
The Notebook
of
Connecting networks

HUY BUI



THE PUBLISHER

Contents

1	WAN concepts	5
1.1	WAN Technologies overview	5
1.1.1	Topology	5
1.1.2	Terminology	6
1.2	WAN connection	8
1.2.1	Private WAN Infrastructures	8
1.2.2	Public WAN Infrastructures	9
2	PPP	11
2.1	Introduction	11
2.2	Operation	11
2.2.1	Frame Structure	11
2.2.2	Establishing a PPP Session	12
2.2.3	LCP	12
2.2.4	NCP	13
2.2.5	Authentication	14
2.3	Configuration	14
3	PPPoE, GRE, eBGP	17
3.1	PPPoE	17
3.2	GRE	18
3.2.1	Introduction	18
3.2.2	Configuration	18
3.3	eBGP	19
3.3.1	Introduction	19
3.3.2	Configuration	20
4	ACL	21
4.1	ACL Operation Overview	21
4.1.1	ACEs Logic Operations	21
4.1.2	Inbound and Outbound ACL Logic	21
4.1.3	Numbered and Named ACLs	22
4.2	Standard ACL	22
4.2.1	Overview	22
4.2.2	Standard ACL placement	22
4.3	Extended ACLs	22
4.3.1	Overview	22
4.3.2	Extended ACL Placement	23
4.4	IPv6 ACLs	23
4.5	Configurations	24
4.6	Troubleshoot	26

5	Network Security and Monitoring	29
5.1	Security attacks	29
5.1.1	CDP Reconnaissance Attack	29
5.1.2	Telnet Attacks	29
5.1.3	MAC Address Table Flooding Attack	29
5.1.4	VLAN Attacks	29
5.1.5	DHCP Attacks	30
5.1.6	Cisco solution	30
5.1.7	The AAA framework	31
5.1.8	802.1X	31
5.2	SNMP	31
5.2.1	Introduction to SNMP	31
5.2.2	SNMP requests	31
5.2.3	SNMP Agent Traps	32
5.2.4	Community string and Object ID	32
5.2.5	Configuration	32
5.3	SPAN	34
5.3.1	Introduction	34
5.3.2	Configuration	35
6	Quality of Service	37
6.1	Introduction	37
6.1.1	Traffic characteristics	37
6.1.2	QoS tools	37
6.2	Congestion management	37
6.2.1	WFQ	38
6.2.2	CBWFQ	38
6.2.3	LLQ	39
6.3	QoS models	39
6.3.1	Best effort	39
6.3.2	Integrated services	39
6.3.3	Differentiated services	40
6.4	Classification and marking	41
6.4.1	Marking at Layer 2	41
6.4.2	Marking at Layer 3	41
6.5	Congestion Avoidance	43
7	Troubleshooting	45
7.1	Documentation	45
7.1.1	Configuration files	45
7.1.2	Topology diagrams	46
7.1.3	Network baseline	46
7.2	Troubleshooting process	46
7.2.1	General procedures	46
7.2.2	Troubleshooting methods	47
7.3	Using IP SLA	48
7.3.1	Introduction	48
7.3.2	Configuration	48
7.3.3	Sample	49
7.4	Troubleshooting tools	49
7.4.1	Software	49
7.4.2	Hardware	49
7.5	Scenarios	50

Chapter 1

WAN concepts

1.1 WAN Technologies overview

1.1.1 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.

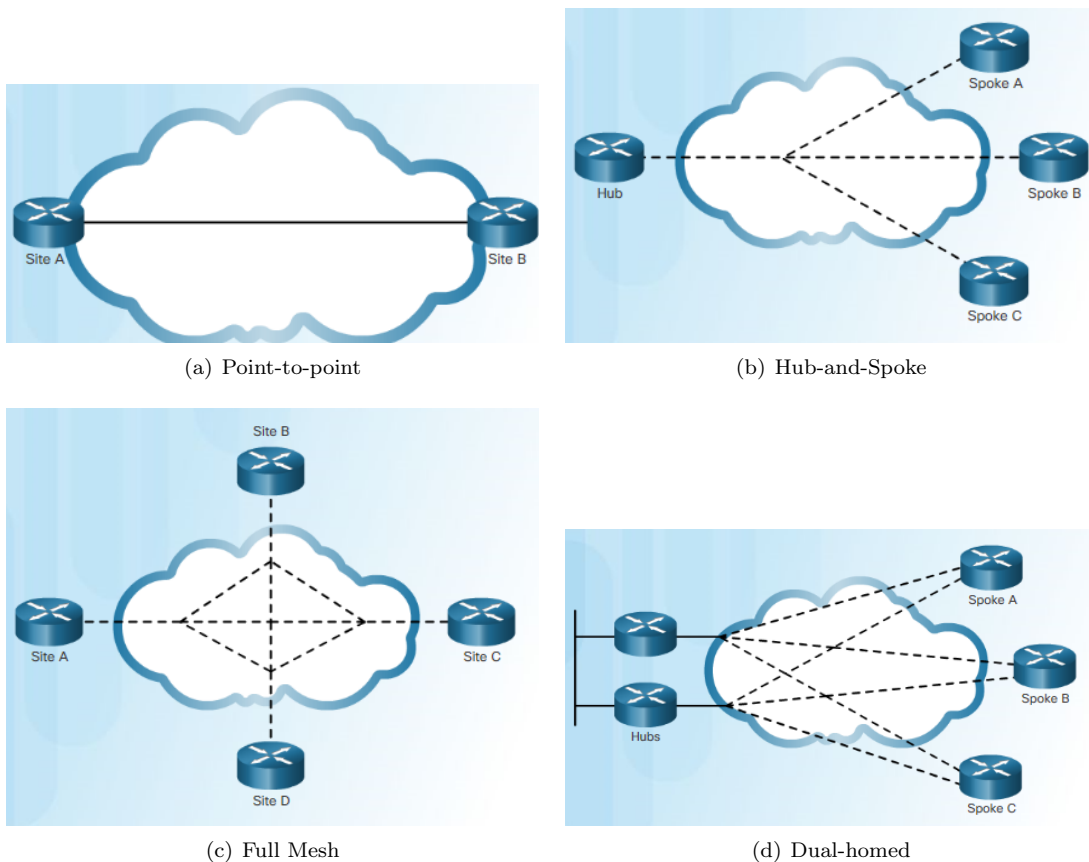


Figure 1.1: Four common WAN topologies

Point-to-Point topology employs a point-to-point circuit between two endpoints (Figure 1.1(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 1.1(b)).

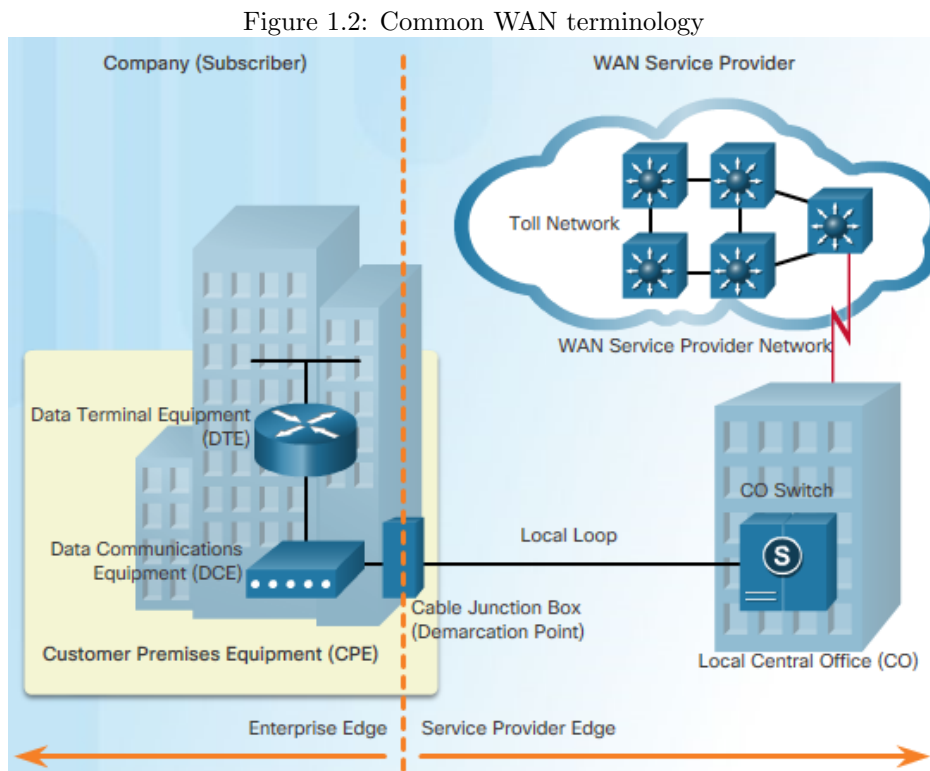
Full Mesh A disadvantage of the hub-and-spoke topology is that all communication has to go through the hub. With a full mesh topology using virtual circuits, any site can communicate directly with any other site (Figure 1.1(c)). A disadvantage is the large number of virtual circuits that need to be configured and maintained.

Dual-homed Topology Provides redundancy and load balancing, however more expensive to implement than single-homed topologies (Figure 1.1(d)). Requires additional networking hardware including routers and switches. More difficult to implement since they require complex configurations.

1.1.2 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 1.2):



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.

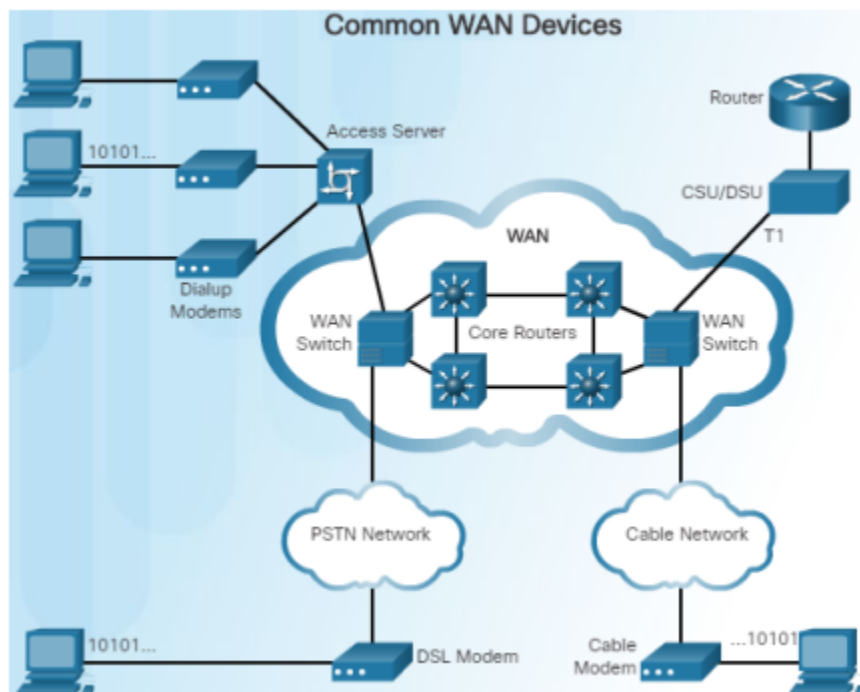
Local Loop (last mile) The actual copper or fiber cable that connects the CPE to the CO of the service provider.

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 1.3: 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**.

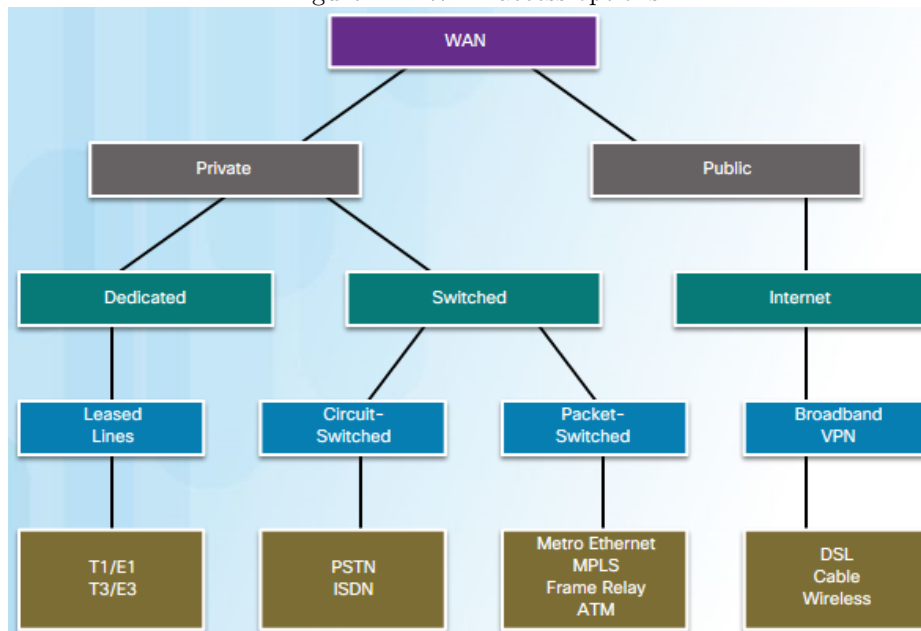
Packet Switching splits traffic data into packets packet that are routed over a shared network. A circuit does not need to be established and many pairs of nodes can communicate over the same channel. Packet switching costs less than circuit switching, however, latency and jitter are greater in packet-switching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

1.2 WAN connection

There are several WAN access connection options (figure 1.4) that ISPs can use to connect the local loop to the enterprise edge.

Figure 1.4: 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).

1.2.1 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.

1.2.2 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.

Chapter 2

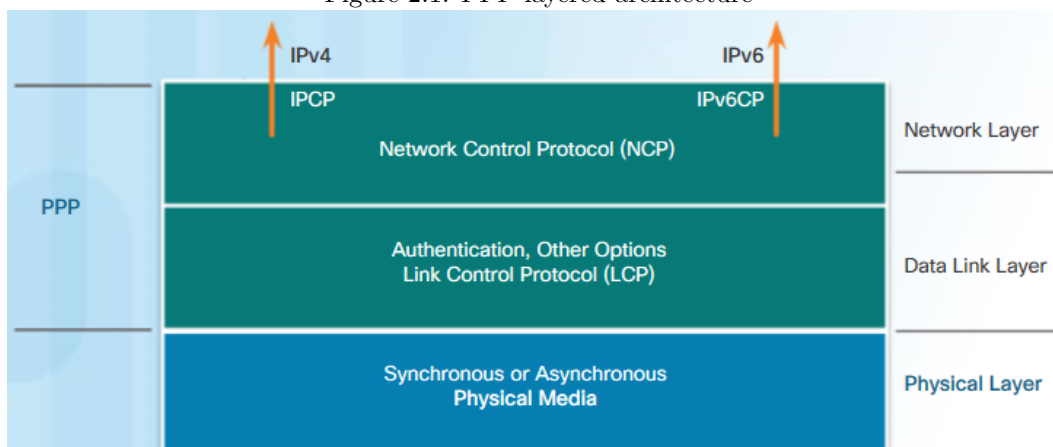
PPP

2.1 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 2.1: PPP layered architecture



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

Figure 2.1 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.

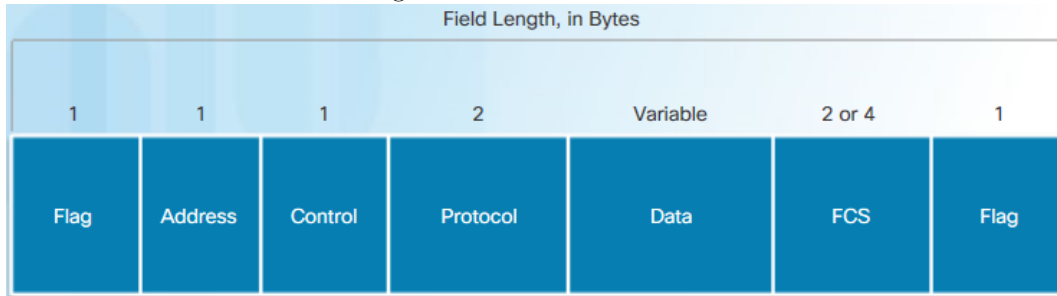
2.2 Operation

2.2.1 Frame Structure

A PPP frame consists of six fields. The following descriptions summarize the PPP frame fields illustrated in the figure 2.2:

- **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 2.2: 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.

2.2.2 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.

2.2.3 LCP

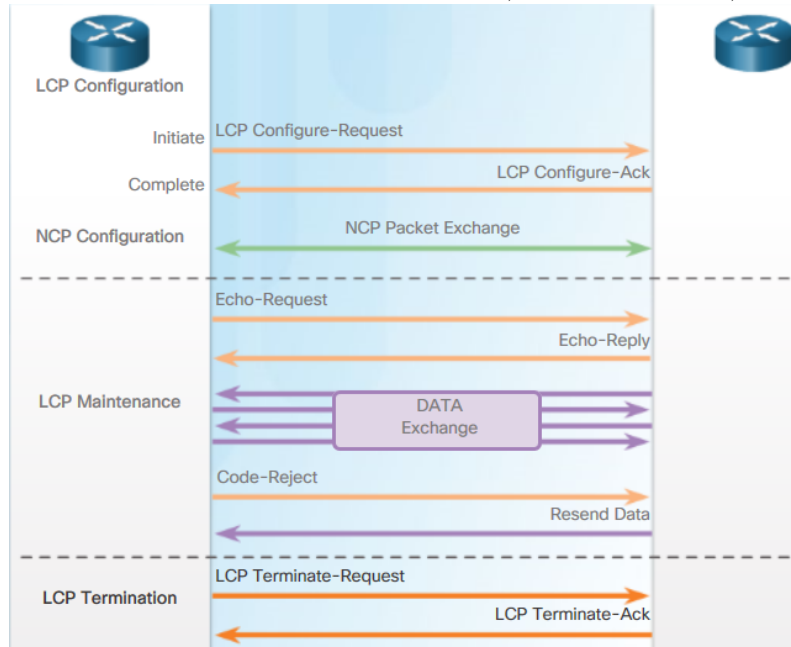
Link Control Protocol (LCP) operation uses three classes of LCP frames to accomplish the work of each of the LCP phases: Link-establishment → Link-maintenance → Link-termination (Figure 2.3).

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 2.3: 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 2.3. 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.

2.2.4 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.

2.2.5 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.

2.3 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> password <password>`. These 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 3

PPPoE, GRE, eBGP

3.1 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}
```

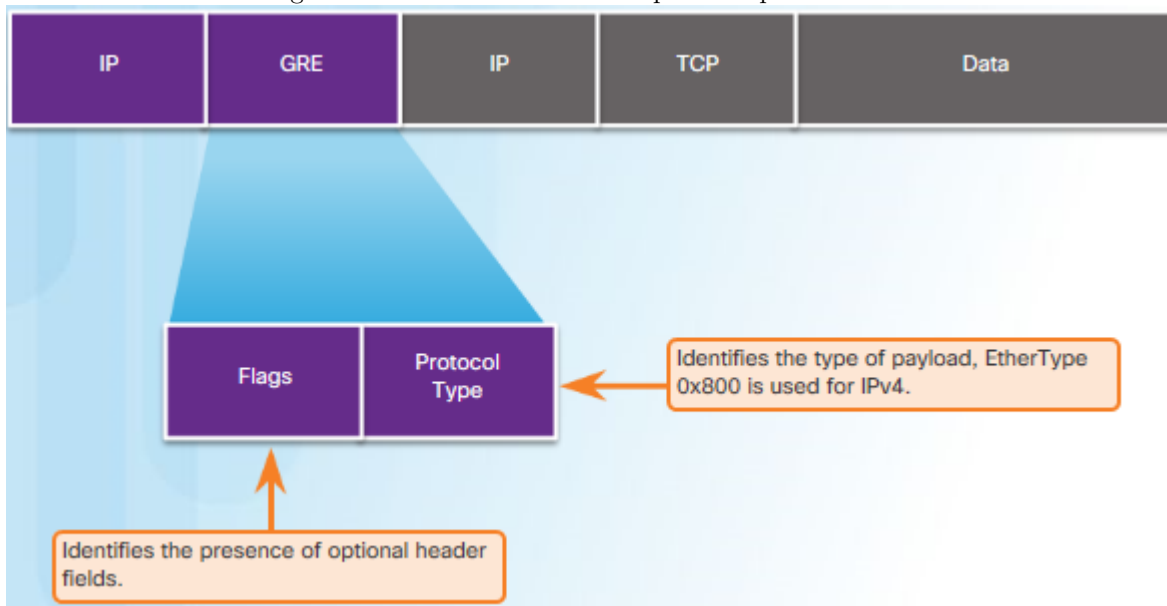
3.2 GRE

3.2.1 Introduction

GRE, IPsec, web-based SSL are the three methods of establishing a VPN connection offered by Cisco devices. GRE is an 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 3.1). 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.

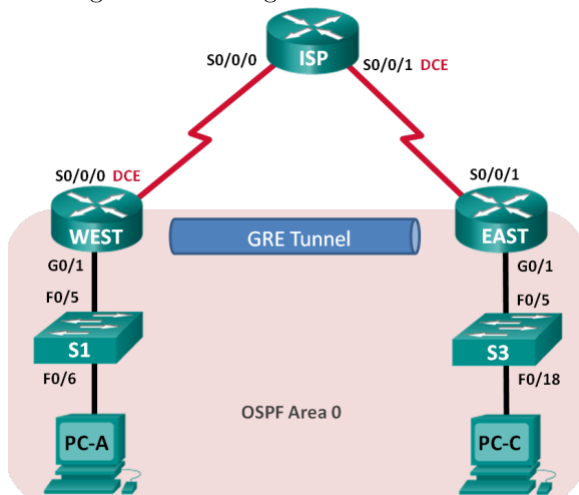
Figure 3.1: Header for GRE encapsulated packet header



3.2.2 Configuration

Five steps to configuring a GRE tunnel (figure 3.2):

Figure 3.2: 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 IP network of the tunnel, 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 IP network of the tunnel, 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
```

3.3 eBGP

3.3.1 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 IGP's. 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.

3.3.2 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 4

ACL

4.1 ACL Operation Overview

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

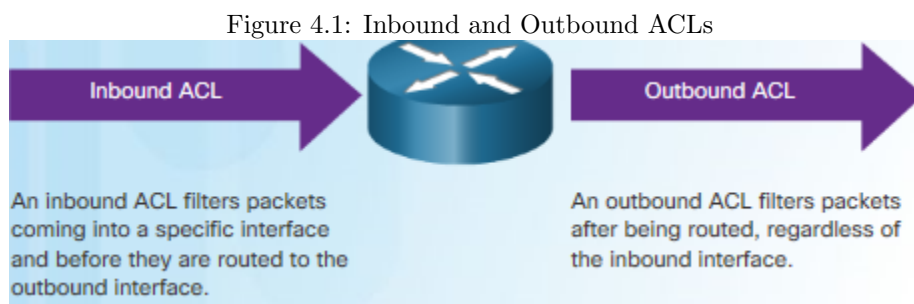
4.1.1 ACEs Logic Operations

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.

4.1.2 Inbound and Outbound ACL Logic

The Figure 4.1 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.



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.

4.1.3 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

4.2 Standard ACL

4.2.1 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.

4.2.2 Standard ACL placement

In the figure 4.2, 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.

4.3 Extended ACLs

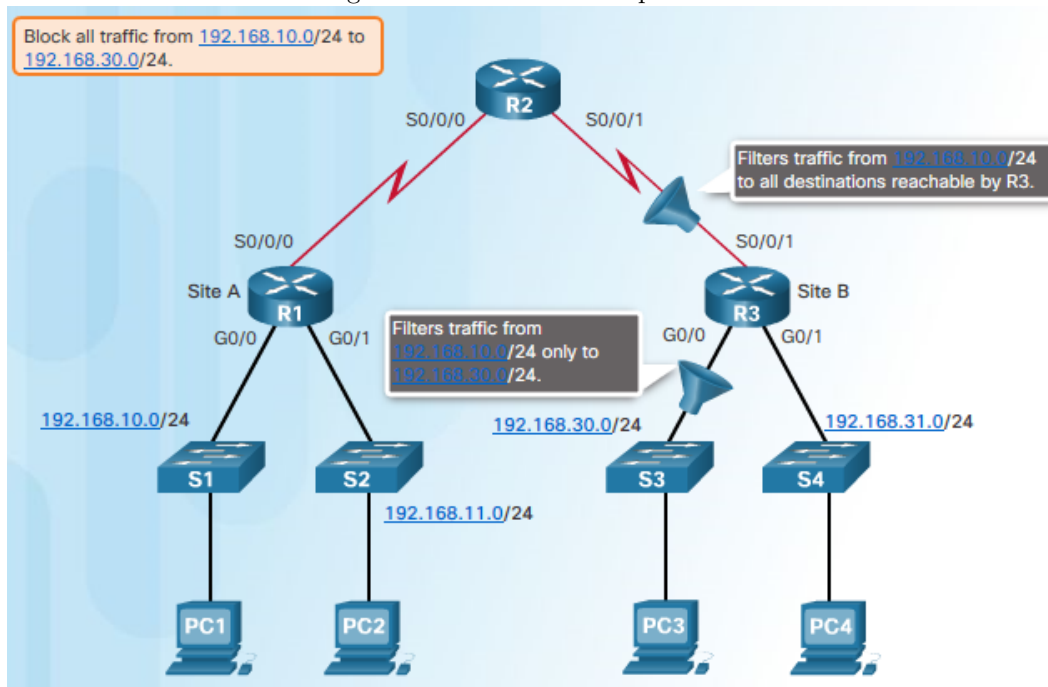
4.3.1 Overview

Extended ACLs filter packets based on:

- Protocol type (e.g. IP, ICMP, UDP, TCP)
- 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 to be filtered. This way, undesirable traffic is denied close to the source network without crossing the network infrastructure.

Figure 4.2: Standard ACL placement



4.3.2 Extended ACL Placement

In figure 4.3, 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.

4.4 IPv6 ACLs

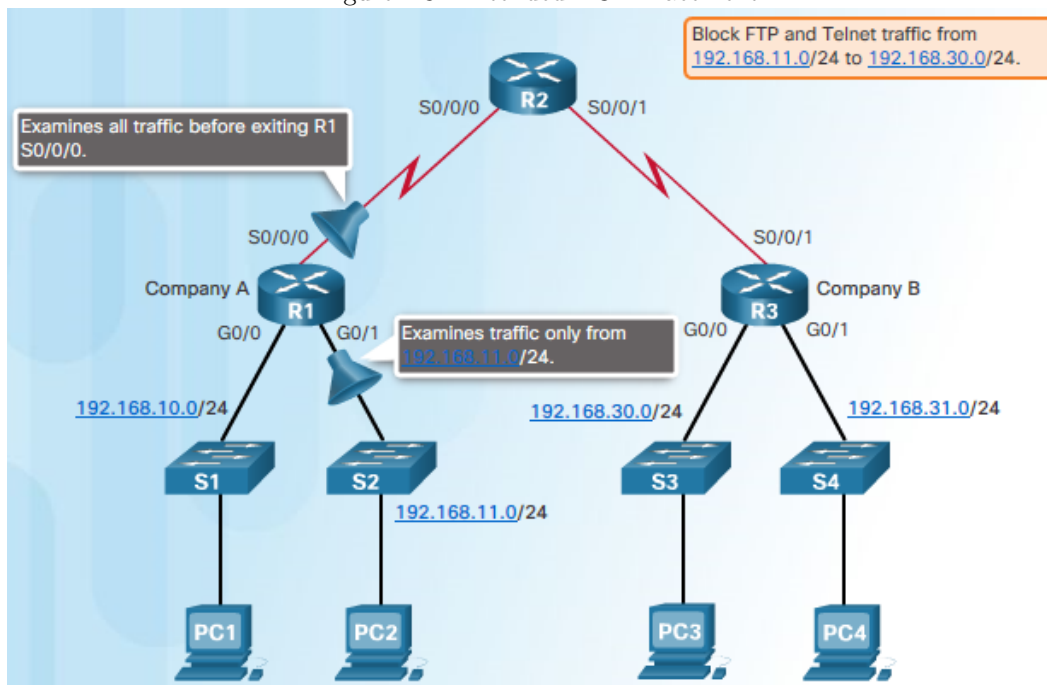
In IPv4 there are two types of ACLs, standard and extended and both types of ACLs can be either numbered or named ACLs. With IPv6, there is only one type of ACL, which is equivalent to an IPv4 extended named ACL and there are no numbered ACLs in IPv6.

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

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

Figure 4.3: Extended ACL Placement



- 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`

4.5 Configurations

Example 4.1. 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-if)# ip access-group 1 out
```

Example 4.2. 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 4.3. 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 4.4. 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.

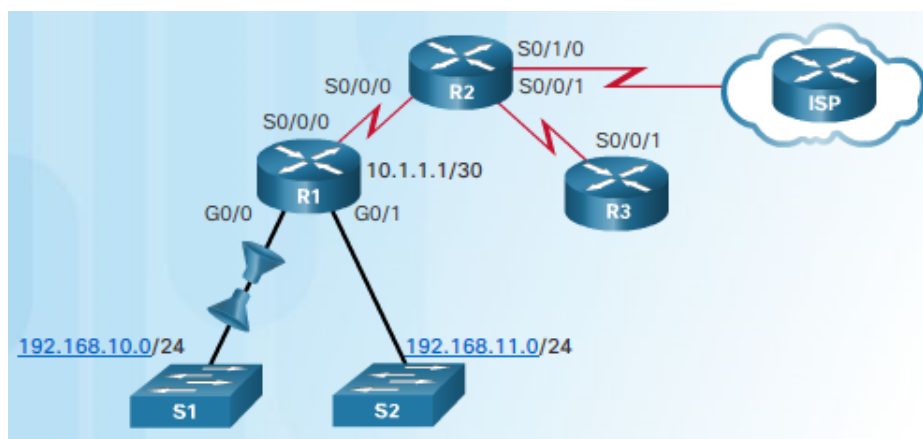
```
HQ(config)#ip access-list extended BranchServer
HQ(config-ext-nacl)#deny tcp any host 172.16.128.1 eq 80
HQ(config-ext-nacl)#deny tcp any host 172.16.128.1 eq 443
HQ(config-ext-nacl)#permit ip any any
HQ(config-ext-nacl)#exit
HQ(config)#int g0/0
HQ(config-if)#ip access-group HQServer in
```

Example 4.5. 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 BranchServer.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 4.6. 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 4.4) 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

Figure 4.4: 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 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 4.7. 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.

```
ip access-list extended INTOHQ
permit tcp any host 172.16.10.5 eq 53
permit udp any host 172.16.10.5 eq 53
permit tcp any host 172.16.10.10 eq 80
permit tcp any any established
exit
interface s0/0/0
ip access-group INTOHQ IN
exit
```

Example 4.8. Configure an extended ACL named SNMPACCESS such that

- 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.

```
ip access-list extended SNMPACCESS
permit udp host 192.168.10.5 host 192.168.10.1 eq 161
deny udp any host 192.168.10.1 eq 161
permit ip any any
exit
interface g0/0
ip access-group SNMPACCESS in
exit
```

4.6 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 4.9. 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
```

Solution: 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 4.10. 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.

Chapter 5

Network Security and Monitoring

5.1 Security attacks

5.1.1 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.

5.1.2 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.

5.1.3 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.

5.1.4 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:

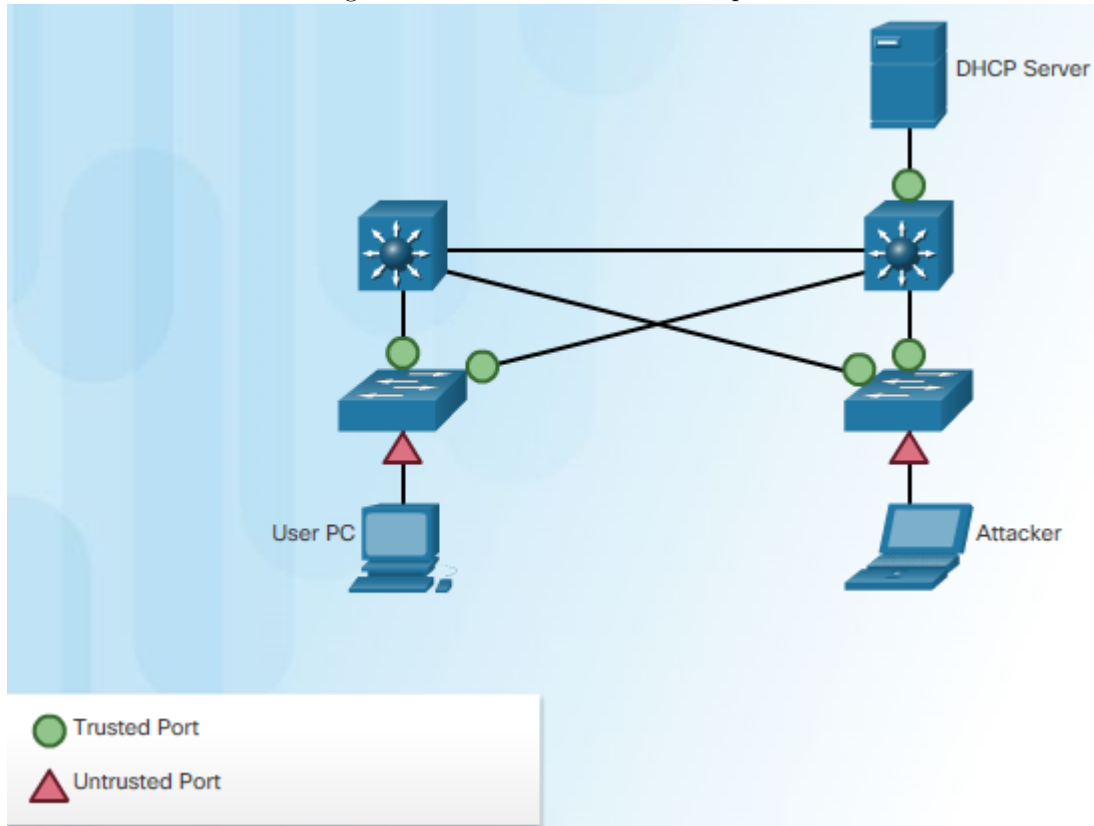
- Disable DTP negotiations on non-trunking ports using the `switchport nonegotiate` interface configuration command.
- Manually enable the trunk link using the `switchport mode trunk` interface configuration command.
- Manually enable access ports using the `switchport mode access` interface configuration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

5.1.5 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 attack¹ as new clients cannot obtain network access.

Figure 5.1: Trusted and Untrusted ports



DHCP snooping recognizes two types of ports (see figure 5.1):

- **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.

5.1.6 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

¹A 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.

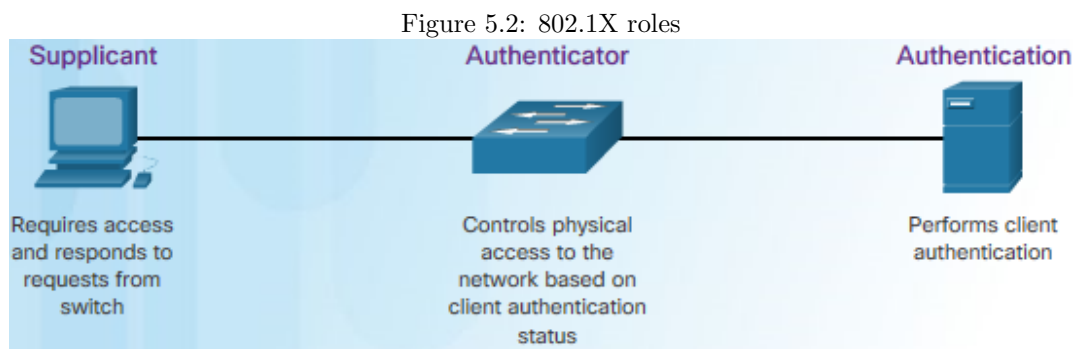
5.1.7 The AAA framework

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.

5.1.8 802.1X

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.



With 802.1X port-based authentication, the devices in the network have specific roles, as shown in the figure 5.2:

- **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.

5.2 SNMP

5.2.1 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

5.2.2 SNMP requests

The SNMP manager uses the get and set actions to perform the operations, as described in the Figure 5.3.

Figure 5.3: SNMP operations

Operation	Description
<code>get-request</code>	Retrieves a value from a specific variable.
<code>get-next-request</code>	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.
<code>get-bulk-request</code>	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.)
<code>get-response</code>	Replies to a <code>get-request</code> , <code>get-next-request</code> , and <code>set-request</code> sent by an NMS.
<code>set-request</code>	Stores a value in a specific variable.

5.2.3 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.

5.2.4 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 5.4).

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.

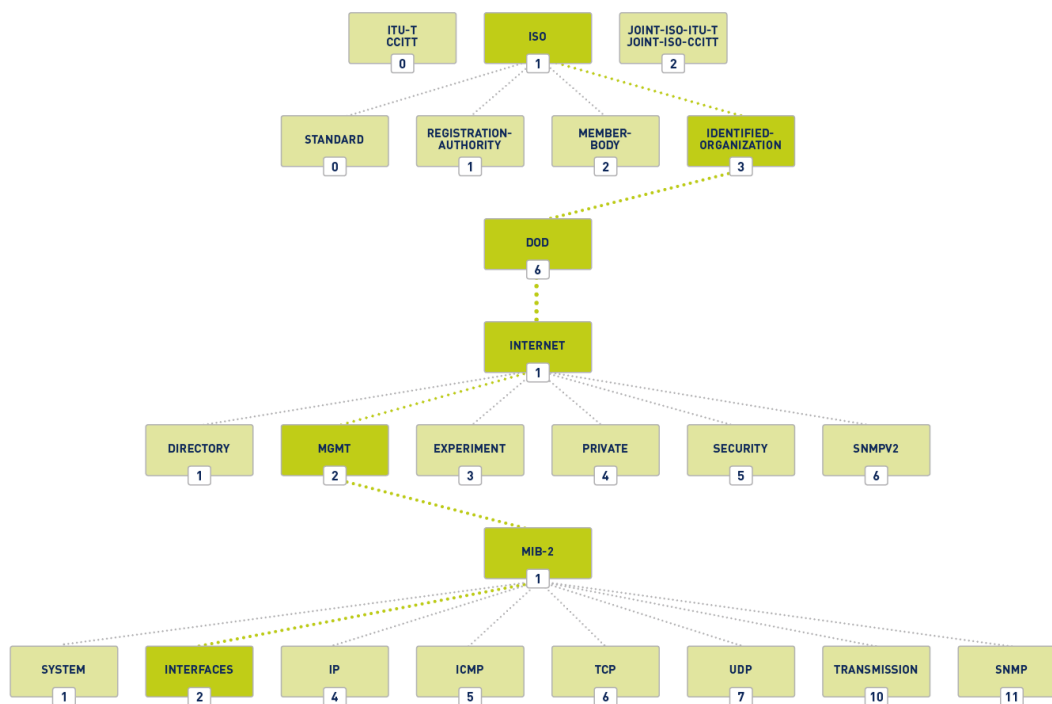
5.2.5 Configuration

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 5.4: 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 host host-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.

5.3 SPAN

5.3.1 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.

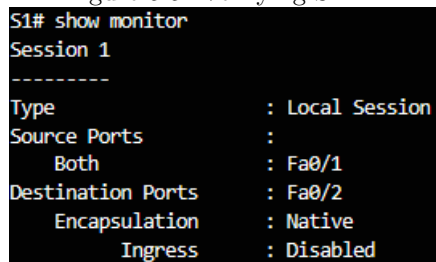
Remote SPAN (RSPAN) allows source and destination ports to be in different switches. RSPAN uses two sessions. One session is used as the source and one session is used to copy or receive the traffic from a VLAN. The traffic for each RSPAN session is carried over trunk links in a user-specified RSPAN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

5.3.2 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 5.5: 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 5.5, 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 6

Quality of Service

6.1 Introduction

6.1.1 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.

6.1.2 QoS tools

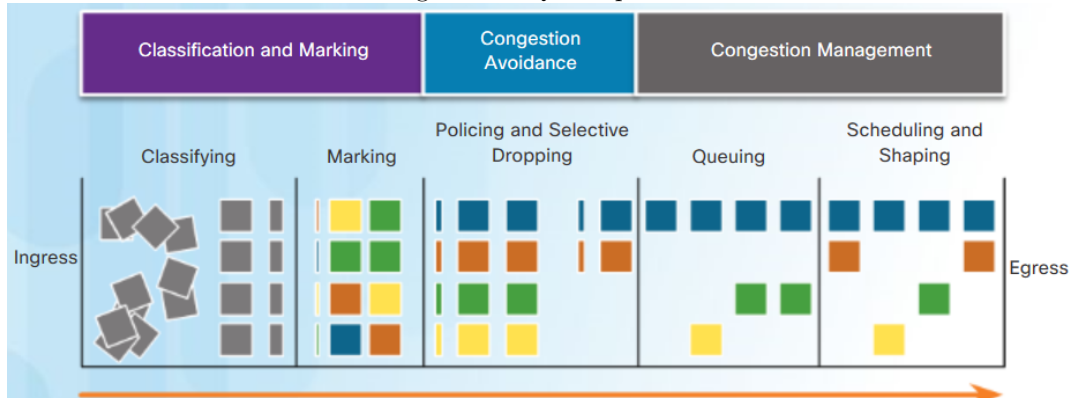
When the volume of traffic is greater than what can be transported across the network, network devices (router, switch, etc.) hold the packets in memory until resources become available to transmit them. If the number of packets continues to increase, the memory within the device fills up and packets 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 6.1 to help understand the sequence of how these tools are used when QoS is applied to packet flows.

6.2 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 6.1: QoS sequence

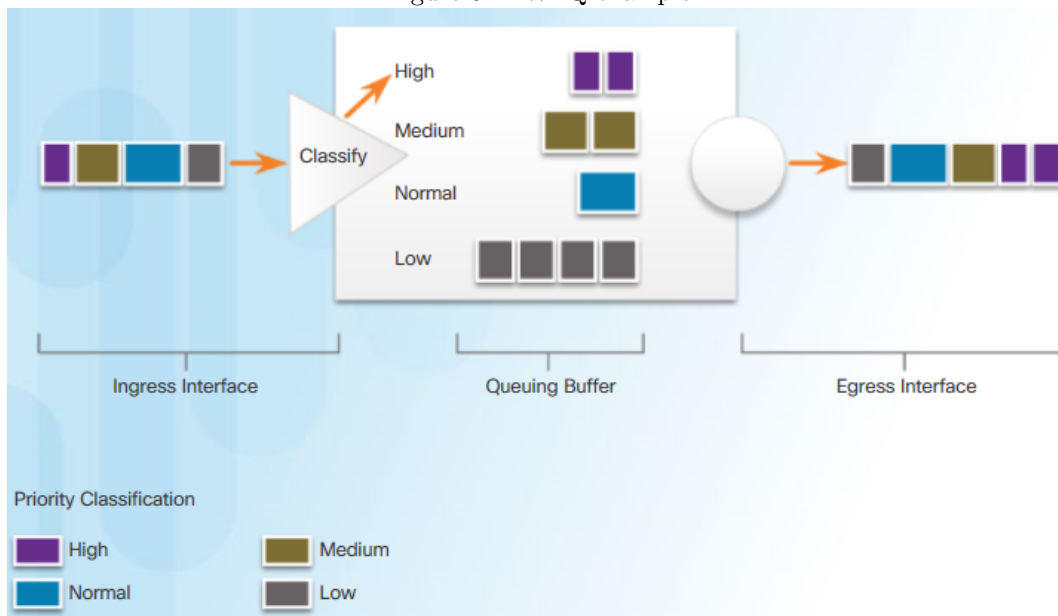


6.2.1 WFQ

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 6.2. WFQ then determines how much bandwidth each flow is allowed. WFQ classifies traffic into different flows based on packet header addressing.

Figure 6.2: WFQ example



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

6.2.2 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.

6.2.3 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.

6.3 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.

6.3.1 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 6.1 lists the benefits and drawbacks of the best effort model.

Table 6.1: 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

6.3.2 Integrated services

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

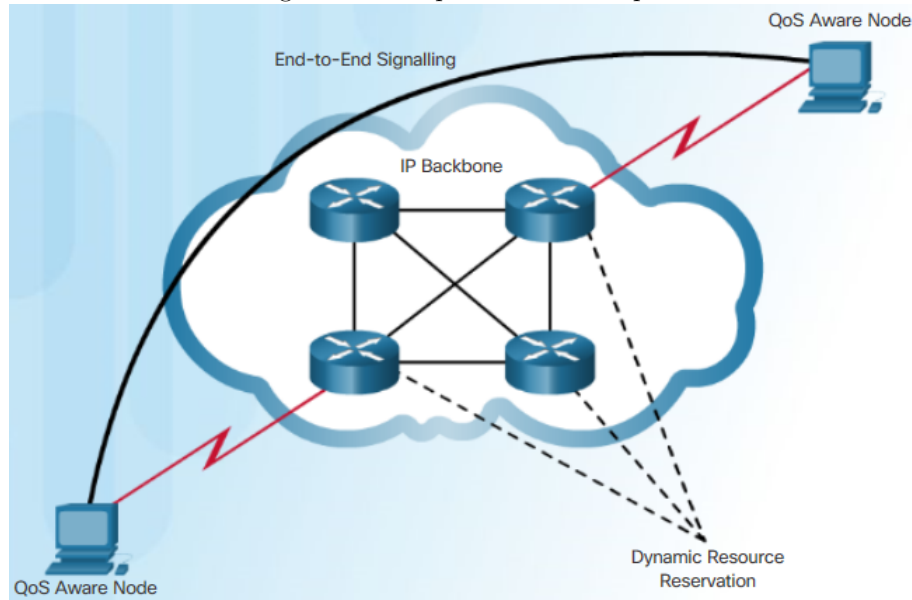
It uses resource reservation and admission-control mechanisms as building blocks to establish and maintain QoS. Each individual communication must explicitly specify its traffic descriptor and requested resources to the network (Figure 6.3). The edge router performs admission control to ensure that available 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 6.2: 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	

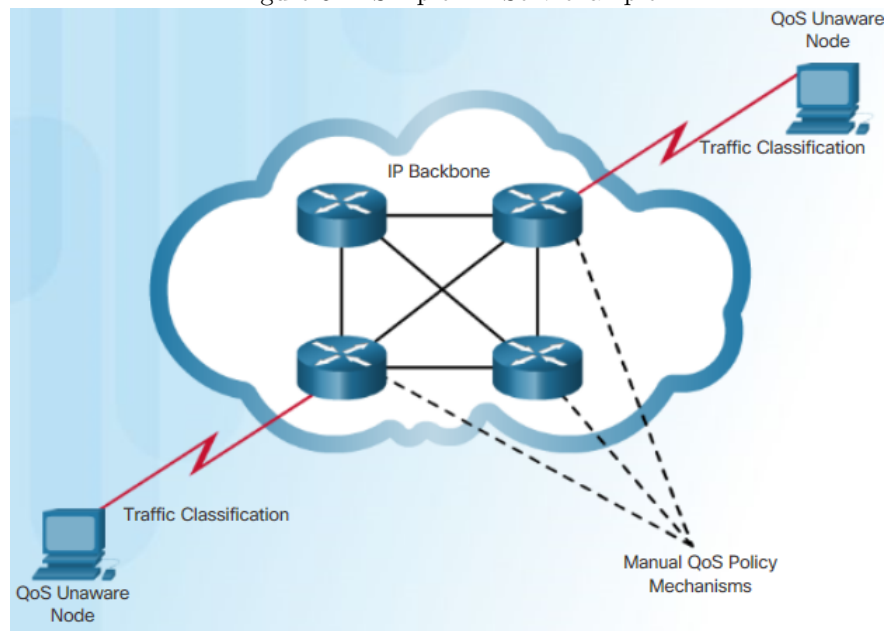
Figure 6.3: Simple IntServ example



6.3.3 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 6.4). 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 6.4: 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 6.3: Pros and Cons of DiffServ

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

6.4 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.

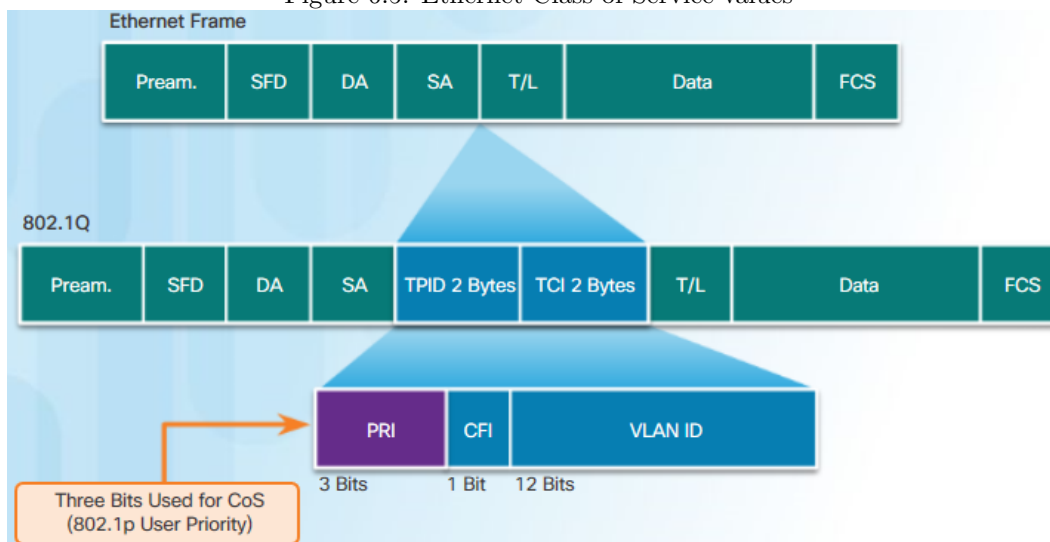
Trusted endpoints have the capabilities and intelligence to mark application traffic to the appropriate Layer 2 CoS and/or Layer 3 DSCP values. Examples of trusted endpoints include IP phones, wireless access points, videoconferencing gateways and systems, IP conferencing stations, and more.

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

6.4.1 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 6.5). Known as the Priority (PRI) field, this 3-bit field identifies the Class of Service (CoS) markings.

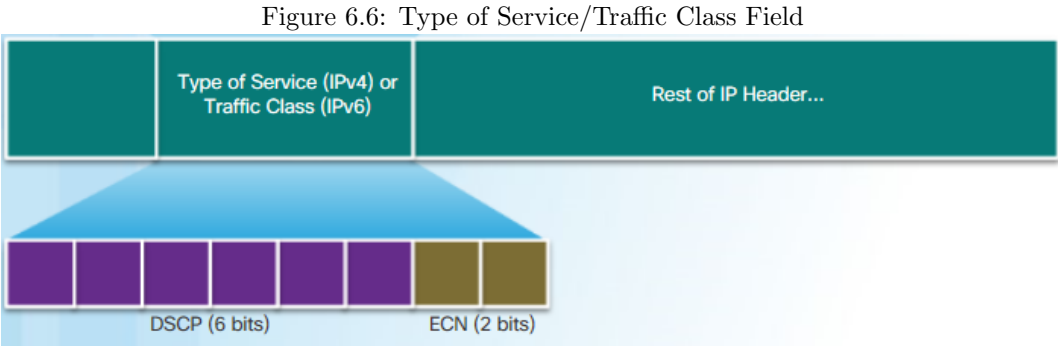
Figure 6.5: Ethernet Class of Service values



6.4.2 Marking at Layer 3

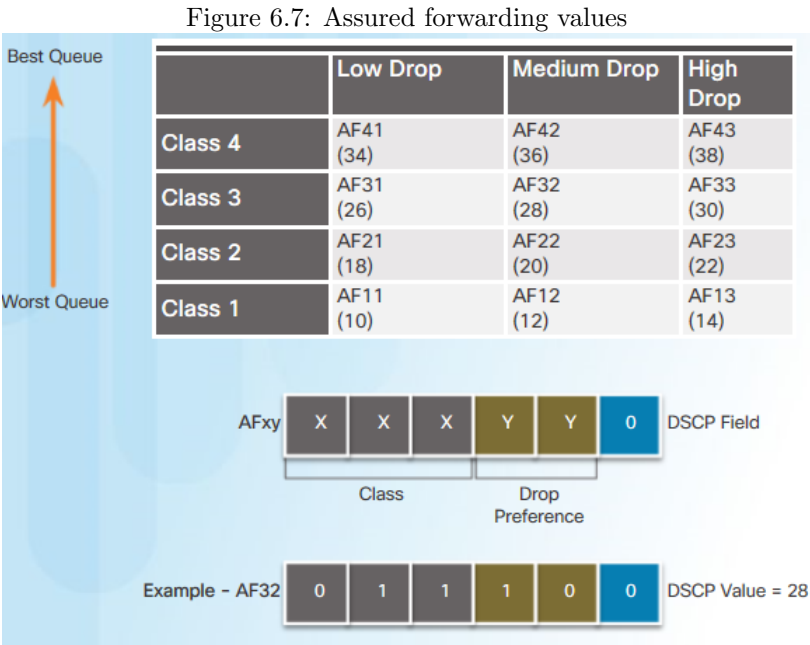
The benefit of deploying Layer 3 marking is that it can carry QoS information end-to-end unlike Layer 2 marking, which changes frame header as well as QoS information hop by hop.

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 6.6 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.



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 6.7, 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).



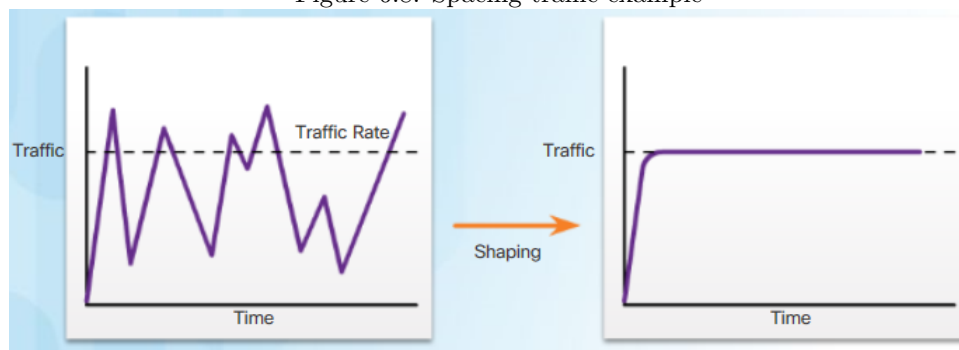
6.5 Congestion Avoidance

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.

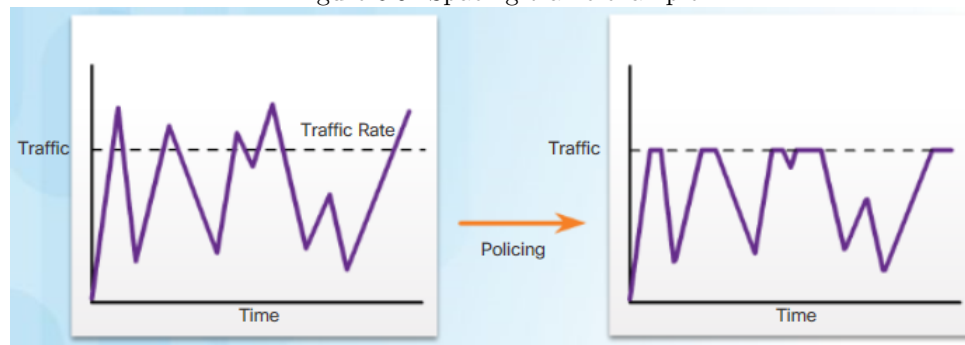
Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. The result of traffic shaping is a smoothed packet output rate, as shown in Figure 6.8. Ensure that you have sufficient memory when enabling shaping.

Figure 6.8: 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 6.9.

Figure 6.9: Spacing traffic example



Chapter 7

Troubleshooting

7.1 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

7.1.1 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 7.1 and 7.2.

Figure 7.1: 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 7.2: 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

7.1.2 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.

7.1.3 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.

7.2 Troubleshooting process

7.2.1 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 7.2.1 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.

7.2.2 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.

7.3 Using IP SLA

7.3.1 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)

7.3.2 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 ]
```

7.3.3 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
```

7.4 Troubleshooting tools

7.4.1 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.

7.4.2 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.

7.5 Scenarios

Example 7.1. 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 7.2. 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 7.3. 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 7.4. 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 7.5. 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 7.6. 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. □