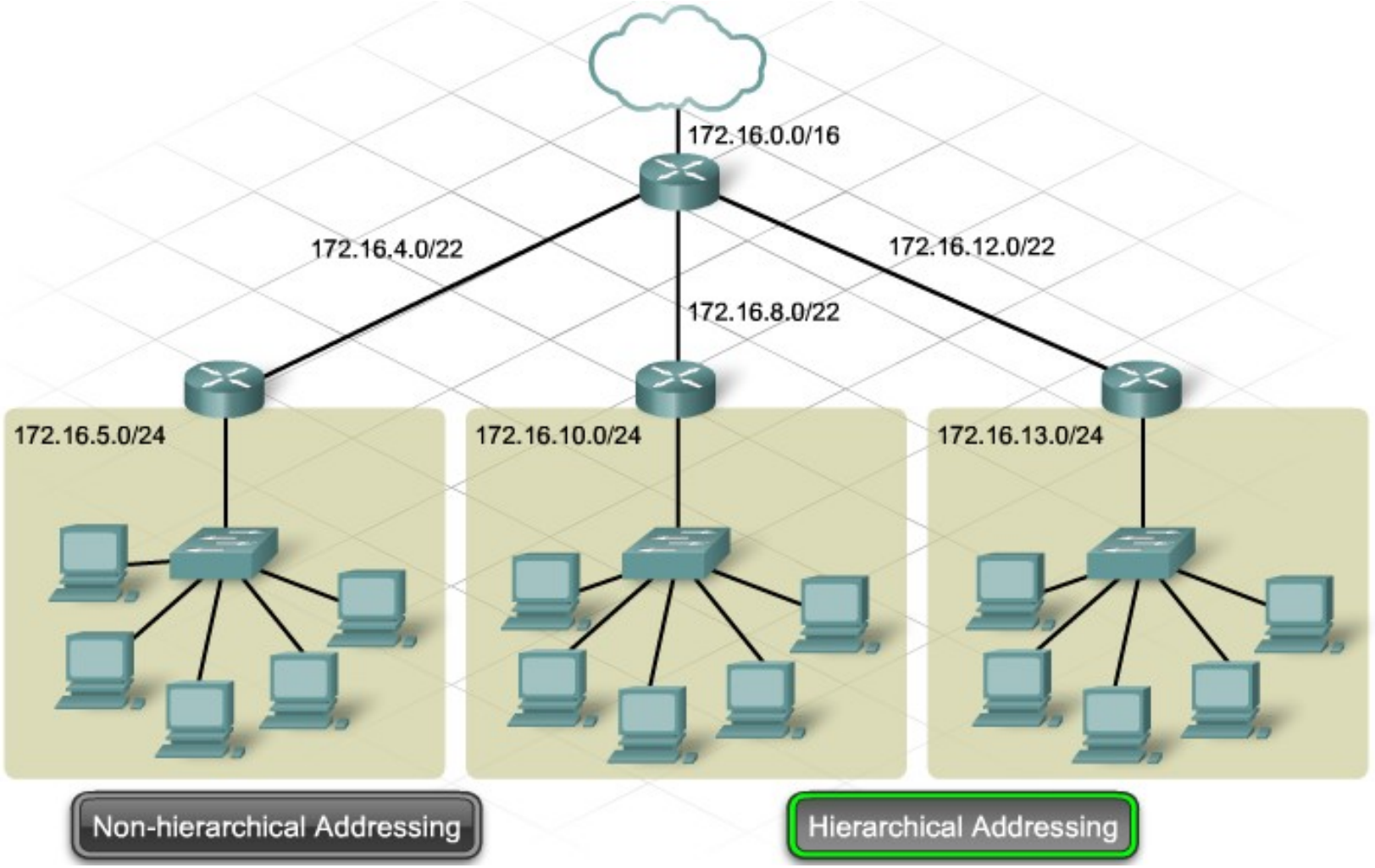
# Using Hierarchical Routing and addressing Schemes

- The allocation of IP addresses must be planned and documented to:
- Prevent duplication of addresses
- Provide and control access
- Monitor security and performance
- Support a modular design
- Support a scalable solution that uses route aggregation
- With a hierarchal IP addressing design, the stadium network is easier to support.

# Using Hierarchical Routing and addressing Schemes



# Using Hierarchical Routing and addressing Schemes



# Using Hierarchical Routing and addressing Schemes

- Using a Hierarchal IP Addressing Scheme
- A flat IP addressing scheme does not meet the stadium network requirements for scalability.
- A network with the correct allocation and deployment of IP address blocks has the following characteristics:
- Routing stability
- Service availability
- Network scalability
- Network modularity

# Using Hierarchical Routing and addressing Schemes

- Using a hierarchical IP addressing scheme for the stadium network makes it easier to increase the size of the network. A larger network can accommodate more users, ticketing kiosks, remote offices, and souvenir shops.
- A properly designed hierarchical IP addressing scheme also makes it easier to perform route summarization.

# Using Hierarchical Routing and addressing Schemes

Examples of devices that require an IP address

# Classful subnets and Summarization

- To support summarization, a network must be designed to have contiguous subnets. If a network is contiguous, all the subnets of the network are adjacent to all other subnets of the same network.
- A discontiguous network has non-adjacent subnets, or subnets that are separated from other subnets of the same network by other networks.

# Classful subnets and Summarization

- Poorly planned IP addressing can result in a discontiguous network. Discontiguous networks can cause routing issues, because there is more than one summary route entry in the routing table used to reach the subnets of a network

# Classful subnets and Summarization

- Disabling Automatic Summarization
- Usually, automatic summarization is desirable. However, in the case of discontiguous subnets, the following command must be entered for both Routing Information Protocol version 2 (RIPv2) and EIGRP to disable automatic summarization:
- Router(config-router)#no auto-summary

# Classful subnets and Summarization


Routers in this network are running auto-summarization. As a result, Router A and Router C both advertise the summary route 172.16.0.0/16. Router B receives both updates and installs both equal cost routes into the routing table. This causes reachability issues for both the 172.16.1.0 and 172.16.2.0 networks.

# Using VLSM when designing IP Addressing

- Variable Length Subnet Mask (VLSM)
- The network designer uses VLSM to create the subnet scheme for the proposed network. Using VLSM eliminates the requirement that all subnets of the same parent network have the same number of host addresses and the same prefix length. VLSM affords more efficient use of IP address space. VLSM also enables routers to summarize routes on boundaries that are not the same as the classed boundaries.

# Using VLSM when designing IP Addressing

- Classless InterDomain Routing (CIDR)
- When VLSM is used in the IP addressing scheme, the designer must use a routing protocol that supports CIDR.
- Classful routing protocols do not send subnet mask or prefix length information in routing updates. These protocols depend on the default subnet masks to determine the network portion of the IP addresses.
- Classless routing protocols send the prefix length along with the route information in routing updates. These protocols enable routers to determine the network portion of the address without using the default masks.

# Using VLSM when designing IP Addressing

| Parent Network | Subnets |
|---|---|
| 172.16.0.0/16 | 172.16.0.0/22 |
| | 172.16.4.0/22 |
| | 172.16.8.0/22 |
| | 172.16.12.0/22 |
| 172.17.0.0/16 | 172.17.0.0/24 |
| | 172.17.1.0/24 |
| | 172.17.2.0/24 |
| | 172.17.3.0/24 |

All subnets of the same classed network are equal size and use the same subnet mask and prefix length

Classful Subnetting

Classless Subnetting using VLSM

# Using VLSM when designing IP Addressing

| Parent Network | Subnets |
|---|---|
| 172.16.0.0/16 | 172.16.0.0/22 |
| | 172.16.4.0/24 |
| | 172.16.5.0/24 |
| | 172.16.6.0/24 |
| | 172.16.7.0/24 |
| | 172.16.8.0/22 |
| | 172.16.12.0/22 |
| 172.17.0.0/16 | 172.17.0.0/24 |
| | 172.17.1.0/24 |
| | 172.17.2.0/24 |
| | 172.17.3.0/27 |
| | 172.17.3.32/27 |
| | 172.17.3.64/27 |
| | 172.17.3.96/27 |
| | 172.17.3.128/27 |

Subnets can be of various sizes and prefix lengths, as long as there are no overlapping address ranges

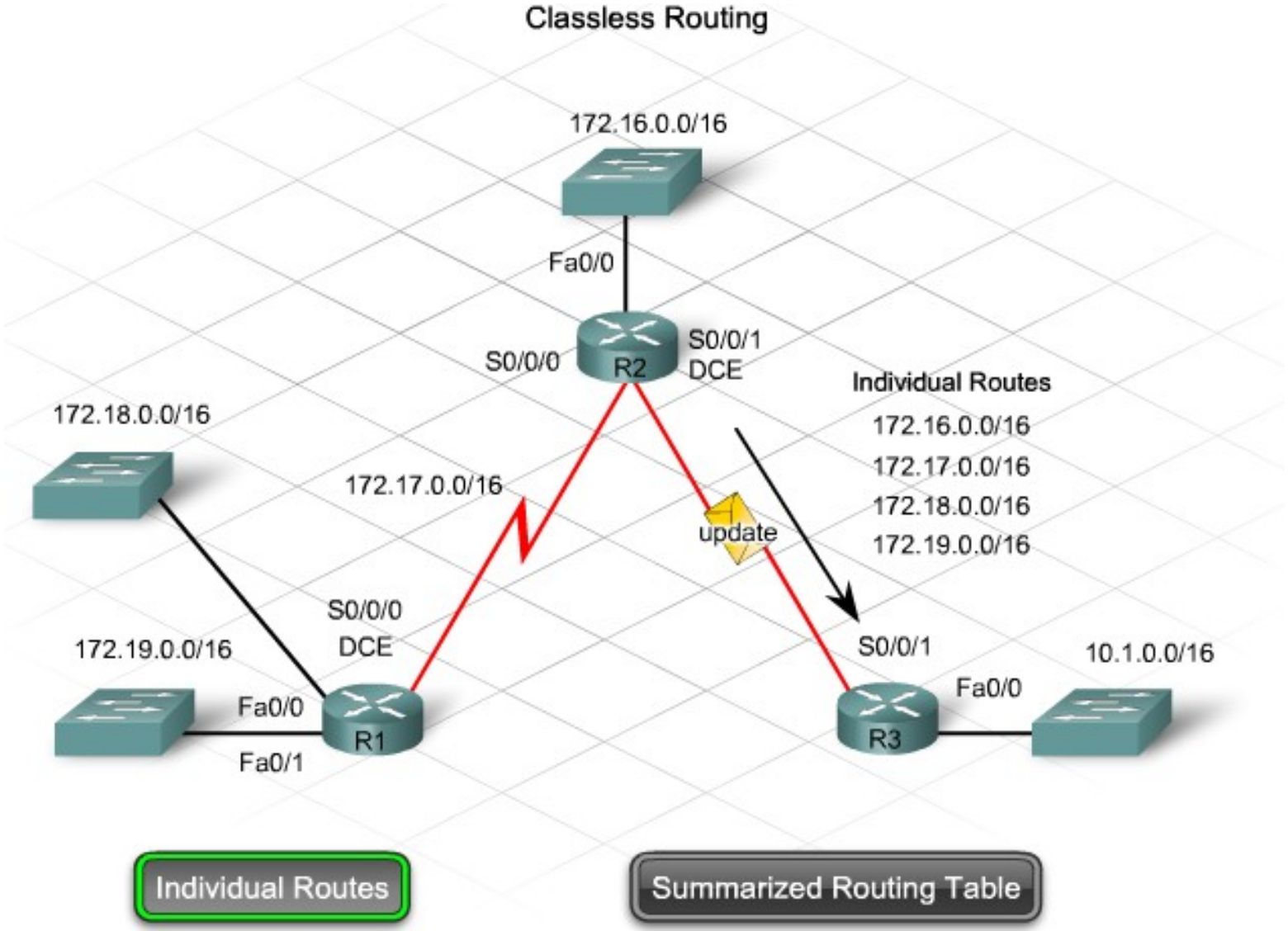
Classful Subnetting

Classless Subnetting using VLSM

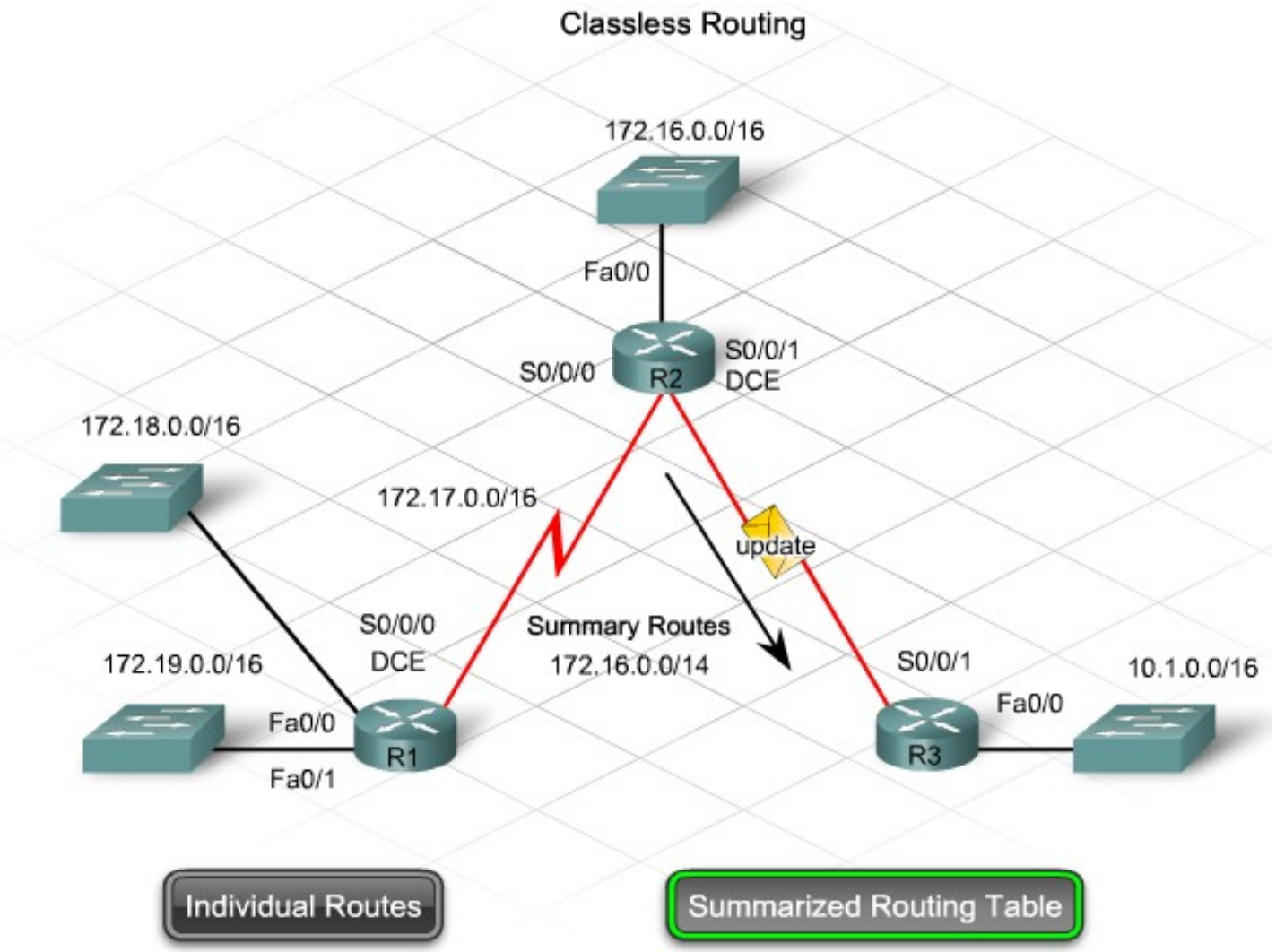
# Using CIDR Routing and Summarization

- CIDR and Summarization
- The hierarchal network design of the stadium is intended to make route summarization easier and to reduce routing protocol processing. Route summarization is also known as route aggregation. It is the process of advertising a set of contiguous addresses as a single entry with a shorter, less specific subnet mask or prefix.
- Because CIDR ignores the limitation of classful boundaries, it enables summarization with VLSMs that are shorter than the default classful mask.

# Using CIDR Routing and Summarization



# Using CIDR Routing and Summarization



# Using CIDR Routing and Summarization

- A network address with a prefix length shorter than the default classed prefix length is referred to as a **supernet**. An example of a **supernet** address is 172.16.0.0/14. The default prefix for the Class B 172.16.0.0 address is 16 bits. Using a /14 prefix, four contiguous Class B addresses can be summarized into one routing table entry.
- This type of summarization helps reduce the number of entries in routing updates and lowers the number of entries in local routing tables. The result is faster routing table lookups.

# Using CIDR Routing and Summarization

- Prefix Addresses and Summarization
- Classless routing protocols carry the prefix length and subnet mask with the 32-bit address in routing updates.
- A complex hierarchy of variable-sized networks and subnetworks can be summarized at various points using a prefix address. For example, a summary route can contain a 14-bit prefix that is common to all the addresses reachable through a router.

# Using CIDR Routing and Summarization

- The prefix :
- 172.16.0.0/14 or
- 10101100.00010000.00000000.00000000
- with a subnet mask of:
- 11111111.11111100.00000000.00000000
- summarizes the 172.16.0.0 /16, 172.17.0.0 /16, 172.18.0.0 /16, and 172.19.0.0 /16 subnets into an aggregate address.
- Route summarization reduces the burden on upstream routers.

# Using CIDR Routing and Summarization

| Routing Table for R1 | |
|---|---|
| Route | Source |
| 172.18.0.0 / 16 | Connected |
| 172.19.0.0 / 16 | Connected |
| 172.17.0.0 / 16 | R2 |
| 172.16.0.0 / 16 | R2 |
| 192.168.1.0 /24 | Connected |
| 10.1.0.0 / 16 | R2 |

| Routing Table for R2 | |
|---|---|
| Route | Source |
| 172.18.0.0 / 16 | R1 |
| 172.19.0.0 / 16 | R1 |
| 172.17.0.0 / 16 | Connected |
| 172.16.0.0 / 16 | Connected |
| 192.168.1.0 /24 | Connected |
| 10.1.0.0 / 16 | Connected |

Summary Address

| Routing Table for R3 | |
|---|---|
| Route | Source |
| 172.16.0.0 / 14 | R2 |
| 192.168.1.0 /24 | Connected |
| 10.1.0.0 / 16 | Connected |

# Designing the Logical LAN addressing Scheme

- For the network designer, some decisions about IP addressing for the stadium network are easy - for example, using a private address range for the LAN rather than a public address range. Other decisions require more careful planning.
- When creating an IP addressing scheme, the designer follows these steps:

# Designing the Logical LAN addressing Scheme

- Step 1: Plan the entire addressing scheme before assigning any addresses.
- Step 2: Allow for significant growth.
- Step 3: Begin with the Core network summary addresses and work out to the edge.
- Step 4: Identify which machines and devices require statically assigned addresses.
- Step 5: Determine where and how dynamic addressing is implemented.
- These considerations apply whether or not the designer is using public or private addressing.

# Designing the Logical LAN addressing Scheme

1. The StadiumCompany is expecting significant growth, especially in the wireless area.

2. The five areas I need to group into contiguous blocks that can be summarized include the StadiumCompany devices, Team devices, Luxury Suites devices, Data Center Devices, and the four remote sites.

3. All of the end user PCs will use DHCP for addressing. I need to statically address the infrastructure devices, including the two core switches, six distribution switches and all of the access switches. I will also need static addresses for the servers and the wireless LAN controllers.

4. I will put my campus DHCP server in the Data Center. I will use the Cisco ISRs at the remote sites for DHCP. I think I can use the DHCP on the wireless controller to assign addresses to the wireless end devices. I will have to figure out what ranges to assign to each DHCP server.

# Designing the Logical LAN addressing Scheme

- Network address design is determined by several criteria:
- The number of hosts and networking devices that are currently supported on the network
- How much growth is anticipated
- The number of hosts that must be reachable from networks that are not part of the local LAN or Intranet
- The physical layout of the network
- The routing and security policies that are in place

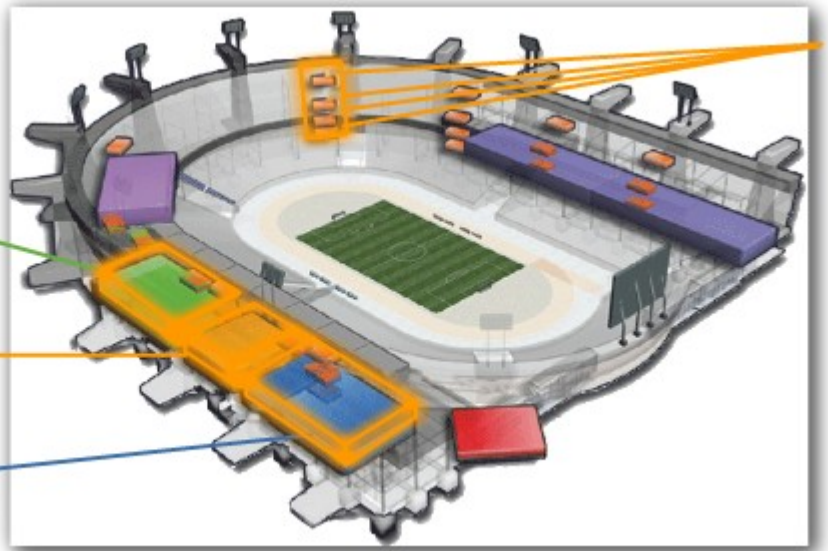
# Designing the Logical LAN addressing Scheme

- In the current stadium network, there are not many hosts. Approximately 500 hosts are attached to the wired network and a small number of hosts connect wirelessly. Based on the anticipated growth of the StadiumCompany, the network designer estimates at least 2000 end user devices within two years. This number includes printers, scanners, APs, wireless devices, IP phones, and cameras on the network that need individual IP addresses. To provide room for this growth, the designer decides to use a private Class B IP address block.

# Designing the Logical LAN addressing Scheme

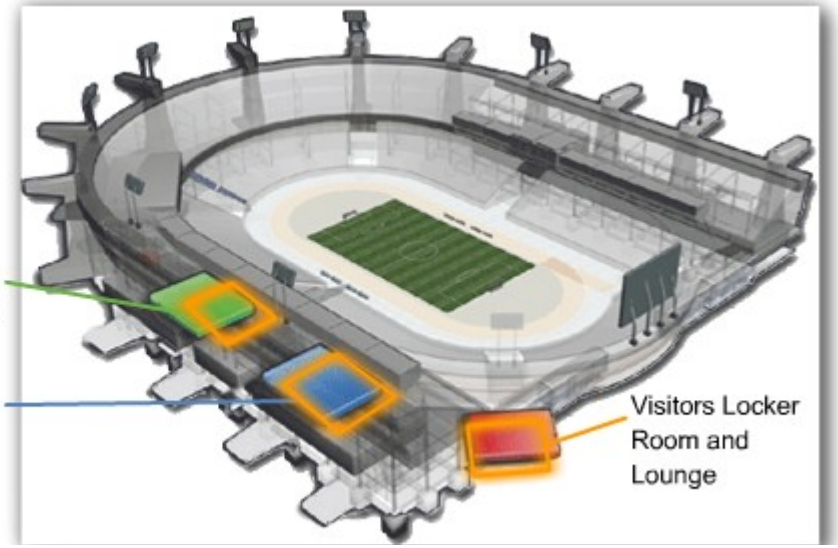
Reset


Reset



# Designing the Logical LAN addressing Scheme

Reset




Reset

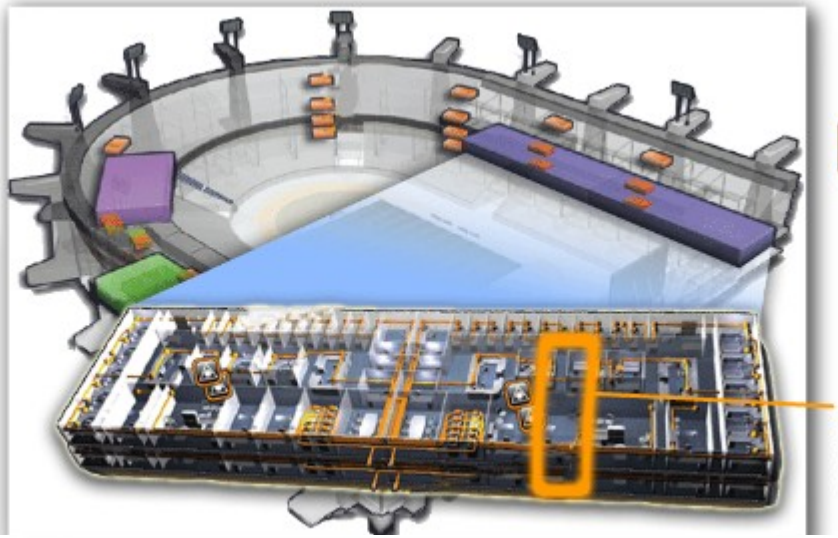
# Designing the Logical LAN addressing Scheme

Reset

Stadium Management Office

Stadium Managment Office: Two floors, 5 large exec offices 20x20, 30 manager offices, 12 large shared offices, 30 small offices, 2 break rooms and 2 conference rooms.

Reset




# Designing the Logical LAN addressing Scheme

Reset

Wireless Access Point Locations

LEGEND:
Existing Wireless APs

Reset

Wireless Access Point Locations

LEGEND:
Planned Wireless APs

# Designing the Logical LAN addressing Scheme

- Reachability of Hosts
- Some hosts in the network must be reachable from networks that are not part of the local LAN or Intranet. To be accessible from the Internet, servers and services must be assigned a publicly registered IP address. There needs to be sufficient public addresses to use with NAT. At the stadium, the two team servers and the web and e-commerce servers offer services that must be accessible from the Internet. The network designer concludes that the existing /27 subnet block of 30 public addresses from the Internet Service Provider is appropriate.

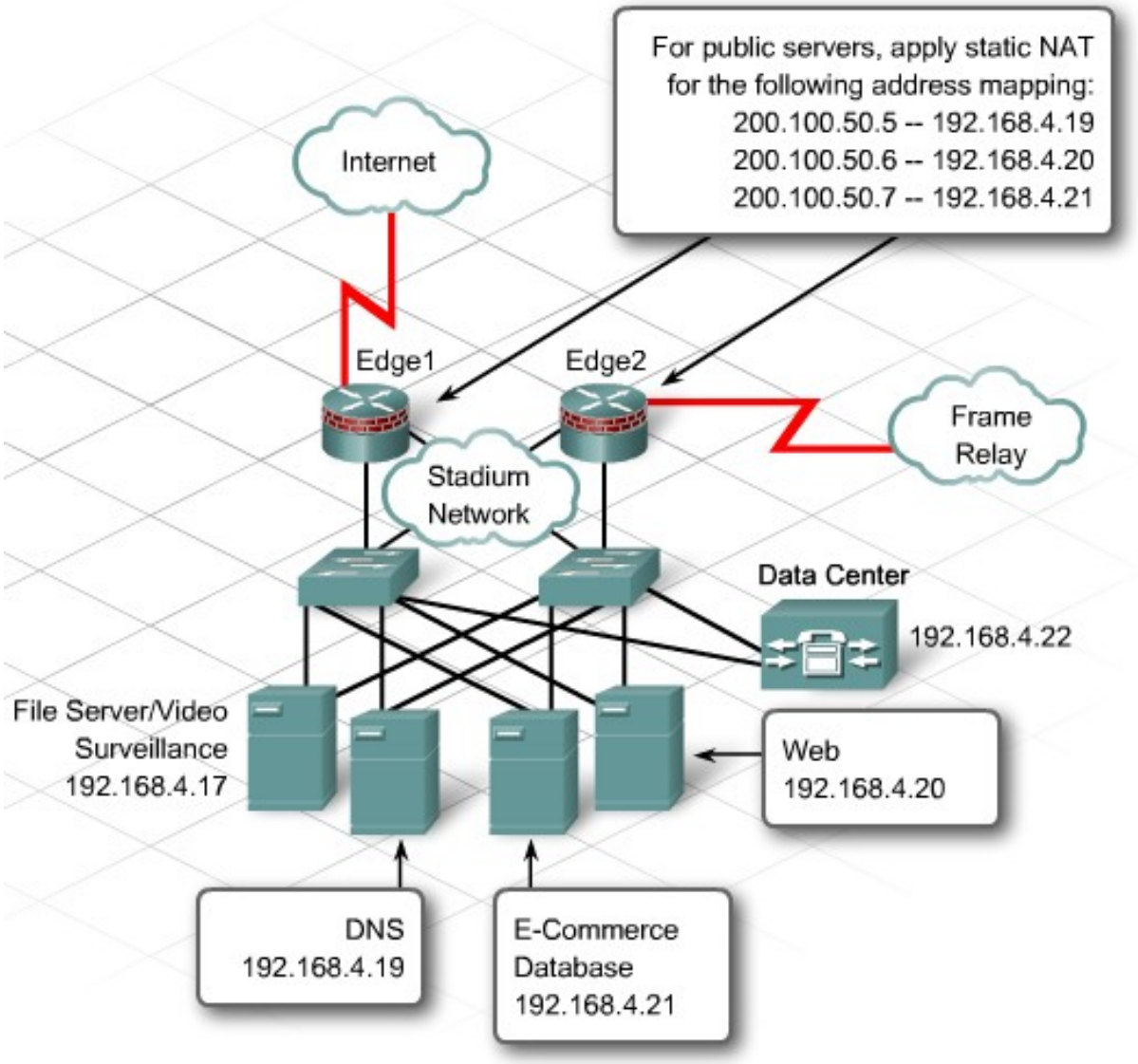
# Designing the Logical LAN addressing Scheme

- Physical Layout of the Network
- At the stadium, 16 separate wiring closets are available to support the geographic distribution of end user devices. It is a good policy to restrict the IP subnets to the individual physical wiring closet locations. Separate network addresses are needed for each redundant connection between the routers, Layer 3 switches, and the WAN.

# Designing the Logical LAN addressing Scheme

- Security and Routing Policies
- Sometimes additional IP networks are needed to separate traffic for security or filtering purposes. In these cases, separate IP subnets are usually created. Wireless and IP telephones require separate IP networks.
- The choice of a routing protocol affects how a network is addressed. Some routing protocols do not support classless IP addressing. The default summarization implemented in the routing protocol is also a consideration. The designer notes that the planned Class B addressing scheme requires a classless routing protocol.

# Determining the Addressing Blocks



# Determining the Addressing Blocks

- The network designer determines the number of IP networks or subnets required, based on the IP addressing strategy for the stadium.
- The designer counts the number of subnets and notes the current and projected number of users or devices on each network.
- Each wiring closet has a minimum of four subnets:
- Data
- IP Voice
- Video surveillance and game video
- Network management services

# Determining the Addressing Blocks

- In some areas, more than four subnets are necessary to separate traffic. VLANs are used on the switches to support each separate subnet.
- For each location within the network, the designer records the following information:
- Location and description
- VLAN or network type
- Number of networks and hosts

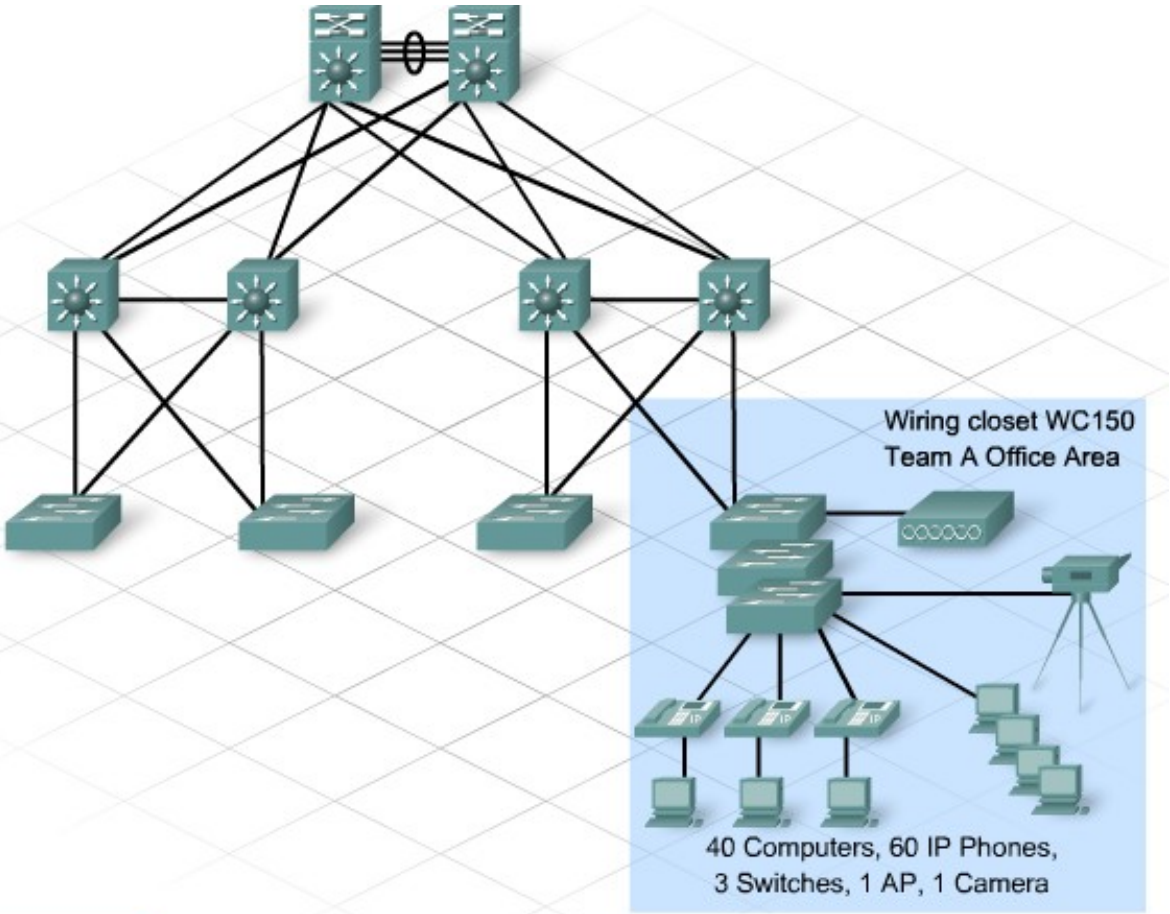
# Determining the Addressing Blocks

- Location and Description
- The designer identifies each location by documenting the wiring closet or data center room number and a description of the area of the stadium to which the wiring closet connects.
- VLAN or Network Type
- Documenting the type of VLAN or network enables the designer to accurately estimate the potential growth in the number of hosts. A data VLAN may increase in size more than a VLAN supporting IP telephones

# Determining the Addressing Blocks

- Number of Networks and Hosts per Network
- Next, the designer counts and lists the number of networks and the number of hosts per network that exist in the new design. This count represents the current address requirements. The designer can then estimate the growth in each area to determine the size of the IP network or subnet.
- The wireless network requirements are specified separately. Adding wirelessly connected devices increases the number of IP addresses needed without adding any new switches or ports.

# Determining the Addressing Blocks



# Determining the Addressing Blocks

IP Network Requirements Chart

| Access Layer Location | Area Description | VLAN or Network Type | Number of Networks | Number of Hosts | Growth |
|---|---|---|---|---|---|
| Access Layer | | | | | |
| W150 | Team A Office Area | Data VLAN | 1 | 40 | 50% |
| W150 | Team A Office Area | Voice VLAN | 1 | 60 | 20% |
| W150 | Team A Office Area | Management VLAN | 1 | 4 | 25% |
| W150 | Team A Office Area | Video Surveillance | 1 | 1 | None |
| W172 | Team B Office Area | Data VLAN | 1 | 22 | 50% |
| W172 | Team B Office Area | Voice VLAN | 1 | 38 | 20% |
| W172 | Team B Office Area | Management VLAN | 1 | 4 | 25% |
| W172 | Team B Office Area | Video Surveillance | 1 | 1 | None |
| Distribution Layer | | | | | |
| DC220 | Team Office and Restaurant Distribution | Layer 3 uplink to Core | 5 | 2 | None |
| DC220 | Management Office and Restaurant Distribution | Layer 3 uplink to Core | 5 | 2 | None |

Network Diagram

IP Network Requirements Chart

# Designating the Routing Strategy

- The network designer needs to select a routing protocol that meets these stadium requirements:
- Classless routing operation that supports VLSM
- Small and infrequent routing table updates to reduce traffic
- Fast convergence in the event of a failure
- The stadium has the constraint that the existing networking staff must be able to support the resulting network. Therefore, the routing protocol must be easy to troubleshoot and reconfigure in the event of a failure.

# Designating the Routing Strategy

- Two members of the network staff have experience using EIGRP. Because EIGRP meets all of the stadium requirements, the network designer selects EIGRP instead of OSPF and RIPv2.
- EIGRP is a Cisco proprietary routing protocol. All of the stadium devices participating in dynamic routing must be Cisco devices.

# Designating the Routing Strategy

- EIGRP Load Balancing
- In the design of the stadium network, redundant and backup links are necessary to meet the availability requirements. EIGRP is a good choice because it can support load balancing over these additional links. By default, EIGRP installs up to four equal cost paths to the same destination in the routing table. To control the number of routes EIGRP installs. the maximum-paths command is used.

# Designating the Routing Strategy

- Acceptable values for the maximum-paths command are between 1 and 6. If a value of 1 is configured, it disables load balancing, since only 1 route can be installed in the routing table for a specific destination.

# Designating the Routing Strategy

- Unequal Cost Load Balancing
- There are times, such as during ticketing for popular events, that it may be necessary to use backup links for load balancing the heavy traffic. Because the backup links do not always have the same routing cost as the primary links, traffic is not load balanced across the backup links by default. A router in an EIGRP network can be configured to use unequal cost load balancing by using the variance command.

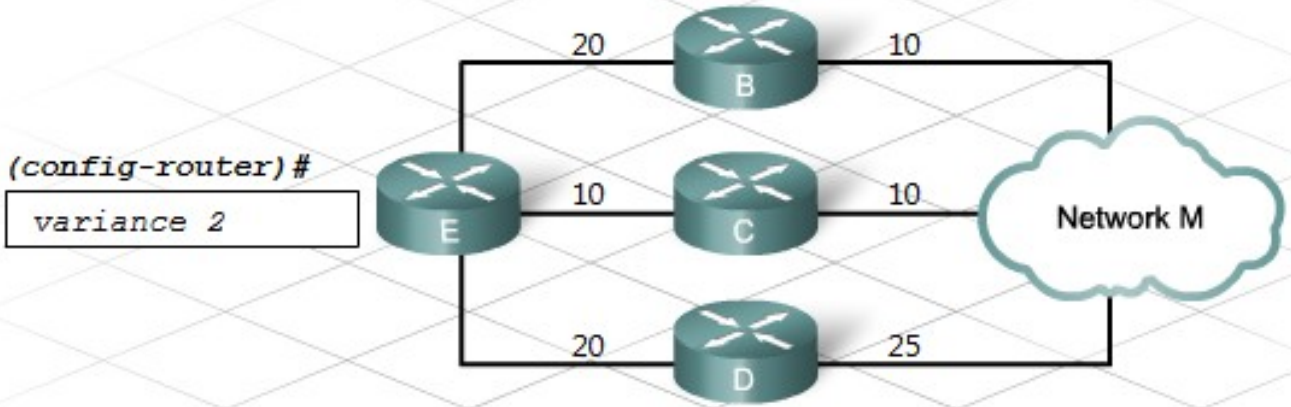
# Designating the Routing Strategy

- A variance is a value that EIGRP uses to determine whether or not to install a specific route in the route table to be available for load balancing. The formula EIGRP uses to set the range of acceptable route costs is variance times metric. Use the variance command followed by a value between 1 and 128. An example of the command is:
- Router(config-router)# variance 2
- Splitting traffic in this way prevents a single path from being overburdened by heavy traffic when alternate paths are available.

# Designating the Routing Strategy

A route is feasible if the next router in the path is closer to the destination than the current router, and if the metric of the alternate path is within the variance. Load balancing can use only feasible paths, and the routing table includes only these paths.

| Network | Neighbor | Metric |
|---|---|---|
| M | B | 30 |
| | C | 20 |
| | D | 45 |



# Designating the Routing Strategy

- Authentication
- In the stadium network, there are vendors and remote sites that participate in the network routing. It is important to know that routing updates are coming from routers that are trusted. Routing protocols can be configured to only accept updates from trusted devices by using neighbor authentication. When neighbor authentication is configured on a router, the router authenticates the source of each routing update packet that it receives.

# Designating the Routing Strategy

- There are two types of neighbor authentication: plain text authentication and Message Digest Algorithm Version 5 (MD5) authentication. Using MD5 authentication is a recommended security practice, because the key or password cannot be intercepted and read in transit.

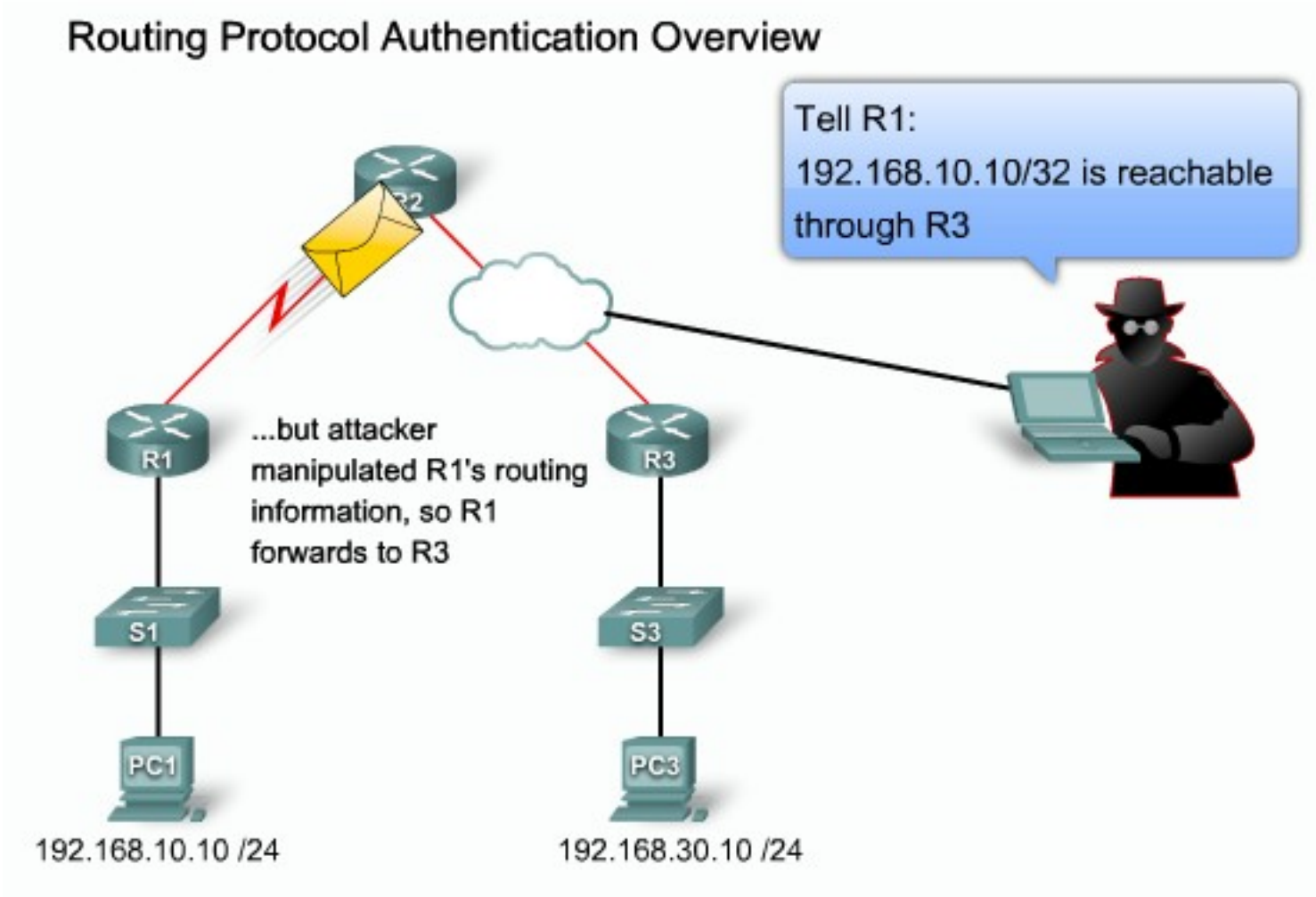
# Designating the Routing Strategy

- Key Management
- In MD5 authentication, each participating neighbor router is configured to share an authenticating key. RIPv2 and EIGRP routing protocols offer the additional function of managing keys by using key chains. A series of keys can be configured and the Cisco IOS software rotates through each of the keys. This decreases the likelihood that keys will be compromised.

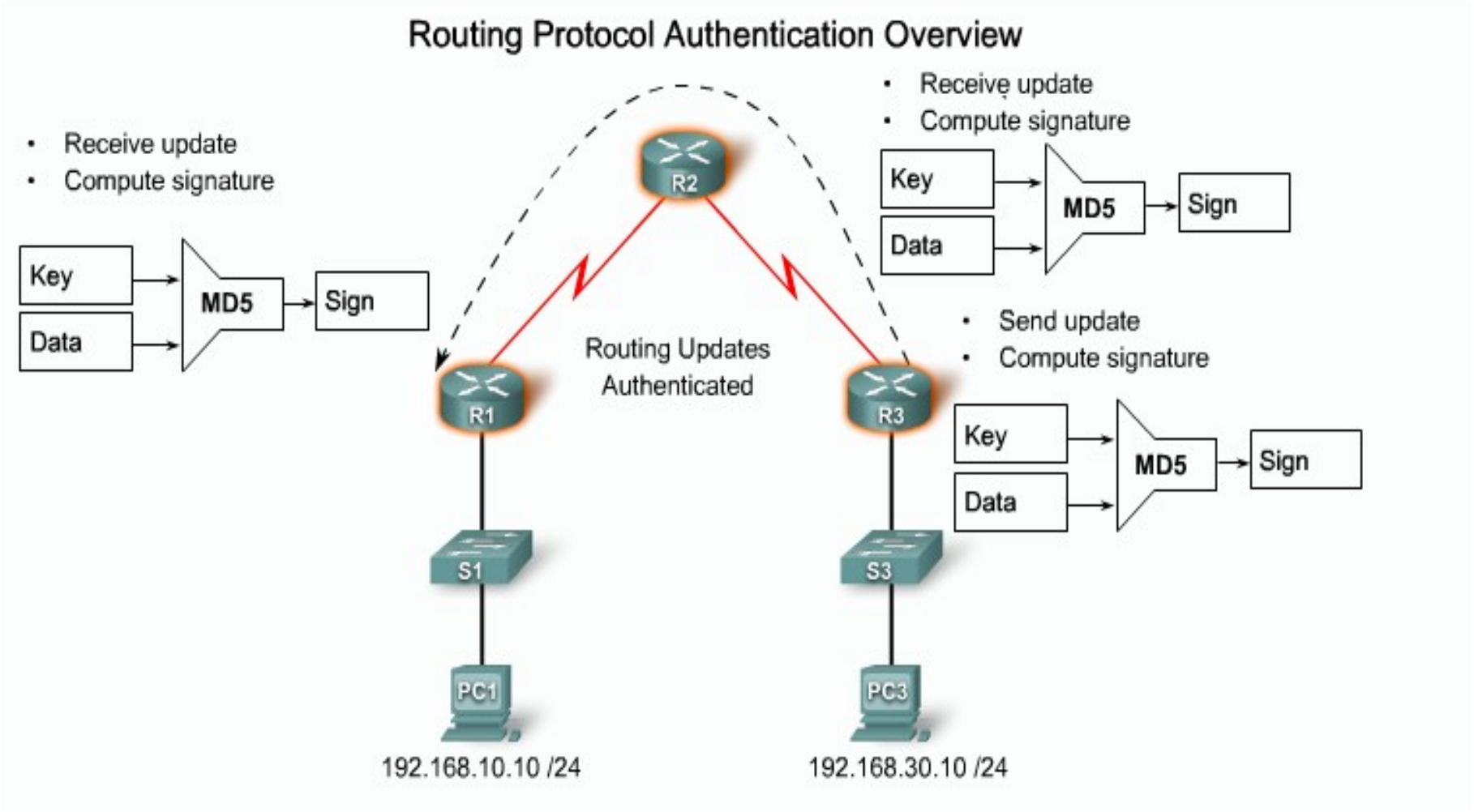
# Designating the Routing Strategy

- Every key definition must specify the time interval when the key is active (its "lifetime"). Then, during a given key's lifetime, routing update packets are sent with the activated key. It is recommended that for a given set of keys, key activation times overlap to avoid any period of time for which no key is active. If a time period occurs during which no key is active, neighbor authentication cannot occur, and therefore routing updates will fail.

# Designating the Routing Strategy



# Designating the Routing Strategy



# Plan for Summarization and route Distribution

- In a hierarchical design, route summarization occurs at the Layer 3 devices that act as gateways for multiple contiguous IP networks. These summary routes are then advertised toward the Core Layer of the network. The summarization in the stadium LAN occurs at the Distribution Layer routers and Layer 3 switches.

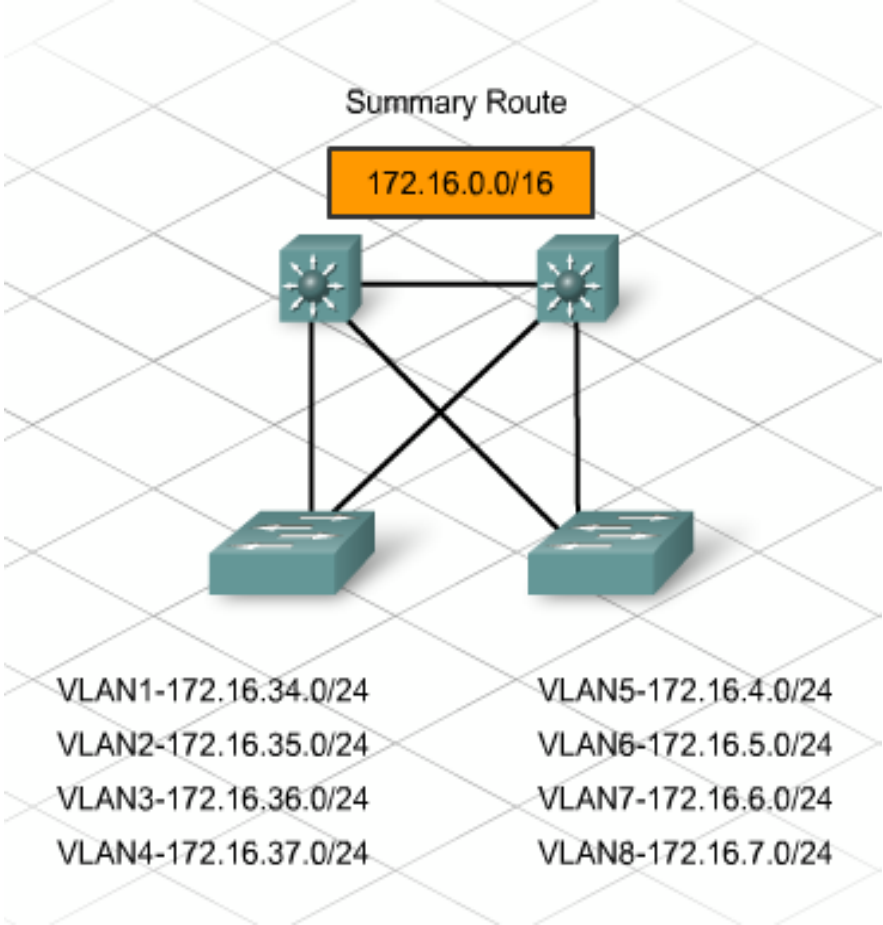
# Plan for Summarization and route Distribution

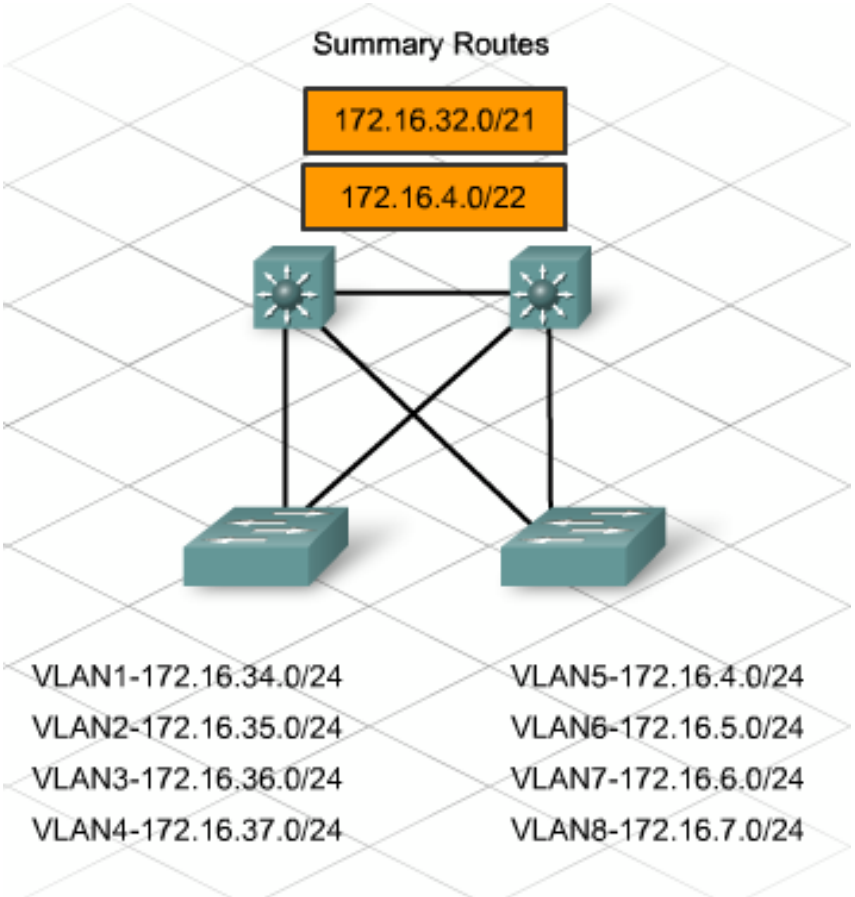
- EIGRP enables classless summarization with masks that are different from the default classful mask. This type of summarization helps reduce the number of entries in routing updates and lowers the number of entries in local routing tables. Summarization reduces the amount of bandwidth used by routing updates and results in faster routing table lookups.

# Plan for Summarization and route Distribution

- EIGRP includes an automatic route summarization feature. However, this automatic summarization occurs only at the default classful network boundary. This feature is not appropriate for the stadium network design. To be able to summarize the subnets of the proposed Class B addressing scheme, the automatic route summarization in EIGRP must be disabled.

# Plan for Summarization and route Distribution

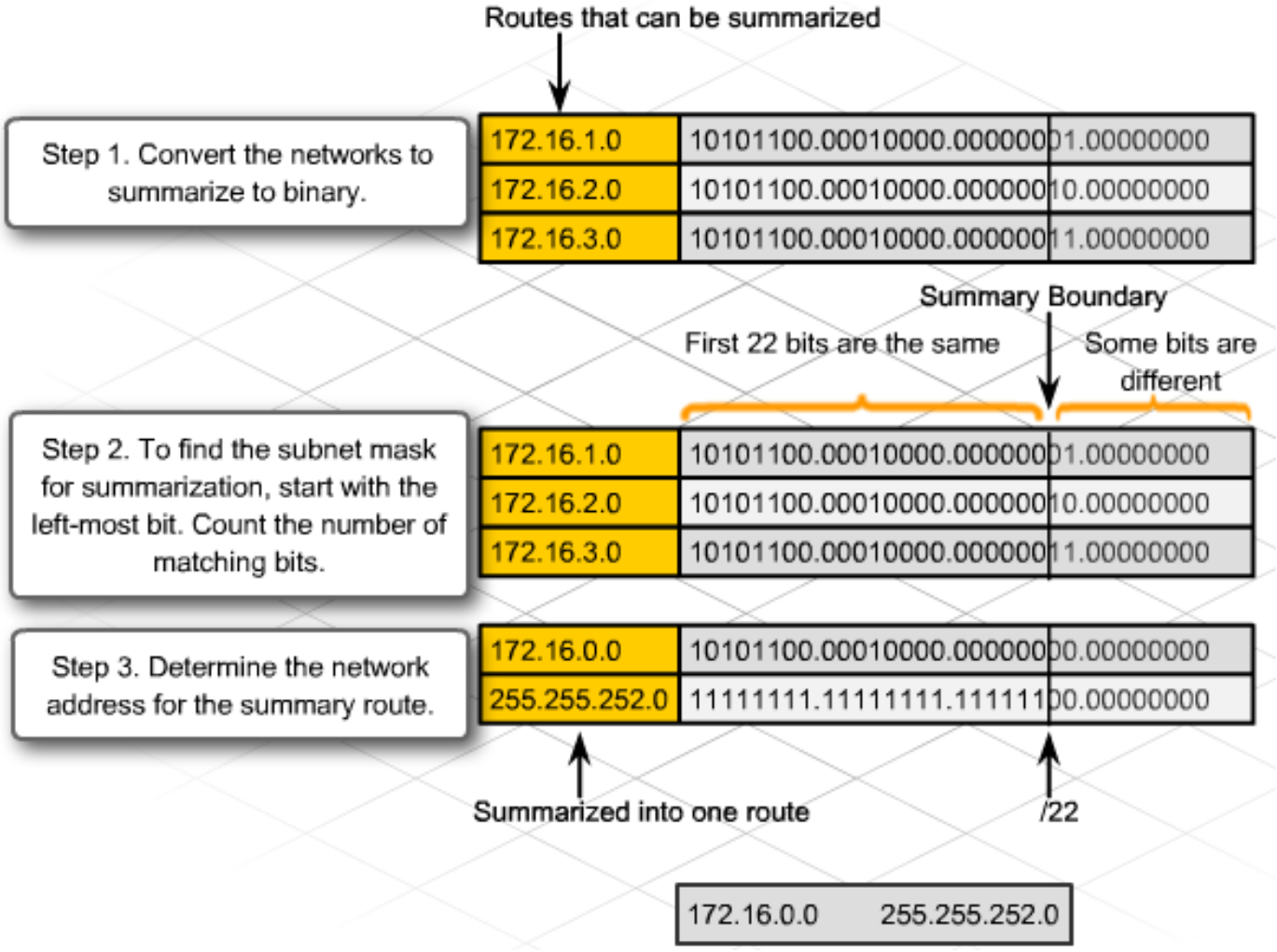


# Plan for Summarization and route Distribution

- When auto summarization is disabled, manual summarization must be configured.
- The network designer determines a summary route by following these steps:
- Step 1: Convert the addresses of the networks into binary format.
- Step 2: Find the subnet mask to be used for the summary route.
- Step 3: Determine the network address of the summary route.
- When using summary routes, the designer must be sure that the routes do not overlap with other summary or individual routes.
- When the route is determined, the designer manually configures this information on the router.

# Plan for Summarization and route Distribution



# Designing the Addressing Scheme

- IP Address Blocks
- Based on the information contained in the IP Network Requirements charts, the network designer determines the size of the IP address blocks that are needed for each area of the network. The designer groups areas that have similar requirements, to reduce the number of different subnet masks that must be supported.

# Designing the Addressing Scheme

- If all the devices needed registered public IP addresses, grouping would be wasteful. However, when using private IP addresses, grouping areas is a good practice. By reducing the number of subnet combinations, the designer simplifies the configurations. This makes it easier for the existing stadium network staff to support and troubleshoot. The designer decides to support 4 subnet masks: /19, /22, /24, and /30.

# Designing the Addressing Scheme

- Assigning Address Blocks
- The designer follows a step-by-step process to allocate the subnets, beginning with the largest block and working to the smallest.
- The network designer reserves the subnet 0 and the subnet containing the all-1s address for special consideration. In certain more complex network situations, these subnets may require unique configuration. Although the stadium network does not currently have any condition that might cause these networks to be unstable, the designer cannot predict what situations might arise.

# Designing the Addressing Scheme

| Stadium Network | Distribution Blocks | Wiring Closet Blocks | Individual VLANs | Point-to-Point Links |
|---|---|---|---|---|
| 172.18.0.0/16 | 172.18.0.0/19 | 172.18.0.0/22 | 172.18.0.0/24 | 172.18.0.0/30 |
| | | | | 172.18.0.4/30 |
| | | | | 172.18.0.8/30 |
| | | | | thru |
| | | | | 172.18.0.252/30 |
| | | | 172.18.1.0/24 | |
| | | | 172.18.2.0/24 | |
| | | | 172.18.3.0/24 | |
| | | | | |
| | | 172.18.4.0/24 | | |
| | | | 172.18.5.0/24 | |
| | | | 172.18.6.0/24 | |
| | | | 172.18.7.0/24 | |

# Designing the Addressing Scheme

- Using Subnet 0 and the All-1s Subnet
- Even though it is not a recommended practice, the use of subnet 0 and the all-1s subnet is explicitly allowed since Cisco IOS Software Release 12.0. In previous releases, subnet 0 could be used by entering the ip subnet-zero global configuration command.

# Designing the Addressing Scheme

- The RFC 1878 states that the practice of excluding all-0s and all-1s subnets is obsolete. Modern software is capable of using all definable networks.
- Today, the use of subnet 0 and the all-1s subnet is generally accepted and most vendors support their use. However, on certain networks, particularly networks using legacy software, the use of subnet 0 and the all-1s subnet can still lead to problems.

# Designing the Addressing Scheme

| Subnet Mask | Effective Subnets | Maximum Hosts | Subnet Mask Bits |
|---|---|---|---|
| | | | |
| 255.255.128.0 | 2 | 32766 | /17 |
| 255.255.192.0 | 4 | 16382 | /18 |
| 255.255.224.0 | 8 | 8190 | /19 |
| 255.255.240.0 | 16 | 4094 | /20 |
| 255.255.248.0 | 32 | 2046 | /21 |
| 255.255.252.0 | 64 | 1022 | /22 |
| 255.255.254.0 | 128 | 510 | /23 |
| 255.255.255.0 | 256 | 254 | 24 |
| 255.255.255.128 | 512 | 126 | /25 |
| 255.255.255.192 | 1024 | 62 | /26 |
| 255.255.255.224 | 2048 | 30 | /27 |
| 255.255.255.240 | 4096 | 14 | /28 |
| 255.255.255.248 | 8192 | 6 | /29 |
| 255.255.255.252 | 16384 | 2 | /30 |

# Designing the Naming Scheme

- A good network naming scheme makes the network easier to manage and easier for users to navigate.
- There are two primary types of network names to assign:
- Internal Device Names - These names can only be seen by administrators. Router and switch names are examples of internal devices.
- External Names - These names can be viewed by users on the network. The Windows device name that can be viewed in network neighborhood is an example. DNS names are also external names.

# Contrasting IPv4 and IPv6 Addressing

- Naming Guidelines
- Common sense often dictates a naming scheme. A good naming scheme follows these guidelines:
- Keep the names as short as possible; fewer than twelve characters is recommended.
- Indicate the device type, purpose, and location with codes, rather than words or abbreviations.
- Maintain a consistent scheme. This makes it easier to sort and report on the devices, and to set up management systems.
- Document the names in the IT department files and on the network maps.
- Avoid names that make it easy to find protected resources.

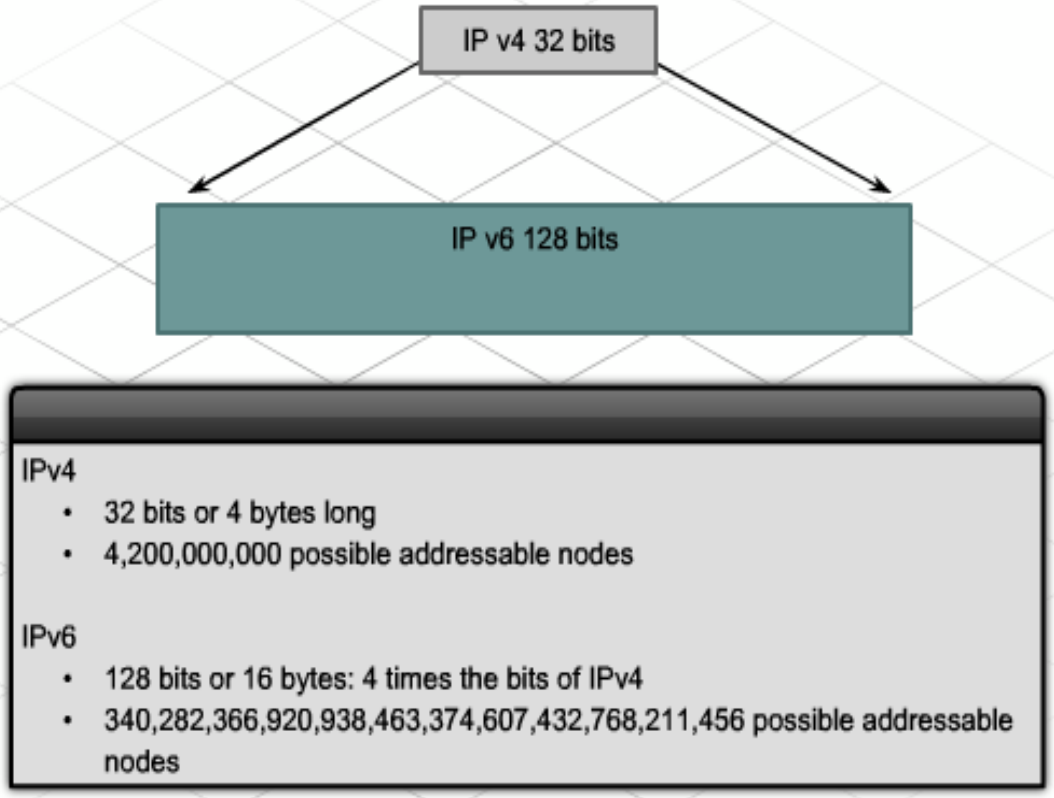
# Contrasting IPv4 and IPv6 Addressing

- The IPv4 address space provides approximately 4.3 billion addresses. Of that address space, approximately 3.7 billion addresses are actually assignable. The other addresses are reserved for special purposes such as multicast, private address space, loopback testing, and research. There are few IPv4 address ranges available for assignment. Some ISPs are beginning to pass out IPv6 address assignments.

# Contrasting IPv4 and IPv6 Addressing

An IPv6 address is a 128-bit binary value, which can be displayed as 32 hexadecimal digits. It provides 3.4 X 10^38 IP addresses. IPv6 offers powerful enhancements to IPv4. The enhancements include:

- Mobility and security
- Simpler header
- Address formatting



# Contrasting IPv4 and IPv6 Addressing

- Mobility and Security
- Mobility enables people with mobile network devices to move around in networks. Mobile IP is an IETF standard that is available for both IPv4 and IPv6. This standard enables mobile devices to move without breaks in established network connections. IPv4 does not support this kind of mobility. Mobility is an IPv6 feature.

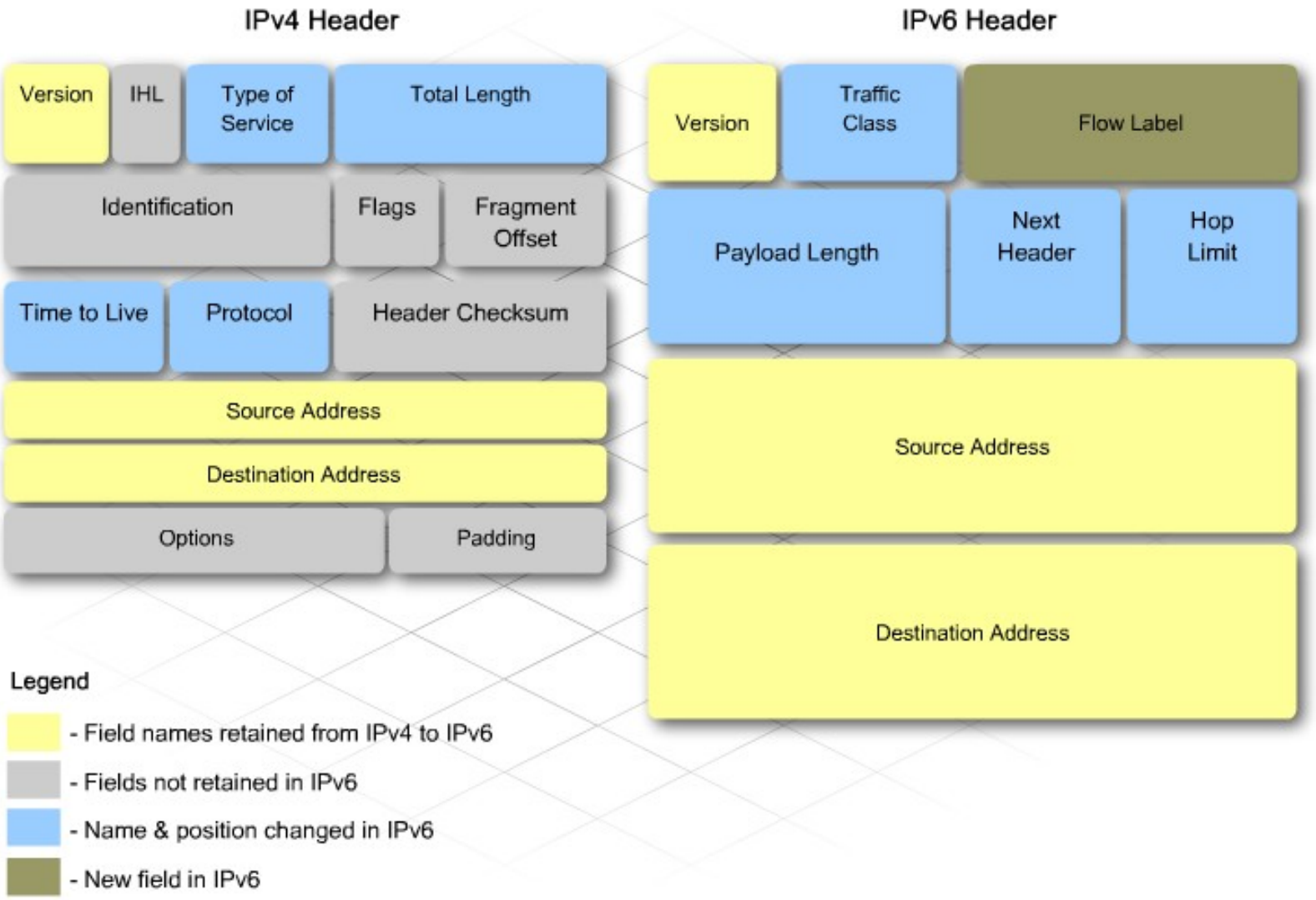
# Contrasting IPv4 and IPv6 Addressing

- IPSec is the IETF standard for IP network security. It is available for both IPv4 and IPv6. The IP network security functions are essentially identical in both environments. IPSec is more tightly integrated in IPv6 and can be enabled on every IPv6 node.

# Contrasting IPv4 and IPv6 Addressing

- Simpler Header
- The header used for IPv6 increases routing efficiency by reducing the number of entries in the routing tables.
- No broadcasts are associated with IPv6. With IPv4, the broadcasts created generate a high level of traffic within the network. This traffic creates an event known as a broadcast storm and the entire network ceases to function. IPv6 replaces broadcasts with multicasts and anycasts.

# Contrasting IPv4 and IPv6 Addressing



# Contrasting IPv4 and IPv6 Addressing

- Address Formatting
- Colons separate entries in a series of eight 16-bit hexadecimal fields that represent IPv6 addresses. The hexadecimal digits A, B, C, D, E, and F represented in IPv6 addresses are not case-sensitive.
- Unlike IPv4, the IPv6 address string format is not fixed.

# Contrasting IPv4 and IPv6 Addressing

- The following guidelines are used for IPv6 address string notations:
- The leading 0s in a field are optional: 09C0 equals 9C0 and 0000 equals 0.
- One or more groups of 0s can be omitted and replaced with "::". Only one "::" is allowed in an address.
- An unspecified address is written as "::" because it contains only 0s.

# Contrasting IPv4 and IPv6 Addressing

- Using the "::" notation greatly reduces the size of most addresses. For example, FF01:0:0:0:0:0:0:1 becomes FF01::1. This formatting is in contrast to the 32-bit dotted decimal notation of IPv4. The primary type of IPv6 address is called unicast.

**IPv6 Address Representation**

Format:
- X:X:X:X:X:X:X:X,Where X is a 16-bit hexadecimal field
  - Case-insensitive for hexadecimal A, B, C, D, E and F
- Leading zeros in a field are optional
- Successive fields of zeros can be represented as :: only once per address

Examples:
- 2031:0000:130F:0000:0000:09C0:876A:130B
  - Can be represented as 2031:0:130f::9c0:876a:130b
  - Cannot be represented as 2031::130f::9c0:876a:130b
- FF01:0:0:0:0:0:0:1 → FF01::1
- 0:0:0:0:0:0:0:1 → ::1
- 0:0:0:0:0:0:0:0 → ::

# Contrasting IPv4 and IPv6 Addressing

- Unicast sends packets to one specific device with one specific address. Multicast sends a packet to every member of a group. Anycast addresses send a packet to any one member of the group of devices that has an anycast address assigned. For efficiency, a packet that is sent to an anycast address is delivered to the closest interface. For that reason, anycast can also be thought of as a one-to-nearest type of address.

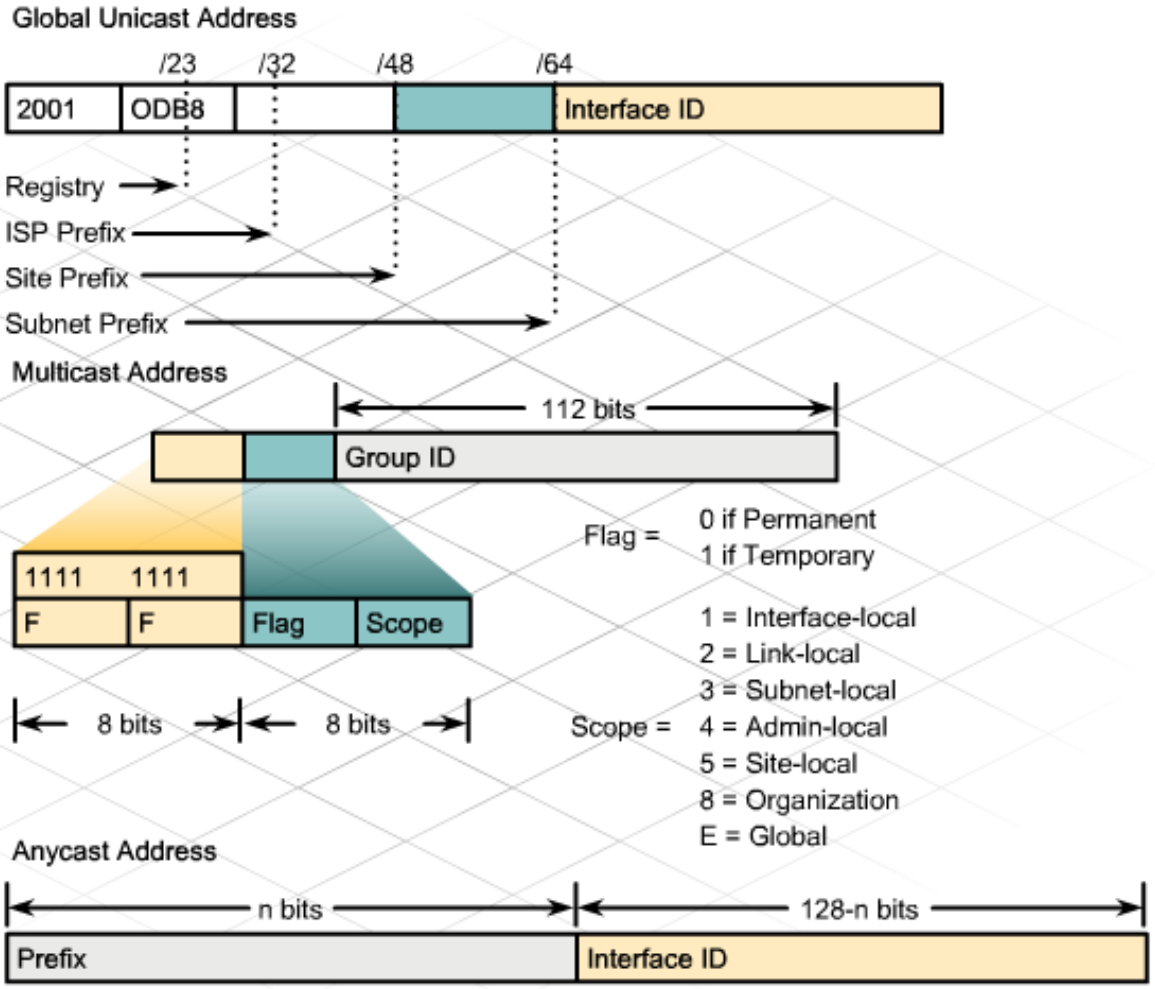
# Contrasting IPv4 and IPv6 Addressing

- The basic types of IPv6 unicast addresses are:
- Global
- Reserved (private, loopback, unspecified)
- Global Unicast Addresses
- The IPv6 host is the equivalent of a registered IPv4 host address. Registered IPv6 host addresses are referred to as global unicast addresses. The global unicast address block is structured to enable the aggregation of routing prefixes. This aggregation reduces the number of entries in the routing table.

# Contrasting IPv4 and IPv6 Addressing

- Reserved Addresses
- The IETF reserves a portion of the IPv6 address space for various uses. In contrast to IPv4, IPv6 supports significantly more reserved addresses. The IPv6 reserves 1/256th of the total IPv6 address space. Some of the other types of IPv6 addresses come from this block, such as private and loopback addresses.
- Like IPv4, a block of IPv6 addresses is set aside for private addresses. Private addresses have a first octet value of FE in hexadecimal notation. The next hexadecimal digit is a value from 8 to F.

# Contrasting IPv4 and IPv6 Addressing




An IPv6 anycast address is a global unicast address that is assigned to more than one interface.

# Migrating from IPv4 to IPv6

- Transition Richness
- There are several ways to integrate an IPv6 structure into an existing IPv4 network. The transition from IPv4 to IPv6 does not have to be done all at once. The three most common transition methods are:
- Dual stack
- Tunneling
- Proxying and translation

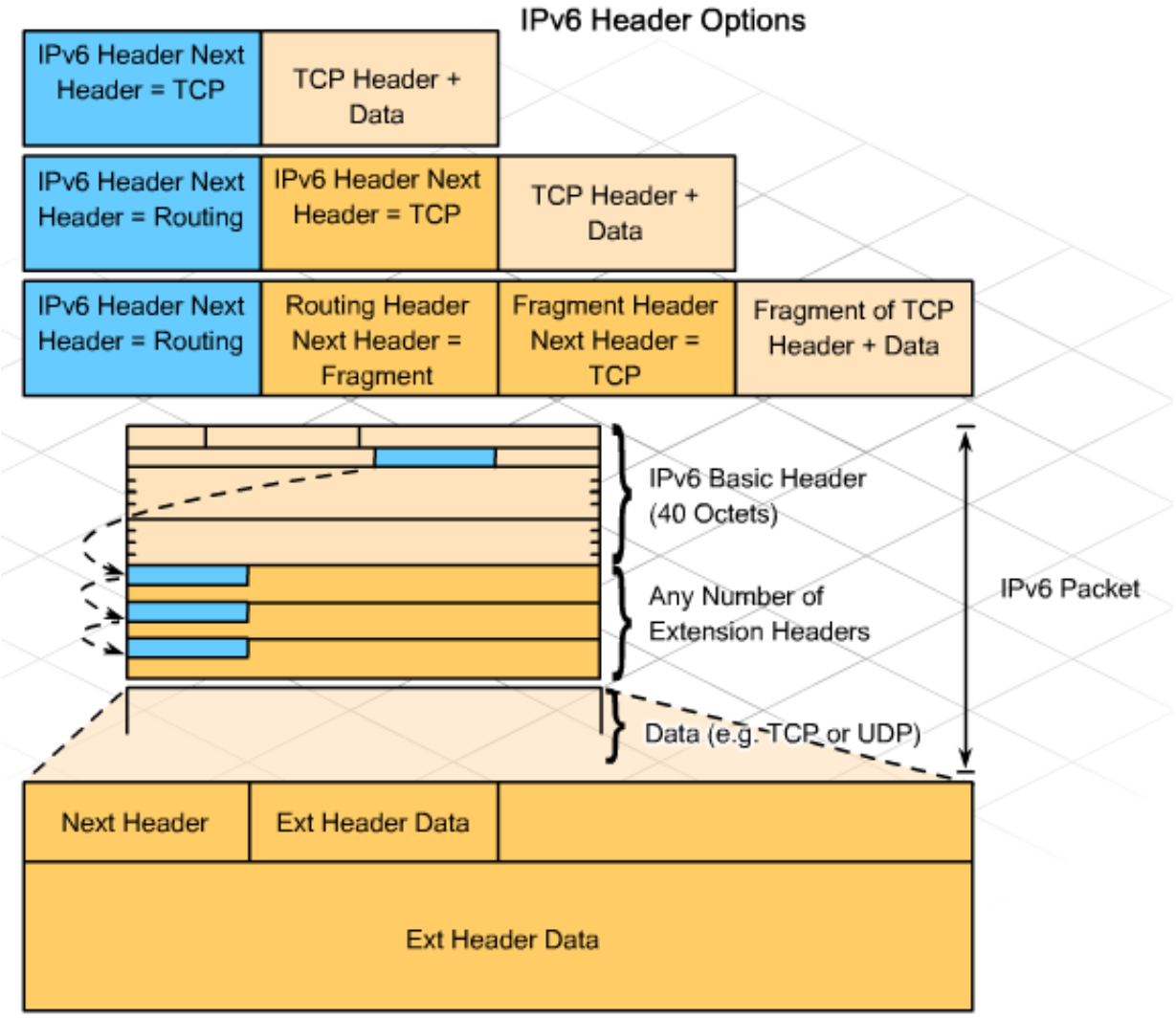
# Migrating from IPv4 to IPv6

- In the dual stack transition method, both IPv4 and IPv6 configurations are implemented on a network device. Both protocol stacks run on the same device. This method enables IPv4 and IPv6 to coexist.
- Tunneling is a technique that is becoming more prominent as the adoption of IPv6 grows. Tunneling is the encapsulation of one protocol packet within another protocol. For example, an IPv6 packet can be encapsulated within an IPv4 protocol. There are a variety of IPv6 over IPv4 tunneling methods. Some methods require manual configuration and others are more automatic.

# Migrating from IPv4 to IPv6

- Cisco IOS Releases 12.3(2)T and later, include Network Address Translation-Protocol Translation (NAT-PT) between IPv6 and IPv4. This translation allows direct communication between hosts that use different versions of the IP protocol.
- A total global migration from IPv4 to IPv6 may not happen in the near future. However, it has already been integrated in parts of the world that have nearly depleted their IPv4 addresses.

# Migrating from IPv4 to IPv6



# Implementing IPv6 on a Cisco Device

- By default, IPv6 traffic forwarding is disabled on a Cisco router. To activate IPv6 on a router, follow these two basic steps:
- Step 1: Activate IPv6 traffic forwarding with the global configuration command ipv6 unicast-routing.
- Step 2: Configure interfaces to support IPv6.

# Implementing IPv6 on a Cisco Device

- Interface identifiers in IPv6 addresses are used to identify interfaces on a link. They can be thought of as the host portion of an IPv6 address. Interface identifiers have to be unique, are always 64 bits, and can be dynamically derived from Layer 2 media and encapsulation.

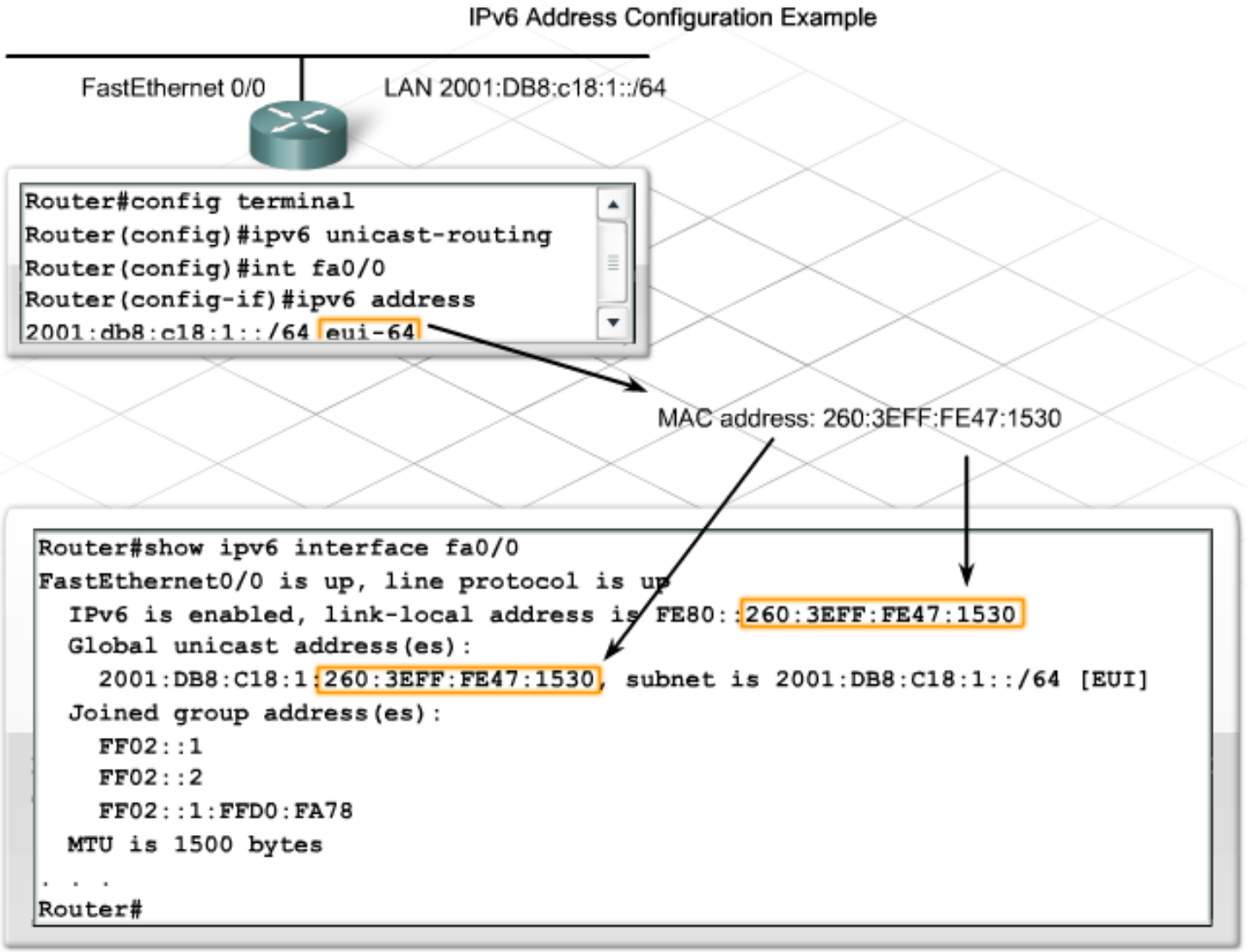
# Implementing IPv6 on a Cisco Device

- The IPv6 address command can configure a global IPv6 address. The entire 128-bit IPv6 address can be specified using the ipv6 address ipv6-address/prefix-length command:
- RouterX(config-if)# ipv6 address 2001:DB8:2222:7272::72/64

# Implementing IPv6 on a Cisco Device

- Another option is to configure the EUI-64 identifier for the network portion of the address. The host identifier is the host portion of the address in the EUI-64 format on an Ethernet network and is the MAC address of the device. The EUI-64 method uses the ipv6 address ipv6-prefix/prefix-length eui-64 command:
- RouterX(config-if)# ipv6 address 2001:DB8:c18:1::/64 eui-64

# Implementing IPv6 on a Cisco Device



# Implementing IPv6 on a Cisco Device

- If it is necessary to configure a router to locally resolve host names to IPv6 addresses, use the ipv6 hostname ipv6addr command.
- To specify an external DNS server to resolve IPv6 addresses, use the ip name-serveraddress command.
- Configuring name resolution on a router is done for the convenience of a technician who uses the router to access other devices on the network by name. It does not affect the operation of the router and does not advertise this DNS server name to DHCP clients.

# Implementing IPv6 on a Cisco Device

## Cisco IOS IPv6 Name Resolution Options

Define a static name for IPv6 addresses

```
Router#config terminal
Router(config)#ipv6 host router1 3ffe:b00:ffff:b::1
Router(config)#
```

Configure a DNS server or servers to query

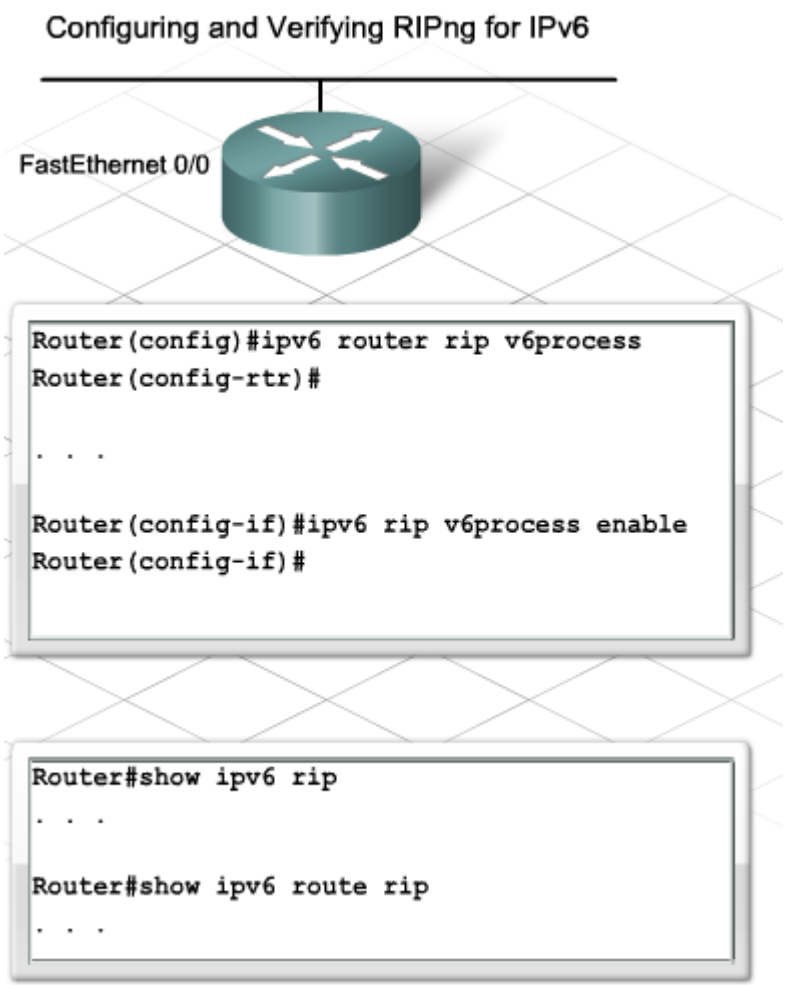
```
Router#config terminal
Router(config)#ipv6 name-server 3ffe:b00:ffff:1::10
Router(config)#
```

# Implementing IPv6 on a Cisco Device

- Configuring and Verifying RIPng for IPv6
- The syntax used to configure RIPng for IPv6 is similar to IPv4, but there are important differences. IPv4 uses the network command to identify which interfaces are included in the routing update. IPv6 uses the command ipv6 rip tag enable in interface configuration mode to enable RIPng on an interface.

# Implementing IPv6 on a Cisco Device

The tag parameter that is used for the ipv6 rip enable command must match the tag parameter in the ipv6 router rip command.
To verify the configuration of RIP use the show ipv6 rip command or show ipv6 route rip command.
Enabling RIP on an interface automatically creates a router rip process as needed.

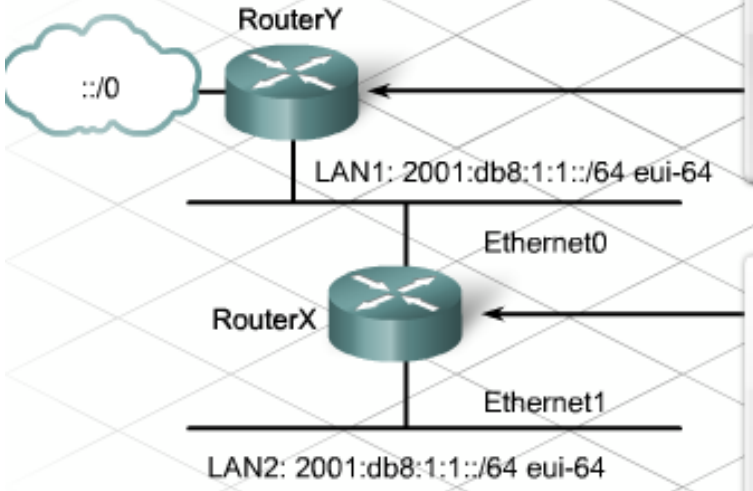


# Implementing IPv6 on a Cisco Device

- RIPng for IPv6 Configuration
- Configuring routers that are directly connected enables the use of the ipv6 rip name enable command.
- For example, if two routers are connected on a network, both routers use the tag RT0 to identify the RIPng process. RIPng is enabled on the Ethernet interface of the routers using the ipv6 rip RT0 enable command.

# Implementing IPv6 on a Cisco Device

## RIPng for IPv6 Configuration Example




```
RouterY RIPng configuration:
ipv6 unicast-routing
ipv6 router rip RT0

interface Ethernet0
 ipv6 address 2001:db8:1:1::/64 eui-64
 ipv6 rip RT0 enable
```

```
RouterX RIPng configuration:
ipv6 unicast-routing
ipv6 router rip RT0

interface Ethernet0
 ipv6 address 2001:db8:1:1::/64 eui-64
 ipv6 rip RT0 enable

interface Ethernet1
 ipv6 address 2001:db8:1:1::/64 eui-64
 ipv6 rip RT0 enable
```