The Notebook
of
CCNA

Huy Bui

$\mathcal{PL}$
THE PUBLISHER

Contents

List of Figures

List of Tables

Part I

NETWORK FUNDAMENTALS

Chapter 1

LAN Design

1.1 Hierarchical Design Model

A hierarchical LAN design includes the following three layers, as shown in Figure 1.1:

- **Access layer** provides endpoints and users direct access to the network
- **Distribution layer** aggregates access layers and provides connectivity to services.
- **Core layer** provides connectivity between distribution layers for large LAN environments.

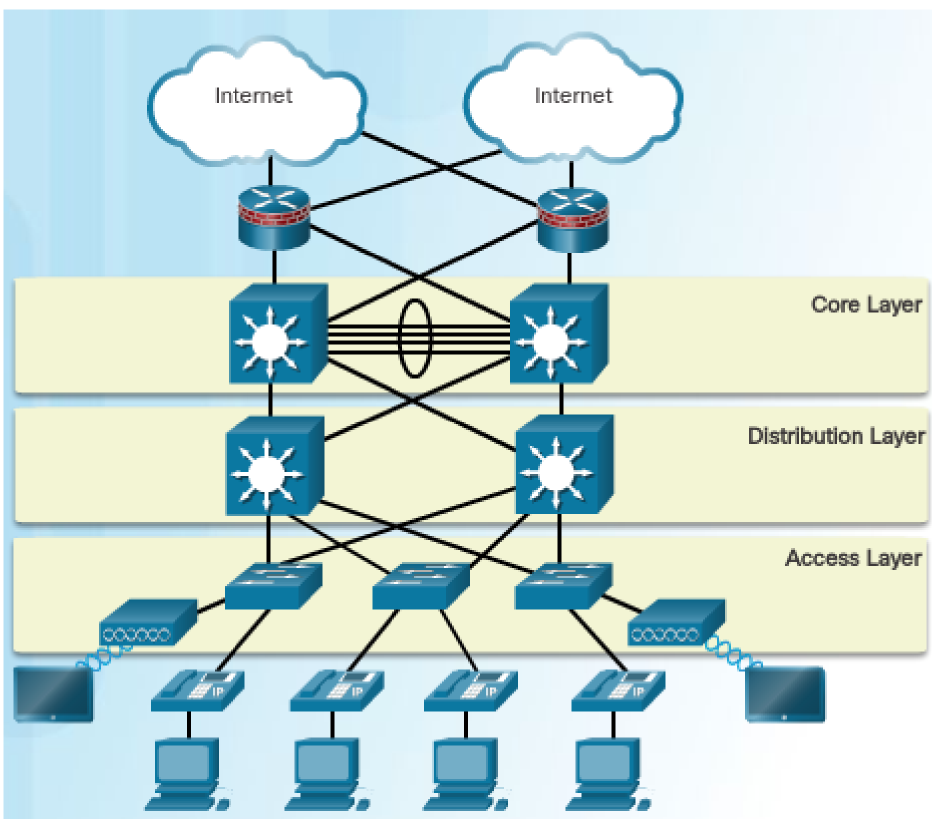


Figure 1.1: Three-layer hierarchical design model

Even though the hierarchical model has three layers, some smaller enterprise networks may implement a two-tier hierarchical design. In a two-tier hierarchical design, the core and distribution layers are collapsed into one layer, as shown in Figure 1.2.

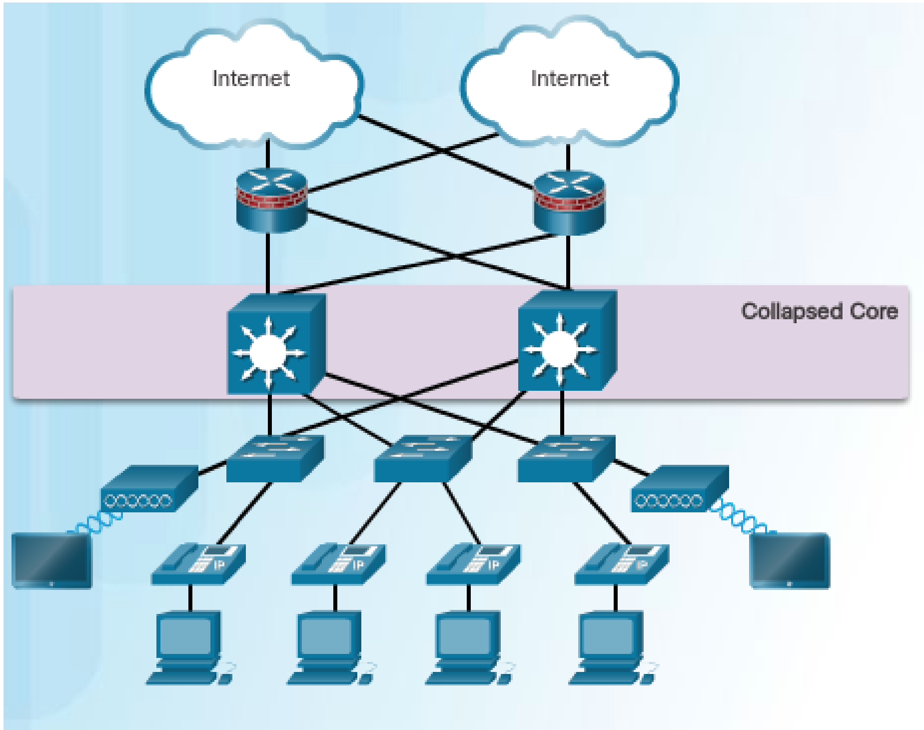


Figure 1.2: Collapsed Core

1.2 Expanding the network

The network designer must develop a strategy to enable the network to be available and to scale effectively and easily. Included in a basic network design strategy are the following recommendations:

- Use expandable, modular equipment or clustered devices that can be easily upgraded.
- Design a hierarchical network to include modules that can be upgraded without affecting the design of the other functional areas of the network.
- Create an IPv4 or IPv6 address strategy that is hierarchical.
- Choose routers or multilayer switches to limit broadcasts and filter other undesirable traffic from the network.

More advanced network design requirements will be described in the following sections.

1.2.1 Planning for redundancy

One method of implementing redundancy is by installing duplicate equipment and providing failover services for critical devices. Another method of implementing redundancy is redundant paths.

1.2.2 Failure domain

A failure domain is the area of a network that is impacted when a critical device or network service experiences problems. The use of redundant links and reliable enterprise-class equipment minimize the chance of disruption in a network. Smaller failure domains reduce the impact of a failure on company productivity.
In the hierarchical design model, it is easiest and usually least expensive to control the size of a failure domain in the distribution layer. In the distribution layer, network errors can be contained to a smaller area; thus, affecting fewer users.
Routers, or multilayer switches, are usually deployed in pairs, with access layer switches evenly divided between them. This configuration is referred to as a building, or departmental, switch block. Each switch block acts independently of the others. As a result, the failure does not affect a significant number of end users.

1.2.3 Increasing Bandwidth

Link aggregation allows an administrator to increase the amount of bandwidth between devices by creating one logical link made up of several physical links. EtherChannel is a form of link aggregation used in switched networks. The EtherChannel is seen as one logical link using an EtherChannel interface. Most configuration tasks are done on the EtherChannel interface, instead of on each individual port, ensuring configuration consistency throughout the links.

1.2.4 Expanding the Access Layer

To communicate wirelessly, end devices require a wireless NIC that incorporates a radio transmitter/receiver and the required software driver to make it operational. Additionally, a wireless router or a wireless access point (AP) is required for users to connect.

1.2.5 Fine-tuning Routing Protocols

Advanced routing protocols, such as OSPF and EIGRP are used in large networks. Link-state routing protocols such as Open Shortest Path First (OSPF) works well for larger hierarchical networks where fast convergence is important. Another popular routing protocol for larger networks is Enhanced Interior Gateway Routing Protocol (EIGRP). Cisco developed EIGRP as a proprietary distance vector routing protocol with enhanced capabilities.

1.3 Selecting network devices

1.3.1 Switch hardwares

There are five categories of switches for enterprise networks:

- **Campus LAN Switches** – To scale network performance in an enterprise LAN, there are core, distribution, access, and compact switches.
- **Cloud-Managed Switches** – The Cisco Meraki cloud-managed access switches enable virtual stacking of switches. They monitor and configure thousands of switch ports over the web, without the intervention of onsite IT staff.
- **Data Center Switches** – A data center should be built based on switches that promote infrastructure scalability, operational continuity, and transport flexibility. The data center switch platforms include the Cisco Nexus Series switches and the Cisco Catalyst 6500 Series switches.
- **Service Provider Switches** – Service provider switches fall under two categories: aggregation switches and Ethernet access switches. Aggregation switches are carrier-grade Ethernet switches that aggregate traffic at the edge of a network. Service provider Ethernet access switches feature application intelligence, unified services, virtualization, integrated security, and simplified management.
- **Virtual Networking** – Cisco Nexus virtual networking switch platforms provide secure multi-tenant services by adding virtualization intelligence technology to the data center network.

There are some terminologies that an administrator to be able to choose the right switch platform:

- **Port density** is the number of ports available on a single switch.
- **Forwarding rates** define the processing capabilities of a switch by rating how much data the switch can process per second.
- **Wire speed** is the data rate that each Ethernet port on the switch is capable of attaining. Data rates can be 100 Mb/s, 1 Gb/s, 10 Gb/s, or 100 Gb/s.
- **PoE** (Power over Ethernet) allows the switch to deliver power to a device over the existing Ethernet cabling. This feature can be used by IP phones and some wireless access points.
- **Multilayer switches**, so called Layer-3 switches, are typically deployed in the core and distribution layers of an organization's switched network

Router hardware

There are three categories of routers:

- **Branch Routers** – Branch routers optimize branch services on a single platform while delivering an optimal application experience across branch and WAN infrastructures.
- **Network Edge Routers** – Network edge routers enable the network edge to deliver high-performance, highly secure, and reliable services that unite campus, data center, and branch networks.
- **Service Provider Routers** – Service provider routers differentiate the service portfolio and increase revenues by delivering end-to-end scalable solutions and subscriber-aware services.

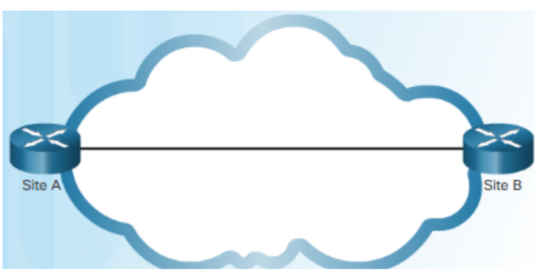
Chapter 2

WAN concepts

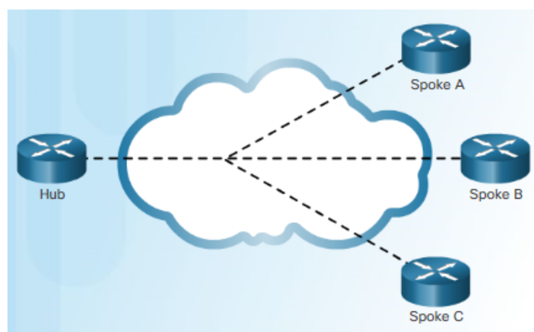
2.1 WAN Technologies overview

2.1.1 Topology

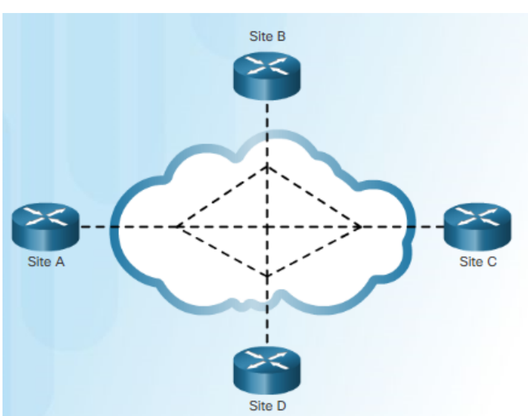
A WAN operates beyond the geographic scope of a LAN. WANs are used to interconnect the enterprise LAN to remote LANs in branch sites and telecommuter sites. A WAN is owned by a service provider whereas a LAN is typically owned by an organization. An organization must pay a fee to use the WAN service provider's network services to connect remote sites.



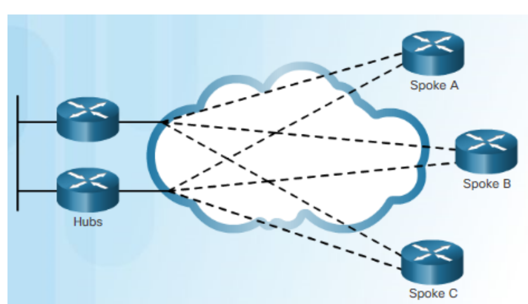
(a) Point-to-point



(b) Hub-and-Spoke



(c) Full Mesh



(d) Dual-homed

Figure 2.1: Four common WAN topologies

Point-to-Point topology employs a point-to-point circuit between two endpoints (Figure 2.1(a)). Typically involves a dedicated leased-line connection such as a T1/E1 line.

Hub-and-Spoke An example of a single-homed topology. Applicable when a private network connection between multiple sites is required. A single interface to the hub can be shared by all spoke circuits (Figure 2.1(b)).

Full Mesh A disadvantage of the hub-and-spoke topology is that all communication has to go through the hub. With a full mesh topology using virtual circuits, any site can communicate directly with any other site (Figure 2.1(c)). A disadvantage is the large number of virtual circuits that need to be configured and maintained.

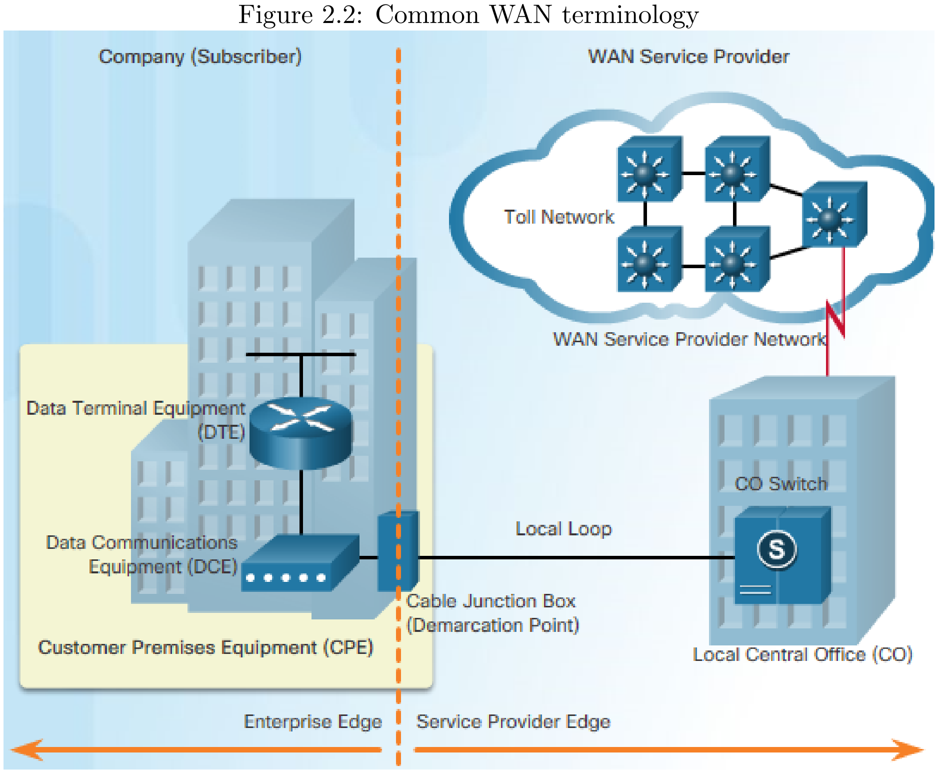
Dual-homed Topology Provides redundancy and load balancing, however more expensive to implement than single-homed topologies(Figure 2.1(d)). Requires additional networking hardware including routers and switches. More difficult to implement since they require complex configurations.

2.1.2 Terminology

WAN operations focus primarily on the Layer 1 and 2 of the OSI Model. One primary difference between a WAN and a LAN is that a company must subscribe to an outside WAN service provider to use WAN carrier network services.

Terminology commonly used to describe WAN connections (Figure 2.2):

Figure 2.2: Common WAN terminology



Customer Premises Equipment (CPE) Consists of devices and inside wiring located on the enterprise edge connecting to a carrier.

Data Communications Equipment (DCE) Also called circuit-terminating equipment, the DCE consists of devices that put data on the local loop. The DCE primarily provides an interface to connect subscribers to a communication link on the WAN cloud.

Data Terminal Equipment (DTE) The customer devices that pass the data from a customer network or host computer for transmission over the WAN. The DTE connects to the local loop through the DCE.

Demarcation Point This is a point established in a building to separate customer equipment from service provider equipment. The the place where the responsibility for the connection changes from the user to the service provider.

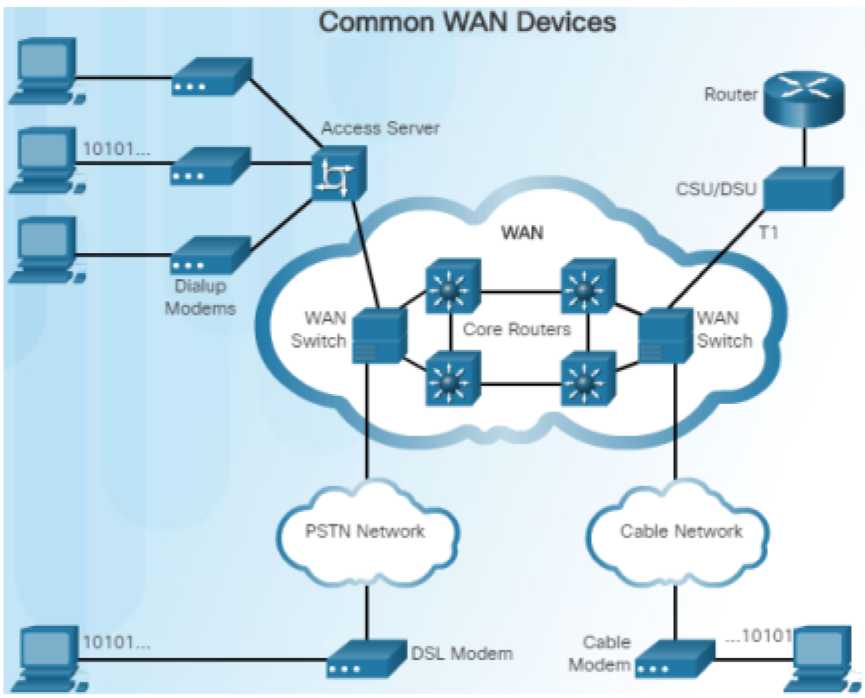
Local Loop (last mile) The actual copper or fiber cable that connects the CPE to the CO of the service provider.

Central Office (CO) The CO is the local service provider facility or building that connects the CPE to the provider network.

Toll network This consists of the longhaul, all-digital, fiber-optic communications lines and other equipment inside the WAN provider network.

There are many types of devices that are specific to WAN environments:

Figure 2.3: WAN devices



Dialup modem Legacy WAN technology that converts (modulates) the digital signals produced by a computer into voice frequencies which are transmitted over the analog lines of the public telephone network to another modem for demodulation.

Access server Legacy technology where the server controls and coordinates dialup modem, dial-in and dial-out user communications.

Broadband modem A type of digital modem used with high-speed DSL or cable Internet service. Both operate in a similar manner to the voiceband modem, but use higher broadband frequencies and transmission speeds

CSU/DSU Digital-leased lines require a CSU and a DSU. The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts line frames into frames that the LAN can interpret and vice versa.

WAN technologies are either circuit-switched or packet-switched:

Circuit Switching dynamically establishes a *dedicated virtual connection* for voice or data between a sender and a receiver. Communication can't start until the connection is established through the service provider network. The two most common types of circuit-switched WAN technologies are **PSTN** and **ISDN**.

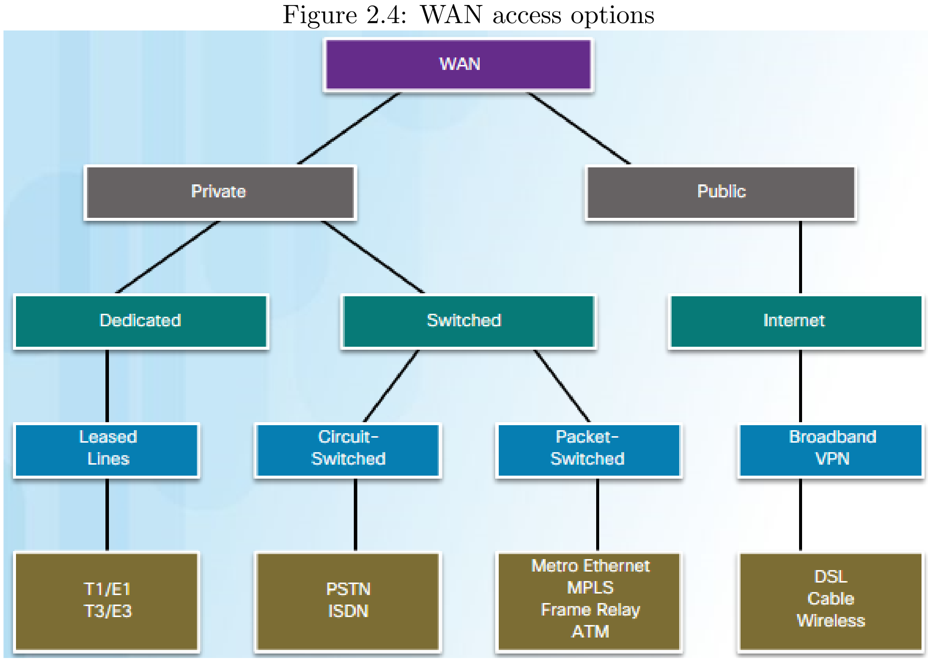
Packet Switching splits traffic data into packets packet that are routed over a shared network. A circuit does not need to be established and many pairs of nodes can communicate over the same channel. Packet switching costs less than circuit switching, however, latency and jitter are greater in packet-switching networks. There are two approaches to packet-switched network link determination:

- **Connectionless systems:** Full addressing information must be carried in each packet. The **Internet** is an example of a connectionless system.
- **Connection-oriented systems:** The network predetermines the route for a packet, and each packet only has to carry an identifier. An example of a connection-oriented system is **Frame Relay** (DLCIs are the identifiers).

2.2 WAN connection

There are several WAN access connection options (figure 2.4) that ISPs can use to connect the local loop to the enterprise edge.

Figure 2.4: WAN access options



Service provider networks are complex and consist mostly of high-bandwidth fiber-optic media, using SONET and SDH standard. A newer fiber-optic media development for long-range communications is called dense wavelength division multiplexing (DWDM).

2.2.1 Private WAN Infrastructures

Leased lines are permanent dedicated point-to-point connections from the customer premises to the provider network. The term leased line refers to the fact that the organization pays a monthly lease fee to a service provider to use the line. Leased lines are simple to implement and offer high quality and availability but are generally the most expensive type of WAN access and has Limited flexibility.

Dialup transport binary computer data through the voice telephone network using a modem. Dialup access is suitable when intermittent, low-volume data transfers are needed. The advantages of modem and analog lines are simplicity, availability, and low implementation cost. The disadvantages are the low data rates and a relatively long connection time.

ISDN is a circuit-switching technology that enables the local loop of a PSTN (Public switched telephone network) to carry digital signals. It can provide additional capacity as needed on a leased line connection or can also be used as a backup. ISDN has declined in popularity due to DSL and other broadband services. There are two types of ISDN Interfaces: BRI (2 B-channels, 1 D-channel), PRI (23 B-channel, 1 D-channel)

Frame Relay Frame Relay is a Layer 2 WAN technology used to interconnect enterprise LANs. A single router can be used to connect multiple sites using Private Virtual Circuits (PVCs) which can carry both voice and data traffic. Frame Relay creates PVCs which are uniquely identified by a data-link connection identifier (DLCI). The PVCs and DLCIs ensure bidirectional communication between one DTE device to another.

ATM is built on a cell-based architecture rather than on a frame-based architecture. ATM cells are always a fixed length of 53 bytes, containing a 5-byte ATM header followed by 48 bytes of ATM payload. Small, fixed-length cells are well-suited for carrying voice and video traffic because this traffic is intolerant of delay. However, when the cell is carrying segmented network layer packets, the overhead is higher because the ATM switch must be able to reassemble the packets at the destination.

Ethernet WAN Originally Ethernet was not suitable as a WAN access technology because the maximum cable length was one kilometer. However, fiber-optic cables have made Ethernet a reasonable WAN access option. There are several benefits to an Ethernet WAN: Reduced expenses and administration, Easy integration with existing networks, Enhanced business productivity. Ethernet WANs have replaced Frame Relay and ATM.

MPLS is a multiprotocol high-performance WAN technology that directs data from one router to the next. MPLS is based on short path labels rather than IP network addresses. It uses labels which tell a router what to do with a packet. The labels identify paths between distant routers rather than endpoints, and while MPLS actually routes IPv4 and IPv6 packets, everything else is switched. Furthermore, MPLS can deliver any type of packet between sites and encapsulate them of various network protocols.

VSAT is a solution that creates a private WAN using satellite communications in remote locations where there are no service providers that offer WAN service.

2.2.2 Public WAN Infrastructures

DSL is an always-on connection technology that uses existing twisted-pair telephone lines to transport high-bandwidth data. A DSL modem converts an Ethernet signal from the user device to a DSL signal. Key components in the DSL connection: DSL modem (subscriber end) and DSLAM (ISP end). The advantage that DSL has over cable technology is that DSL is not a shared medium – each user has a separate direct connection to the DSLAM.

Cable Coaxial cable is widely used in urban areas to distribute television signals. Network access is available from many cable television providers. This allows for greater bandwidth than the conventional telephone local loop. Two types of equipment are required: CMTS (ISP end), and Cable Modem (subscriber end).

WiMAX is a new technology that operates in a similar way to Wi-Fi, but at higher speeds, over greater distances, and for a greater number of users. It uses a network of WiMAX towers that are similar to cell phone towers.

Satellite Internet Typically used by rural users where cable and DSL are not available. Cable and DSL have higher download speeds, but satellite systems are about 10 times faster than an analog modem.

VPN is an encrypted connection between private networks over Internet. VPN uses virtual connections called VPN tunnels, which are routed through the Internet from the private network of the company to the remote site or employee host. There are several benefits to using VPN: cost savings, security, scalability, compatibility with broadband technology. There are two types of VPN access:

- **Site-to-site VPN:** connect entire networks to each other, for example, connecting a branch office network to a company headquarters network.
- **Remote-access VPN:** enable individual hosts, such as extranet consumers, to access a company network securely over the Internet.

Dynamic Multipoint VPN (DMVPN) is a Cisco software solution for building multiple VPNs. DMVPN is built on three protocols: NHRP, IPsec, and mGRE. NHRP is the distributed address mapping protocol for VPN tunnels. IPsec encrypts communications on VPN tunnels. The mGRE protocol allows the dynamic creation of multiple spoke tunnels from one permanent VPN hub.

Part II

SWITCHING TECHNOLOGIES

Chapter 3

VTP

3.1 Overviews

VLAN trunking protocol (VTP) allows a network administrator to manage VLANs on a switch configured as a VTP server. The VTP server distributes and synchronizes VLAN information over trunk links to VTP-enabled switches throughout the switched network. The following provides a brief description of important components of VTP:

VTP domain A VTP domain consists of all interconnected switches. All switches in a domain share VLAN configuration details. Switches resides in different domains do not exchange VTP messages. The boundary of a VTP domain is a router or a layer-3 switch.

Revision number The revision number is a 32-bit number that indicates the level of revision for a VTP advertisements. Each VTP device tracks the VTP configuration revision number that is assigned to it. Each time that you make a VLAN change in a VTP device, the configuration revision is incremented by one. Therefore, this number is used to determine whether the received information is more recent than the current version.

password Switches in the same domain are configured with the same password for security reason.

VTP modes A switch can be configured as a VTP server, client, or transparent.

VTP server stores the VLAN information in NVRAM (vlan.dat), then advertises it to other switches. VLAN configuration is allowed, and affects the entire VTP domain.

VTP client stores the VLAN information in RAM, therefore, a switch reset deletes all VLAN information. VLAN configuration is not allowed.

VTP transparent Switches in this mode do not participate in VTP except to forward VTP advertisements to VTP clients and VTP server. VLANs that are created, renamed, or deleted on transparent switches are local to that switch only.

Each switch in a VTP domain sends periodic VTP advertisements so that its neighbors can update VLAN configuration. VTP includes three types of advertisements:

- **Summary advertisements** – These inform adjacent switches of VTP domain name and configuration revision number. By default, Cisco switches issue summary advertisements every five minutes.
- **Advertisement request** – These are in response to a summary advertisement message when the summary advertisement contains a higher configuration revision number than the current value.
- **Subset advertisements** – These contain VLAN information including any changes.

3.2 Operations

When the switch receives a summary advertisement packet, the switch compares the VTP domain name to its own VTP domain name. If the name is different, the switch simply ignores the packet. If the name is the same, the

switch then compares the configuration revision to its own revision. If its own configuration revision number is higher or equal to the packet's configuration revision number, the packet is ignored. If its own configuration revision number is lower, an advertisement request is sent asking for the subset advertisement message.
The subset advertisement message contains the VLAN information with any changes. When you add, delete, or change a VLAN on the VTP server, the VTP server increments the configuration revision and issues a summary advertisement. One or several subset advertisements follow the summary advertisement containing the VLAN information including any changes. This process is shown in the figure 3.1.

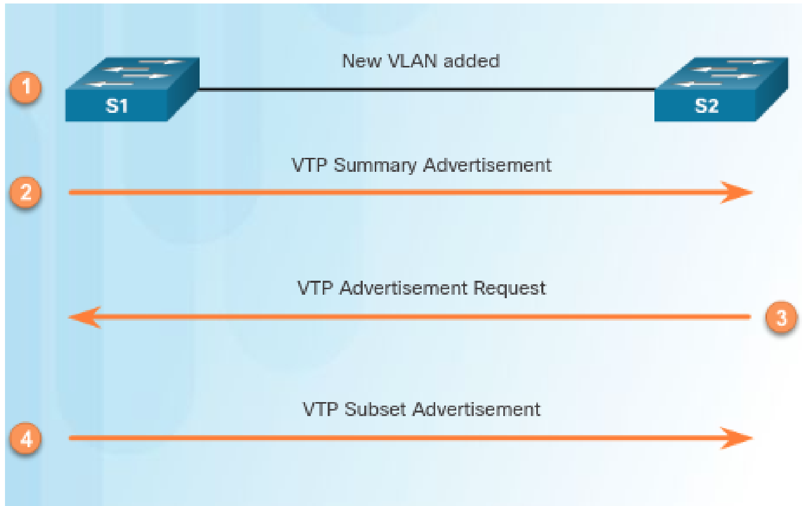


Figure 3.1: VTP operation

3.3 VTP Caveats

Adding a VTP-enabled switch to an existing VTP domain will wipe out the existing VLAN configurations in the domain if the new switch is configured with different VLANs and has a higher configuration revision number than the existing VTP server (see figure 3.2). Therefore, when a switch is added to a network, ensure that it has a default VTP configuration. The VTP configuration revision number is stored in NVRAM and is not reset if you erase switch configuration and reload it. To reset VTP configuration revision number to zero you have two options:

- Change the switch's VTP domain to a nonexistent VTP domain and then change the domain back to the original name.
- Change the switch's VTP mode to transparent and then back to previous VTP mode (Recommended).

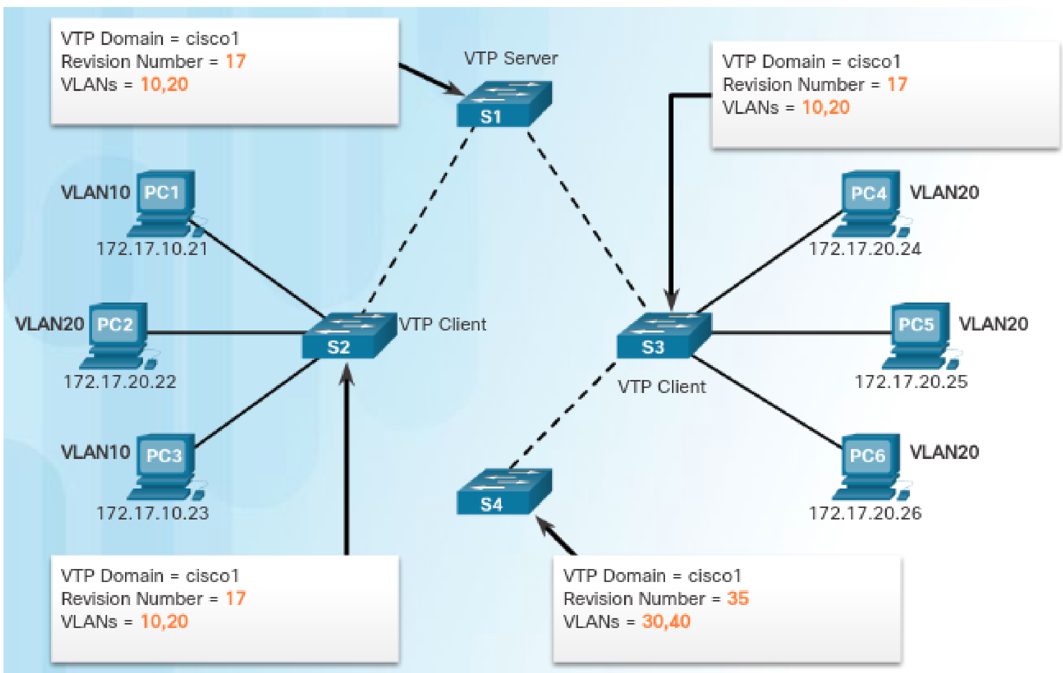


Figure 3.2: Incorrect VTP configuration revision number scenario

Chapter 4

Layer 3 Switching

Inter-VLAN routing using the router-on-a-stick method was simple to implement because routers were usually available in every network. However, most modern enterprise networks use multilayer switches to achieve high-packet processing rates using hardware-based switching. Layer 3 switches usually have packet-switching throughputs in the millions of packets per second (pps), whereas traditional routers provide packet switching in the range of 100,000 pps to more than 1 million pps.
Many users are in separate VLANs, and each VLAN is usually a separate subnet. Therefore, it is logical to configure the distribution switches as Layer 3 gateways for the users of each access switch VLAN. This implies that each distribution switch must have IP addresses matching each access switch VLAN. This can be achieved by using Switch Virtual Interfaces (SVIs) and routed ports.

- **Routed port** – A pure Layer 3 interface similar to a physical interface on a Cisco IOS router.
- **Switch virtual interface (SVI)** – A virtual VLAN interface for inter-VLAN routing. In other words, SVIs are the virtual-routed VLAN interfaces.

A routed port is a physical port that acts similarly to an interface on a router. Unlike an access port, a routed port is not associated with a particular VLAN. A routed port behaves like a regular router interface. Unlike Cisco IOS routers, routed ports on a Cisco IOS switch do not support subinterfaces. Routed ports are used for point-to-point links. In a switched network, routed ports are mostly configured between switches in the core and distribution layer.
An SVI is a virtual interface that is configured for each VLAN that exists on the switch. It is considered to be virtual because there is no physical port dedicated to the interface. It can perform the same functions for the VLAN as a router interface would, and can be configured in much the same way as a router interface (i.e., IP address, inbound/outbound ACLs, etc.).

Chapter 5

STP

5.1 Layer 2 loop

Multiple cabled paths between switches provide physical redundancy. However, when redundancy is introduced into a design, loops and duplicate frames occur. Loops and duplicate frames have severe consequences for network:

- Duplicate unicast frames
- MAC database instability
- Broadcast storm

MAC Database Instability Broadcast frames are forwarded out all switch ports, except the original ingress port. If there is more than one path to the destination, the frames may be forwarded back to the original switch, and create an endless loop. When a loop occurs, the MAC address table constantly changes with the updates from the broadcast frames, which results in MAC database instability. See this link for more explanation.

Duplicate unicast frame MAC Database Instability makes the switch overwhelming and confused. It does not know destination MAC address and must forward the frame out all ports. Consequently, unicast frames arrive at the destination device more than once.

Broadcast storm occurs when there are so many broadcast frames caught in a Layer 2 loop. Consequently, all available bandwidth is consumed. No bandwidth is available for legitimate traffic and the network becomes unavailable for data communication. This is an effective denial of service (DoS). Broadcast storm also cause the end device to malfunction because of the processing requirements needed to sustain such a high traffic load on the NIC.

5.2 STP overview

5.2.1 Operation

The Spanning Tree Protocol (STP) was developed to prevent loops and duplicate frames. STP ensures that there is only one logical path between all destinations on the network by blocking redundant paths that could cause a loop. If failure occurs, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active.

There is a root bridge elected for each spanning tree instance. It is possible to have multiple distinct root bridges for different sets of VLANs.

5.2.2 Types of STP

- **802.1D** – The first STP version, provide one spanning tree instance for the entire bridged network.
- **PVST+** – Cisco enhancement of STP, provide a separate spanning tree instance for each VLAN.
- **RSTP or 802.1w** – An evolution of STP.
- **Rapid PVST+** – Cisco enhancement of RSTP.
- **MSTP** – Multiple Spanning Tree Protocol, an IEEE standard, map multiple VLANs into the same spanning tree instance.
- **MST** – Cisco implementation of MSTP, provide up to 16 instances of RSTP.

5.3 Bridge ID

Bridge ID (BID) uniquely identifies a switch. The BID contains a bridge priority, the MAC address of the sending switch, and an extended system ID. The BID value is determined by the combination of these three fields.

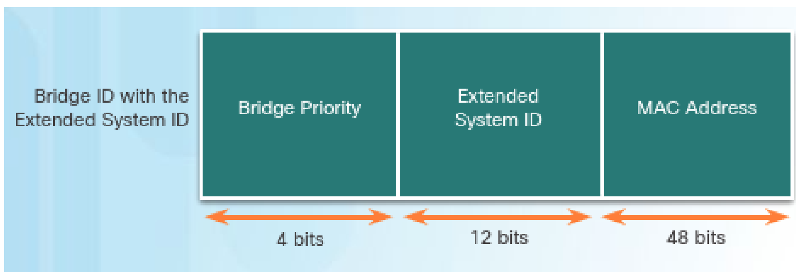


Figure 5.1: BID fields

The extended system ID reserves the rightmost 12 bits for the VLAN ID and the far left 4 bits for the bridge priority. Therefore, the bridge priority value can only be the multiples of 4096 ($2^{1}2$). If we consider BID as a hexadecimal number, the lowest left-most 4 bits (meaning lowest priority) always leads to lowest BID value.

To be more accurate, the root bridge election is based on the following criteria, in sequential order:

1. The switch with the lowest priority is the root bridge.
2. If the priorities are equal, then the switch with the lowest MAC address is elected the root bridge.

5.4 BPDU frame

A Bridge Protocol Data Units (BPDU) is a frame exchanged by switches for STP. BPDUs have a destination MAC address of **01:80:C2:00:00:00**, which is a multicast address for the spanning tree group. A BPDU frame contains 12 distinct fields:

- The first four fields identify the protocol, version, message type, and status flags.
- The next four fields are *root ID*, *bridge ID (BID)*, path cost.
- The last four fields are all timer fields. They determine how frequently BPDU messages are sent and how long the information received through the BPDU process is retained.

Root ID indicates the BID of the root bridge. When a switch first boots, the root ID is the same as the BID. However, as the election occurs, the lowest BID replaces the root ID to identify the root bridge.

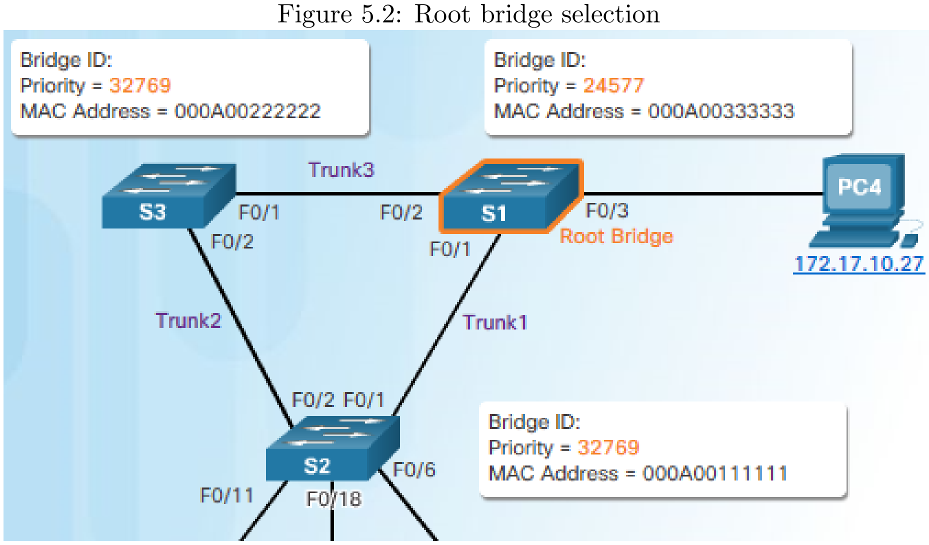
Path cost is the cost of the path from the sending switch to the root bridge. When a switch receives the BPDU, it adds the ingress port cost of the segment to determine its internal root path cost. The path cost is determined by summing up the individual port costs along the path from the switch to the root bridge. The default port costs are defined by the speed at which the port operates.

Port and speed	Cost
10 Gb/s Ethernet	2
1 Gb/s Ethernet	4
100 Mb/s Ethernet	19
10 Mb/s Ethernet	100

5.5 Root bridge election

All switches in the broadcast domain participate in the election process. After a switch boots, it begins to send out BPDU frames every two seconds. These BPDUs contain the switch BID and the root ID.

Figure 5.2: Root bridge selection



Assuming that switch A, B, C resides in the same broadcast domain (figure 5.2). As the switch A forward its BPDU frames, adjacent switch B reads the root ID information from the BPDU frames. If the root ID from the BPDU received is lower than the root ID on B, then the B updates its root ID, identifying the A as the root bridge. Switch B then forwards new BPDU frames with the lower root ID to switch C. The same process repeats, switch C compares its current root ID with the root ID identified in the frames, and then updates its current root ID if needed.

Eventually, the root ID of all switches equals the lowest BID. Therefore, all switches know exactly which one is the root bridge, based on the root ID. At this point, the election is terminated.

5.6 Port Roles

5.6.1 What is port role?

Spanning Tree Algorithm (STA) determines which switch ports on a network must be blocked to prevent loops. It designates a single switch as the root bridge and uses it as the reference point for all path calculations (see figure 5.3).

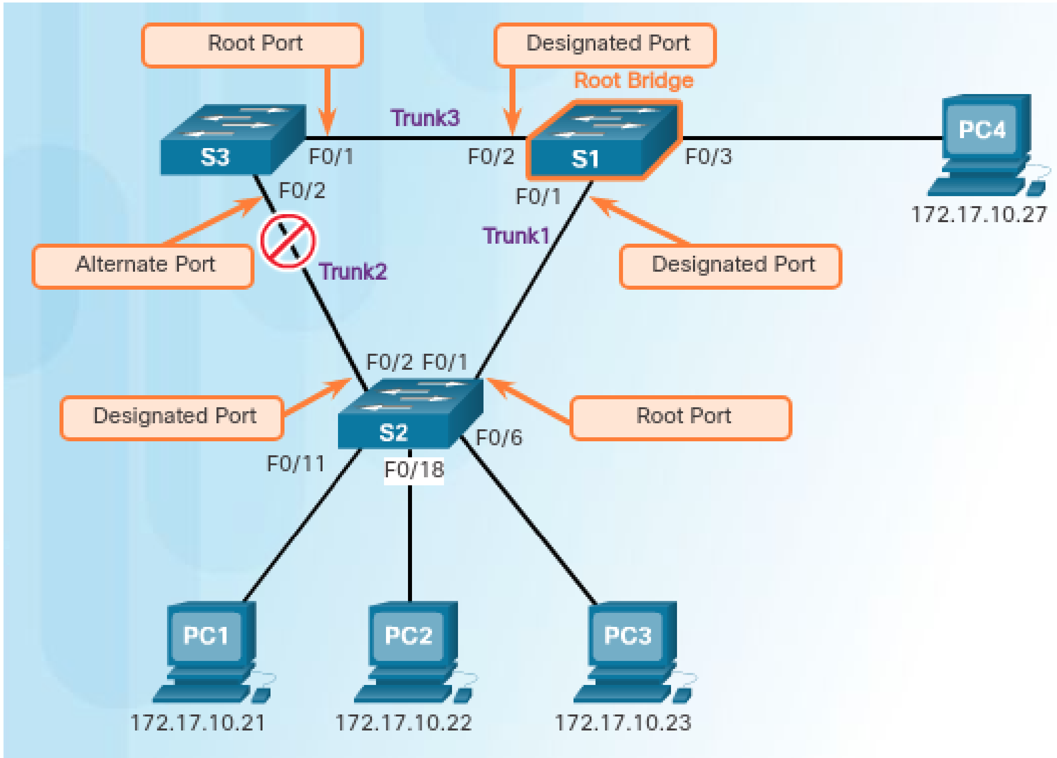


Figure 5.3: The STA designates a single switch as the root bridge

After the root bridge has been determined, STA assigns port roles to the switch ports:

- **Root port** – Switch ports closest to the root bridge in terms of overall cost to the root bridge.
- **Designated port** – All non-root ports that are still permitted to forward traffic on the network.
- **Alternate and backup ports** – Alternate ports and backup ports are blocked to prevent loops.

5.6.2 Port role rules

- There can only be one root port per non-root switch
- If one end of a segment (the link between two switches) is a root port, then the other end is a designated port.
- All ports on the root bridge are designated ports.
- Alternate ports are elected only on segments where neither end is a root port.

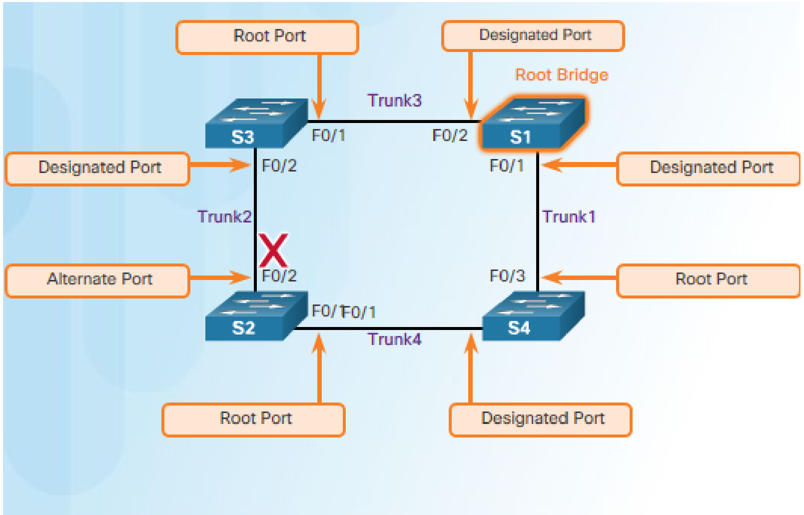
5.6.3 Port role decision

After the root bridge is elected, the STA determines port roles (figure 5.4) on the following steps in sequential order:

1. The root bridge automatically configures all of its switch ports in the designated role.
2. STP determines root port role. On each non-root switch, the port with lowest path cost to root bridge will become root port.
3. Non-root switches configure their non-root ports as designated or alternate ports.

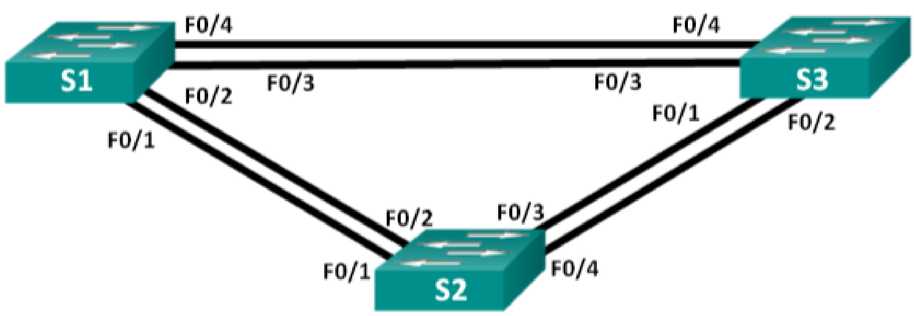
In the last step, two ports on the same segment will negotiate with each other. If one end of a segment is a root port, then the other end is a designated port. In figure 5.4, the segment between S1(F0/1) and S2(F0/1) is an example.

Figure 5.4: Port role assignment



However, when neither end of a segment cannot be a root port, the two switches on that segment exchange BPDU frames to decide which port to configure as a designated port. The switch with the lower path cost to the root bridge will have its port configured as a designated port. The other port will become an alternate port. If the path costs are equal, then the switch with the lower BID has its port configured as a designated port while the other has its port configured as an alternate port.

Figure 5.5: Redundant links



If there are more than two paths in a segment (figure 5.5), then the port with the lower number (e.g. port number of F0/3 is lower than F0/4) will become active, while the other will be blocked.

5.7 PVST+

5.7.1 Port state

To facilitate the learning of the logical spanning tree, each switch port transitions through five possible port states:

Blocking – The port is an alternate port and does not participate in frame forwarding. The port receives BPDU frames to determine the location and root ID of the root bridge switch and which port roles each switch port should assume in the final active STP topology.

Listening – The port is preparing to participate in frame forwarding. It listens for the path to the root. It also processes its own BPDU frames, and broadcast them to inform adjacent switches that the switch port is about to join the active topology.

Table 5.1: Five port states in PVST+

	Port states				
Operation allowed	**Blocking**	**Listening**	**Learning**	**Forwarding**	**Disabled**
Receive BPDUs	*	*	*	*	
Process BPDUs		*	*	*	
Learn MAC addresses			*	*	
Forward data frames				*	

Learning – The port learns the MAC addresses and populates the MAC address table.

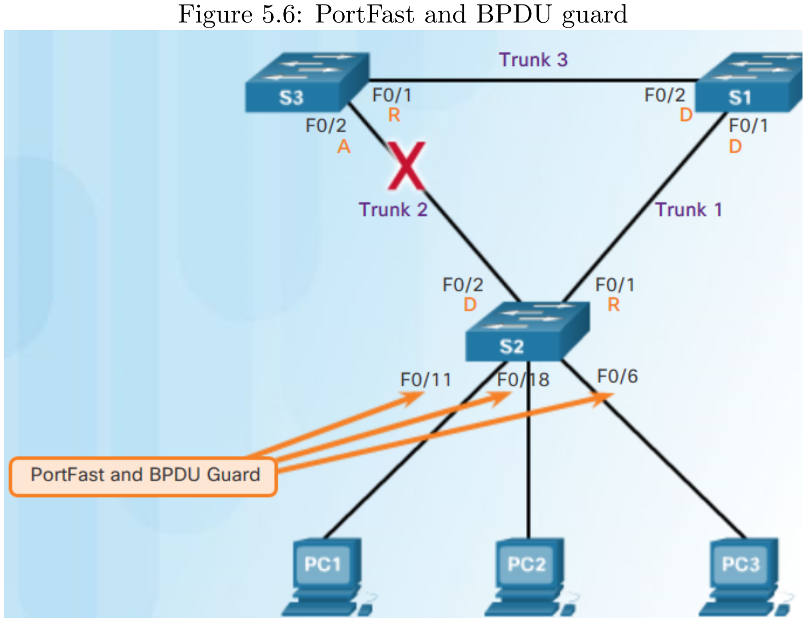
Forwarding – The port is considered part of the active topology. It forwards data frames and sends and receives BPDU frames.

Disabled – The Layer 2 port does not participate in spanning tree and does not forward frames. The disabled state is set when the switch port is administratively disabled.

5.7.2 PortFast and BPDU guard

When a switch port is configured with PortFast that port transitions from blocking to forwarding state immediately, bypassing the usual transition states (the listening and learning states). You can use PortFast on *access ports*[1] to help devices connect to the network immediately, rather than waiting for STP to converge on each VLAN.

Figure 5.6: PortFast and BPDU guard



Because a PortFast-configured port is not connected to a switch, BPDUs should never be received. Otherwise, the broadcast domain will "think" that the port is connected to a switch. This consumption potentially causes layer 2 loops. To address this issue, Cisco switches support a feature called BPDU guard. This will effectively shut down the port. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back into service.

[1] Access ports are ports which are connected to an end device such as a PC or a server.

Cisco PortFast technology is useful for DHCP. Because PortFast immediately changes the state to forwarding, the PC always gets a usable IP address from DHCP server.

5.8 RSTP and Rapid PVST+

Rapid PVST+ is Cisco enhancement of RSTP. In this section, only the common features of these two protocols are discussed.

5.8.1 BPDU

RSTP uses BPDU version 2, while 802.1D uses version 0. Protocol information can be immediately aged on a port if Hello packets are not received for three consecutive Hello times (six seconds, by default) or if the max age timer expires. BPDUs are used as a keepalive mechanism. Therefore, three consecutively missed BPDUs indicate lost connectivity between a bridge and its neighboring.

5.8.2 Port state

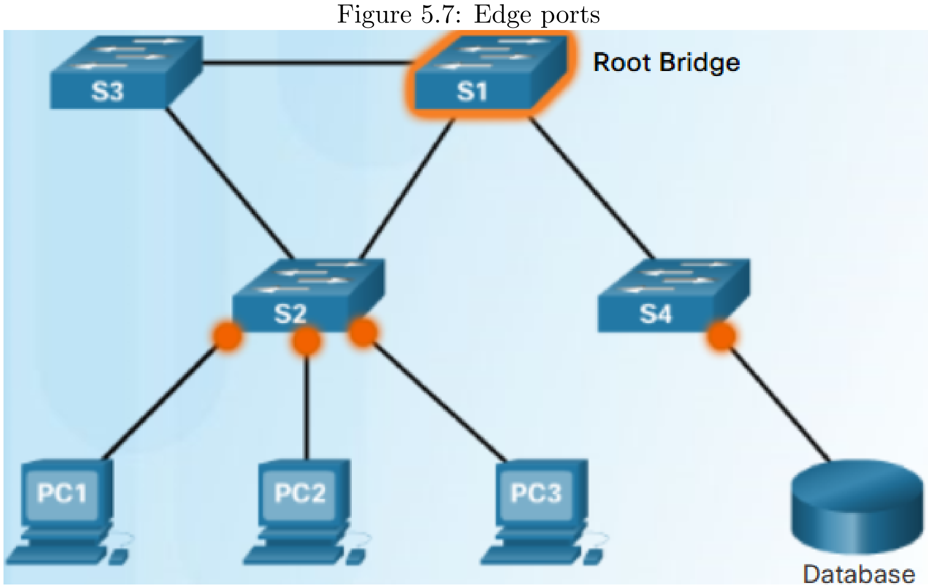
RSTP does not have a blocking port state. Port states are defined as *discarding*, *learning*, or *forwarding*. RSTP discarding state is equivalent to PVST+ blocking and disabled state. RSTP learning state is equivalent to PVST+ listening and learning state.

RSTP speeds the recalculation of the spanning tree when the Layer 2 network topology changes. If a port is configured to be an alternate port, it can immediately change to a forwarding state without waiting for the network to converge.

5.8.3 Edge port

RSTP introduces new types of port: edge port. An RSTP edge port is a switch port that is never intended to be connected to another switch. It immediately transitions to the forwarding state when enabled. An edge port is any port that does not have a switch connected to it.

Figure 5.7: Edge ports



5.9 Configuration

5.9.1 STP type

You can enable either PVST+ or Rapid PVST+ on a switch:

```
S1(config)# spanning-tree mode pvst
S1(config)# spanning-tree mode rapid-pvst
```

5.9.2 Priority

The default priority value of a switch is 32,768. When an administrator wants a specific switch to become a root bridge, the bridge priority value must be adjusted to ensure it is lower than the bridge priority values of all the other switches on the network. There are two different methods to configure the bridge priority value:

Method 1

To ensure that the switch has the lowest bridge priority value, use the following command.

```
S1(config)# spanning-tree vlan 10 root primary
```

This command dynamically makes priority of the switch to be the lowest in the broadcast domain. By default, the priority for the switch is 24,576. If an alternate root bridge is desired, use the following command.

```
S1(config)# spanning-tree vlan 10 root secondary
```

This command ensures that the alternate switch becomes the root bridge if the primary root bridge fails. This command, by default, sets the priority to 28,672.

Method 2

Another method for configuring the bridge priority value is using the following command

```
S1(config)# spanning-tree vlan 10 priority 24576
```

This command gives more granular control over the bridge priority value. Remember the priority value is configured in increments of 4,096 between 0 and 61,440. Cisco recommends caution when using this command.

5.9.3 PortFast and BPDU guard

To configure PortFast and BPDU guard on a switch port, enter the following command:

```
S1(config)# interface F0/1
S1(config-if)# spanning-tree portfast
S1(config-if)# spanning-tree bpduguard enable
```

To enable PortFast on all nontrunking interfaces, and enable BPDU guard on all PortFast-enabled ports, use the following command:

```
S1(config)# spanning-tree portfast default
S1(config)# spanning-tree portfast bpduguard default
```

To verify that PortFast and BPDU guard has been enabled for a switch port, use the show command, as shown in Figure 5.8. *Note!* PortFast and BPDU guard are disabled, by default, on all interfaces.

5.9.4 Verification

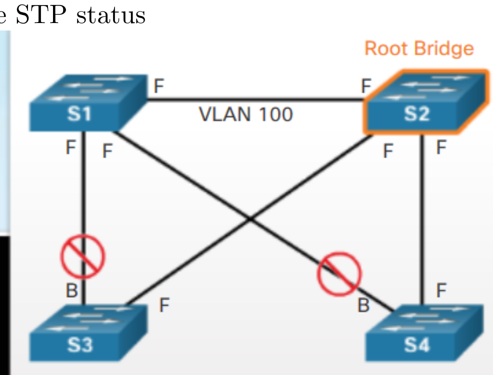
Using the `show spanning-tree` command without specifying any additional options provides a quick overview of the status of STP for all VLANs that are defined on a switch. Use the show `spanning-tree vlan <vlan_id>` command to get STP information for a particular VLAN (figure 5.8).

Figure 5.8: Verify PortFast and BPDU guard

```
S2# show running-config interface f0/11
Building configuration...

Current configuration : 90 bytes
!
interface FastEthernet0/11
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Figure 5.9: Analyze STP status




```
S1# show spanning-tree vlan 100

VLAN0100
 Spanning tree enabled protocol rstp
 Root ID    Priority    28772
            Address     0000.0c9f.3127
            Cost        2
            Port        88 (TenGigabit9/1)
            Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
 Bridge ID  Priority    28772 (priority 28672 sys-id-ext 100)
            Address     0000.0cab.3724
            Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
            Aging Time  300

Interface      Role Sts Cost      Prio.Nbr Type
---------      ------------       ----------------------------
Gi3/1          Desg FWD 4         128.72   P2p
Gi3/2          Desg FWD 4         128.80   P2p
Te9/1          Root FWD 2         128.88   P2p
```

Chapter 6

EtherChannel

6.1 Advantages

- Most configuration tasks can be done on the EtherChannel interface instead of each individual port, ensuring configuration consistency throughout the links.
- EtherChannel creates an aggregation that is seen as one logical link.
- EtherChannel provides redundancy.
- Load balancing takes place between links that are part of the same EtherChannel.
- EtherChannel relies on existing switch ports. There is no need to upgrade the link to a faster and more expensive connection to have more bandwidth.

6.2 Port Aggregation Protocol (PagP)

PAgP (pronounced "Pag – P") is a Cisco-proprietary protocol that aids in the creation of EtherChannel links. PAgP helps create the EtherChannel link by detecting the configuration of each side and ensuring that links are compatible so that the EtherChannel link can be enabled when needed. PAgP can be configured in one of three models:

- **On** – This mode forces the interface to channel without PAgP. Interfaces configured in the on mode do not exchange PAgP packets.
- **PAgP Active** – This PAgP mode places an interface in an active negotiating state in which the interface initiates negotiations with other interfaces by sending PAgP packets.
- **PAgP Passive** – This PAgP mode places an interface in a passive negotiating state in which the interface responds to the PAgP packets that it receives, but does not initiate PAgP negotiation.

The modes must be compatible on each side as shown in table 6.1.

Table 6.1: PAgP Establishment

S1	S2	EtherChannel establishment
Active	Passive/Active	Yes
On	On	Yes
Passive	Passive/On	No
Not configured	Passive/Active/On	No
Active	on	No

6.3 Link Aggregation Control Protocol (LACP)

LACP is part of an 802.3ad that aids in the creation of EtherChannel links. Because LACP is an IEEE standard, it can be used to facilitate EtherChannels in multivendor environments, including Cisco devices. LACP allows for eight active links, and also eight standby links. A standby link will become active should one of the current active links fail. PAgP can be configured in one of three models:

- **On** – This mode forces the interface to channel without LACP. Interfaces configured in the on mode do not exchange LACP packets.
- **LACP active** – Similar to PAgP Active mode.
- **LACP passive** – Similar to PAgP Passive mode. negotiation.

The modes must be compatible on each side as shown in table 6.1.

Table 6.2: LACP Establishment

S1	S2	EtherChannel establishment
Active	Passive/Active	Yes
On	On	Yes
Passive	Passive/On	No
Not configured	Passive/Active/On	No
Active	on	No

6.4 Configuration

6.4.1 Implementation restrictions

The EtherChannel provides full-duplex bandwidth between one switch and another switch or host. Currently each EtherChannel can consist of up to eight compatibly-configured Ethernet ports. However, interface types cannot be mixed. For example, Fast Ethernet and Gigabit Ethernet cannot be mixed within a single EtherChannel.

EtherChannel creates a one-to-one relationship; that is, one EtherChannel link connects only two devices. The individual EtherChannel group member port configuration must be consistent on both devices:

- **EtherChannel support:** All Ethernet interfaces on all modules must support EtherChannel with no requirement that interfaces be physically contiguous, or on the same module.
- **Speed and duplex:** Configure all interfaces in an EtherChannel to operate at the same speed and in the same duplex mode.
- **VLAN match:** All interfaces in the EtherChannel bundle must be assigned to the same VLAN. If the physical ports of one side are configured as trunks, the physical ports of the other side must also be configured as trunks within the same native VLAN.
- **Range of VLANs:** An EtherChannel supports the same allowed range of VLANs on all the interfaces in a trunking EtherChannel. If the allowed range of VLANs is not the same, the interfaces do not form an EtherChannel, even when set to auto or desirable mode.

6.4.2 Configuration

Step 1: Specify the interfaces that compose the EtherChannel group using the `interface range <interface>` global configuration mode command. A good practice is to start by shutting down those interfaces, so that any incomplete configuration does not create activity on the link. At the end of this step, make sure that none of restrictions above are broken.

Step 2: Create the port channel interface with a channel group number. The mode active keywords identify this as an LACP EtherChannel configuration.

```
S1(config)# interface range f0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# channel-group 1 mode active
S1(config-if-range)# no shutdown
```

Step 3: Change layer 2 settings on port channel interface, so that two sides of the EtherChannel link have the same configuration.

```
S1(config)# interface port-channel 1
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 1,10,20,99
```

Part III

ROUTING TECHNOLOGIES

Chapter 7

EIGRP

7.1 Basic features

Enhanced Interior Gateway Routing Protocol (EIGRP) is a powerful *distance vector* routing protocol and is relatively easy to configure for basic networks. Features of EIGRP:

- Use DUAL algorithm
- Use RTP instead of TCP or UDP
- Partial and Bounded Updates – Sends updates only when there is a change and only to the routers that need the information
- Supports Equal and Unequal cost load balancing
- Does not encrypt the routing updates
- **Authentication:** Only accepts routing information from other routers with the same authentication information

Protocol Dependent Modules (PDM) sends and receives EIGRP packets that are encapsulated in IPv4 or IPv6.

Reliable Transport Protocol (RTP) EIGRP was designed as a network layer independent routing protocol. Because of this design, EIGRP cannot use UDP or TCP, but use RTP instead. RTP includes both reliable and unreliable delivery of EIGRP packets, similar to TCP and UDP, respectively. RTP can send EIGRP packets as unicast or multicast. EIGRP multicast address is 224.0.0.10 for IPv4 and FF02::A for IPv6.

7.2 Packet types

7.2.1 Hello packets

EIGRP uses small Hello packets to discover other EIGRP-enabled routers on directly connected links. Hello packets are used by routers to form EIGRP neighbor adjacencies.

Hello packets are sent as multicast packets *every five seconds*. However, on slow network (e.g. multipoint, NBMA networks with access links of T1), Hello packets are sent as unicast packets every 60 seconds.

EIGRP uses a Hold timer to determine the maximum time the router should wait to receive the next Hello before declaring that neighbor as unreachable. By default, the Hold timer is *three times the Hello interval*. If the hold time expires, EIGRP declares the route as down and DUAL searches for a new path by sending out queries.

Hello intervals and hold times are configurable on a per-interface basis and *do not have to match* with other EIGRP routers to establish or maintain adjacencies. If the Hello interval is changed, ensure that the Hold time value is not less than the Hello interval. Otherwise, neighbor adjacency goes down after the Hold timer expires and before the next Hello interval.

7.2.2 Update packets

EIGRP sends Update packets to propagate routing information. Update packets are sent only when necessary. EIGRP updates contain only the routing information needed, and are sent only to those routers that require it.

EIGRP uses *partial update* and *bounded update*. A partial update means that the update only includes information about route changes. A bounded update refers to the sending of partial updates only to the routers that are affected by the changes. Bounded updates help EIGRP minimize the bandwidth that is required to send EIGRP updates.

7.2.3 Acknowledgment packets

EIGRP sends Acknowledgment (ACK) packets when RTP reliable delivery is used. An EIGRP acknowledgment is an EIGRP Hello packet without any data. RTP uses reliable delivery for Update, Query, and Reply packets.

7.2.4 Query and reply packets

DUAL uses Query and Reply packets when searching for networks and other tasks. Queries can use multicast or unicast, whereas replies are always sent as unicast.

7.3 Encapsulating EIGRP Messages

The EIGRP packet headers and TLV (Type, Length, Value) field are encapsulated in an IP packet.

7.3.1 IP packet header

In the IP packet header (figure 11.1), the protocol field is set to **88** to indicate EIGRP. The destination address is set to the multicast 224.0.0.10 for IPv4, and FF02::A for IPv6. If the EIGRP packet is encapsulated in an Ethernet frame, the destination MAC address is the multicast address 01-00-5E-00-00-0A.

7.3.2 EIGRP packet header

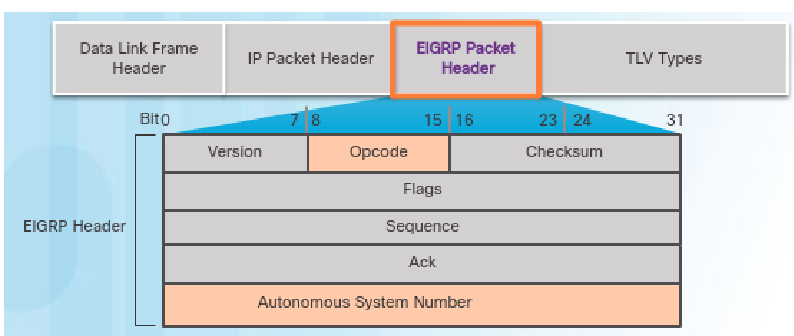


Figure 7.1: EIGRP packet header

Opcode field specifies EIGRP packet type. Specifically, it identifies the EIGRP messages as either Update (1), Query (3), Reply (4), and Hello (5).

Autonomous system (AS) number specifies the EIGRP routing process. Unlike RIP, multiple instances of EIGRP can run on a network. The autonomous system number is used to track each running EIGRP process.

7.3.3 TLV fields

There are three types of TLV: EIGRP parameters (figure 11.2), IP internal routes (figure 11.3), and IP external routes (figure 11.4).

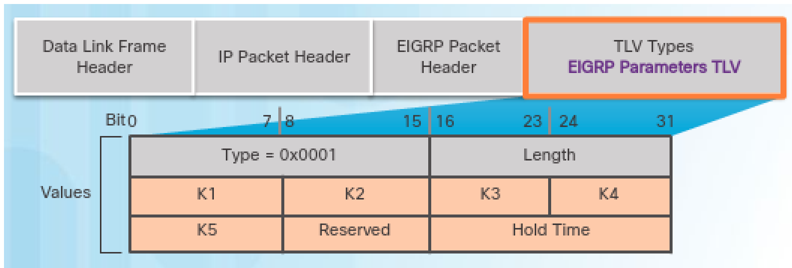


Figure 7.2: EIGRP TLV: EIGRP parameters

The *length* field identifies the size (in bytes) of the *value* field. The *value* field contains data for EIGRP message. The *type* field specifies the type of TLV: EIGRP parameters (1), IP internal routes (258), and IP external routes (259).

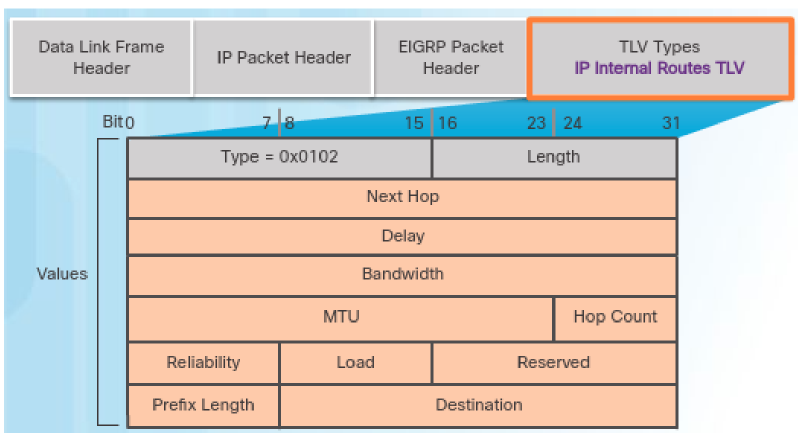


Figure 7.3: EIGRP internal routes TLV fields

The EIGRP parameters include the weights that EIGRP uses for its composite metric (K1 – K5). By default, only bandwidth and delay are weighted. Both are weighted equally; therefore, the K1 field for bandwidth and the K3 field for delay are both set to one (1). The other K values are set to zero (0).

Each IP internal route or IP external route contains one route entry and the metric information for specific route. These types of TLV are included in EIGRP Update packets. The IP internal route message is used to advertise EIGRP routes within an autonomous system. The IP external message is used to import default static route, as well as routes outside the autonomous system, into the EIGRP routing process.

7.4 Operation

7.4.1 Neighbor adjacency

EIGRP uses Hello packets to establish and maintain neighbor adjacencies. To accomplish this, two EIGRP routers must use the same K values and autonomous system number.

Each EIGRP router maintains a neighbor table, which contains a list of routers that have an EIGRP adjacency with this router. The neighbor table is used to track the status of these EIGRP neighbors.

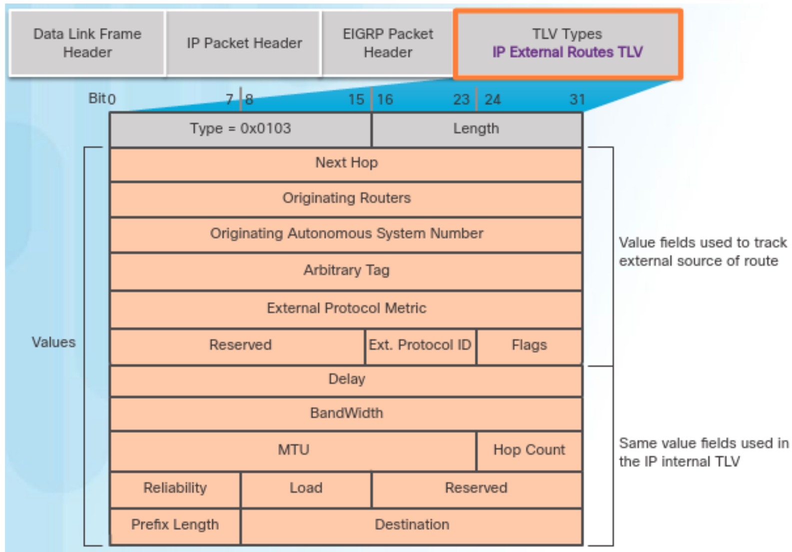


Figure 7.4: EIGRP external route TLV fields

Figure 7.5: Establish EIGRP adjacency

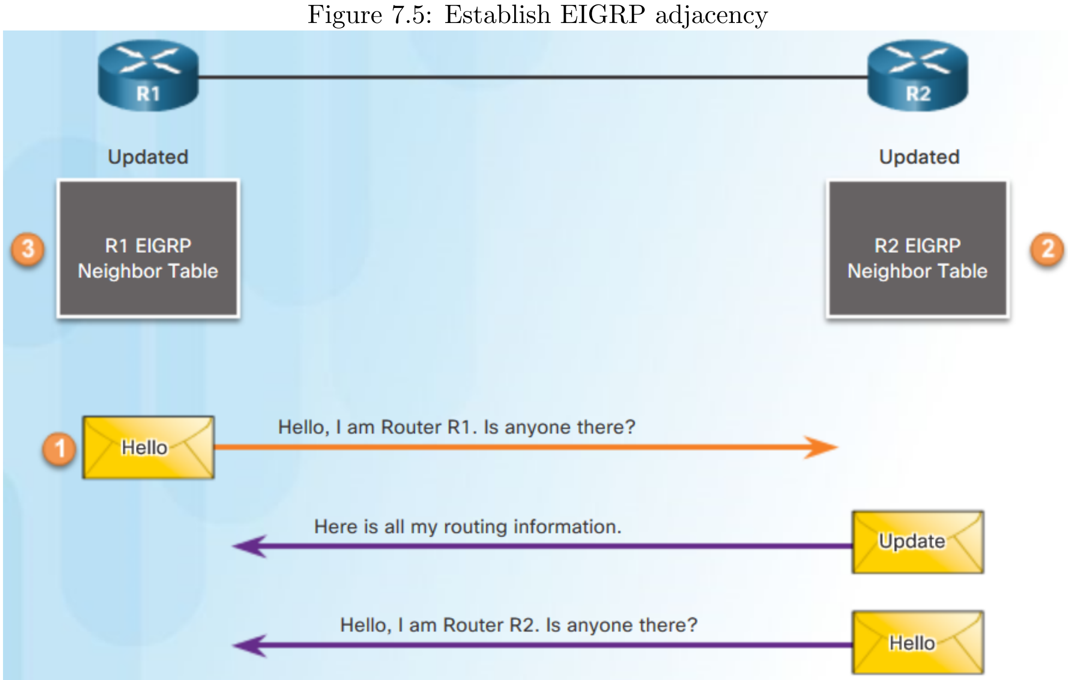


Figure 11.5 shows two EIGRP routers exchanging initial EIGRP Hello packets. When an EIGRP enabled router receives a Hello packet on an interface, it adds that router to its neighbor table:

1. A new router (R1) comes up on the link and sends an EIGRP Hello packet through all of its EIGRP-configured interfaces.
2. Router R2 receives the Hello packet on an EIGRP-enabled interface. R2 replies with an EIGRP update packet that contains all the routes it has in its routing table, except those learned through that interface (split horizon). However, the neighbor adjacency is not established until R2 also sends an EIGRP Hello packet to R1.
3. After both routers have exchanged Hellos, the neighbor adjacency is established. R1 and R2 update their EIGRP neighbor tables adding the adjacent router as a neighbor.

7.4.2 Topology table

The topology table includes all destinations advertised by neighboring (adjacent) routers and the cost (metric) to reach each network. When a router receives the EIGRP update from a neighbor, it adds all update entries to its topology table. Because EIGRP update packets use RTP reliable delivery, the router replies with an EIGRP acknowledgment packet.

7.4.3 Metric

By default, EIGRP uses the following values in its composite metric to calculate the preferred path to a network:

- **Bandwidth** – The slowest bandwidth among all of the outgoing interfaces, along the path from source to destination.
- **Delay** – The cumulative (sum) of all interface delay along the path (in tens of microseconds).

Default composite formula:

$$\text{metric} = (\text{bandwidth} + \text{bandwidth}) \times 256$$

Complete composite formula:

$$\text{metric} = \left(K1 \times \text{bandwidth} + \frac{K2 \times \text{bandwidth}}{256 \times \text{load}} + K3 \times \text{delay} \right) \times \frac{K5}{K4 + \text{reliability}} \times 256$$

This is a conditional formula. If $K5 = 0$, the last term is replaced by 1. Default values for each parameter:

- K1 (bandwidth) = 1
- K2 (load) = 0
- K3 (delay) = 0
- K4 (reliability) = 0
- K5 (reliability) = 0

Examining interface metric values

The `show interfaces <interface>` command displays interface information (figure 11.6), including the parameters used to compute the EIGRP metric.

- **BW** – Bandwidth of the interface (in kilobits per second).
- **DLY** – Delay of the interface (in microseconds).
- **Reliability** - Reliability of the interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over five minutes. By default, EIGRP does not include its value in computing its metric.
- **Txload, Rxload** – Transmit and receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over five minutes. By default, EIGRP does not include its value in computing its metric.

Figure 7.6: Examine interface metric values

```
R1# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
<output omitted>
R1#
```

Bandwidth

EIGRP uses the slowest bandwidth along the path to the destination network. EIGRP divides a reference bandwidth value of 10^7 by the interface bandwidth value in kb/s. If the result is not a whole number, then the value is rounded down. For example, 10^7 divided by 1024 equals 9765.625. The .625 is dropped to yield 9765 for the bandwidth portion of the composite metric.

Delay

EIGRP uses the sum of all delays along the path to the destination. The sum of these delays is divided by 10. See also table 11.1 for default delay values.

For example, along the path R1→R2→R3, the s0/0/1 interface on R2 has a delay of 20,000 microseconds, the g0/0 interface on R3 has a delay of 10 microseconds. The delay is $(20000 + 10) \div 10 = 2001$.

Table 7.1: Default delay values

Media	Delay
Ehternet	1000
Fast Ethernet	100
Gigabit Ethernet	10
Serial link	20000

7.4.4 DUAL algorithm

EIGRP uses the Diffusing Update Algorithm (DUAL) to provide the best loop-free path and loop-free backup paths. DUAL uses several terms, which are discussed in more detail throughout this section:

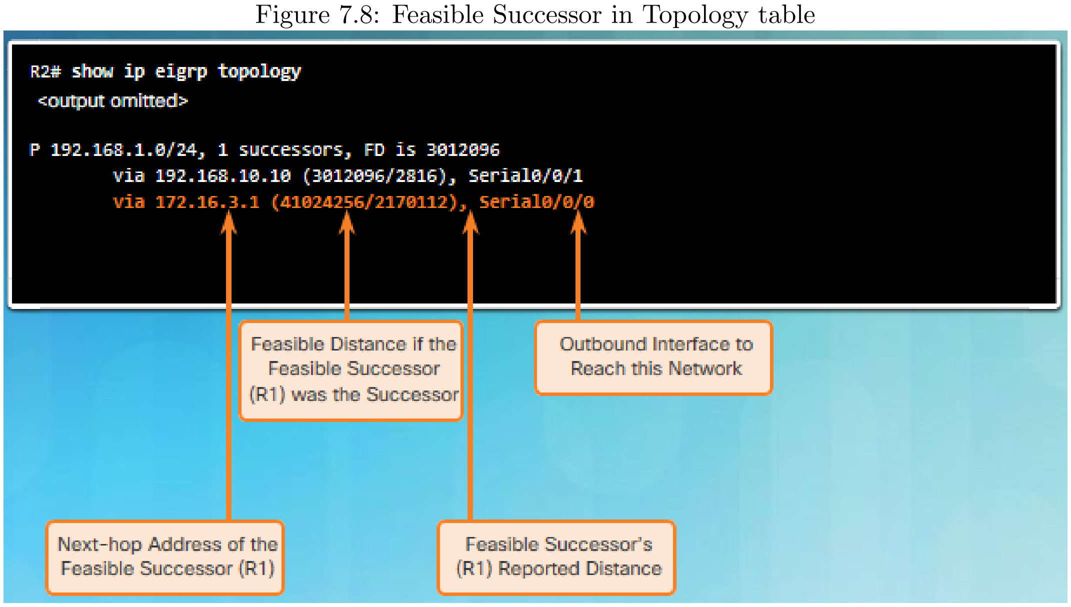
- **Successor** is a neighboring router that is used for packet forwarding and is the least-cost route to the destination network. The IP address of a successor is shown in a routing table entry right after the word via (see figure 11.7).
- **Feasible Distance (FD)** is the lowest calculated metric to reach the destination network. FD is the metric listed in the routing table entry as the second number inside the brackets (see figure 11.7). As with other routing protocols, this is also known as the metric for the route.
- **Feasible Successor (FS)** is a neighbor that has a loop-free backup path to the same network as the successor, and it satisfies the Feasibility Condition (FC). FS is not represented in the routing table until the Successor is down. Instead, we can view FS in topology table (figure 11.8).
- **Reported Distance (RD)** is simply an EIGRP neighbor's FD to the same destination network.

- **Feasible Condition (FC)** is met when a neighbor's RD to a network is less than the local router's FD to the same destination network. If the RD is less, it represents a loop-free path.

Figure 7.7: Successor and Feasible Distance

The decision process for all route computations is done by the DUAL Finite State Machine (FSM). The DUAL FSM tracks all routes and uses EIGRP metrics to select efficient, loop-free paths, and to identify the routes with the least-cost path to be inserted into the routing table.

Figure 7.8: Feasible Successor in Topology table



Recomputation of the DUAL algorithm can be processor-intensive. EIGRP avoids recomputation whenever possible by maintaining a list of backup routes that DUAL has already determined to be loop-free. If the primary route in the routing table fails, the best backup route is immediately added to the routing table.

When the Successor is no longer available and there is no FS, DUAL puts the route into an *active* state. DUAL sends EIGRP queries asking other routers for a path to the network. Other routers return EIGRP replies, letting the sender of the EIGRP query know whether or not they have a path to the requested network. If none of the EIGRP replies have a path to this network, the sender of the query does not have a route to this network. See also figure 11.9.

7.4.5 Automatic summarization

Route summarization allows a router to group networks together and advertises them as one large group using a single, summarized route. Summarization decreases the number of entries in routing updates and lowers the number of entries in local routing tables. It also reduces bandwidth utilization for routing updates and results in faster

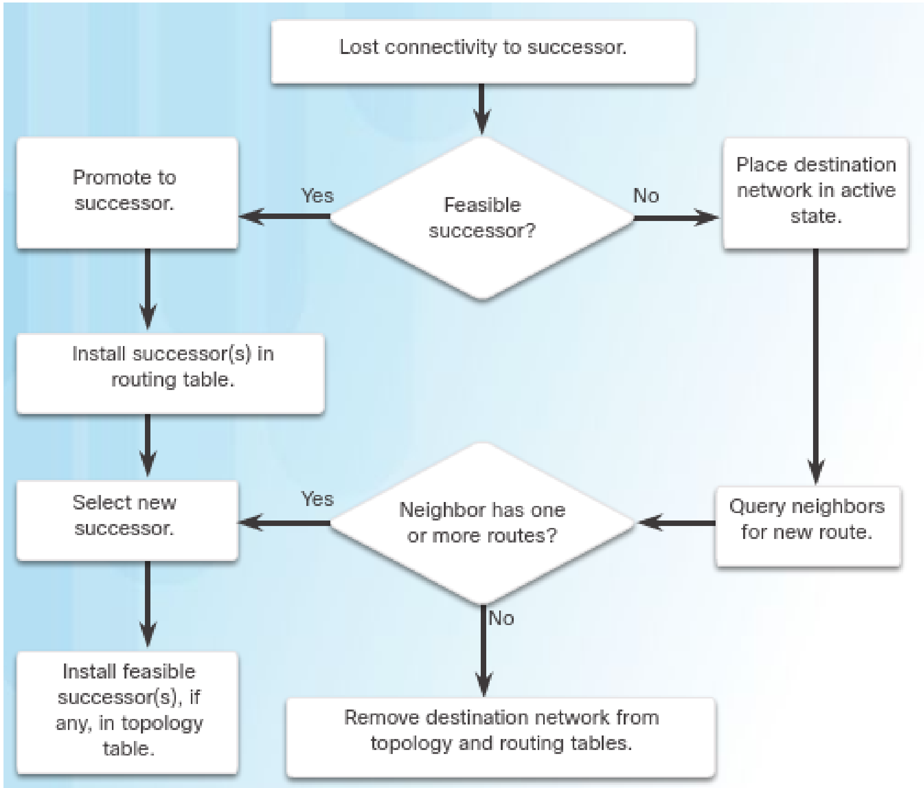


Figure 7.9: DUAL Finite State machine

routing table lookups.

However, in classes IP network, the only way that all routers can find the best routes for each individual subnet is for neighbors to send subnet information. In this situation, automatic summarization should be disabled.

A problem associated with automatic route summarization is that a summary address also advertises networks that are not available on the advertising router. For example, R1 is advertising the summary address 172.16.0.0/16, but it is only connected to 172.16.1.0/24. Therefore, R1 may receive incoming packets to destinations that do not exist (for example, 172.16.2.0/24). It then forwards a request to a destination network that does not exist, creating a routing loop.

EIGRP uses the Null0 interface to avoid the above problem. The Null0 interface is a virtual IOS interface that is a route to nowhere. If R1 receives a packet destined for a network that is advertised by the classful mask but does not exist, it discards the packets by sending them to Null0.

Note! The Null0 summary route is removed when autosummarization is disabled.

7.5 Configuration

7.5.1 EIGRP for IPv4

1. Enable EIGRP routing with AS number

   ```
   R1(config)# router eigrp 10
   ```

2. (Optional) Disable auto summarization using `no auto-summary` command.

3. Advertise the directly connected networks using the wildcard mask

```
R1(config-router)# do show ip route | inc C
R1(config-router)# network 10.1.1.0 0.0.0.3
R1(config-router)# network 192.168.1.0 0.0.0.255
R1(config-router)# network 10.3.3.0 0.0.0.3
```

4. Configure passive interfaces

```
R1(config-router)# passive-interface g0/0
R1(config-router)# passive-interface g0/1
```

5. If there are too many passive interfaces, you can make all interfaces of the router to be passive using `passive-interface default`, then configure necessary interface to be active again using `no passive-interface`

```
R1(config-router)# passive-interface default
R1(config-router)# no passive-interface s0/0/0
R1(config-router)# no passive-interface s0/0/1
```

6. Examine the EIGRP neighbor table (figure 11.10

Figure 7.10: Examine EIGRP neigbor table

```
R1# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(10)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q   Seq
                                                   (sec)         (ms)        Cnt Num
1   10.3.3.2                Se0/0/1                  13 00:24:58    8    100  0   17
0   10.1.1.2                Se0/0/0                  13 00:29:23    7    100  0   23
```

7. Examine the IP EIGRP routing table using `show ip route eigrp` (figure 11.11)

Figure 7.11: EIGRP routing table

```
      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D        10.2.2.0/30 [90/2681856] via 10.3.3.2, 00:29:01, Serial0/0/1
                     [90/2681856] via 10.1.1.2, 00:29:01, Serial0/0/0
D     192.168.2.0/24 [90/2172416] via 10.1.1.2, 00:29:01, Serial0/0/0
D     192.168.3.0/24 [90/2172416] via 10.3.3.2, 00:27:56, Serial0/0/1
```

8. Examine the EIGRP topology table using `show ip eigrp topology` (figure 11.12)
9. Verify the EIGRP routing parameters, passive interfaces and networks advertised (figure 11.13)

7.5.2 EIGRP for IPv6

1. Enable IPv6 routing on the router

```
R1(config)# ipv6 unicast-routing
```

2. Enable EIGRP for IPv6

```
R1(config)# ipv6 router eigrp 1
R1(config-rtr)# no shutdown
```

3. Assign a router ID to each router and

```
R1(config)# ipv6 router eigrp 1
R1(config-rtr)# eigrp router-id 1.1.1.1
```

Figure 7.12: EIGRP topology table

```
EIGRP-IPv4 Topology Table for AS(10)/ID(192.168.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.3.0/24, 1 successors, FD is 2172416
        via 10.3.3.2 (2172416/28160), Serial0/0/1
P 192.168.2.0/24, 1 successors, FD is 2172416
        via 10.1.1.2 (2172416/28160), Serial0/0/0
P 10.2.2.0/30, 2 successors, FD is 2681856
        via 10.1.1.2 (2681856/2169856), Serial0/0/0
        via 10.3.3.2 (2681856/2169856), Serial0/0/1
P 10.3.3.0/30, 1 successors, FD is 2169856
        via Connected, Serial0/0/1
P 192.168.1.0/24, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/0
P 10.1.1.0/30, 1 successors, FD is 2169856
        via Connected, Serial0/0/0
```

Figure 7.13: EIGRP routing parameters and networks advertised

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 10"
  Outgoing update filter list for all interface
  Incoming update filter list for all interface
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updat
  EIGRP-IPv4 Protocol for AS(10)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 192.168.1.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    10.1.1.0/30
```

4. Configure passive interfaces

```
R1(config)# ipv6 router eigrp 1
R1(config-rtr)# passive-interface g0/0
```

5. If there are too many passive interfaces, you can make all interfaces of the router to be passive using `passive-interface default`, then configure necessary interface to be active again using `no passive-interface`

```
R1(config-router)# passive-interface default
R1(config-router)# no passive-interface s0/0/0
R1(config-router)# no passive-interface s0/0/1
```

6. Configure EIGRP for IPv6 with AS number on each interface

```
R1(config)# interface g0/0
R1(config-if)# ipv6 eigrp 1
R1(config-if)# no shutdown
```

7. Examine the neighbor adjacencies using `show ipv6 eigrp neighbors`
8. Examine the IPv6 EIGRP routing table using `show ipv6 route eigrp`
9. Examine the EIGRP topology using `show ipv6 eigrp topology`
10. Verify the parameters and current state of the active IPv6 routing protocol processes using `show ipv6 protocols`

Chapter 8

OSPF

8.1 Overview

8.1.1 Operation

1. **Establish neighbor adjacencies:** An OSPF-enabled router sends Hello packets out all OSPF-enabled interfaces to determine if neighbors are present on those links.

2. **Building the Link-State Packets:** Each router builds a link-state packet (LSP) containing the state of *each* directly connected link.

3. **Flooding the LSP:** Routers flood their LSPs to all neighbors. To do this, whenever a router receives an LSP from a neighboring router, it immediately sends that LSP out all other interfaces, except the interface that received the LSP. This process creates a flooding effect of LSPs from all routers throughout the routing area.

4. **Build the Topology Table:** Routers build the topology table (LSDB) based on the received LSPs.

5. **Execute the SPF Algorithm:** Routers use the SPF algorithm to create the SPF tree.

6. **Insert best path to routing table:** From the SPF tree, the best paths are inserted to the IP routing table. The route will remain the routing table unless there is another route with lower administrative distance (AD). Routing decisions are made based on the entries in the routing table, not LSDB.

8.1.2 OSPF network types

OSPF defines five network types:

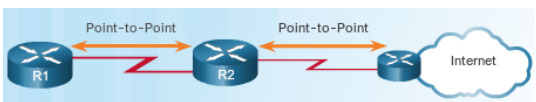
- **Point-to-point** – Two routers interconnected over a common link. No other routers are on the link. (Figure 12.1(a))

- **Multiaccess** – Multiple routers interconnected over a switch. (Figure 12.1(b))

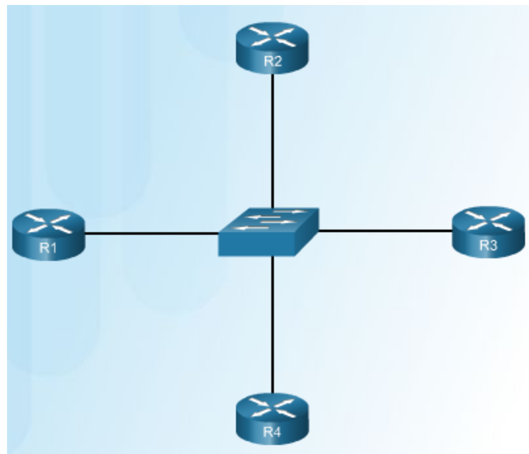
- **Nonbroadcast multiaccess (NBMA)** – Multiple routers interconnected in a network that does not allow broadcasts, such as Frame Relay. (Figure 12.1(c))

- **Point-to-multipoint** – Multiple routers interconnected in a hub-and-spoke topology over an NBMA network (Figure 12.1(d)).

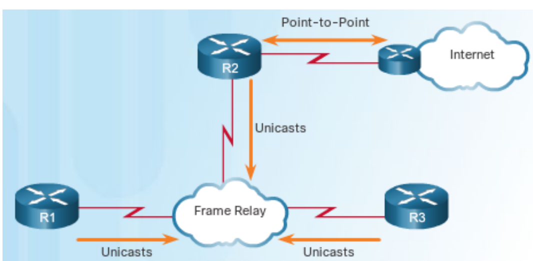
- **Virtual links** – Special OSPF network used to interconnect distant OSPF areas to the backbone area (Figure 12.1(e)). In this scenario, area 51 cannot connect directly to area 0. A special OSPF area must be configured to connect area 51 to area 0. The R1 and R2 in area 1 must be configured as a virtual link.



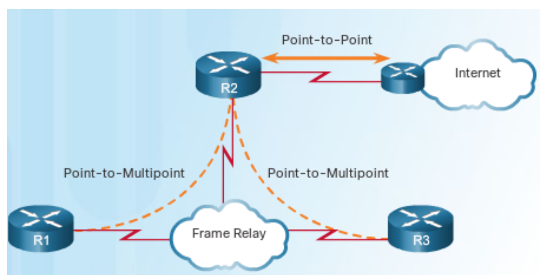
(a) Point-to-point



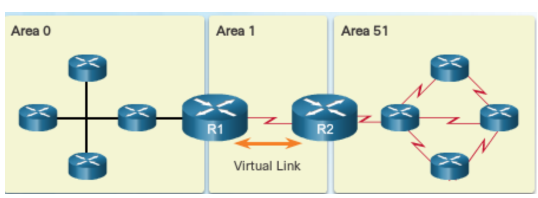
(b) Multiaccess



(c) Nonbroadcast multiaccess



(d) Point-to-multipoint



(e) Virtual link

Figure 8.1: OSPF network types

8.1.3 OSPF cost

OSPF uses **cost** as a metric, where lower cost indicates a better path. The cost of an interface is inversely proportional to the bandwidth of the interface:

$$\text{cost} = \frac{\text{Reference bandwidth}}{\text{Interface bandwidth}}$$

The default reference bandwidth is 100 Mb/s, therefore the formula is:

$$\text{cost} = \frac{10^8}{\text{Interface bandwidth in bps}}$$

Notice that any interfaces faster than 100 Mb/s share the same cost 1, because the OSPF cost value must be an integer. To avoid this, changing reference bandwidth to a higher value than 100 Mb/s is required.

Note! Changing the reference bandwidth does not actually affect the physical bandwidth of the device; rather, it simply affects the calculation used to determine the metric.

8.2 Protocol components

The OSPF routing protocol has three main components:

- Data structures
- Routing protocol messages
- Algorithm

8.2.1 Data structure

Data structures are the tables or databases that OSPF builds in order to operate. OSPF creates and maintains three databases. These databases are kept and maintained in RAM.

- **Adjacency database** (neighbor table) is a list of all neighbor routers, and unique for each router. It can be viewed using `show ip ospf neigbor` command.
- **Link-state database or LSDB** (topology table) shows the network topology and is identical for all routers in one area. It can be viewed using `show ip ospf database` command.
- **Forwarding database** (Routing table) is a list of best routes to reach networks. In the routing table, OSPF intra-area routes start with O, inter-area routes start with O IA, external routes start with O E1 (or O E2).

8.2.2 Messages

OSPF messages are transmitted to multicast address 01-00-5E-00-00-0**5** and 01-00-5E-00-00-0**6** in MAC address, 224.0.0.5 and 224.0.0.4 in IPv4, or FF02::5 and FF02::6 in IPv6. The protocol field in IP packet header is set to **89** for OSPF protocol.

OSPF uses five types of packets to convey routing information:

- **Hello packets** establish neighbor adjacency, and facilitate the DR, BDR election in multiaccess network.
- **Database description (DBD) packets** contain an abbreviated LSDB.
- **Link-State Request (LSR) packets** request additional information about network.
- **Link-State Update (LSU) packets** are sent only to neighbors *every 30 minutes*, or as a response to LSRs, or when a change is perceived.
- **Link-State Acknowledgment (LSAck) packets** are used to confirm receipt of the LSU.

Hello and dead intervals

The frequency at which the router sends hello packets is specified by hello interval in packet header. The default hello interval on point-to-point and multiaccess network is 10 seconds, on NBMA is 30 seconds.

Another important timer is dead interval, which is the period that the router waits to receive a hello packet before declaring the neighbor down. By default, dead interval is *four times hello interval*.

Link-State Advertisement

The link-state advertisement (LSA) is a basic communication means of the OSPF routing protocol. It describes a building block of the LSDB. Individually, they act as database records and provide specific OSPF network details.

LSAs are not LSPs, they are actually packaged inside LSPs to convey different kinds of routing information. The use of terms LSU, LSP and LSA can sometimes confusing because these terms are often used interchangeably. However, they are different: *An LSU is a type of LSP, an LSP contains one or more LSAs.*

LSA has its own header, which includes link-state type, link's cost, sequence number, the address of advertising router, and link ID. The *link ID* field identifies the piece of the routing domain based on LSA type (see table 12.1).

Table 8.1: Link-State Advertisment types

LSA type	Sending router	Description	Flooding area	Link ID
1	all routers	Introduce directly connected networks to its neighbors	one area	router ID of the originating router
2	DR	Give other routers info about multiaccess network	one area	IP interface address of DR
3	ABR	Propagates info of each area to all other routers	between areas	network address
4	ABR	Identify ASBR and provide the route to it	entire routing domain	router ID of ASBR
5	ASBR, ABR	Advertise external network	entire routing domain	external network address

Receiving a type 3 LSA does not cause a router to run the SPF algorithm, but the routes being advertised in the type 3 LSAs are appropriately updated to the routing table.

8.2.3 Algorithm

When an OSPF router is initially connected to a network, it goes through the following states in order:

1. **Down state** (send hello packets but not able to receive them)
2. **Init state** (hello packets are received)
3. **Two-way state** (elect a DR and a BDR)
4. **ExStart state** (decide which router will send the DBD packets first, the router with higher router ID will be the first one to send DBD packets)
5. **Exchange state** (exchange DBD packets)
6. **Loading state** (if the information in DBD packets is different from the LSDB, a router will transition to this state to gain additional route information, using LSRs)
7. **Full state** (reach convergence)

SPF algorithm calculates the best paths in order: calculate intra-area routes → calculate inter-area routes → calculate external routes.

8.3 DR election

8.3.1 Terminologies

Multiaccess network can create challenges for the flooding of LSPs. Ethernet network interconnects routers over a common link, therefore each router considers all counterparts in multiaccess network are its neighbors and establish adjacency to each of them (see figure 12.2). This could lead to extensive flooding of LSPs when OSPF is initialized or when topology changes.

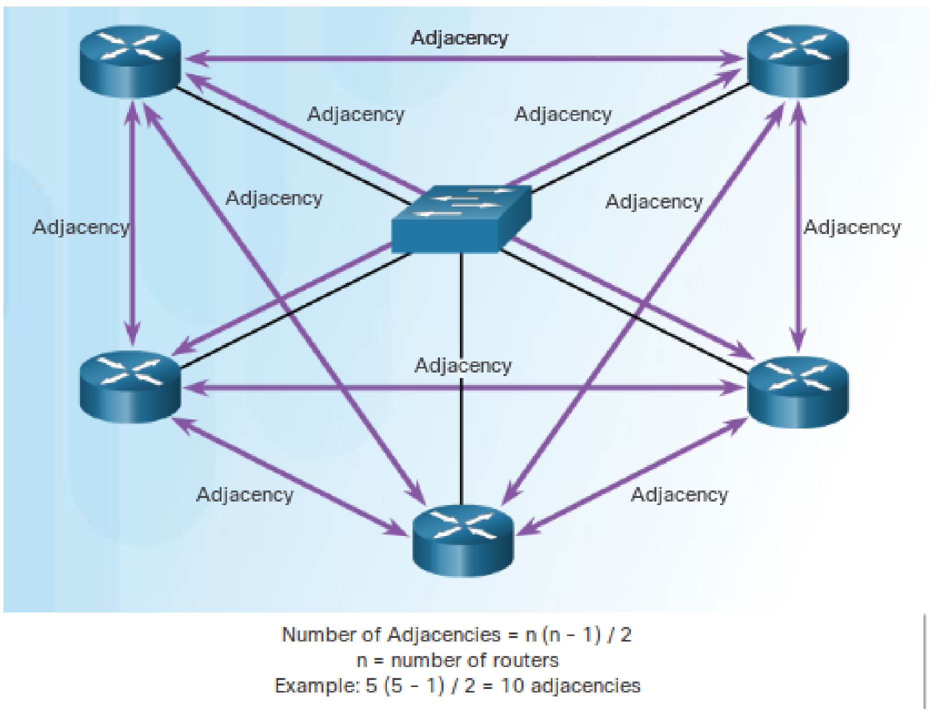


Figure 8.2: Creating adjacencies with every neighbors in multiaccess network

Designated Router (DR) is the solution to the problems on multiaccess network. On multiaccess networks and multiaccess networks only, OSPF elects a DR to be the collection and distribution point for LSPs sent and received. The router with the The router ID of DR can be viewed using `show ip ospf interface` command on any routers within the multiaccess network.

Backup Designated Router (BDR) is also elected. The BDR listens passively to this exchange and maintains a relationship with all the routers. If the DR stops producing Hello packets, the BDR promotes itself and assumes the role of DR.

DROTHER All other routers become DROTHERs (a router that is neither the DR nor the BDR). Each DROTHER forms full adjacencies (Full state) with the DR and BDR and form 2-way adjacencies (Two-way state) with any DROTHERs (see figure 12.3). DROTHERs only send their LSPs to the DR and BDR using the multicast address 224.0.0.6 (all DR routers). All DROTHER routers still receive Hello packets from each other.

8.3.2 Router ID

Every router requires a router ID to participate in an OSPF domain. The router ID is used by the OSPF-enabled router to:

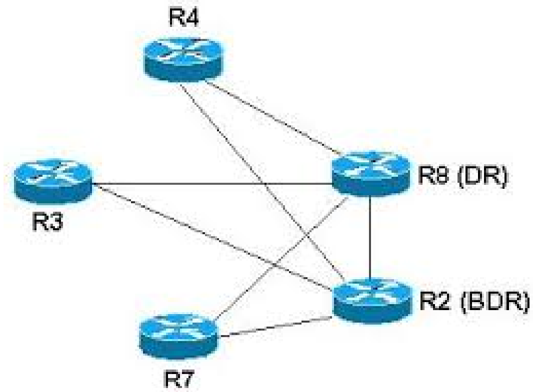


Figure 8.3: DROTHERs only form full adjacencies with the DR and BDR in the network

- Uniquely identify the router
- Participate in DR election

Cisco routers derive the router ID in one of three ways and with the following precedence:

1. IP address configured with the OSPF router-id command, if present
2. Highest IP address of any of the router's loopback addresses, if present
3. Highest active IP address on any of the router's physical interfaces

8.3.3 Election decision

The OSPF DR and BDR election decision is based on the following criteria, in sequential order:

1. The routers in the network elect the router with the highest interface priority as the DR. The router with the second highest interface priority is elected as the BDR.
2. If the interface priorities are equal, then the router with the highest router ID is elected the DR. The router with the second highest router ID is the BDR.

After the DR is elected, it remains the DR until one of the following events occurs:

- The DR fails
- The OSPF process on the DR fails or is stopped
- The multiaccess interface on the DR fails or is shutdown

OSPF DR and BDR elections are not pre-emptive. If a new router with a higher priority or higher router ID is added to the network after the DR and BDR election, the newly added router does not take over the DR or the BDR role. This is because those roles have already been assigned. The addition of a new router does not initiate a new election process.

If the DR fails, the BDR is automatically promoted to DR. This is the case even if a new router A with a higher priority or router ID is added to the network after the initial DR/BDR election. However, after a BDR is promoted to DR, a new BDR election occurs and the router A is elected as the new BDR.

8.4 OSPF area

An OSPF area is a group of routers that share the same link-state information in their LSDBs. An instance of OSPF can have several areas (called Multi-area OSPF).

8.4.1 Advantages of OSPF area

- Smaller routing table (There are fewer routing table entries as network addresses can be summarized between areas.)
- Reduced link-state update overhead (Fewer routers exchanging LSAs because LSA flooding stops at the area boundary.)
- Reduced frequency of SPF calculations (Routing still occurs between the areas, however, the CPU intensive routing operation of recalculating the SPF algorithm is done only for routes within an area.)

8.4.2 Two-layer area hierarchy

To make OSPF more efficient and scalable, OSPF is implemented in a two-layer area hierarchy:

- **Backbone (Transit) area** – A backbone area directly connected with all other areas. All traffic moving from one area to another area must traverse the backbone area. Generally, end users are not found within a backbone area. The backbone area is also called OSPF area 0.
- **Regular (Non-backbone) area** – Connects users and resources. By default, a regular area does not allow traffic from another area to use its links to reach other areas. All traffic from other areas must cross a transit area.

8.4.3 Types of routers

There are four different types of OSPF routers:

- Internal router (have all interfaces in the same area)
- Backbone router (reside in backbone area)
- Area border router or ABR (have interfaces attached to multiple areas)
- Autonomous System Boundary Router or ASBR (have at least one interface attached to an external network)

8.5 Configuration

8.5.1 Recommendations

The optimal number of routers per area varies based on factors such as network stability, but Cisco recommends the following guidelines:

- An area should have no more than 50 routers.
- A router should not be in more than three areas.
- Any single router should not have more than 60 neighbors.

Also keep the following notes in mind:

- Propagating type 3 and 5 LSAs can cause significant flooding problems. For this reason, it is strongly recommended that manual route summarization be configured on the ABRs and ASBR.
- For routers to become adjacent, their Hello interval, Dead interval, process ID and subnet masks must match.
- The dead interval must be larger than Hello interval.

8.5.2 OSPF for IPv4

1. Enable OSPF routing with process ID

```
R1(config)# router ospf 1
```

2. Configure the network statements for directly connected network

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 192.168.12.0 0.0.0.3 area 1
R1(config-router)# network 192.168.13.0 0.0.0.3 area 2
```

3. Configure passive interfaces

```
R1(config-rtr)# passive-interface g0/0
R1(config-rtr)# passive-interface g0/1
```

4. If there are too many passive interfaces, you can make all interfaces of the router to be passive using `passive-interface default`, then configure necessary interface to be active again using `no passive-interface`

```
R1(config-router)# passive-interface default
R1(config-router)# no passive-interface s0/0/0
R1(config-router)# no passive-interface s0/0/1
```

5. Propagating a default static route. *Note!* Do not use `redistribute static` as this command will not recognize default static route (due to auto summarization, it only recognizes classful route).

```
R1(config)# router ospf 1
R1(config-router)# default-information originate
```

6. Verify configuration using the following commands:
   - `show ip protocols`
   - `show ip ospf neighbor`
   - `show ip route ospf`
   - `show ip ospf`
   - `show ip ospf interface brief`

8.5.3 OSPF for IPv6

1. Enable IPv6 routing on the router

```
R1(config)# ipv6 unicast-routing
```

2. Enable OSPF for IPv6

```
R1(config)# ipv6 router ospf 1
R1(config-rtr)# no shutdown
```

3. Assign a router ID to each router

```
R1(config)# ipv6 router ospf 1
R1(config-rtr)# router-id 1.1.1.1
```

4. Configure passive interfaces

```
R1(config)# ipv6 router ospf 1
R1(config-rtr)# passive-interface g0/0
```

5. If there are too many passive interfaces, you can make all interfaces of the router to be passive using `passive-interface default`, then configure necessary interface to be active again using `no passive-interface`

```
R1(config-router)# passive-interface default
R1(config-router)# no passive-interface s0/0/0
R1(config-router)# no passive-interface s0/0/1
```

6. Configure OSPF for IPv6 with area number on each interface

```
R1(config)# interface g0/0
R1(config-if)# ipv6 ospf 1 area 0
R1(config-if)# no shutdown
R1(config-if)# interface g0/1
R1(config-if)# ipv6 ospf 1 area 55
R1(config-if)# no shutdown
```

8.5.4 Summarization

The following command enables Inter-area route summarization (for ABRs only). It summarizes all routes in an area to the specified summary address.

```
R1(config)# router ospf 1
R1(config-router)# area 1 range 192.168.64.0 255.255.224.0
```

The following command enables External route summarization (for ASBRs only). It advertises a single route for all redistributed routes that are covered by a specified network.

```
R1(config)# router ospf 1
R1(config-router)# summary-address 192.168.64.0 255.255.224.0
```

8.5.5 Priority

Configure OSPF priority for each interface. The higher the priority value (from 0 to 255), the more likely the router becomes the DR or BDR on the interface. The priority of 0 means that the router will never become a DR or BDR. On the other hand, 255 means the router will always be DR or BDR. As for IPv6, replace `ip` by `ipv6`.

```
R1(config)# interface g0/0
R1(config)# ip ospf priority 150
```

8.5.6 Dead and Hello interval

Configure OSPF Dead interval, Hello interval (in seconds). *Note!* The Dead interval must not be smaller than the Hello interval. By default, the Dead interval is four times the Hello interval. As for IPv6, replace `ip` by `ipv6`.

```
R1(config)# interface g0/0
R1(config-if)# ip ospf hello-interval 20
R1(config-if)# ip ospf dead-interval 80
```

8.5.7 Reference bandwidth

Change reference bandwidth to 1000 Mb/s.

```
R1(config)# interface g0/0
R1(config-if)# auto-cost reference-bandwidth 1000
```

8.5.8 Assign OSPF cost

Directly assign OSPF cost. The cost is a number between 1 and 65,535. As for IPv6, replace `ip` by `ipv6`.

```
R1(config)# interface g0/0
R1(config-if)# ip ospf cost 1564
```

8.5.9 Verification

As for IPv6, replace `ip` by `ipv6`.

1. Examine the neighbor adjacencies using `show ipv6 ospf neighbors`
2. Examine the IPv6 EIGRP routing table using `show ipv6 route ospf`
3. Examine the EIGRP topology using `show ipv6 ospf interface`
4. Verify the parameters and current state of the active IPv6 routing protocol processes using `show ipv6 protocols`

Part IV

WAN TECHNOLOGIES

Chapter 9

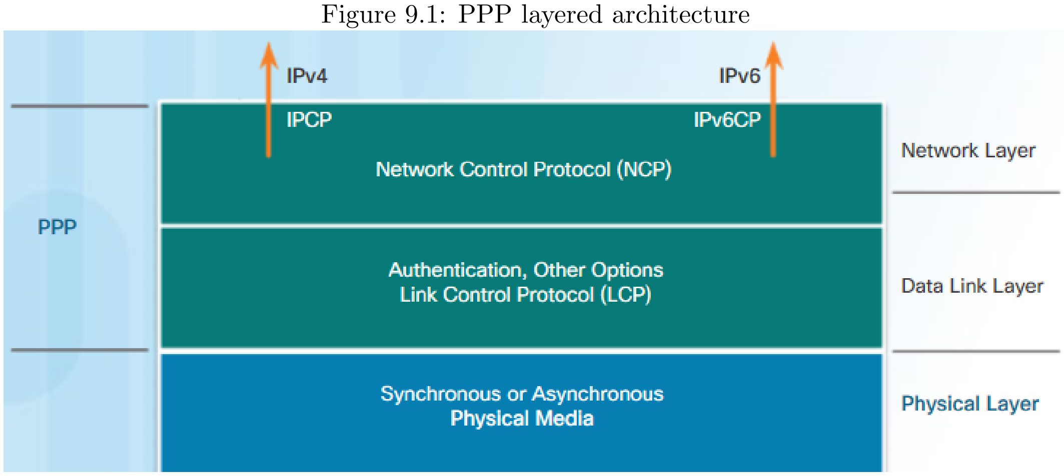
PPP

9.1 Introduction

HDLC is the default serial encapsulation method when connecting two Cisco routers and it can only work with other Cisco devices. However, when there is a need to connect to a non-Cisco router, PPP encapsulation should be used.

There are many advantages to using PPP, including the fact that it is not proprietary. PPP includes many features not available in HDLC: The link quality management feature (LQM) monitors the quality of the link, PPP supports PAP and CHAP authentication.

Figure 9.1: PPP layered architecture



PPP contains three main components: HDLC-like framing, LCP, and NCPs.

Figure 13.1 maps the layered architecture of PPP against the OSI model. PPP and OSI share the same physical layer, but PPP distributes the functions of LCP and NCP differently. Most of the work done by PPP happens at the data link and network layers, by LCP and NCPs.

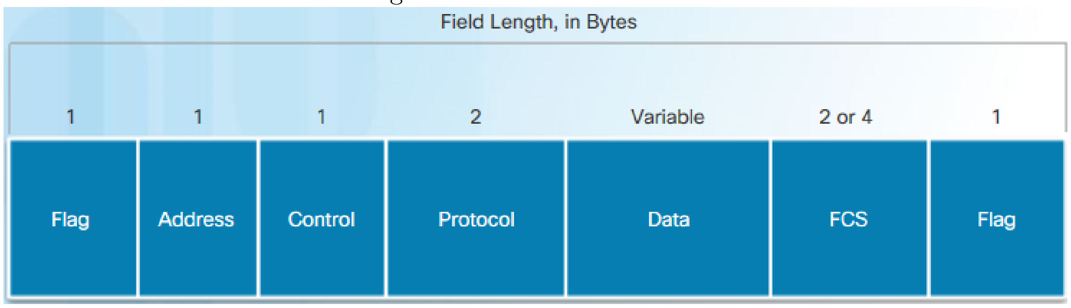
9.2 Operation

9.2.1 Frame Structure

A PPP frame consists of six fields. The following descriptions summarize the PPP frame fields illustrated in the figure 13.2:

- **Flag:** A single byte that indicates the beginning or end of a frame. The Flag field consists of the binary sequence 01111110 (63 in decimal).

Figure 9.2: PPP Frame fields



- **Address:** A single byte that contains the broadcast address because PPP does not assign individual station addresses.
- **Control:** A single byte that contains the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame.
- **Protocol:** Two bytes that identify the protocol encapsulated in the information field of the frame. The 2-byte Protocol field identifies the protocol of the PPP payload.
- **Frame Check Sequence (FCS):** This is 2 bytes. If the receiver's calculation of the FCS does not match the FCS in the PPP frame, the PPP frame is silently discarded.

9.2.2 Establishing a PPP Session

There are three phases of establishing a PPP session, as shown in the figure:

- **Phase 1: Link establishment and configuration negotiation** – The LCP opens the connection and negotiates configuration options. This phase is complete when the receiving router sends a configuration-acknowledgment frame back to the router initiating the connection.
- **Phase 2: Link quality determination (optional)** – The LCP tests the link to determine whether the link quality is sufficient to bring up network layer protocols. The LCP can delay transmission of network layer protocol information until this phase is complete.
- **Phase 3: Network layer protocol configuration negotiation** – After the LCP has finished the link quality determination phase, the appropriate NCP can separately configure the network layer protocols. If the LCP closes the link, it informs NCPs so that they can take appropriate action.

9.2.3 LCP

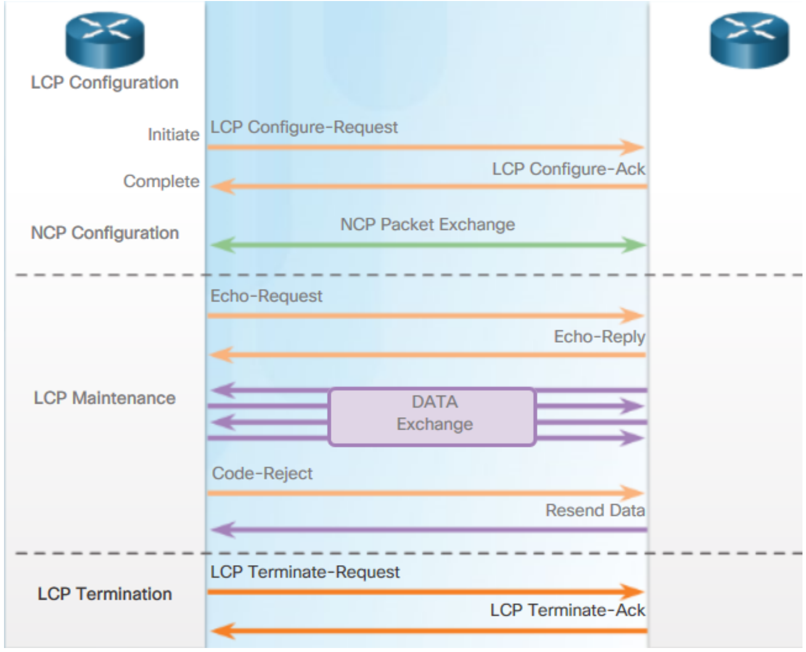
Link Control Protocol (LCP) operation uses three classes of LCP frames to accomplish the work of each of the LCP phases: Link-establishment → Link-maintenance → Link-termination (Figure 13.3).

Link Establishment

The link establishment process starts with the initiating device sending a Configure-Request frame to the responder. The initiator includes the options for how it wants the link created, including protocol or authentication parameters. The responder processes the request:

- If the options are not acceptable or not recognized, the responder sends a Configure-Nak or Configure-Reject message. If this occurs and the negotiation fails, the initiator must restart the process with new options.
- If the options are acceptable, the responder responds with a Configure-Ack message and the process moves on to the authentication stage. The operation of the link is handed over to the NCP.

Figure 9.3: Establish PPP session: Link-establishment, Link-maintenance, Link-termination



Link Maintenance

When NCP has completed all necessary configurations, LCP transitions into link maintenance. During link maintenance, LCP can use messages to provide feedback and test the link using:

- Echo-Request, Echo-Reply, and Discard-Request: These frames can be used for testing the link.
- Code-Reject and Protocol-Reject: These frame types provide feedback when one device receives an invalid frame. The sending device will resend the packet.

Link termination

After the transfer of data at the network layer completes, the LCP terminates the link, as shown in Figure 13.3. NCP only terminates the network layer and NCP link. The link remains open until the LCP terminates it. If the LCP terminates the link before NCP, the NCP session is also terminated.

The LCP closes the link by exchanging Terminate packets. The device initiating the shutdown sends a Terminate-Request message. The other device replies with a Terminate-Ack.

9.2.4 NCP

After the LCP has configured and authenticated the basic link, the appropriate NCP is invoked to complete the specific configuration of the network layer protocol being used.

IPCP is an example of NCP. IPCP is responsible for configuring, enabling, and disabling the IPv4 modules on both ends of the link. IPCP negotiates two options:

- **Compression:** Allows devices to negotiate an algorithm to compress TCP and IP headers and save bandwidth.
- **IPv4-Address:** Allows the initiating device to specify an IPv4 address to use for routing IP over the PPP link, or to request an IPv4 address for the responder.

9.2.5 Authentication

PAP is a very basic two-way process. There is no encryption. The username and password are sent in plaintext. If it is accepted, the connection is allowed. CHAP is more secure than PAP. PAP may be used in the following environments: CHAP is not supported, or simulate a login at the remote host.

PAP Process After PPP completes the link establishment phase, the remote node repeatedly sends a username-password pair across the link. At the receiving node, the username-password is checked. This device either allows or denies the connection. An accept or reject message is returned to the requester.

CHAP Unlike PAP, which only authenticates once, CHAP conducts periodic challenges to make sure that the remote node still has a valid password value. The password value is variable and changes unpredictably while the link exists. Thus, CHAP provides protection against a playback attack.

CHAP process After the PPP link establishment phase is complete, the local router sends a challenge message to the remote node. The remote node responds with a value that is calculated using a one-way hash function. The local router checks the response against its own calculation. If the values match, the initiating node acknowledges the authentication. If the values do not match, the initiating node immediately terminates the connection.

9.3 Configuration

Basic To set PPP as the encapsulation method used by a serial interface, use the encapsulation ppp interface configuration command.

```
interface s0/0/0
encapsulation ppp
no shutdown
```

Compression Point-to-point software compression on serial interfaces can be configured after PPP encapsulation is enabled. If the traffic already consists of compressed files, such as .zip, .tar, or .mpeg, do not use this option.

```
compress [predictor | stac]
```

Quality check The `ppp quality 80` command ensures that the link meets the quality requirement set (80%); otherwise, the link closes down.

Multilink PPP provides a method for spreading traffic across multiple physical WAN links. allows packets to be fragmented and sends these fragments simultaneously over multiple point-to-point links to the same remote address.

```
interface s0/0/0
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 1
no shutdown

interface s0/0/1
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 1
no shutdown

interface Multilink 1
ip address 10.0.1.1 255.255.255.252
```

```
ppp multilink
ppp multilink group 1
```

CHAP Authentication The hostname (e.g. R3, R2, ISP) on one router must match the username the other router has configured in the command `username <name> password <password>` . The passwords must also match.

```
Router(config)# hostname ISP
ISP(config)# username R3 secret cisco
ISP(config)# interface s0/0/0
ISP(config-if)# ppp authentication chap

Router(config)# hostname R3
R3(config)# username ISP secret cisco
R3(config)# interface serial0/1/0
R3(config-if)# ppp authentication chap
```

PAP Authentication The PAP username and password are configured in the command `ppp pap sent-username <name> pas` Theses username and password must match those specified with the `username <name> password <password>` command on the other router.

```
R1(config)# username R3 secret class
R1(config)# interface s0/0/0
R1(config-if)# ppp authentication pap
R1(config-if)# ppp pap sent-username R1 password cisco

R3(config)# username R1 secret cisco
R3(config)# interface s0/0/0
R3(config-if)# ppp authentication pap
R3(config-if)# ppp pap sent-username R3 password class
```

Chapter 10

PPPoE, GRE, eBGP

10.1 PPPoE

Ethernet links do not natively support PPP. PPP over Ethernet (PPPoE) provides a solution to this problem. PPPoE creates a PPP tunnel over an Ethernet connection. This allows PPP frames to be sent across the Ethernet cable to the ISP from the customer's router.

To create the PPP tunnel a dialer interface is configured.

```
interface dialer 1
  encapsulation ppp
  ip address negotiated
```

The PPP CHAP is then configured with hostname Cust1 and password cisco123.

```
interface dialer 1
  ppp authentication chap callin
  ppp chap host name Cust1
  ppp chap password cisco123
```

Dialer interface is linked to the Ethernet interface with the `dialer pool` command. Remember to set MTU to 1492 to accommodate PPPoE headers.

```
interface dialer 1
  dialer pool 1
  mtu 1492
  no shutdown
```

The physical Ethernet interface g0/1 with PPPoE is enabled with the command `pppoe enable` interface configuration command. Then it is linked to the Dialer interface with the `pppoe-client dial-pool-number <number>` interface configuration command.

```
interface g0/1
  no ip address
  pppoe enable
  pppoe-client dial-pool-number 1
```

Finally, use the following commands to verify PPPoE:

```
show ip int brief
show int dialer 1
show ip route
show pppoe session
debug ppp {negotiation | authentication | events}
```

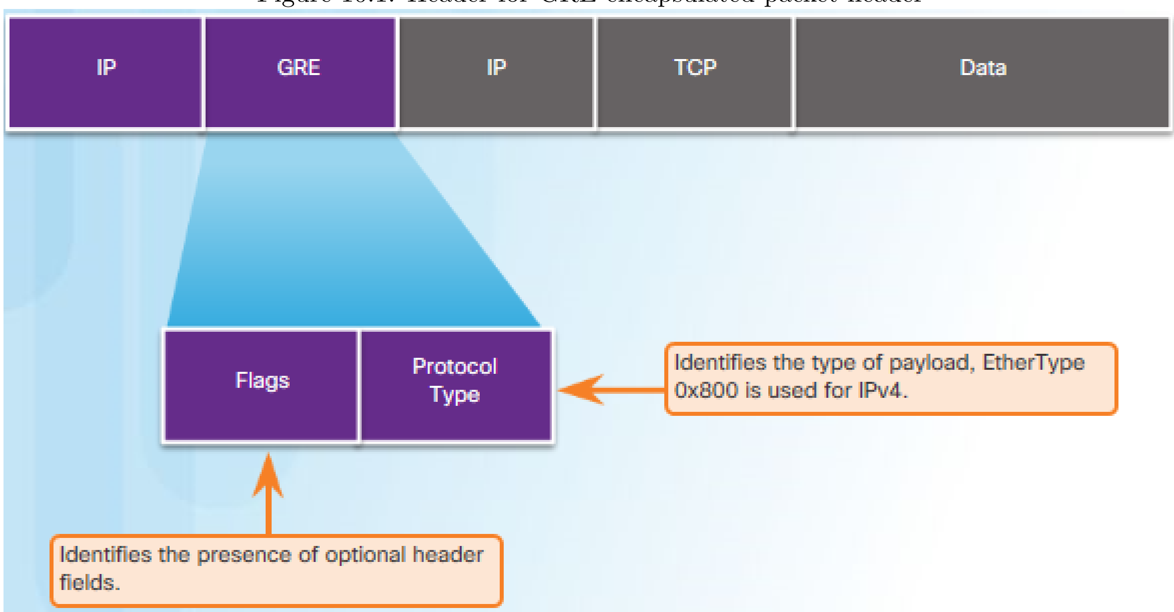
10.2 GRE

10.2.1 Introduction

GRE, IPsec, web-based SSL are the three methods of establishing a VPN connection offered by Cisco devices. GRE is a out-dated, non-secure, stateless, site-to-site VPN tunneling protocol. GRE supports the encapsulation of **any OSI Layer 3 protocol** and **47** is used in the protocol field in IP header (figure 14.1). GRE also supports multiprotocol and IP multicast tunneling.

GRE is the default tunnel interface mode for Cisco IOS software. GRE does not provide encryption or any other security mechanisms. Therefore, data that is sent across a GRE tunnel is not secure.

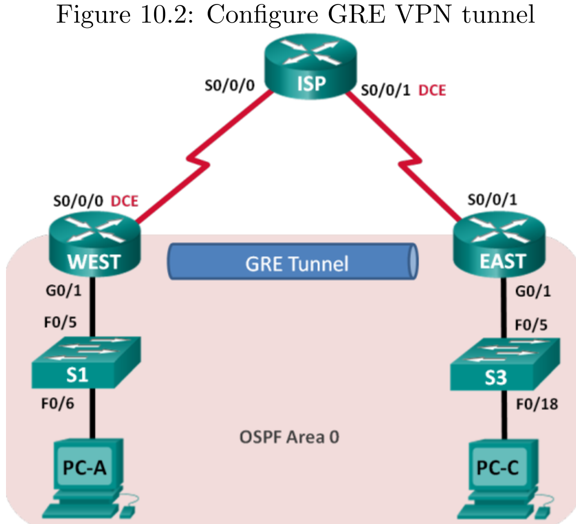
Figure 10.1: Header for GRE encapsulated packet header



10.2.2 Configuration

Five steps to configuring a GRE tunnel (figure 14.2):

Figure 10.2: Configure GRE VPN tunnel



1. **Create a tunnel interface:**

   Configure the tunnel interface on the WEST router. Use s0/0/0 as the tunnel source interface and 10.2.2.1 (IP address of EAST router s0/0/1) as the tunnel destination.

   ```
   WEST(config)# interface tunnel 0
   WEST(config-if)# ip address 172.16.12.1 255.255.255.252
   WEST(config-if)# tunnel source s0/0/0
   WEST(config-if)# tunnel destination 10.2.2.1
   ```

   Configure the tunnel interface on the EAST router. Use s0/0/1 as the tunnel source interface and 10.1.1.1 (IP address of WEST router s0/0/0) as the tunnel destination.

   ```
   EAST(config)# interface tunnel 0
   EAST(config-if)# ip address 172.16.12.2 255.255.255.252
   EAST(config-if)# tunnel source 10.2.2.1
   EAST(config-if)# tunnel destination 10.1.1.1
   ```

2. **Verify that the GRE tunnel is functional:** Verify the status of the tunnel interface on the WEST and EAST routers using `show interface tunnel 0` and `show ip interface brief` commands.

3. **Enable routing over the GRE Tunnel:** After the GRE tunnel is set up, the routing protocol can be implemented. For GRE tunneling, a network statement will include the <u>IP network of the tunnel</u>, instead of the network associated with the serial interface. Remember that the ISP router is not participating in this routing process.

   ```
   WEST(config)# router ospf 1
   WEST(config-router)# network 172.16.12.0 0.0.0.3 area 0

   EAST(config)# router ospf 1
   EAST(config-router)# network 172.16.12.0 0.0.0.3 area 0
   ```

   If BGP is used instead of OSPF or EIGRP, the neighbor statement will include the <u>IP network of the tunnel</u>, instead of the network associated with the serial interface.

   ```
   WEST(config)# router bgp 65000
   WEST(config-router)# neighbor 172.16.12.2 remote-as 65001

   EAST(config)# router bgp 65001
   EAST(config-router)# neighbor 172.16.12.1 remote-as 65000
   ```

10.3 eBGP

10.3.1 Introduction

Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP). BGP updates are encapsulated over TCP on port **179**. We use BGP when an autonomous system (AS) has connections to *multiple* ASs (known as multi-homed). BGP should not be used when there is a *single* connection to the Internet or another AS (known as single-homed).

There are three common ways an organization can choose to implement BGP in a multi-homed environment: Default Route Only, Default Route and ISP Routes, All Internet Routes (this would include routes to over 550,000 networks).

External BGP is the routing protocol used between routers in different autonomous systems. Internal BGP is the routing protocol used between routers in the same AS. Two routers exchanging BGP routing information are known as BGP peers.

Internal routing protocols (OSPF, EIGRP, RIP, etc.) use a specific metric (e.g. OSPF's cost) for determining the best paths to destination networks. BGP does *not* use a *single* metric like IGPs. Instead it uses several *attributes* including a list of AS numbers necessary to reach a destination network. Therefore BGP is known as a *path vector* routing protocol. Also, because of this, a misconfiguration of a BGP router could have negative effects throughout the entire Internet.

10.3.2 Configuration

To implement eBGP for this course, you will need to complete the following tasks:

1. Enable BGP routing and identify the AS number
2. Configure BGP neighbor(s) (peering).
3. Advertise network(s) originating from this AS.

```
R2(config)# router bgp 65000
R2(config-router)# neighbor 209.165.200.1 remote-as 65001
R2(config-router)# network 198.133.219.0 mask 255.255.255.248
R2(config-router)# end
R2# show ip route
R2# show ip bgp
R2# show ip bgp summary
```

Chapter 11

Quality of Service

11.1 Introduction

11.1.1 Traffic characteristics

Voice Voice traffic is predictable and smooth. However, voice is delay-sensitive and there is no reason to re-transmit voice if packets are lost. Therefore, voice packets must receive a higher priority than other types of traffic. Latency should be no more than **150 ms**. Jitter should be no more than **30 ms**, and voice packet loss should be no more than **1%**. Voice traffic requires at least **30 Kbps** of bandwidth.

Video Video traffic tends to be unpredictable, inconsistent, and bursty compared to voice traffic. Compared to voice, video is less resilient to loss and has a higher volume of data per packet. Latency should be no more than **400 ms**. Jitter should be no more than **50 ms**, and video packet loss should be no more than **1%**. Video traffic requires at least **384 Kbps** of bandwidth.

Data Data traffic is relatively insensitive to drops and delays compared to voice and video. The two main factors a network administrator needs to ask about the flow of data traffic are the following: Does the data come from an interactive application? Is the data mission critical?

Delay Network congestion causes delay. Two types of delays are fixed and variable. A fixed delay is a specific amount of time a specific process takes, such as how long it takes to place a bit on the transmission media. A variable delay take an unspecified amount of time and is affected by factors such as how much traffic is being processed. *Jitter* is the variation in the delay of received packets.

11.1.2 QoS tools

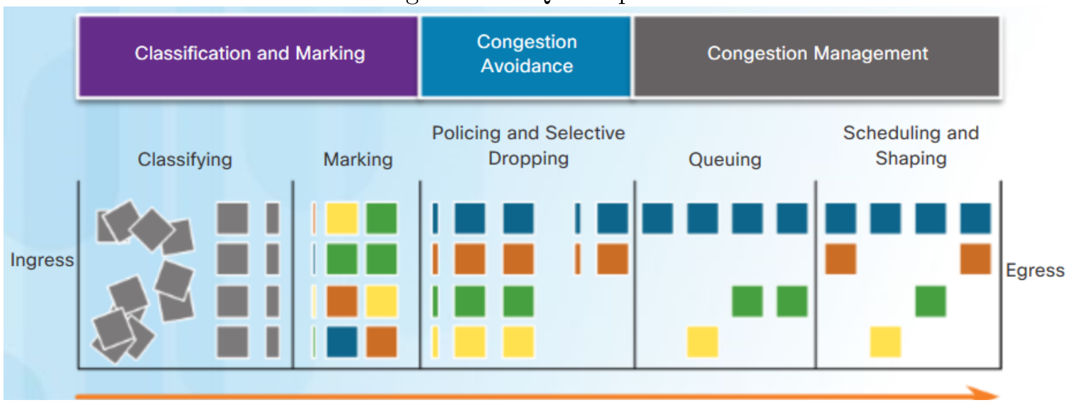
When the volume of traffic is greater than what can be transported across the network, network devices (router, switch, etc.) hold the packets in memory until resources become available to transmit them. If the number of packets continues to increase, the memory within the device fills up and packets are dropped. This problem can be solved by either increasing link capacity or implementing QoS.

A device implements QoS only when it is experiencing congestion. There are three categories of QoS tools: Classification and marking, Congestion avoidance, Congestion management. Refer to Figure 15.1 to help understand the sequence of how these tools are used when QoS is applied to packet flows.

11.2 Congestion management

When traffic exceeds available network resources, Congestion management buffers and prioritizes packets before being transmitted to the destination. Common Cisco IOS-based congestion management tools include CBWFQ and LLQ algorithms.

Figure 11.1: QoS sequence

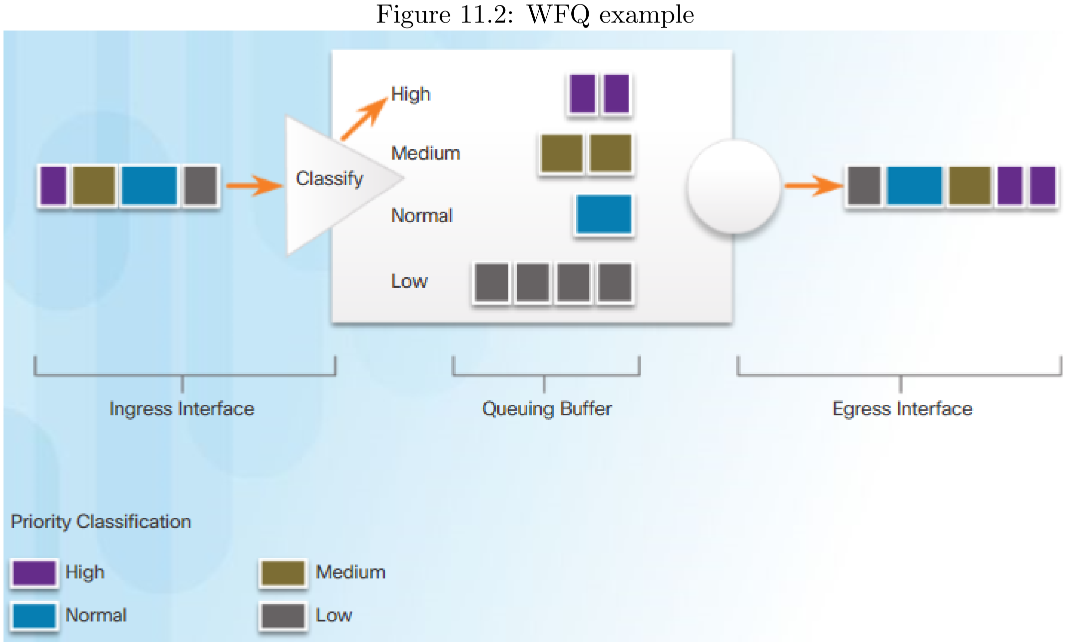


11.2.1 WFQ

WFQ (Weighted Fair Queuing) is an automated scheduling method that provides fair bandwidth allocation to all network traffic.

WFQ applies priority to identified traffic and classifies it into flows, as shown in the figure 15.2. WFQ then determines how much bandwidth each flow is allowed. WFQ classifies traffic into different flows based on packet header addressing.

Figure 11.2: WFQ example



WFQ is not supported with tunneling and encryption. It does not allow users to take control over bandwidth allocation.

11.2.2 CBWFQ

Class-Based Weighted Fair Queuing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces.

To characterize a class, you assign it bandwidth, weight, and queue limit. After a queue has reached its configured queue limit, adding more packets to the class causes tail drop. Tail drop means a router simply discards any packet that arrives at the end of a queue.

11.2.3 LLQ

The Low Latency Queuing (LLQ) feature brings strict priority queuing to CBWFQ. Strict PQ allows voice to be sent first. Without LLQ, CBWFQ services fairly based on weight; no class of packets may be granted strict priority. This scheme poses problems for voice traffic that is largely intolerant of delay.

11.3 QoS models

The three models for implementing QoS are: Best-effort model, Integrated services (IntServ), Differentiated services (DiffServ). Best-effort model means *no QoS* is implemented. QoS is really implemented in a network using either IntServ or DiffServ.

11.3.1 Best effort

The best-effort model (meaning no QoS) treats all network packets in the same way. This model is used when QoS is not required. The table 15.1 lists the benefits and drawbacks of the best effort model.

Table 11.1: Pros and Cons of Best-effort

Benefits	**Drawbacks**
Most scalable	No guarantees of delivery
Scalability is limited by bandwidth	Packets can arrive in any order
No special QoS mechanism required	No packets have preferential treatment
Easy to deploy	Critical data is treated the same as casual one

11.3.2 Integrated services

Integrated Services (IntServ) is a multiple-service model that can accommodate multiple QoS requirements.

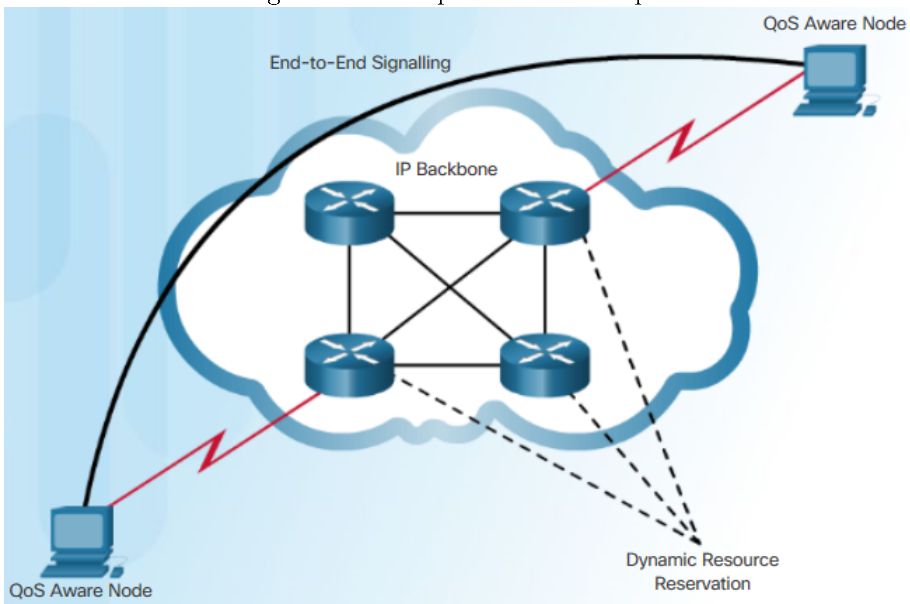
It uses resource reservation and admission-control mechanisms as building blocks to establish and maintain QoS. Each individual communication must explicitly specify its traffic descriptor and requested resources to the network (Figure 15.3). The edge router performs admission control to ensure that available resources are sufficient in the network.

IntServ uses the Resource Reservation Protocol (RSVP) to signal the QoS needs of an application's traffic along devices in the end-to-end path through the network. If network devices along the path can reserve the necessary bandwidth, the originating application can begin transmitting. If the requested reservation fails along the path, the originating application does not send any data.

Table 11.2: Pros and Cons of IntServ

Benefits	**Drawbacks**
Explicit end-to-end resource admission control	Resource intensive
Per-request policy admission control	Not scalable
Signaling of dynamic port numbers	

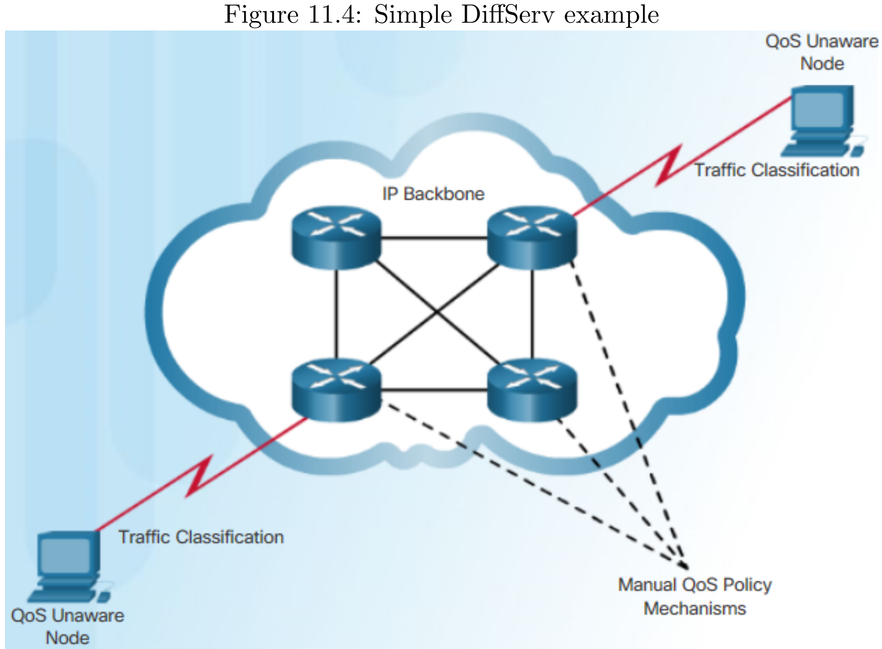
Figure 11.3: Simple IntServ example



11.3.3 Differentiated services

The DiffServ design overcomes the limitations of both the best-effort and IntServ models. Unlike IntServ, DiffServ is not an end-to-end QoS strategy and does not use signaling. Instead, DiffServ uses a "soft QoS" approach (Figure 15.4). For example, DiffServ can provide low-latency guaranteed service to voice or video while providing best-effort traffic to web traffic or file transfers.

Figure 11.4: Simple DiffServ example



Specifically, DiffServ divides network traffic into classes based on business requirements. Each of the classes can then be assigned a different level of service. You pay for a level of service. Throughout the network, the level of service you paid for is recognized and your package is given either preferential or normal traffic, depending on what you requested.

Table 11.3: Pros and Cons of DiffServ

Benefits	Drawbacks
Highly scalable	No absolute guarantee of delivery
Many different levels of quality	Requires complex mechanisms

11.4 Classification and marking

Before a packet can have a QoS policy applied to it, the packet has to be classified. Classification and marking identifies types of packets. Traffic should be classified and marked as close to its source as technically and administratively feasible. This defines the trust boundary.

Marking means that we are adding a value to the packet header. Devices receiving the packet look at this field to see if it matches a defined policy.

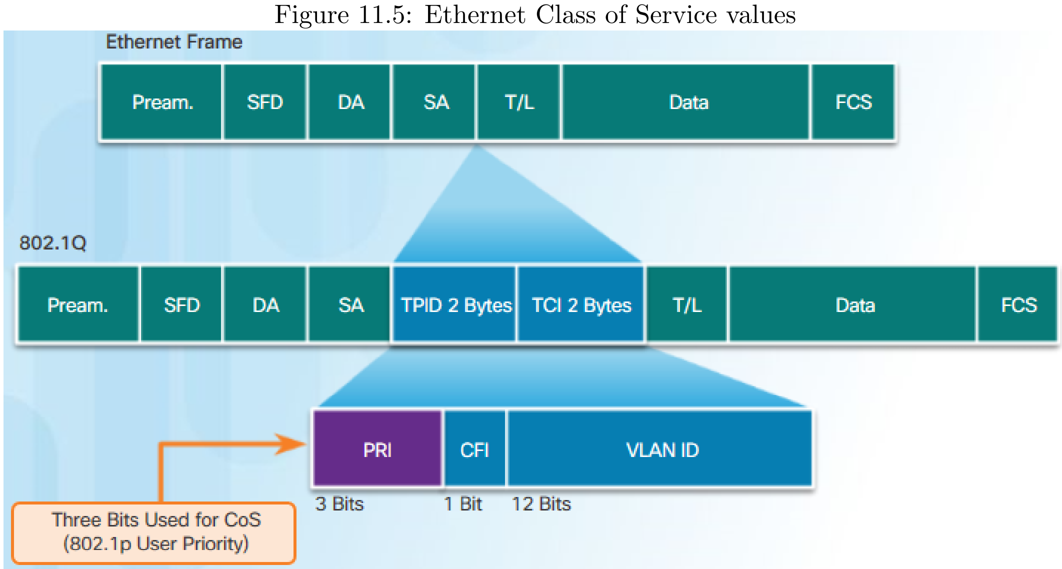
Trusted endpoints have the capabilities and intelligence to mark application traffic to the appropriate Layer 2 CoS and/or Layer 3 DSCP values. Examples of trusted endpoints include IP phones, wireless access points, videoconferencing gateways and systems, IP conferencing stations, and more.

Methods of classifying traffic flows at Layer 2 and 3 include using interfaces, ACLs, and class maps.

11.4.1 Marking at Layer 2

802.1Q is the IEEE standard that supports VLAN tagging at layer 2 on Ethernet networks. The 802.1Q standard also includes the QoS prioritization scheme known as IEEE 802.1p. The 802.1p standard uses the first three bits in the Tag Control Information (TCI) field (Figure 15.5). Known as the Priority (PRI) field, this 3-bit field identifies the Class of Service (CoS) markings.

Figure 11.5: Ethernet Class of Service values

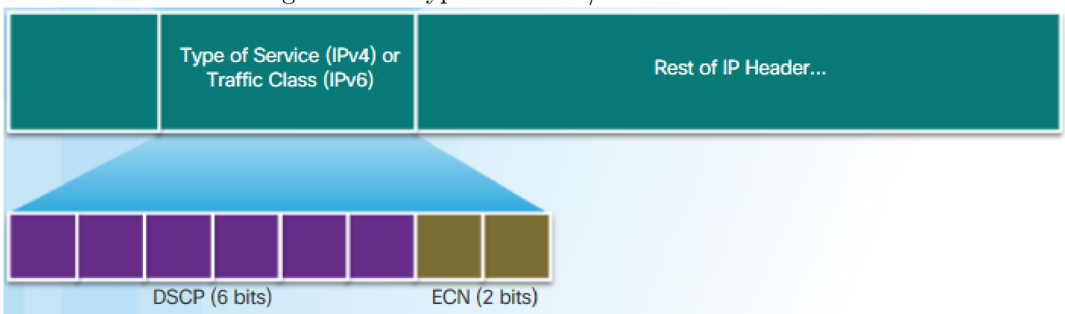


11.4.2 Marking at Layer 3

The benefit of deploying Layer 3 marking is that it can carry QoS information end-to-end unlike Layer 2 marking, which changes frame header as well as QoS information hop by hop.

Both IPv4 and IPv6 support an 8-bit field for marking, the Type of Service (ToS) field for IPv4 and the Traffic Class field for IPv6. Figure 15.6 displays the contents of the 8-bit field. The field has 6-bits allocated for QoS, called the **DiffServ** Code Point (DSCP) field. The remaining two IP Extended Congestion Notification (ECN) bits can be used by ECN-aware routers to mark packets instead of dropping them. The ECN marking informs downstream routers that there is congestion in the packet flow.

Figure 11.6: Type of Service/Traffic Class Field



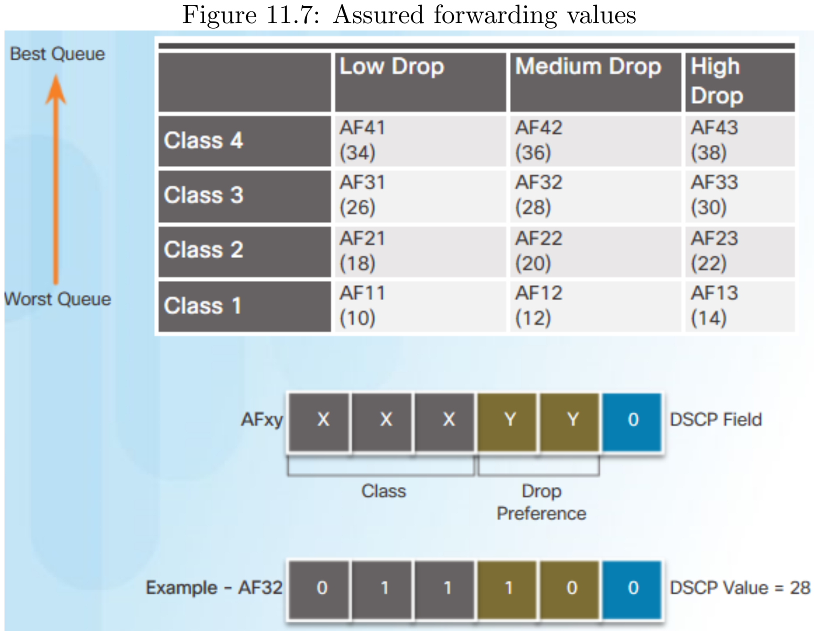
The DSCP values are organized into three categories:

- **Best-Effort (BE):** When a router experiences congestion, these packets will be dropped. No QoS plan is implemented.

- **Expedited Forwarding (EF):** DSCP decimal value is 46 (binary 101110). At Layer 3, Cisco recommends that EF only be used to mark voice packets.

- **Assured Forwarding (AF):** Use the 5 most significant DSCP bits to indicate queues and drop preference. As shown in Figure 15.7, the first 3 most significant bits are used to designate the class. The 4th and 5th most significant bits are used to designate the drop preference. The 6th most significant bit is set to zero. The AFxy formula shows how the AF values are calculated. For example, AF32 belongs to class 3 (binary 011) and has a medium drop preference (binary 10).

Figure 11.7: Assured forwarding values



	Low Drop	Medium Drop	High Drop
Class 4	AF41 (34)	AF42 (36)	AF43 (38)
Class 3	AF31 (26)	AF32 (28)	AF33 (30)
Class 2	AF21 (18)	AF22 (20)	AF23 (22)
Class 1	AF11 (10)	AF12 (12)	AF13 (14)

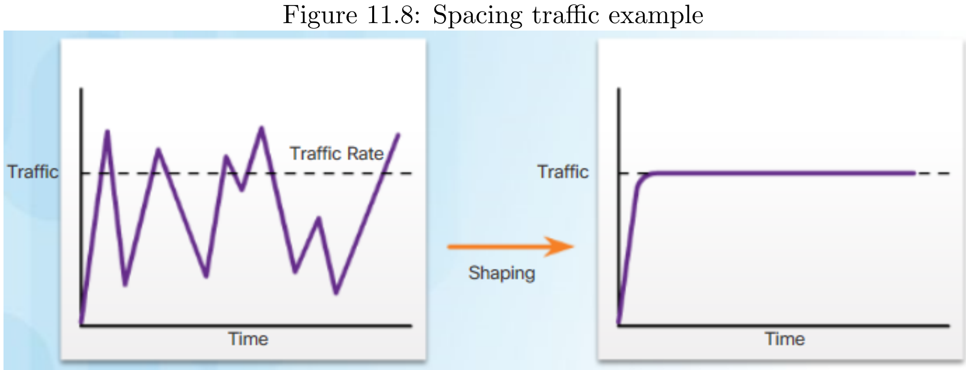
11.5 Congestion Avoidance

We avoid congestion by dropping lower-priority packets before congestion occurs. When the queue fills up to the maximum threshold, a small percentage of packets are dropped. When the maximum threshold is passed, all packets are dropped. WRED, traffic shaping, and traffic policing are three mechanisms provided by Cisco IOS QoS software to prevent congestion.

WRED is the primary congestion avoidance tool. It regulates TCP data traffic before tail drops (caused by queue overflows) occur.

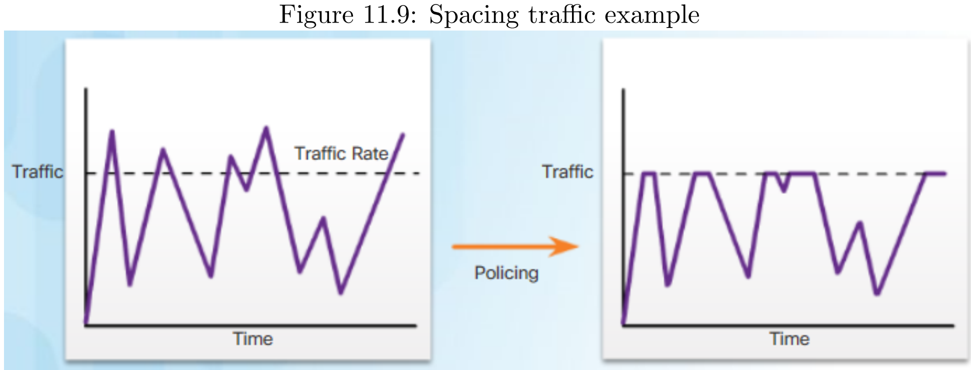
Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. The result of traffic shaping is a smoothed packet output rate, as shown in Figure 15.8. Ensure that you have sufficient memory when enabling shaping.

Figure 11.8: Spacing traffic example



Traffic policing Shaping is an outbound concept; packets going out an interface get queued and can be shaped. In contrast, policing is applied to inbound traffic on an interface. When the traffic rate reaches the configured maximum rate, excess traffic is dropped (or remarked), as shown in figure 15.9.

Figure 11.9: Spacing traffic example



Part V

INFRASTRUCTURE SERVICE

Chapter 12

DHCPv4

12.1 Operation

DHCPv4 works in a client/server mode. When a client communicates with a DHCPv4 server, the server assigns or leases an IPv4 address to that client. The client connects to the network with that leased IP address until the lease expires.

The client must contact the DHCP server periodically to extend the lease. This lease mechanism ensures that clients that move or power off do not keep addresses that they no longer need. When a lease expires, the DHCP server returns the address to the pool where it can be reallocated as necessary.

12.1.1 Lease origination

When the client boots (or otherwise wants to join a network), it begins DORA[1] process to obtain a lease.

1. A client starts the process with a broadcast **DHCP-DISCOVER** message to finds available DHCPv4 servers.
2. When the DHCPv4 server receives a DHCP-DISCOVER message, it reserves an available IPv4 address to lease to the client. It then sends a **DHCP-OFFER** message to the requesting client. The server also creates an ARP entry consisting of the MAC address of the requesting client and the leased IPv4 address of the client.
3. When the client receives the DHCP-OFFER from the server, it broadcasts**DHCP-REQUEST** messages. The DHCP-REQUEST serves as an acceptance notice to the selected server and an implicit decline to any other servers.
4. On receiving the DHCP-REQUEST message, the server verifies the lease information with an ICMP ping to that address to ensure it is not being used already. If there is *no* ICMP echo reply, then the address is is not being used by any client. Otherwise, that address is being used and the server has to send DHCP-OFFER again.
5. DHCP server sends unicast **DHCP-ACK** message to the client. The DHCP-ACK message informs the client that the IP address is valid. Because The DHCP-ACK message is a duplicate of the DHCP-OFFER, it also provides IP information for the client.
6. When the client receives the DHCPACK message, performs an ARP lookup for the assigned address. If there is no reply to the ARP, the client knows that the IPv4 address is valid and starts using it as its own.

12.1.2 Lease renewal

1. Before the lease expires, the client sends a DHCPREQUEST message directly to DHCPv4 server. If a DHCPACK is not received within a specified amount of time, the client broadcasts another DHCPREQUEST so that one of the other DHCPv4 servers can extend the lease.
2. On receiving the DHCPREQUEST message, the server verifies the lease information by returning a DHCPACK

[1]DORA = Discovery, Offer, Request, Acknowledgement

12.1.3 Relay agent

Sometimes, network clients are not on the same subnet as DHCP servers. Because routers do not forward broadcasts, the DHCP-REQUEST from clients are not sent to DHCP server.

Cisco offers a solution called Cisco IOS helper address. This solution enables a router to forward DHCP-REQUEST broadcasts to the DHCPv4 server. When a router forwards address assignment/parameter requests, it is acting as a DHCPv4 *relay agent*.

12.2 Message

DHCPv4 messages UDP encapsulation. The server uses port 67, the client uses port 68.

12.2.1 Message format

Operation (OP) code specifies general type of message: request (1), reply (2).

Figure 12.1: DHCPv4 message format

8	16	24	32
OP Code (1)	Hardware Type (1)	Hardware Address Length (1)	Hops (1)
Transaction Identifier			
Seconds - 2 bytes		Flags - 2 bytes	
Client IP Address (CIADDR) - 4 bytes			
Your IP Address (YIADDR) - 4 bytes			
Server IP Address (SIADDR) - 4 bytes			
Gateway IP Address (GIADDR) - 4 bytes			
Client Hardware Address (CHADDR) - 16 bytes			
Server Name (SNAME) - 64 bytes			
Boot Filename - 128 bytes			
DHCP Options - variable			

Hardware type Ethernet (1), Frame Relay (15), Serial (20)

Hop Controls the forwarding of messages. Set to 0 by a client before transmitting a request.

Transaction identifier used by client to match the request with replies from DHCPv4 server.

Seconds amount of time (in seconds) elapsed since a client attempted to acquire or renew a lease.

Flag Used by a client that does not know its IPv4 address when it sends a request. Only one of the 16 bits—the broadcast flag—is used. A value of 1 in this field tells the DHCPv4 server or relay agent receiving the request that the reply should be sent as a broadcast.

12.2.2 DHCP-DISCOVER

When the client boots, it has no way of knowing the subnet to which it belongs. Therefore, destination IPv4 address of DCHP-DISCOVER is 255.255.255.255, the destination MAC address is FF:FF:FF:FF:FF:FF. The source MAC address is the MAC address of the client. The client does not have a configured IPv4 address yet, so the source IPv4 address is 0.0.0.0

12.2.3 DHCP-OFFER

DHCP-OFFER contains initial configuration information for the client: IPv4 address for client, subnet mask, lease duration, and IPv4 address of the DHCPv4 server. The DHCPOFFER message can be configured to include other information, such as the lease renewal time and DNS address.

12.3 Configuration

12.3.1 DHCPv4 server

Step 1. Exclude addresses: Some IPv4 addresses in a pool are assigned to network devices that require static address assignments. Therefore, these IPv4 addresses should not be assigned to other devices.

```
R1(config)# ip dhcp excluded-address <ip-address>
R1(config)# ip dhcp excluded-address 192.168.10.1

R1(config)# ip dhcp excluded-address <range-of-address>
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
```

Step 2. Configure address pool: Define a pool of addresses to assign to clients.

```
R1(config)# ip dhcp pool <pool-name>
R1(dhcp-config)# network <network-range>

R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
```

Step 3. Define the default gateway router for clients.

```
R1(dhcp-config)# default-router 192.168.10.1
```

Step 4. Relay agent: If network clients are not on the same subnet as DHCP servers, configure the default gateway as a relay agent.

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.11.6
```

Step 4 (Optional) Other DHCP specifics

```
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
```

Step 5. Verification The `show ip dhcp binding` command displays a list of all IPv4 address to MACaddress bindings that have been provided by the DHCPv4 service. The `show ip dhcp server statistics` command verifies that messages are being received or sent by the router. This command displays count information regarding the number of DHCPv4 messages that have been sent and received.

```
R1# show run | sec dhcp
R1# show ip dhcp binding
R1# show ip dhcp statistics
```

12.3.2 DHCPv4 client

```
SOHO(config)# interface g0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
```

Chapter 13

DHCPv6

13.1 General Operation

When the client boots up, it sends DHCPv6 SOLICIT message to FF02::1:2, which is the multicast all-DHCPv6-server address. One or more servers respond with a DHCPv6 ADVERTISE unicast message to inform the client that the server is available for DHCPv6 service. The client responds with either a DHCPv6 REQUEST or a DHCPv6 INFORMATION-REQUEST unicast message:

- DHCPv6 INFORMATION-REQUEST unicast message is used for Stateless DHCPv6 (i.e. SLAAC, Stateless DHCPv6 and SLAAC) to request only additional information, such as DNS server addresses, domain name.
- DHCPv6 REQUEST unicast message is used for Stateful DHCPv6 to ask for IP configuration parameters from the server.

The server sends a DHCPv6 REPLY unicast message to the client containing the information requested in the DHCPv6 REQUEST or DHCPv6 INFORMATION REQUEST message.

13.2 SLAAC

Stateless Address AutoConfiguration (SLAAC) is enabled by default. Both the M flag and the O flag are set to 0 in the RA. In SLAAC, a host automatically obtains its IP configuration from an IPv6-enabled router. The host generates its own unique IPv6 address. A DHCPv6 server is not required. SLAAC operation includes the following steps:

1. Client asks for IPv6 configuration by sending an RS to the router R1.
2. R1 receives the RS message and responds with an RA message.
3. PC1 receives the RA, and uses the information in the message to create its own IPv6 global unicast address.
4. Because SLAAC is a stateless process, PC1 must verify that this newly created IPv6 address is unique using DAD process.

Figure 13.1: Verify SLAAC method

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::D68C:B5FF:FECE:A0C1
  <output omitted>
  Hosts use stateless autoconfig for addresses.
R1#
```

To configure SLAAC, use the `no ipv6 nd managed-config-flag` and `ipv6 nd other-config-flag` in router interface configuration mode.

13.3 SLAAC and Stateless DHCPv6

A host obtains IP configuration (prefix, prefix-length, default gateway) using SLAAC and additional information (DNS server, domain name, etc.) from a stateless DHCPv6 server. The host generates its own unique IPv6 address.

There are four steps to configure a router as a DHCPv6 server:

1. Enable IPv6 Routing using `ipv6 unicast-routing` command
2. Use `ipv6 dhcp pool <pool-name>` command to create a pool and enter the router in DHCPv6 configuration mode
3. (Optional) In DHCPv6 configuration mode, configure DNS server address (`dns-server <ip-address>`) and domain name (`domain-name <name>`).
4. In the interface configuration mode, we bind the DHCPv6 pool to the interface using `ipv6 dhcp server <pool-name>`
5. For stateless DHCPv6, the O flag is 1 and the M flag is 0, therefore, to indicate stateless DHCPv6, use the `ipv6 nd other-config-flag` in router interface configuration mode.

Figure 13.2: Verify Stateless DHCPv6 method

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::D68C:B5FF:FECE:A0C1
  <output omitted>
  Hosts use DHCP to obtain other configuration.
R1#
```

```
R1(config)# ipv6 unicast-routing
R1(config)#
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)#
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# end
R1# show ipv6 dhcp pool
R1# show ipv6 interface
R1# debug ipv6 dhcp detail
```

The `show ipv6 dhcp pool` command verifies the name of the DHCPv6 pool and its parameters. The `show ipv6 interface` command confirms that the interface has "Stateless address autoconfig enabled" and has an IPv6 global unicast address.

13.4 Stateful DHCPv6

In stateful DHCPv6, all IP information information must be obtained from a stateful DHCPv6 server. However, the default router information is not from the DHCPv6 server, but it was determined by using the source IPv6 address from the RA message. This is known as *stateful* DHCPv6 because the DHCPv6 server maintains IPv6 state information.

DHCPv6 messages from the server to the client use **UDP** destination port **546**. The client sends DHCPv6 messages to the server using **UDP** destination port **547**.

There are four steps to configure a router as a DHCPv6 server:

1. Enable IPv6 Routing using `ipv6 unicast-routing` command
2. Use `ipv6 dhcp pool <pool-name>` command to create a pool and enter the router in DHCPv6 configuration mode
3. In DHCPv6 configuration mode, `address prefix <prefix/length> lifetime <time> <preferred-time>`. The `lifetime` option indicates the valid and preferred lease times in seconds.
4. (Optional) Configure DNS server address (`dns-server <ip-address>`) and domain name (`domain-name <name>`).
5. In the interface configuration mode, we bind the DHCPv6 pool to the interface using `ipv6 dhcp server <pool-name>`
6. Because the M flag indicates whether or not to use stateful DHCPv6 and the O flag is not involved, to signify stateful DHCPv6, we set the M flag as 1 using `ipv6 nd managed-config-flag` in router interface configuration mode.

Figure 13.3: Verify stateful DHCPv6

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::D68C:B5FF:FECE:A0C1
  <output omitted>
  Hosts use DHCP to obtain routable addresses.
R1#
```

```
R1(config)# ipv6 unicast-routing
R1(config)#
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:DB8:CAFE:1::/64 lifetime infinite infinite
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)#
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# end
```

The `show ipv6 dhcp pool` command verifies the name of the DHCPv6 pool and its parameters. The `show ipv6 dhcp binding` command in Example 8-22 displays the automatic binding between the link-local address of the client and the address that the server assigns.

13.5 Router as DHCPv6 client

In the following commands, a Cisco router is used as the stateless DHCPv6 client. The `ipv6 enable` command is used because the router does not yet have a global unicast address. The `ipv6 address autoconfig` command enables automatic configuration of IPv6 addressing using SLAAC. By assumption, the server router is configured for stateless DHCPv6, so it sends an RA message to inform the client router to use stateless DHCPv6 to obtain DNS information.

```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address autoconfig
R3(config-if)# end
```

13.6 Relay agent

If the DHCPv6 server is located on a different network than the client, the IPv6 router can be configured as a DHCPv6 relay agent using `ipv6 dhcp relay destination 2001:db8:cafe:1::6` command in interface configuration mode.

13.7 Message

Router solicitation (RS) The client sends an RS message to the router. The destination address of the message is **all-routers** multicast address **FF02::2**.

Router advertisement (RA) is sent by routers to provide IP configuration to clients. The RA message includes IPv6 configuration for clients (prefix, prefix-length, DNS server, MTU, and default gateway information). A router sends an RA message periodically (every 200s) or in response to an RS message. RA messages are always sent to the IPv6 **all-nodes** multicast address **FF02::1**.

The two flags are the Managed Address Configuration flag (M flag) and the Other Configuration flag (O flag). Using different combinations of the M and O flags, RA messages have one of three addressing options for the IPv6 device:

- SLAAC (M = 0, O = 0)
- SLAAC and Stateless DHCPv6 (M = 0, O = 1)
- Stateful DHCPv6 (M = 1)

Chapter 14

HSRP

14.1 Operations

One way to prevent a single point of failure at the default gateway, is to implement a virtual router. To implement this type of router redundancy, multiple routers are configured by First Hop Redundancy Protocol (FHRP) to work together as an illusion of a single router to the hosts on the LAN. One the most popular options for FHRP is Hot Standby Router Protocol (HSRP). HSRP was designed by Cisco to allow for gateway redundancy without any additional configuration on end devices.

One of the routers is selected by HSRP to be the active router. The active router will act as the default gateway for end devices. The other router will become the standby router. The default gateway address is a virtual IPv4 address along with a virtual MAC address that is shared amongst both HSRP routers. End devices use this virtual IPv4 address as their default gateway address.(See figure 10.1). The virtual IPv4 address is configured by the network administrator. The virtual MAC address is created automatically.

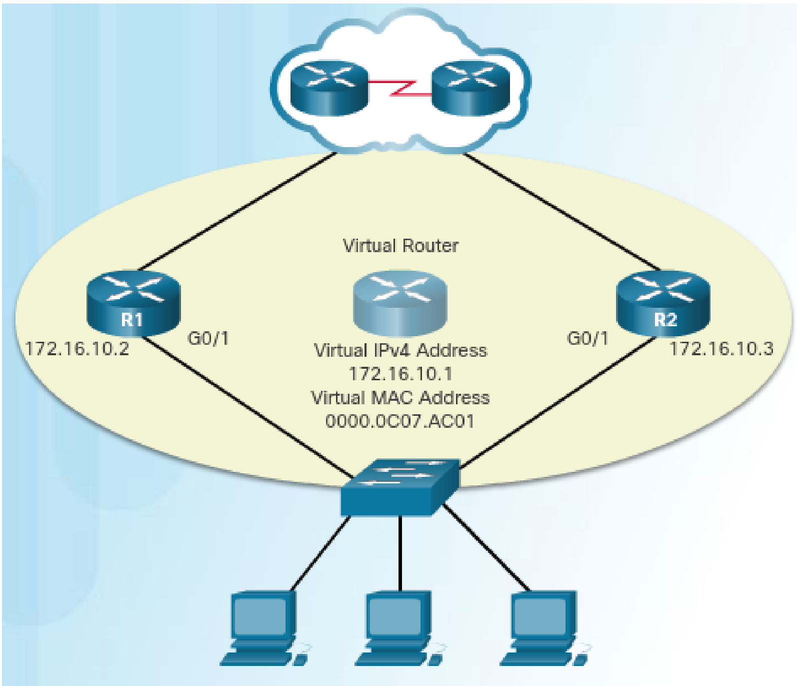


Figure 14.1: HSRP topology

14.2 Priority

HSRP priority can be used to determine the active router. The router with the highest HSRP priority will become the active router. By default, the HSRP priority is 100. If the priorities are equal, the router with the numerically highest IPv4 address is elected as the active router.

14.3 Preemption

By default, after a router becomes the active router, it will remain the active router even if another router comes online with a higher HSRP priority. This means that the router which boots up first will become the active router if there are no other routers online during the election process.

To force a new HSRP election process, preemption must be enabled. Preemption is the ability of an HSRP router to trigger the re-election process. With preemption enabled, a router that comes online with a higher HSRP priority will assume the role of the active router. Preemption only allows a router to become the active router if it has a higher priority. However, a router with equal priority will not preempt an active router, even if it has higher IPv4 address.

14.4 States and timers

When an interface is configured with HSRP, it exchanges HSRP hello packets to determine which router is active. Hello packets are sent to the HSRP group multicast address every 3 seconds (hello timer), by default. The standby router will become active if it does not receive a hello message from the active router after 10 seconds (hold timer). To avoid increased CPU usage and unnecessary standby state changes, do not set the hello timer below 1 second or the hold timer below 4 seconds.

14.5 Configuration

Complete the following steps to configure HSRP (see figure **??** for example):

1. Configure HSRP version 2.
2. Configure the virtual IP address for the group.
3. Configure the priority for the desired active router to be greater than 100.
4. Configure the active router to preempt the standby router in cases where the active router comes online after the standby router.

```
R1(config)# interface g0/1
R1(config-if)# ip address 172.16.10.2 255.255.255.0
R1(config-if)# standby version 2
R1(config-if)# standby 1 ip 172.16.10.1
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
R1(config-if)# no shutdown
```

Part VI

INFRASTRUCTURE SECURITY

Chapter 15

ACL

15.1 ACL Operation Overview

An ACL contains a sequential list of permit or deny statements, known as access control entrie (ACEs). ACEs are also commonly called ACL statements.

15.1.1 ACEs Logic Operations

ACLs are processed in a top down manner. When an ACL is inspected, if the information in a packet header and an ACL statement match, the remaining statements are not examined, and the packet is either denied or permitted through as specified by the ACL.

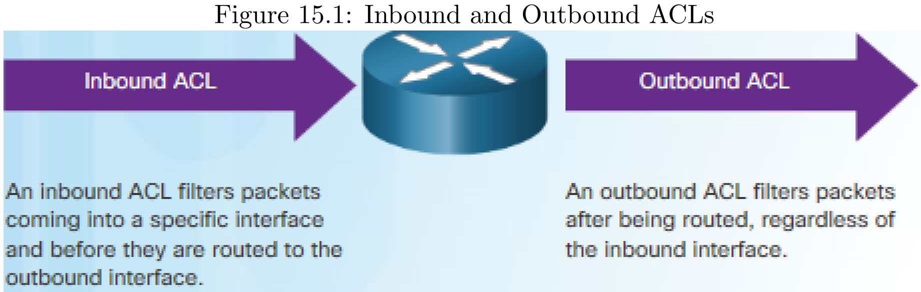
If a packet header does not match an ACL statement, the packet is tested against the next statement in the list. This matching process continues until the end of the list is reached. If no conditions match, the address is rejected. In a nut shell, ACL always stops testing conditions after the first match, therefore, the order of the ACEs is critical.

At the end of every ACL is a statement is an implicit deny any statement and because of this statement, an ACL should have at least one permit statement in it; otherwise, the ACL blocks all traffic.

15.1.2 Inbound and Outbound ACL Logic

The Figure 9.1 shows the logic of routing and ACL processes. When a packet arrives at a router interface, the router checks for an ACL on the inbound interface. If an ACL exists, the packet is tested against the statements in the list.

Figure 15.1: Inbound and Outbound ACLs



If the packet matches a statement, the packet is either permitted or denied. If the packet is accepted, it is then checked against routing table entries to determine the destination interface. If a routing table entry exists for the destination, the packet is then switched to the outgoing interface, otherwise the packet is dropped.

Next, the router checks whether the outgoing interface has an ACL. If an ACL exists, the packet is tested against the statements in the list. If the packet matches a statement, it is either permitted or denied.

If there is no ACL or the packet is permitted, the packet is encapsulated in the new Layer 2 protocol and forwarded out the interface to the next device.

15.1.3 Numbered and Named ACLs

Standard and extended ACLs can be created using either a number or a name to identify the ACL and its list of statements.

Numbered ACL Assign a number based on the following rules:

- (1 to 99) and (1300 to 1999): Standard ACL
- (100 to 199) and (2000 to 2699): Extended ACL

Named ACL Assign a name based on the following rules:

- Cannot contain spaces or punctuation
- Names are case-sensitive
- Can contain alphanumeric characters
- It is suggested that the name be written in CAPITAL LETTER

15.2 Standard ACL

15.2.1 Overview

A standard IPv4 ACL can filter traffic based on source IP addresses only. Unlike an extended ACL, it cannot filter traffic based on Layer 4 ports.

Because standard ACLs do not specify destination addresses, place them as close to the destination as possible. If a standard ACL was placed at the source of the traffic, the *permit* or *deny* will occur based on the given source address no matter where the traffic is destined.

15.2.2 Standard ACL placement

In the figure 9.2, the administrator wants to prevent traffic originating in the 192.168.10.0/24 network from reaching the 192.168.30.0/24 network.

Following the basic placement guidelines of placing the standard ACL close to the destination, the figure shows two possible interfaces on R3 to apply the standard ACL:

- R3 S0/0/1 interface - Applying a standard ACL to prevent traffic from 192.168.10.0/24 from entering the S0/0/1 interface will prevent this traffic from reaching 192.168.30.0/24 and all other networks that are reachable by R3. This includes the 192.168.31.0/24 network. Because the intent of the ACL is to filter traffic destined only for 192.168.30.0/24, a standard ACL should not be applied to this interface.
- R3 G0/0 interface - Applying the standard ACL to traffic exiting the G0/0 interface will filter packets from 192.168.10.0/24 to 192.168.30.0/24. This will not affect other networks that are reachable by R3. Packets from 192.168.10.0/24 will still be able to reach 192.168.31.0/24.

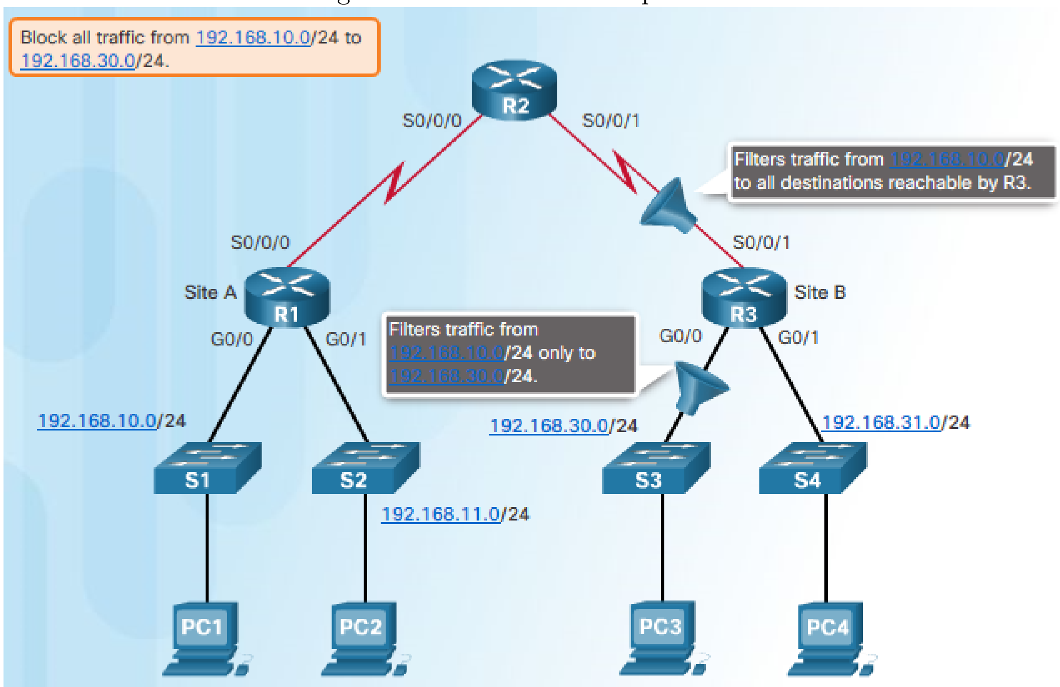
15.3 Extended ACLs

15.3.1 Overview

Extended ACLs filter packets based on:

- Protocol type (e.g. IP, ICMP, UDP, TCP)

Figure 15.2: Standard ACL placement



- Source and destination IP addresses
- Source and destination TCP and UDP ports (HTTP port 80, SSH port 22, etc.)

Extended ACLs are used more often than standard ACLs because they provide a greater degree of control. We usually locate extended ACLs as close as possible to the source of the traffic. This way, undesirable traffic is denied close to the source network without crossing the network infrastructure.

15.3.2 Extended ACL Placement

In figure 9.3, the administrator wants to deny Telnet and FTP traffic from the .11 network to Company B's 192.168.30.0/24 (.30, in this example) network. At the same time, all other traffic from the .11 network must be permitted to leave Company A without restriction.

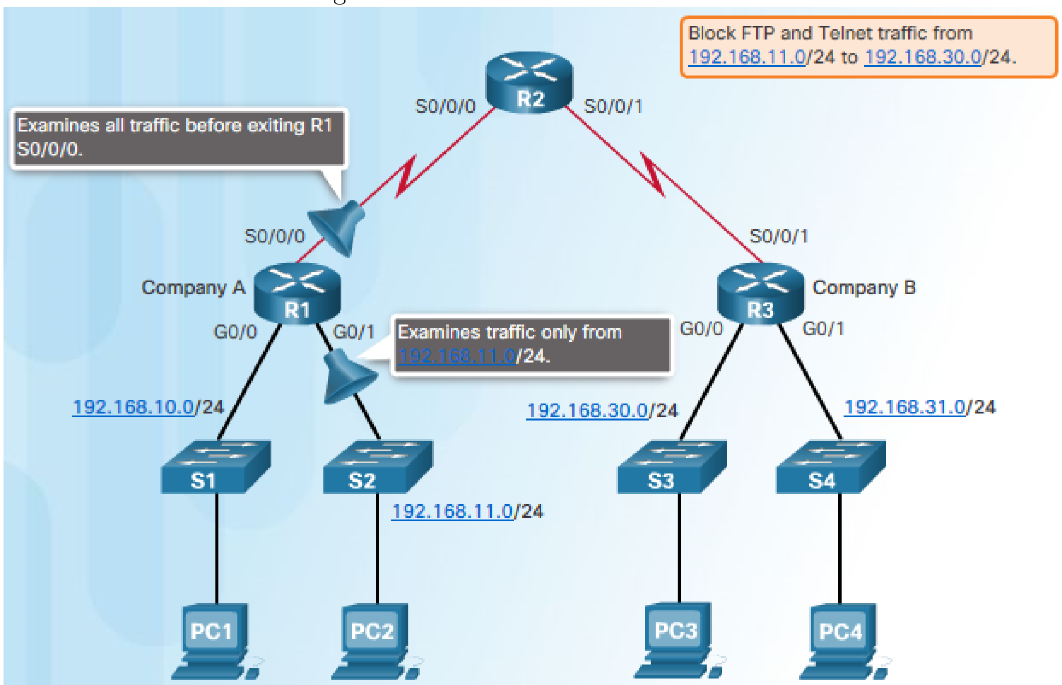
A better solution is to place an extended ACL on R1. There are two possible interfaces on R1 to apply the extended ACL:

- R1 S0/0/0 interface (outbound) - One possibility is to apply an extended ACL outbound on the S0/0/0 interface. Because the extended ACL can examine both source and destination addresses, only FTP and Telnet packets from 192.168.11.0/24 will be denied. Other traffic from 192.168.11.0/24 and other networks will be forwarded by R1. The disadvantage of placing the extended ACL on this interface is that all traffic exiting S0/0/0 must be processed by the ACL including packets from 192.168.10.0/24.
- R1 G0/1 interface (inbound) - Applying an extended ACL to traffic entering the G0/1 interface means that only packets from the 192.168.11.0/24 network are subject to ACL processing on R1. Because the filter is to be limited to only those packets leaving the 192.168.11.0/24 network, applying the extended ACL to G0/1 is the best solution.

15.4 IPv6 ACLs

In IPv4 there are two types of ACLs, standard and extended and both types of ACLs can be either numbered or named ACLs. With IPv6, there is only one type of ACL, which is equivalent to an IPv4 extended named ACL and

Figure 15.3: Extended ACL Placement



there are no numbered ACLs in IPv6. An IPv4 ACL and an IPv6 ACL cannot share the same name. There are three significant differences between IPv4 and IPv6 ACLs:

- The command used to apply an IPv6 ACL to an interface is `ipv6 traffic-filter` command.
- IPv6 ACLs do not use wildcard masks but instead specifies the prefix-length
- Besides `deny ipv6 any any`, An IPv6 ACL adds two implicit permit statements at the end of each IPv6 access list: `permit icmp any any nd-na` and `permit icmp any any nd-ns`

Because IPv6 ACLs must be configured with both a source and a destination, they should be applied closest to the source of the traffic.

15.5 Configurations

Example 15.1. The figure shows an example of an ACL designed to permit a single network. Only traffic from the 192.168.10.0/24 network will be permitted out the Serial 0/0/0 interface.

```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config)# ip access-group 1 out
```

Example 15.2. Figure below shows the commands used to configure a standard named ACL on router R1, interface G0/0, which denies host 192.168.11.10 access to the 192.168.10.0 network.

```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

Example 15.3. Design an IPv4 named access list HQServer to prevent any computers attached to the g0/0 interface of the Branch router from accessing HQServer.pka (172.16.0.1). All other traffic is permitted. Configure the access list on the appropriate router, apply it to the appropriate interface and in the appropriate direction.

```
Branch(config)# ip access-list extended HQServer
Branch(config-ext-nacl)# deny ip any host 172.16.0.1
Branch(config-ext-nacl)# permit ip any any
Branch(config-ext-nacl)# exit
Branch(config)# int g0/0
Branch(config-if)# ip access-group HQServer in
```

Example 15.4. Design an IPv4 named access list BranchServer to prevent any computers attached to the Gigabit Ethernet 0/0 interface of the HQ router from accessing the HTTP and HTTPS service of the Branch server (172.16.128.1/20). All other traffic is permitted. Configure the access list on the appropriate router, apply it to the appropriate interface and in the appropriate direction.

```
HQ(config)# ip access-list extended BranchServer
HQ(config-ext-nacl)# deny tcp any host 172.16.128.1 eq 80
HQ(config-ext-nacl)# deny tcp any host 172.16.128.1 eq 443
HQ(config-ext-nacl)# permit ip any any
HQ(config-ext-nacl)# exit
HQ(config)# int g0/0
HQ(config-if)# ip access-group HQServer in
```

Example 15.5. Design an IPv6 access-list named NO-B1 to prevent any IPv6 traffic originating on B1 (2001:DB8:ACAD:B1::2/64 to reach the BranchServer.pka (2001:DB8:ACAD:B2::3/64). No traffic should be permitted from B1 to Branch-Server.pka. Apply the IPv6 access to the most appropriated location (interface and direction).

```
Branch(config)# ipv6 access-list NO-B1
Branch(config-ipv6-acl)# deny ipv6 host 2001:DB8:ACAD:B1::2 host 2001:DB8:ACAD:B2::3
Branch(config-ipv6-acl)# permit ipv6 any any
Branch(config-ipv6-acl)# exit
Branch(config)# int g0/1
Branch(config-if)# ipv6 traffic-filter NO-B1 out
```

Example 15.6. The network administrator configured an ACL to allow users from the 192.168.10.0/24 network to browse both insecure and secure websites. In this topology (figure 9.4) the interface closest to the source of the target traffic is the G0/0 interface of R1. Web request traffic from users on the 192.168.10.0/24 LAN is inbound to the G0/0 interface. Return traffic from established connections to users on the LAN is outbound from the G0/0 interface. The example applies the ACL to the G0/0 interface in both directions. The inbound ACL, 103, checks for the type of traffic. The outbound ACL, 104, checks for return traffic from established connections. This will restrict 192.168.10.0 Internet access to allow only website browsing.

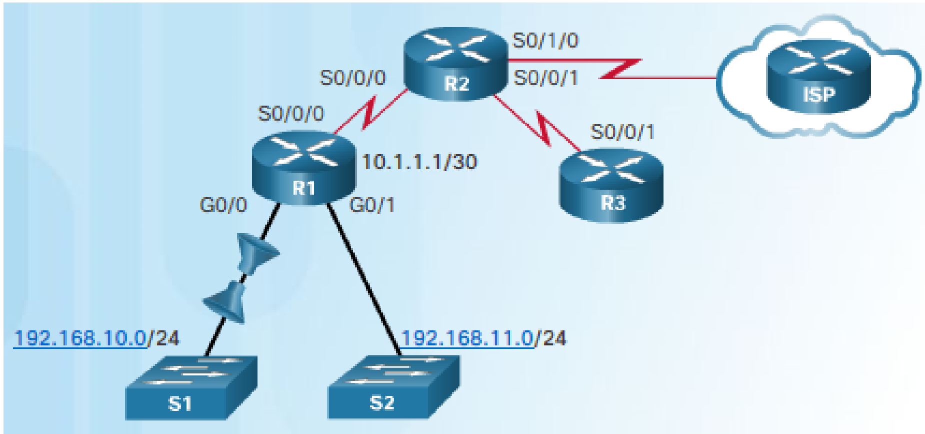
Example 15.7. Configure an extended IPv4 ACL named INTOHQ such that:

- Allow any hosts from the Internet to access the County DNS Svr. There should be two ACEs, one for TCP and the other UDP. Both use port 53.
- Allow any hosts from the Internet to access the County Web Svr. Only port 80 is needed.
- Allow return TCP traffic from the Internet that was initiated from the hosts in the Central networks to pass (with the established keyword).
- Apply the ACL to the Central S0/0/0 interface.

```
R1(config)# ip access-list extended INTOHQ
R1(config-std-nacl)# permit tcp any host 172.16.10.5 eq 53
R1(config-std-nacl)# permit udp any host 172.16.10.5 eq 53
R1(config-std-nacl)# permit tcp any host 172.16.10.10 eq 80
R1(config-std-nacl)# permit tcp any any established
R1(config-std-nacl)# exit
R1(config)# interface s0/0/0
R1(config-if)# ip access-group INTOHQ in
```

Example 15.8. Configure an extended ACL named SNMPACCESS such that

Figure 15.4: Extended ACL example



(a)

```
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)# interface g0/0
R1(config-if)# ip access-group 103 in
R1(config-if)# ip access-group 104 out
```

(b)

- The SNMP operation runs UDP on port 161.
- Allow only the County-Admin-PC to access the Central router for the SNMP connection.
- SNMP connections from other hosts on the Central LAN should fail.
- Allow all other IP traffic.
- Apply this ACL on the Central router, G0/0 interface.

```
R1(config)# ip access-list extended SNMPACCESS
R1(config-std-nacl)# permit udp host 192.168.10.5 host 192.168.10.1 eq 161
R1(config-std-nacl)# deny udp any host 192.168.10.1 eq 161
R1(config-std-nacl)# permit ip any any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group SNMPACCESS in
```

15.6 Troubleshoot

Using the `show access-lists` command to reveal most of the common ACL errors. The most common errors are entering ACEs in the wrong order and not applying adequate criteria to the ACL rules. Following these steps to troubleshoot ACL:

1. Check the criteria of ACL rules
2. Check the order of ACEs
3. Check the direction of ACL (inbound, outbound)
4. Check the location of ACL (which router, which interface). Remember that extended ACLs are placed as close as possible to the source and standard ACLs are placed as close as possible to the destination.

Example 15.9. The 192.168.10.0/24 network cannot use TFTP to connect to the 192.168.30.0/24 network.

```
R3# show access-lists 120
Extended IP access list 120
    10 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
    20 deny tcp 192.168.10.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any
```

The 192.168.10.0/24 network cannot use TFTP to connect to the 192.168.30.0/24 network because TFTP uses the transport protocol UDP. Statement 30 in access list 120 allows all other TCP traffic. However, because TFTP uses UDP instead of TCP, it is implicitly denied. Recall that the implied deny any statement does not appear in show access-lists output and therefore matches are not shown. Statement 30 should be `permit ip any any`.

Example 15.10. The 192.168.11.0/24 network can use Telnet to connect to 192.168.30.0/24, but according to company policy, this connection should not be allowed. The results of the show access-lists 130 command indicate that the permit statement has been matched.

```
R1# show access-lists 130
Extended IP access list 130
    10 deny tcp any eq telnet any
    20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any (12 match(es))
```

The 192.168.11.0/24 network can use Telnet to connect to the 192.168.30.0/24 network because the Telnet port number in statement 10 of access list 130 is listed in the wrong position in the ACL statement. Statement 10 currently denies any source packet with a port number that is equal to Telnet. To deny Telnet traffic inbound on G0/1, deny the destination port number that is equal to Telnet, for example, 10 deny tcp 192.168.11.0 0.0.0.255 192.168.30.0 0.0.0.255 eq telnet.

Part VII

INFRASTRUCTURE MANAGEMENT

Chapter 16

Network Security and Monitoring

16.1 Security attacks

16.1.1 CDP Reconnaissance Attack

The Cisco Discovery Protocol (CDP) is enabled on Cisco devices by default. CDP broadcasts are sent unencrypted and unauthenticated. Therefore, an attacker could interfere with the network infrastructure by sending crafted CDP frames containing bogus device information to directly-connected Cisco devices. To mitigate the exploitation of CDP, limit the use of CDP on devices or ports. For example, disable CDP on edge ports that connect to untrusted devices.

16.1.2 Telnet Attacks

There are two types of Telnet attacks:

- Brute Force Password Attack: The attacker tries to discover the administrative password.
- Telnet DoS Attack: The attacker continuously requests Telnet connections in an attempt to render the Telnet service unavailable and preventing an administrator from remotely accessing a device.

16.1.3 MAC Address Table Flooding Attack

MAC address tables are limited in size. MAC flooding attacks exploit this limitation with fake source MAC addresses until the switch MAC address table is full. When the MAC address table becomes full of fake MAC addresses, the switch enters into what is known as fail-open mode. In this mode, the switch broadcasts all frames to all machines on the network. As a result, the attacker can capture all of the frames, even frames that are not addressed to its MAC address table. Configure **port security** on the switch to mitigate MAC address table overflow attacks.

16.1.4 VLAN Attacks

The attacker attempts to gain VLAN access by configuring a host to trunk with the connecting switch. If successful, the switch establishes a trunk link with the host and the attacker can then access all the VLAN traffic on the switch. The best way to prevent basic VLAN attacks:

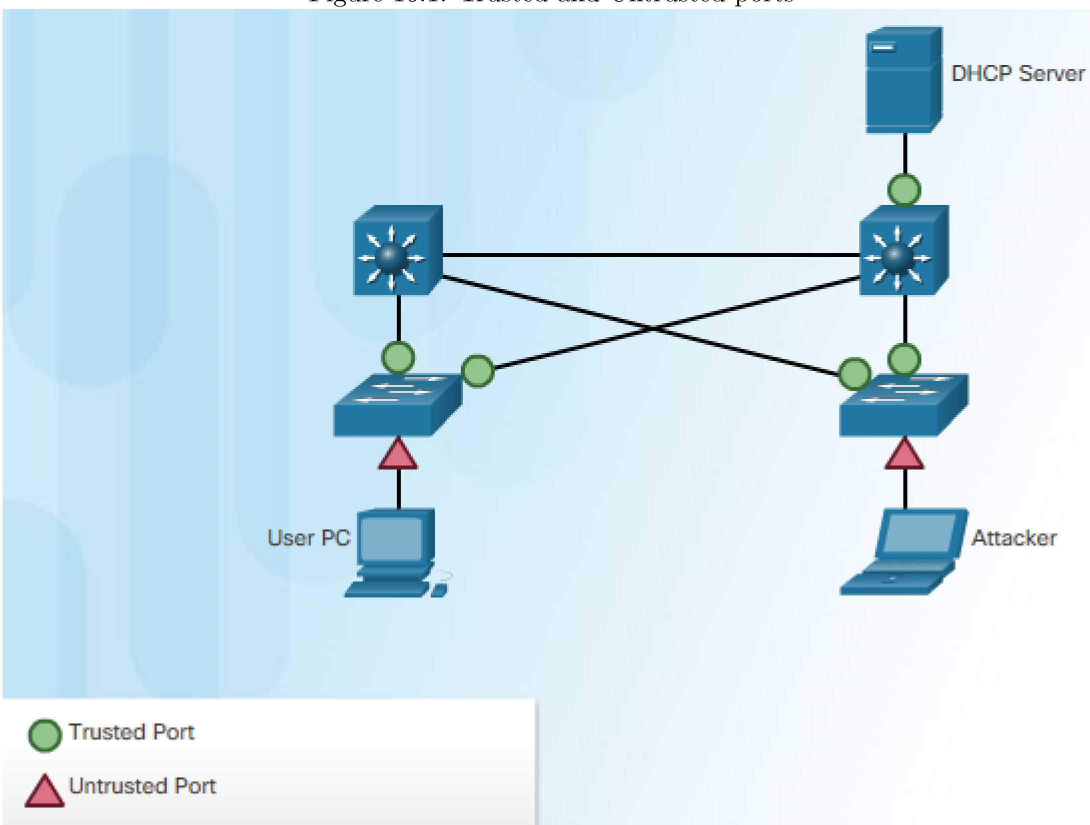
- Disable DTP negotiations on non-trunking ports using the `switchport nonegotiate` interface configuration command.
- Manually enable the trunk link using the `switchport mode trunk` interface configuration command.
- Manually enable access ports using the `switchport mode access` interface configuration command.
- Set the native VLAN to be something other than VLAN 1.
- Administratively shut down unused ports, and assign them to an unused VLAN.

16.1.5 DHCP Attacks

DHCP spoofing attack: A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. Use *DHCP snooping* to mitigate DHCP spoofing attacks.

DHCP starvation attack: An attacker floods the DHCP server with bogus DHCP requests and eventually leases all of the available IP addresses in the DHCP server pool. After these IP addresses are issued, the server cannot issue any more addresses, and this situation produces a DoS attack[1] as new clients cannot obtain network access.

Figure 16.1: Trusted and Untrusted ports



DHCP snooping recognizes two types of ports (see figure 16.1):

- **Trusted DHCP ports:** Only ports connecting to *upstream* DHCP servers should be trusted. Trusted ports must be explicitly identified in the configuration.
- **Untrusted ports:** These ports connect to hosts that should not be providing DHCP server messages. By default, all switch ports are untrusted.

16.1.6 Cisco solution

There are four Cisco switch security solutions to help mitigate Layer 2 attacks:

- Port security prevents MAC address flooding, DHCP starvation
- DHCP snooping prevents DHCP spoofing and DHCP starvation
- DAI (Dynamic ARP inspection) prevents ARP spoofing and ARP poisoning
- IPSG (IP Source Guard) prevents MAC and IP address spoofing

[1] A DoS attack is any attack that is used to overload specific devices and network services with illegitimate traffic, thereby preventing legitimate traffic from reaching those resources.

16.1.7 The AAA framework

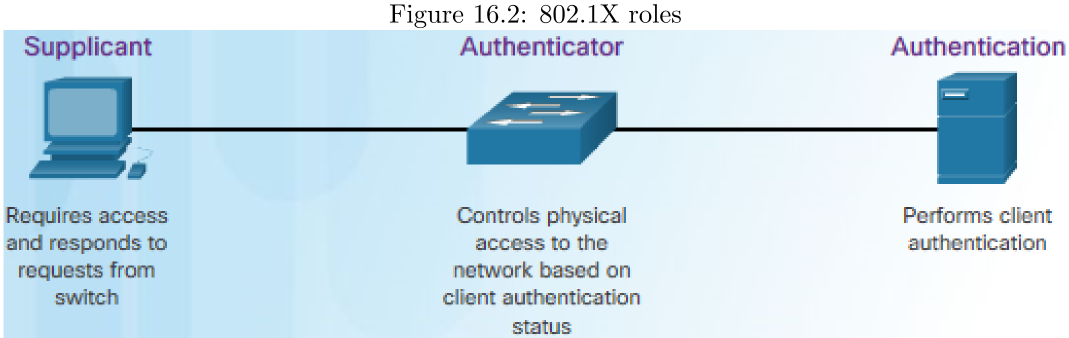
The Authentication, Authorization, and Accounting (AAA) framework is used to secure device access. An AAA-enabled router uses either TACACS+ or RADIUS protocol to communicate with the AAA server. TACACS+ is considered the more secure protocol, because all TACACS+ protocol exchanges are encrypted, while RADIUS only encrypts the user's password. RADIUS does not encrypt user names, accounting information, or any other information carried in the RADIUS message. Cisco provides two common methods of implementing AAA services:

- **Local AAA:** use a local database for authentication, store usernames and passwords locally in the Cisco router, and users authenticate against the local database. Local AAA is ideal for small networks.
- **Server-Based AAA Authentication:** The AAA server contains the usernames and password for all users and serves as a central authentication system for all infrastructure devices.

16.1.8 802.1X

The IEEE 802.1X standard defines a port-based access control and authentication protocol. IEEE 802.1X restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports.

Figure 16.2: 802.1X roles



With 802.1X port-based authentication, the devices in the network have specific roles, as shown in the figure 16.2:

- Client (Supplicant): The device is a PC running 802.1X-compliant client software.
- Switch (Authenticator): This controls physical access to the network based on the authentication status of the client. The switch requests identifying information from the client, verifies that information with the authentication server, and relays a response to the client.
- Authentication server: validates the identity of the client and notifies the switch or other authenticator such as a wireless access point whether the client is authorized to access the LAN and switch services.

16.2 SNMP

16.2.1 Introduction to SNMP

Simple Network Management Protocol (SNMP) was developed to allow administrators to manage nodes such as servers, workstations, routers, switches, and security appliances, on an IP network. The SNMP system consists of three elements:

- **SNMP manager**: a part of a network management system (NMS), run SNMP management software.
- **SNMP agents** (managed node): responsible for providing access to the local MIB, the SNMP agent and MIB reside on SNMP client devices.
- **MIB** (Management Information Base): store data about the device and operational statistics

16.2.2 SNMP requests

The SNMP manager uses the get and set actions to perform the operations, as described in the Figure 16.3.

Figure 16.3: SNMP operations

Operation	Description
`get-request`	Retrieves a value from a specific variable.
`get-next-request`	Retrieves a value from a variable within a table; the SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
`get-bulk-request`	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (Only works with SNMPv2 or later.)
`get-response`	Replies to a `get-request`, `get-next-request`, and `set-request` sent by an NMS.
`set-request`	Stores a value in a specific variable.

16.2.3 SNMP Agent Traps

An *NMS periodically polls* the SNMP agents residing on managed devices, by querying the device for data using the get request. Using this process, a network management application can collect information to monitor traffic loads and to verify device configurations of managed devices. Periodic SNMP polling does have disadvantages. First, there is a delay between the time that an event occurs and the time that it is noticed (via polling) by the NMS. Second, there is a trade-off between polling frequency and bandwidth usage.

To mitigate these disadvantages, it is possible for SNMP agents to generate and send traps to inform the NMS immediately of certain events. Traps are unsolicited messages alerting the SNMP manager to a condition or event on the network.

16.2.4 Community string and Object ID

SNMPv1 and SNMPv2c use community strings as plaintext password to control access to the MIB. There are two types of community strings: Read-only (**ro**) and Read-write (**rw**).

MIB saves data in variables and organizes them hierarchically. Formally, the MIB defines each variable as an object ID (OID). OIDs uniquely identify managed objects in the MIB hierarchy (figure 16.4).
For example, OIDs belonging to Cisco, are numbered as follows: .iso (1).org (3).dod (6).internet (1).private (4).enterprises (1).cisco (9). Therefore the OID is 1.3.6.1.4.1.9. The data is retrieved via the *snmpget* utility, issued on the NMS. Using the snmpget utility, one can manually retrieve real-time data or have a report containing a period of time that you could use the data to get the average.

16.2.5 Configuration

SNMPv2

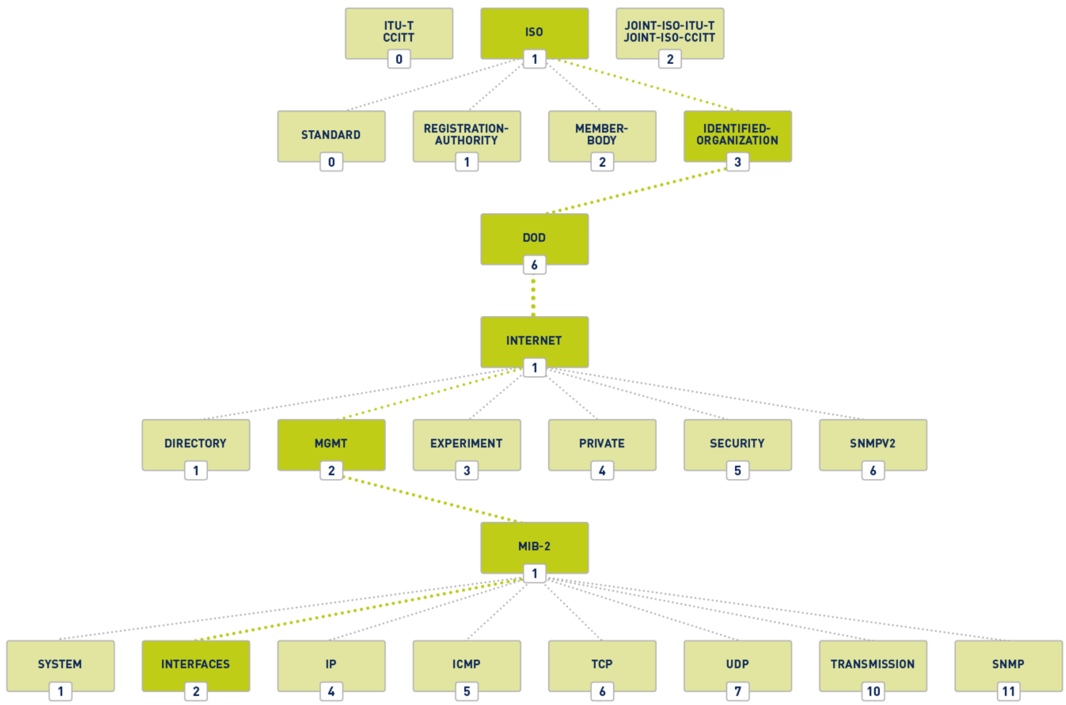
```
R1(config)# snmp-server community batonaug ro SNMP_ACL
R1(config)# snmp-server location NOC_SNMP_MANAGER
R1(config)# snmp-server contact Wayne World
R1(config)# snmp-server host 192.168.1.3 version 2c batonaug
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.1.3
```

1. (Required) Configure the community string and access level (read-only or read-write) with the snmp-server community string ro — rw command.

2. (Optional) Document the location of the device using the snmp-server location text command.

3. (Optional) Document the system contact using the snmp-server contact text command.

Figure 16.4: OID tree



4. (Optional) Restrict SNMP access to NMS hosts (SNMP managers) that are permitted by an ACL: define the ACL and then reference the ACL with the snmp-server community string access-list-number-or-name command. This command can be used both to specify a community string and to restrict SNMP access via ACLs. Step 1 and Step 4 can be combined into one step, if desired; the Cisco networking device combines the two commands into one if they are entered separately.

5. (Optional) Specify the recipient of the SNMP trap operations with the snmp-server hosthost-id [version 1— 2c — 3 [auth — noauth — priv]] community-string command. By default, no trap manager is defined.

6. (Optional) Enable traps on an SNMP agent with the snmp-server enable traps notification-types command. If no trap notification types are specified in this command, then all trap types are sent. Repeated use of this command is required if a particular subset of trap types is desired.

Note! To verify SNMP configuration, use any of the variations of the `show snmp` command.
Note! Only the first step is required, the rest are optional.
Note! By default, SNMP does not have any traps set. Without this command, SNMP managers must poll for all relevant information.

SNMPv3

SNMPv3 provides three security features: Message integrity and authentication, Encryption, Access control. SNMPv3 can be secured with the four steps.

Step 1: Configure an ACL to permit access to the protected management network.

```
Router(config)# ip access-list standard acl-name
Router(config-std-nacl)# permit source_net
```

Step 2: Configure an SNMP view.

```
Router(config)# snmp-server view view-name oid-tree
```

Step 3: Configure an SNMP group.

```
Router(config)# snmp-server group group-name v3 priv read view-name access [acl-
number | acl-name]
```

Step 4: Configure a user as a member of the SNMP group.

```
Router(config)# snmp-server user username group-name v3 auth {md5 | sha} auth-
password priv {des | 3des | aes {128 | 192 | 256}} privpassword
```

```
1 R1(config)# ip access-list standard PERMIT-ADMIN
2 R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
3 R1(config-std-nacl)# exit
4 R1(config)# snmp-server view SNMP-RO iso included
5 R1(config)# snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
6 R1(config)# snmp-server user BOB ADMIN v3 auth sha cisco12345 priv aes 128 cisco54321
7 R1(config)# end
```

line 1,2 The above example configures a standard ACL named PERMIT-ADMIN.

line 4 An SNMP view is named SNMP-RO and is configured to include the entire ISO tree from the MIB.

line 5 An SNMP group is configured with the name ADMIN. SNMP is set to version 3 with authentication and encryption required. The group is allowed read-only access to the view SNMP-RO. Access for the group is limited by the PERMIT-ADMIN ACL.

line 6 An SNMP user, BOB, is configured as a member of the group ADMIN. Authentication is set to use SHA, and an authentication password is configured. Although R1 supports up to AES 256 encryption, the SNMP management software only supports AES 128. Therefore, the encryption is set to AES 128 and an encryption password is configured.

16.3 SPAN

16.3.1 Introduction

A packet analyzer (such as Wireshark) is typically software that captures packets entering and exiting a network interface card (NIC). However, the basic operation of a modern switched network disables the packet analyzer ability to capture traffic from other sources. For instance, a user running Wireshark can only capture traffic going to their NIC.

The solution to this dilemma is to enable *port mirroring*. The port mirroring feature allows a switch to copy and send Ethernet frames from specific ports to the destination port connected to a packet analyzer. The Switched Port Analyzer (SPAN) feature on Cisco switches is a type of port mirroring. SPAN is commonly implemented to deliver traffic to specialized devices including: Packet analyzers and IPSs (Intrusion Prevention Systems).

There are three important things to consider when configuring SPAN:

- The destination port cannot be a source port, and the source port cannot be a destination port.

- The number of destination ports is platform-dependent. Some platforms allow for more than one destination port.
- The destination port is no longer a normal switch port. Only monitored traffic passes through that port.

Local SPAN is when traffic is mirrored to another port on the same switch. A SPAN session is the association between source ports (or VLANs) and a destination port. Traffic entering or leaving the source port (or VLAN) is replicated on the destination port.

Remote SPAN (RSPAN) allows source and destination ports to be in different switches. RSPAN uses two sessions. One session is used as the source and one session is used to copy or receive the traffic from a VLAN. The traffic for each RSPAN session is carried over trunk links in a user-specified RSPAN VLAN that is dedicated (for that RSPAN session) in all participating switches.

16.3.2 Configuration

```
S1(config)# monitor session 1 source interface f0/1
S1(config)# monitor session 1 destination interface f0/2
S1(config)# end
S1# show monitor
```

The above command is used to associate a source port and a destination port with a SPAN session. A separate `monitor session` command is used for each session. A VLAN can be specified instead of a physical port.

Figure 16.5: Verifying SPAN

```
S1# show monitor
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Fa0/1
Destination Ports      : Fa0/2
    Encapsulation      : Native
          Ingress      : Disabled
```

In the output of show command in Figure 16.5, the session number is 1, the source port for both traffic directions (receive and transmit) is F0/1, and the destination port is F0/2. The ingress SPAN is disabled on the destination port, so only traffic that leaves the destination port is copied to that port.

Chapter 17

Troubleshooting

17.1 Documentation

For network administrators to be able to monitor and troubleshoot a network, they must have a complete set of accurate and current network documentation. This documentation includes:

- Configuration files, including network configuration files and end-system configuration files
- Physical and logical topology diagrams
- A network baseline

17.1.1 Configuration files

Network configuration files contain accurate, up-to-date records of the hardware (routers, switches, cables etc.) and software (routing protocols, IOS, etc.) used in a network. End-system configuration files focus on the hardware and software used in end-system devices, such as servers, network management consoles, and user workstations. See also figures 17.1 and 17.2.

Figure 17.1: Network configuration file

Switch Information	Port	Speed	Duplex	STP	Port Fast	Trunk Status	Ether Channel L2 or L3	VLANs	Key
S1, Cisco WS-2960-24TT, 192.168.10.2/24, 2001:db6:acad:99::2, c2960-lanbasek9-mz.150-2.SE7.bin	G0/1	100 Gb/s	Auto	Fwd	No	On	None	1	Connects to R1
	F0/2	100 Mb/s	Auto	Fwd	Yes	No	None	1	Connects to PC1

Figure 17.2: End-system configuration file

Device Name, Purpose	Operating System	MAC Address	IP Address	Default Gateway
PC2	Windows 10	5475.D08E.9AD8	192.168.11.10 /24	192.168.11.1 /24
			2001:DB8:ACAD:11::10/64	2001:DB8:ACAD:11::1
SRV1	Linux	000C.D991.A138	192.168.20.254 /24	192.168.20.1 /24
			2001:DB8:ACAD:4::100/64	2001:DB8:ACAD:4::1

17.1.2 Topology diagrams

There are two types of network topology diagrams: the physical topology and the logical topology. A physical network topology shows the physical layout of the devices connected to the network. It is useful when troubleshooting physical layer problems. A logical network topology illustrates how devices are logically connected to the network, meaning how devices actually transfer data across the network when communicating with other devices. Symbols are used to represent network elements.

17.1.3 Network baseline

A baseline is used to establish normal network or system performance. Establishing a network performance baseline requires collecting performance data from the ports and devices that are essential to network operation. A network baseline helps:

- monitor network behavior
- keep track of the performance
- keep track of the traffic patterns
- check whether the current network design can meet business requirements
- measure the optimum nature of network traffic and congestion levels
- show the true nature of congestion or potential congestion in a network
- reveal areas in the network that are underutilized

To establish and capture an initial network baseline, perform the following steps:

1. Determine what types of data to collect
2. Identify devices and ports of interest
3. Determine the baseline duration (a baseline needs to last no more than six weeks, a two-to-four-week baseline is adequate.)

Baseline measurements should not be performed during times of unique traffic patterns, because the data would provide an inaccurate picture of normal network operations. Baseline analysis of the network should be conducted on a regular basis. Perform an annual analysis of the entire network or different sections of the network on a rotating basis. Analysis must be conducted regularly to understand how the network is affected by growth and other changes.

17.2 Troubleshooting process

17.2.1 General procedures

1. **Gather symptoms:** the network administrator determines which network components have been affected and how the functionality of the network has changed compared to the baseline.
2. **Isolate the problem:** Isolating is the process of eliminating variables until a single problem, or a set of related problems has been identified as the cause.
3. **Implement corrective action:** implementing, testing, and documenting possible solutions.

Gathering symptoms

There are five information gathering steps:

1. **Gather information:** Get information from trouble ticket or questioning users. Table 17.2.1 provides some guidelines and sample end-user question.
2. **Determine ownership:** If the problem is outside the boundary of the organization's control, contact an administrator for the external system.
3. **Narrow the scope:** Determine in which layer the problem occurs (core, distribution, or access layer).
4. **Gather symptoms from suspect devices:** Use a layered troubleshooting approach and Gather hardware and software symptoms. To gather symptoms, use Cisco IOS commands (ping, traceroute, telnet, show, debug) or packet captures, device logs.
5. **Document symptoms**

Guidelines	Sample questions
Ask questions that are pertinent to the problem	What does not work?
Questions that help eliminate or discover the possible problems	Are things that do work and the things that do not work related?
Speak at technical level that the user can understand	Has the thing that does not work ever worked?
Ask the user when the problem was first noticed	When was the problem first noticed?
Determine whether anything unusual since the last time it worked	What has changed since the last time it did work?
Recreate the problem	Can you reproduce the problem?
What happened before the problem occurred	When exactly does the problem occur?

Implement corrective action

The severity of the problem should be weighed against the impact of the solution. For example, if a critical server or router must be offline for a significant amount of time, it may be better to wait until the end of the workday to implement the fix. This is called **change-control procedures**.

If the corrective action creates another problem or does not solve the problem, the attempted solution is documented, the changes are removed, and the network administrator returns to gathering symptoms and isolating the issue.

17.2.2 Troubleshooting methods

Bottom-up you start with the physical components of the network and move up through the layers of the OSI model until the cause of the problem is identified. Bottom-up troubleshooting is a good approach to use when the problem is suspected to be a physical one.

Top-down starts with the end-user applications and moves down through the layers of the OSI model until the cause of the problem has been identified. Use this approach for simpler problems, or when you think the problem is with a piece of software. The disadvantage with the top-down approach is it requires checking every network application until the possible cause of the problem is found.

Divide-conquer The network administrator selects a layer and tests in both directions from that layer. You make an informed guess as to which OSI layer to start your investigation. When a layer is verified to be functioning properly, it can be assumed that the layers below it are functioning. The administrator can work up the OSI layers. If an OSI layer is not functioning properly, the administrator can work down the OSI layer model.

Educated guess The network administrator guesses the solution based on the symptoms of the problem. This method is more successfully implemented by seasoned network administrators, because seasoned network administrators rely on their extensive knowledge and experience to decisively isolate and solve network issues.

Comparison Comparing a working to a non-working situation involves comparing configurations, software versions, and hardware changes. The aim is to identify the changes that led to a non-working environment. Using this method may lead to a working solution, but without clearly revealing the cause of the problem. This method can be helpful when the network administrator is lacking an area of expertise, or when the problem needs to be resolved quickly. After the fix has been implemented, the network administrator can do further research on the actual cause of the problem.

Substitution involves swapping the problematic device with a known, working one. If the problem is fixed, that the network administrator knows the problem is with the removed device. If the problem remains, then the cause may be elsewhere. In specific situations, this can be an ideal method for quick problem resolution.

17.3 Using IP SLA

17.3.1 Introduction

Network engineers use IP SLAs to simulate network data and IP services to collect network performance information in real time. Multiple IP SLA operations may be configured on a device. There are additional benefits for using IP SLAs:

- Service-level agreement monitoring, measurement, and verification
- Network performance monitoring
- IP service network health assessment to verify that the existing QoS is sufficient for IP services
- Edge-to-edge network availability monitoring for proactive connectivity verification of network resources

Instead of using ping manually, a network engineer can use the IP SLA ICMP Echo operation to test the availability of network devices. The IP SLA ICMP Echo operation provides the following measurements:

- Availability monitoring (packet loss statistics)
- Performance monitoring (latency and response time)
- Network operation (end-to-end connectivity)

17.3.2 Configuration

To create an IP SLA operation and enter IP SLA configuration mode, use the `ip sla <operation-number>` global configuration command. From IP SLA configuration mode, you can configure the IP SLA operation as an ICMP Echo operation and enter ICMP echo configuration mode using the following command:

```
Router(config-ip-sla)# icmp-echo { dest-ip-address | dest-hostname }
[ source-ip { ip-address | hostname }
| source-interface interface-id ]
```

Next, set the rate at which a specified IP SLA operation repeats using the `frequency <seconds>` command. To schedule the IP SLA operation, use the following global configuration command:

```
Router(config)# ip sla schedule operation-number
                [ life { forever | seconds }]
                [ start-time { hh : mm [: ss ] [ month day | day month ]
                | pending | now | after hh:mm:ss ] [ ageout seconds ]
                [ recurring ]
```

17.3.3 Sample

The configuration below configures an IP SLA operation with an operation number of 1. Each operation can be referred to by its operation-number. The `icmp-echo` command identifies the destination address to be monitored. The frequency command is setting the IP SLA rate to 30 second intervals. The `ip sla schedule` command is scheduling the IP SLA operation number 1 to start immediately (now) and continue until manually cancelled (forever).

```
R1(config)# ip sla 1
R1(config-ip-sla)# icmp-echo 192.168.1.5
R1(config-ip-sla)# frequency 30
R1(config-ip-sla)# exit
R1(config)# ip sla schedule 1 start-time now life forever
```

17.4 Troubleshooting tools

17.4.1 Software

Network management system (NMS) includes device-level monitoring, configuration, and fault-management tools. These tools can be used to investigate and correct network problems.

Knowledge base is a vendor-based webpage that provides information on hardware and software. It contains troubleshooting procedures, implementation guides, and original white papers on most aspects of networking technology.

Baselining tools automate the network documentation and baselining process. For example, they can draw network diagrams, help keep network software and hardware documentation up-to-date, and help to cost-effectively measure baseline network bandwidth use.

Protocol analyzer useful to investigate packet content while flowing through the network. The information displayed by a protocol analyzer includes the physical, data link, protocol, and descriptions for each frame. Protocol analyzers such as Wireshark can help troubleshoot network performance problems, verify authentication, etc.

17.4.2 Hardware

Digital multimeters (DMMs) are test instruments that are used to directly measure electrical values of voltage, current, and resistance. We use them to check power supply voltage levels.

Cable testers are designed for testing data communication cabling. It can be used to detect broken wires, crossed-over wiring, shorted connections, and improperly paired connections. There is one type of cable testers called time-domain reflectometers (TDRs). These devices are used to pinpoint the distance to break in a cable.

Cable analyzers are used to test and certify copper and fiber cables. It can detect near-end crosstalk (NEXT), return loss (RL), etc.

Portable network analyzers are used for troubleshooting VLANs and switched networks. Using this device, the network engineer can view interface details, see which switch port is connected to which device, discover VLAN configuration, analyze network traffic, etc.

Network analysis module (NAM) provides embedded browser-based interface that generates report on the network resources. NAM can also capture and decode packets, track response time, etc.

17.5 Scenarios

Example 17.1. A network engineer is troubleshooting a network problem where users cannot access the FTP server at the same IP address where a website can be successfully accessed. Which troubleshooting method would be the best to apply in this case?

Proof. The fact that some application layer services provided by a network device are operating successfully but others are not means that the lower OSI or TCP/IP layers are functional with the problem likely to be in the application layer. Therefore, the troubleshooting method is *bottom-up*. □

Example 17.2. A network engineer is troubleshooting a network that has recently been updated with a new routing protocol, but the network is not working as expected. The engineer is comparing the running configuration from before and after the change was made. Which approach to troubleshooting the problem is the engineer using?

Proof. This is a variation on the divide-and-conquer method. Since a routing protocol change was recently made, the administrator can be fairly certain the issue resides with the network layer. □

Example 17.3. A company is setting up a web site with SSL technology to protect the authentication credentials required to access the web site. A network engineer needs to verify that the setup is correct and that the authentication is indeed encrypted. Which tool should be used?

Proof. To verify that the authentication is indeed encrypted, the authentication process needs to be captured and investigated, which can be accomplished through a protocol analyzer, such as Wireshark. □

Example 17.4. A user in a large office calls technical support to complain that a PC has suddenly lost connectivity to the network. The technician asks the caller to talk to nearby users to see if other machines are affected. The caller reports that several immediate neighbors in the same department have a similar problem and that they cannot ping each other. Those who are seated in other departments have connectivity. What should the technician check as the first step in troubleshooting the issue?

Proof. The status of the departmental workgroup switch in the wiring closet □

Example 17.5. A user reports that after an OS patch of the networking subsystem has been applied to a workstation, it performs very slowly when connecting to network resources. A network technician tests the link with a cable analyzer and notices that the workstation sends an excessive number of frames smaller than 64 bytes and also other meaningless frames. What is the possible cause of the problem?

Proof. The symptom of excessive runt packets and jabber is typically a Layer 1 issue, such as caused by a corrupted NIC driver, which could be the result of a software error during the NIC driver upgrade process. Note that A NIC driver is part of the operating system, it is not an application. □

Example 17.6. An internal corporate server can be accessed by internal PCs, but not by external Internet users that should have access. What could be the issue?

Proof. NAT/PAT allows a private IP address to be translated into a public address so that external users can access internal devices. Static NAT assigns one public address to a private address and is used with internal servers. □