CCNAX

Interconnecting Cisco Networking Devices: Accelerated

Student Guide Volume 4

Version 3.0

Part Number: 97-3639-01

Americas Headquarters	Asia Pacific Headquarters	Europe Headquarters
Cisco Systems, Inc. San Jose, CA	Cisco Systems (USA) Pte. Ltd. Singapore	Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Table of Contents

Module 11: Implementing Wide-Area Networks

Introduction

WANs are most often fee-for-service networks, providing the means for users to access resources across a wide geographical area. Some services are considered Layer 2 connections between your remote locations, typically provided by a telco over its WAN switches. Some of these technologies include a serial point-to-point (leased line) connection and Frame Relay connections.

Other connections leverage the Internet infrastructure, a Layer 3 alternative, to interconnect the remote locations of an organization. To provide security across the public Internet, you can implement a VPN solution.

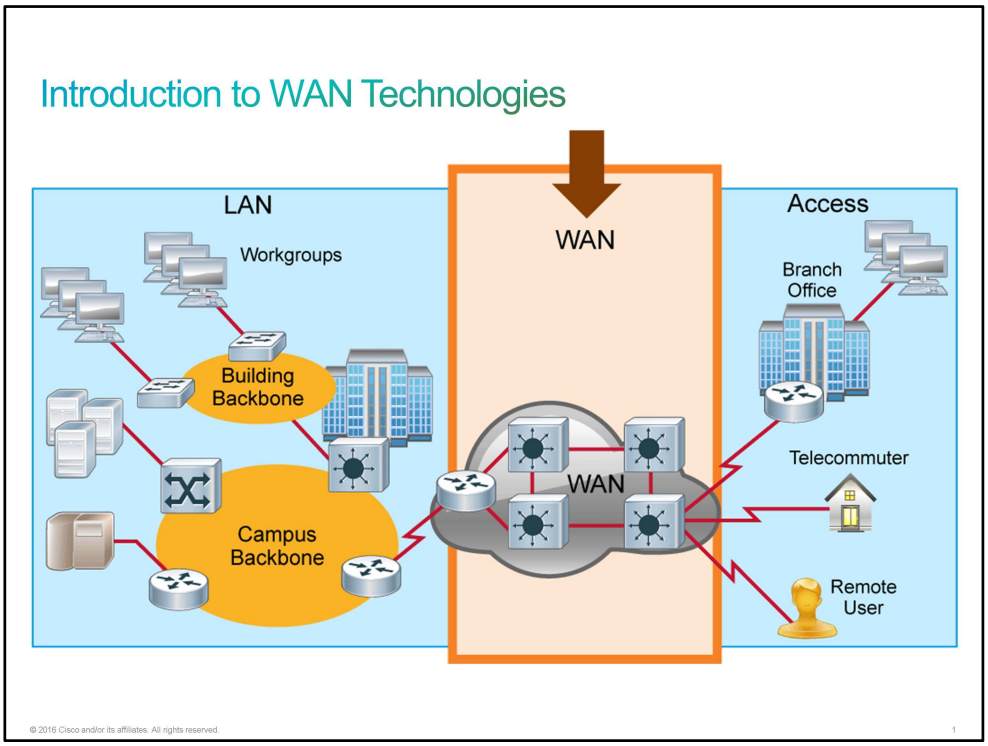
Lesson 1: Understanding WAN Technologies

Introduction

In order to continue to advance in your career, you have asked Bob if you can get more involved in WAN deployments. Although Bob is glad that you want to expand your skills and knowledge, he wants to assess your level of preparedness before taking you with him on WAN deployment jobs. To gauge your level of preparedness for WAN deployments, CCS provides a test. Bob tells you that the test will require you to demonstrate your knowledge of WAN devices, WAN cabling, WAN protocols, and WAN technologies.

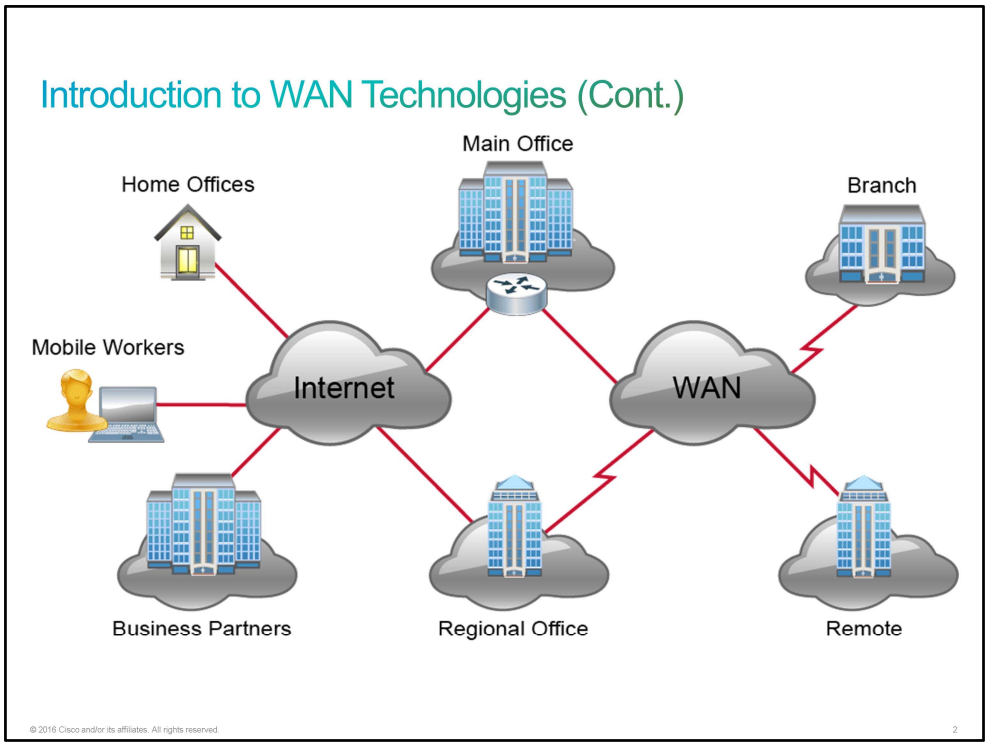
Introduction to WAN Technologies

A WAN is a data communications network that operates beyond the geographic scope of a LAN. WANs use facilities that a service provider or carrier, such as a telephone or cable company, provide. They connect the locations of an organization to each other, to locations of other organizations, to external services, and to remote users. WANs carry various traffic types such as voice, data, and video.



The following are three major characteristics of WANs:

- WANs generally connect devices that are separated by a broader geographic area than a LAN can serve.
- WANs use the services of carriers such as telcos, cable companies, satellite systems, and network providers.
- WANs use connections of various types to provide access to bandwidth over large geographic areas.



There are several reasons why WANs are necessary in a communications environment.

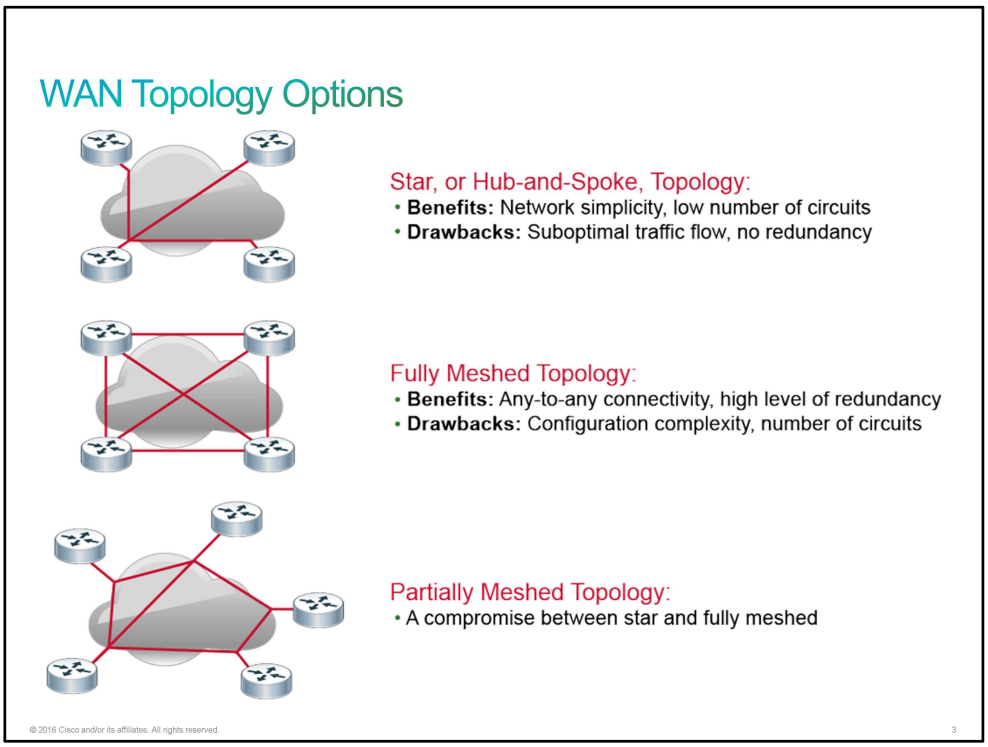
LAN technologies provide speed and cost efficiency for the transmission of data in organizations in relatively small geographic areas. You need WANs in a communications environment because some business needs require communication among remote sites for many reasons, including the following:

- People in the regional or branch offices of an organization need to be able to communicate and share data.
- Organizations often want to share information with other organizations across large distances.
- Employees who travel on company business frequently need to access information that resides on their corporate networks.

Because it is not feasible to connect computers across a country or around the world in the same way that computers are connected in a LAN environment with cables, different technologies have evolved to support this need. Increasingly, the Internet is being used as an inexpensive alternative to an enterprise WAN for some applications.

WAN Topology Options

A physical topology describes the physical arrangement of network devices that allow for data to move from a source to a destination network. There are three basic topologies for a WAN design.



Star or hub-and-spoke topology: This topology features a single hub (central router) that provides access from remote networks to a core router. All communication among the networks goes through the core router. The advantages of a star approach are simplified management and minimized tariff costs. However, the disadvantages are significant:

- The central router (hub) represents a single point of failure.
- The central router limits the overall performance for access to centralized resources. The central router is a single pipe that manages all traffic that is intended either for the centralized resources or for the other regional routers.

Fully meshed topology: In this topology, each routing node on the periphery of a given packet-switching network has a direct path to every other node on the cloud. The key rationale for creating a fully meshed environment is to provide a high level of redundancy. A fully meshed topology is not viable in large packet-switched networks. The following are the key issues of a fully meshed topology:

- Many virtual circuits are required (one for every connection between routers).
- Configuration is complex for routers without multicast support in nonbroadcast environments.

Partially meshed topology: This topology reduces the number of routers within a region that have direct connections to all other nodes in the region. All nodes are not connected to all other nodes. There are many forms of partially meshed topologies. In general, partially meshed approaches provide the best balance for regional topologies, which are based on the number of virtual circuits, redundancy, and performance.

Note	Large networks usually deploy a layered combination of these technologies—for example, a partial mesh in the network core, redundant hub-and-spoke for larger branches, and simple hub-and-spoke for noncritical remote locations.

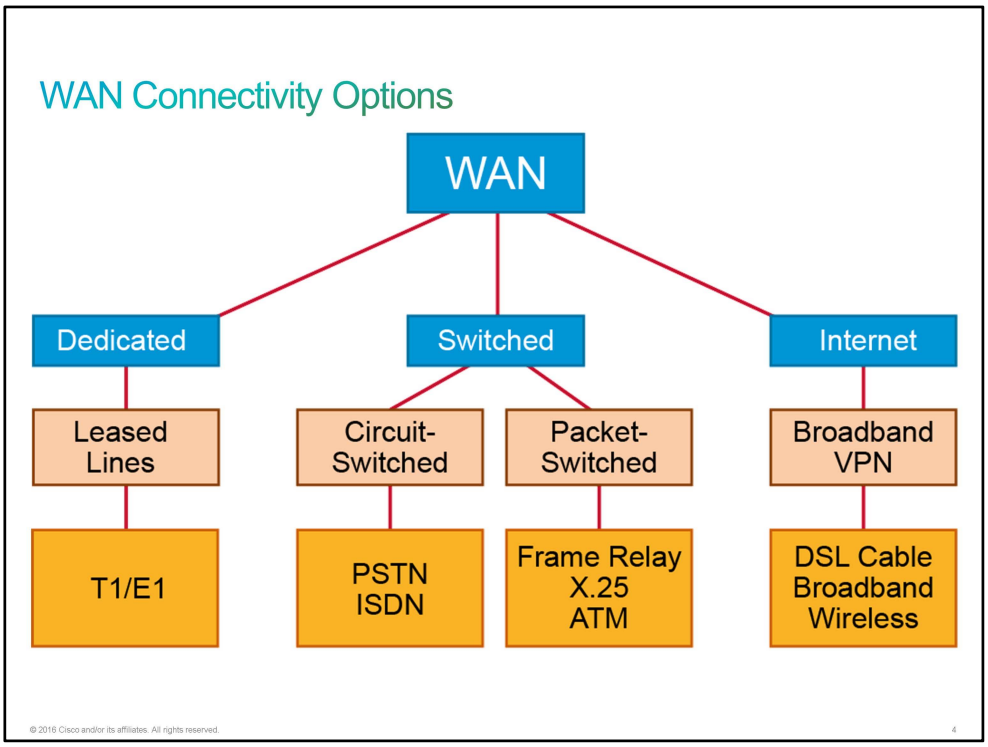
Network downtime can be very expensive in terms of decreased productivity and potential loss of revenue. To increase network availability, many organizations deploy a dual-carrier WAN design to increase redundancy and path diversity.

Single-carrier WANs are simpler and easier to support and manage. However, network outages can be catastrophic. You should perform an analysis of the downtime cost. You should make sure that there are adequate penalties in the contract with the service provider to cover the cost of downtime.

Dual-carrier WANs provide better path diversity with better fault isolation between providers. The cost of downtime to your organization usually exceeds the additional cost of the second provider and the complexity of managing redundancy.

WAN Connectivity Options

You have many options for implementing WAN solutions currently available. They differ in technology, speed, and cost. WAN connections can be either over a private infrastructure or over a public infrastructure such as the Internet.

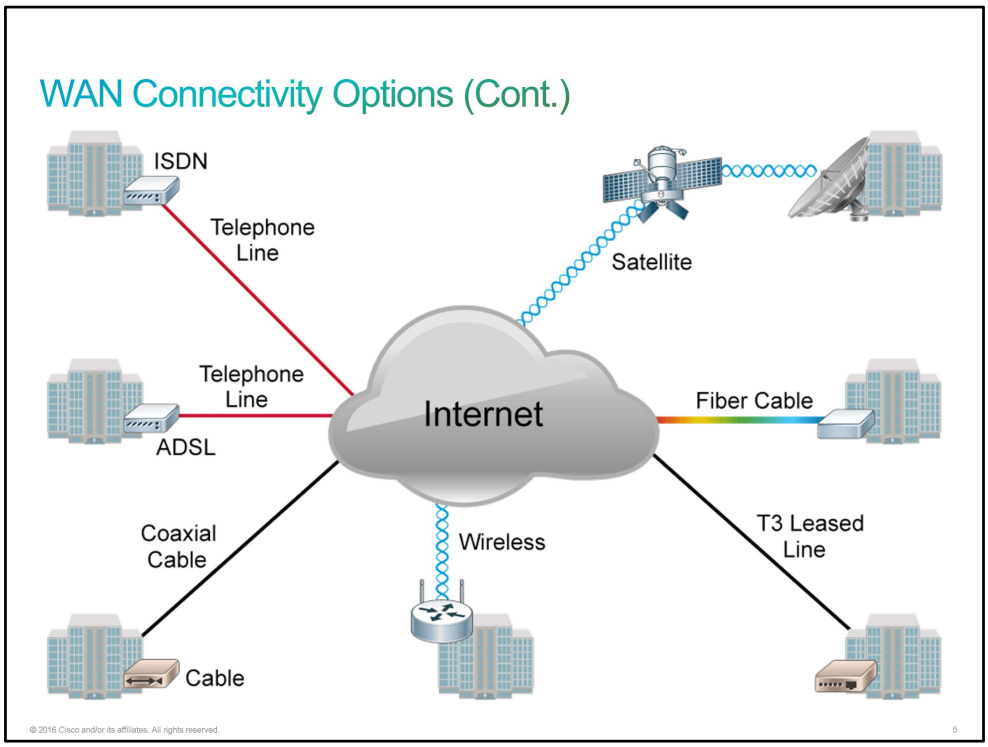


Private WAN connections include dedicated and switched communication link options:

- **Dedicated communication links:** When permanent dedicated connections are required, point-to-point lines are used with various capacities that are limited only by the underlying physical facilities and the willingness of users to pay for these dedicated lines. A point-to-point link provides a pre-established WAN communications path from the customer premises through the provider network to a remote destination. You usually lease point-to-point lines from a carrier, so they are also called leased lines. Leased lines were more popular in the past. Now companies rather use provider-managed VPN or enterprise-managed VPN over Internet. Companies prefer enterprise- or provider-managed VPNs because leased lines are by far the most expensive solution.
- **Switched communication links:** Switched communication links can be either circuit-switched or packet-switched.
  - **Circuit-switched communication links:** Circuit switching dynamically establishes a dedicated virtual connection for voice or data between a sender and a receiver. Before communication can start, the connection through the network of the service provider must be established. Examples of circuit-switched communication links are analog dialup (PSTN) and ISDN.
  - **Packet-switched communication links:** Many WAN users do not make efficient use of the fixed bandwidth that is available with dedicated, switched, or permanent circuits because the data flow fluctuates. Communications providers have data networks that are available to more appropriately service these users. In packet-switched networks, the data is transmitted in labeled frames, cells, or packets. Packet-switched communication links include Frame Relay, ATM, and X.25.

Public connections use the global Internet infrastructure. Now companies use provider-managed VPNs or enterprise-managed VPNs over Internet. Until recently, the Internet was not a viable networking option for many organizations because of the significant security risks and lack of adequate performance guarantees in an end-to-end Internet connection. With the development of the VPN technology, however, the Internet is now an inexpensive and secure option for connecting to teleworkers and remote offices where performance guarantees are not critical. Internet WAN connection links go through broadband services such as DSL, cable modem, and broadband wireless, and they are combined with VPN technologies (for example, DMVPN, GET VPN) to provide privacy across the Internet. Broadband connection options are typically used to connect telecommuting employees to a corporate site over the Internet.

Service providers build networks using different underlying technologies, the most popular being MPLS. Examples of provider-managed VPNs are Layer 3 MPLS VPN and Layer 2 MPLS VPNs (VPWS and VPLS). MPLS is an IETF standard that defines a packet label-based switching technique, which was originally devised to perform fast switching in the core of IP networks. This technique helped carriers and large enterprises scale their networks as increasingly large routing tables become more complex to manage. The industry began using MPLS over a decade ago as a way to allow enterprises to create end-to-end circuits across any type of transport medium using any available WAN technology.

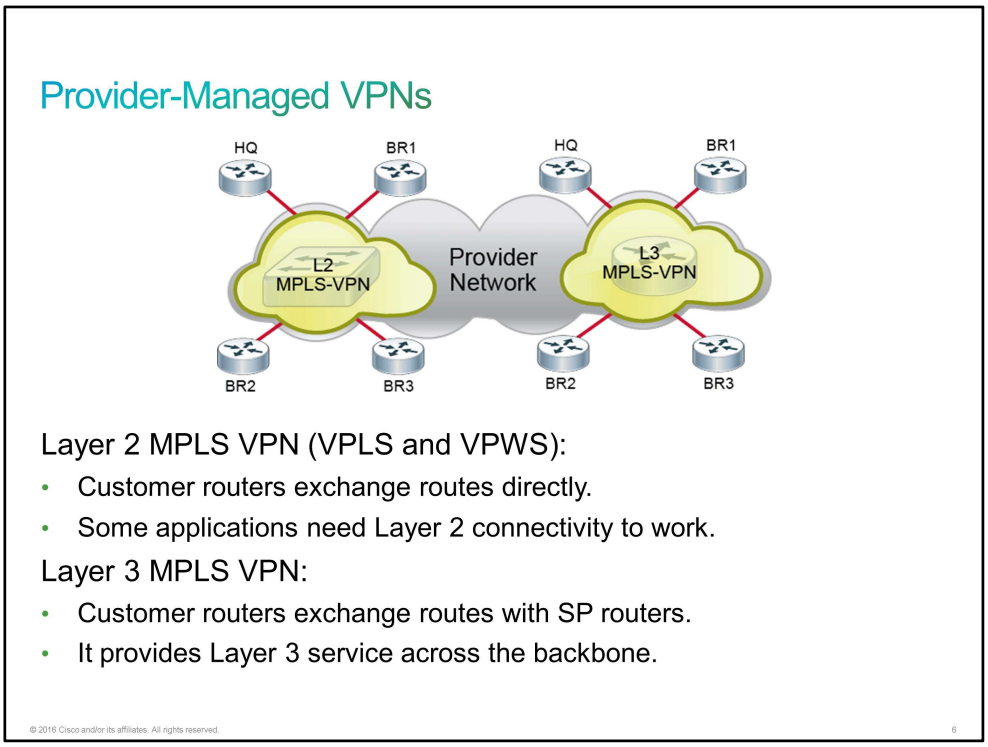


ISPs use several different WAN technologies to connect their subscribers. The connection type that is used on the local loop, or last mile, may not be the same as the WAN connection type that the ISP employs within the ISP network or between various ISPs.

Each of these technologies provides advantages and disadvantages for the customer. Not all technologies are available at all locations. When a service provider receives data, it must forward this data to other remote sites for final delivery to the recipient. These remote sites connect either to the ISP network or pass from ISP to ISP and to the recipient. Long-range communications are usually those connections between ISPs or among branch offices in very large companies.

Provider-Managed VPNs

Provider-managed VPNs can either offer Layer 2 or Layer 3 connectivity. MPLS is a technology that was designed to support efficient forwarding of packets across the network core that is based on a simplified header.



Layer 2 MPLS VPN is useful for customers who run their own Layer 3 infrastructure and require Layer 2 connectivity from the service provider. In this case, the customer manages its own routing information. One advantage that Layer 2 VPN has over its Layer 3 counterpart is that some applications do not work if nodes are not in the same Layer 2 network.

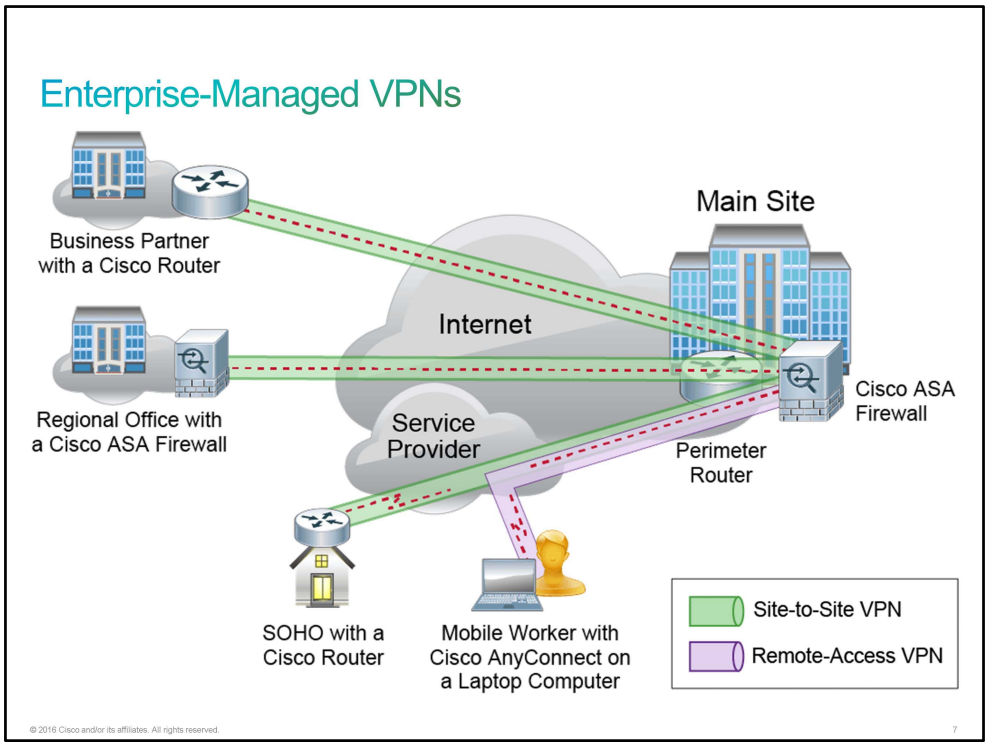
Some typical examples of Layer 2 VPN are VPLS and VPWS. If you look from the customer's perspective, with Layer 2 MPLS VPN, you can imagine a whole service provider network as one big virtual switch.

Layer 3 MPLS VPN provides Layer 3 service across the backbone. A separate IP subnet is used on each customer site. When you deploy a routing protocol over this VPN, the service provider needs to participate in the exchange of routes. Neighbor adjacency is established between your CE router and PE router (which the service provider owns). Within the service provider network, there are many P routers (service provider core routers). The job of P routers is to provide connectivity between PE routers. What this situation means is that the service provider becomes the backbone of your (customer) network.

Layer 3 VPN is appropriate for customers who prefer to outsource their routing to a service provider. The service provider maintains and manages routing for the customer sites. If you look from the customer's perspective, with Layer 3 MPLS VPN, you can imagine whole service provider network as one big virtual router.

Enterprise-Managed VPNs

Organizations need secure, reliable, and cost-effective ways to connect corporate headquarters, branch offices, and teleworkers working in home offices and other remote locations. A VPN is usually a bridge between two private networks. You build that bridge over a public network, typically the Internet. VPN enables headquarters and branch office devices to send and receive data as if they were directly connected.



A VPN is a virtual private network that is constructed within a public network infrastructure, such as the global Internet. VPNs provide an inexpensive alternative to private WAN connections. They are particularly helpful in organizations whose workforce is highly mobile and frequently needs to connect remotely to the corporate network and access sensitive data.

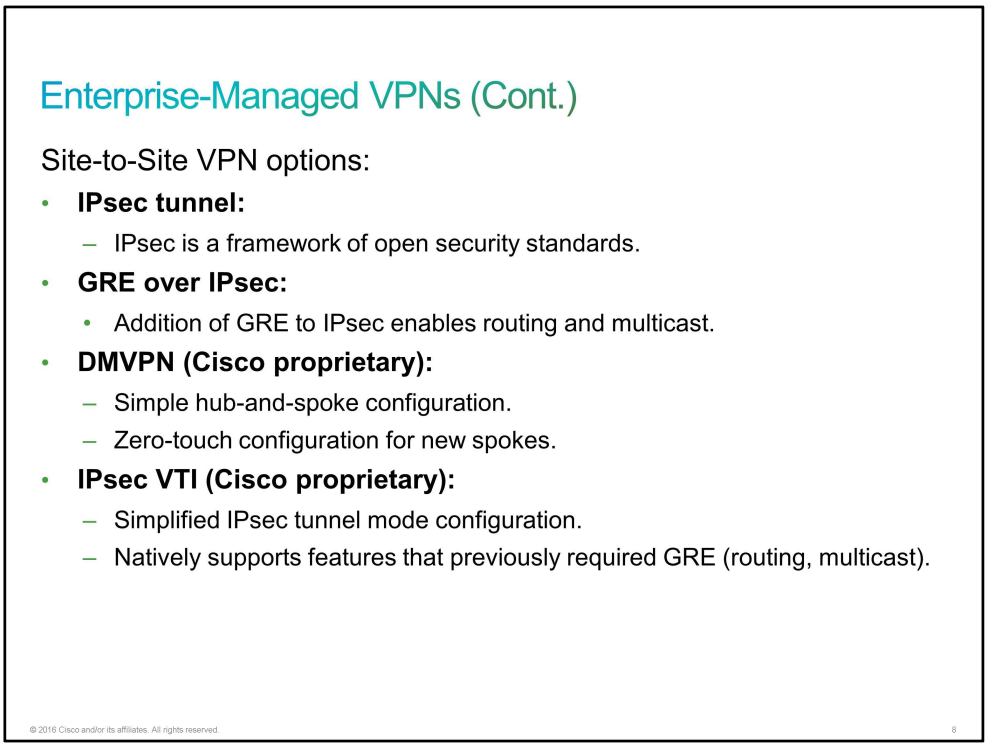
As shown in the figure, there are two types of VPN networks:

- **Site-to-site VPN:** A site-to-site VPN is an extension of a classic WAN network. End hosts send and receive traffic through a VPN device, which could be a router or Cisco Adaptive Security Appliance (Cisco ASA). This device is responsible for encapsulating and encrypting outbound traffic for all traffic from a particular site and sending it through a VPN tunnel over the Internet to a peer VPN device on the target site. Upon receipt, the peer VPN gateway strips the headers, decrypts the content if it was encrypted, and relays the packet toward the target host that is inside its private network. There are many site-to-site VPN options available.
- **Remote-access VPN:** Remote-access VPNs can support the needs of telecommuters, mobile users, and extranet, consumer-to-business traffic. In a remote-access VPN, each host typically has Cisco AnyConnect VPN Client software that is installed. Whenever the host tries to send any traffic, the Cisco AnyConnect VPN Client software encapsulates the traffic before sending it over the Internet to the VPN gateway at the edge of the target network. The VPN client may also encrypt the traffic before sending it over the Internet to the VPN gateway. Upon receipt, the VPN gateway behaves as it does for site-to-site VPNs.

VPNs provide the following benefits:

- **Cost savings:** VPNs enable organizations to use cost-effective, third-party Internet transport to connect remote offices and remote users to the main corporate site. The use of VPNs therefore eliminates expensive, dedicated WAN links. Furthermore, with the advent of cost-effective, high-bandwidth technologies such as DSL, organizations can use VPNs to reduce their connectivity costs while simultaneously increasing remote connection bandwidth.
- **Scalability:** VPNs enable corporations to use the Internet infrastructure, which makes new users easy to add. Therefore, corporations can add large amounts of capacity without adding significant infrastructure. For example, a corporation with an existing VPN between a branch office and the headquarters can securely connect new offices by simply making a few changes to the VPN configuration and ensuring that the new office has an Internet connection. Scalability is a major benefit of VPNs.
- **Compatibility with broadband technology:** VPNs allow mobile workers, telecommuters, and people who want to extend their work day to take advantage of high-speed, broadband connectivity, such as DSL and cable, to gain access to their corporate network. This ability provides workers with significant flexibility and efficiency. Furthermore, high-speed, broadband connections provide a cost-effective solution for connecting remote offices.
- **Security:** VPNs can provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access. The two available options are IPsec and SSL.

There are many site-to-site VPN options available. However, each option is a little bit different than the other.



IPsec Tunnel

IPsec provides a tunnel mode of operation that enables you to use it as a standalone connection method. This option is the most fundamental IPsec VPN design model. IPsec provides four important security services:

- **Confidentiality (encryption):** The sender can encrypt the packets before transmitting them across a network. By doing so, nobody can eavesdrop on the communication. If another device intercepts the communication, it cannot read it.
- **Data integrity:** The receiver can verify that the data was transmitted through the path without being changed or altered in any way. IPsec ensures data integrity by using checksums, which is a simple redundancy check.
- **Authentication:** Authentication makes sure that the connection is made with the desired communication partner. The receiver can authenticate the source of the packet by guaranteeing and certifying the source of the information. IPsec uses IKE to authenticate users and devices that can carry out communication independently. IKE uses several types of authentication including username and password, one-time password, biometrics, PSKs, and digital certificates.
- **Antireplay protection:** Antireplay protection verifies that each packet is unique and not duplicated. IPsec packets are protected by comparing the sequence number of the received packets with a sliding window on the destination host. A packet that has a sequence number that is before the sliding window is considered either a late or duplicate packet. Late and duplicate packets are dropped.

GRE over IPsec

Although IPsec provides a secure method for tunneling data across an IP network, it has limitations. IPsec does not support IP broadcast or IP multicast, preventing the use of protocols that rely on these features, such as routing protocols. IPsec also does not support the use of the multiprotocol traffic. GRE is a protocol that can be used to "carry" other passenger protocols, such as IP broadcast or IP multicast, and non-IP protocols. Using GRE tunnels with IPsec will give you the ability to run a routing protocol, IP multicast, or multiprotocol traffic across the network between the head end or head ends and branch offices.

With a generic hub-and-spoke topology, you can typically implement static tunnels (typically GRE over IPsec) between the central hub and remote spokes. When you want to add a new spoke to the network, you need to configure it on the hub router. Also, the traffic between spokes has to traverse the hub, where it must exit one tunnel and enter another. Static tunnels may be an appropriate solution for small networks, but this solution becomes unacceptable as the number of spokes grows larger and larger.

Cisco DMVPN

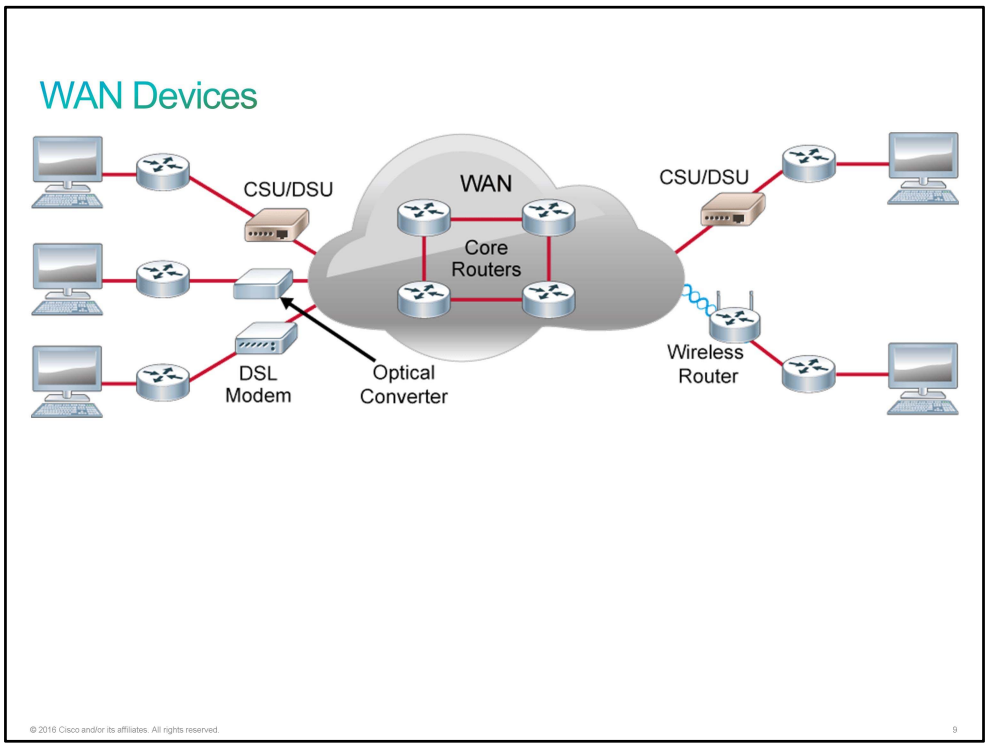
The Cisco Dynamic Multipoint Virtual Private Network (DMVPN) feature enables you to better scale large and small IPsec VPNs. The Cisco DMVPN feature provides simple provisioning of many VPN peers. It also easily supports dynamically addressed spoke routers by its design, if you use an appropriate peer authentication method, such as PKI-enabled peer authentication. The DMPVN feature enables you to configure a single mGRE tunnel interface and a single IPsec profile on the hub router to manage all spoke routers. Thus, the size of the configuration on the hub router remains constant even if you add more spoke routers to the network. DMVPN also allows IPsec to be immediately triggered to create point-to-point GRE tunnels without any IPsec peering configuration.

Cisco IPsec VTI

The VTI mode of an IPsec configuration simplifies a VPN configuration. There are two types of VTI—static and dynamic. With VTI, you implement the IPsec session as an interface. Simple configuration and routing adjacency directly over the virtual interface are great benefits. But keep in mind that all traffic is encrypted and that it supports, like standard IPsec, only one protocol (IPv4 or IPv6). The IPsec tunnel protects the routing protocol and multicast traffic, like with GRE over IPsec. The only difference is that with VTI, you do not need GRE and the overhead that it brings.

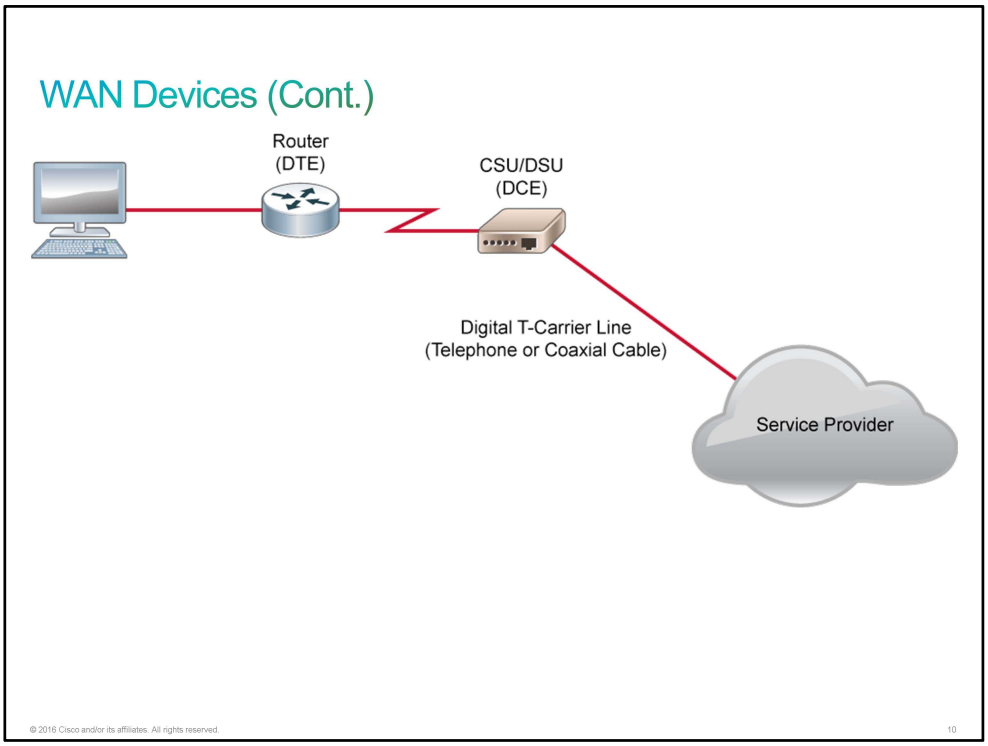
WAN Devices

Several types of devices are specific to WAN environments, including CSU/DSU devices, modems, and certain types of routers and switches.

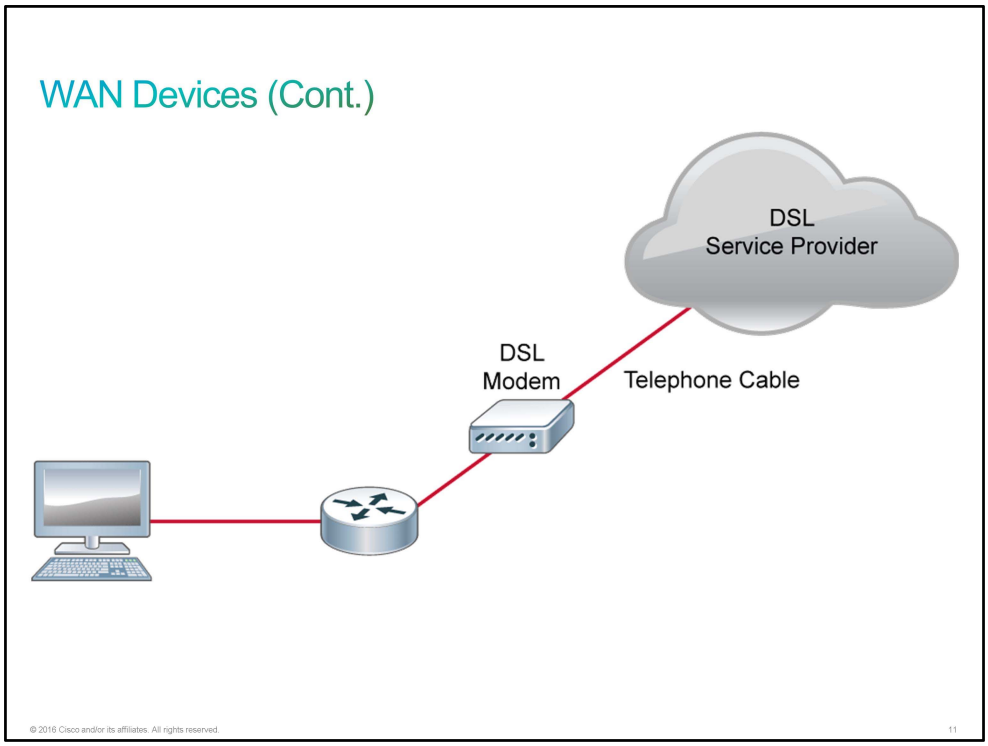


The following are common WAN devices and their descriptions.

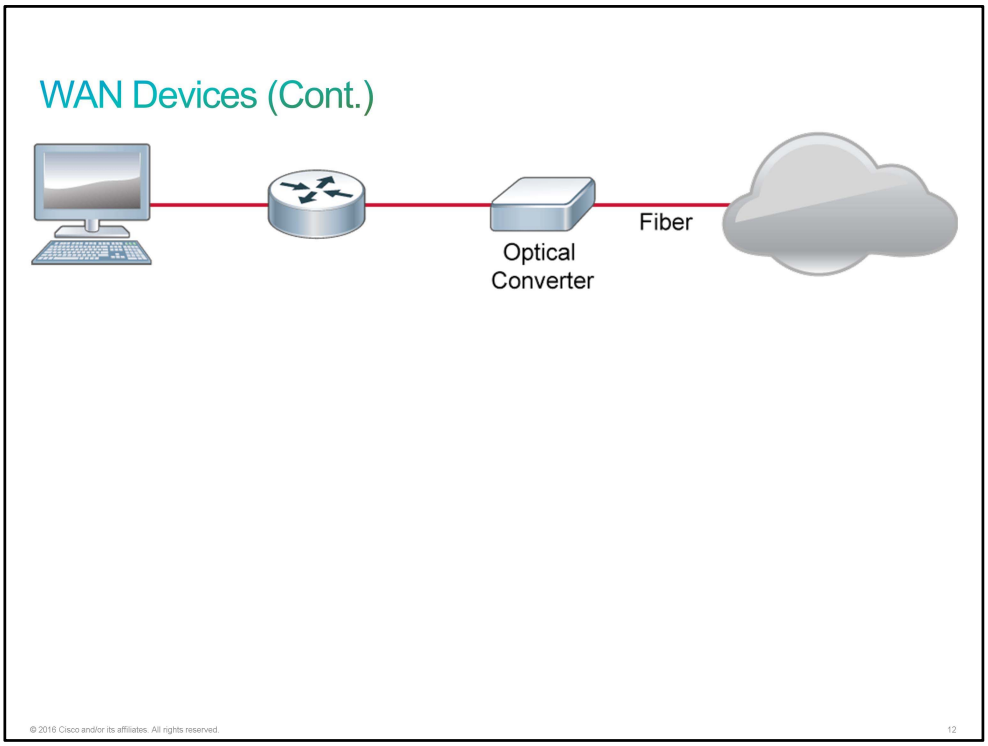
- **Router:** A router provides internetworking and WAN access interface ports that are used to connect to the service provider network. These interfaces may be serial connections or other WAN interfaces. With some types of WAN interfaces, you need an external device such as a CSU/DSU or modem (analog, cable, or DSL) to connect the router to the local POP of the service provider.
- **Core router:** A core router resides within the middle or backbone of the WAN, rather than at its periphery. To fulfill the role of core router, a router must be able to support multiple telecommunications interfaces of the highest speed in use in the WAN core. It must also be able to forward IP packets at wire speed on all these interfaces. The router must support the routing protocols that are being used in the core.
- **CPE:** Devices on subscriber premises are referred to as CPE. A subscriber to a service provider owns the CPE or leases the CPE from the service provider. A copper or fiber cable connects the CPE to the nearest exchange or CO of the service provider. This cabling is often called the local loop or "last mile." CSU/DSU devices, DSL modems, and optical fiber converters are just three of many WAN connection types.



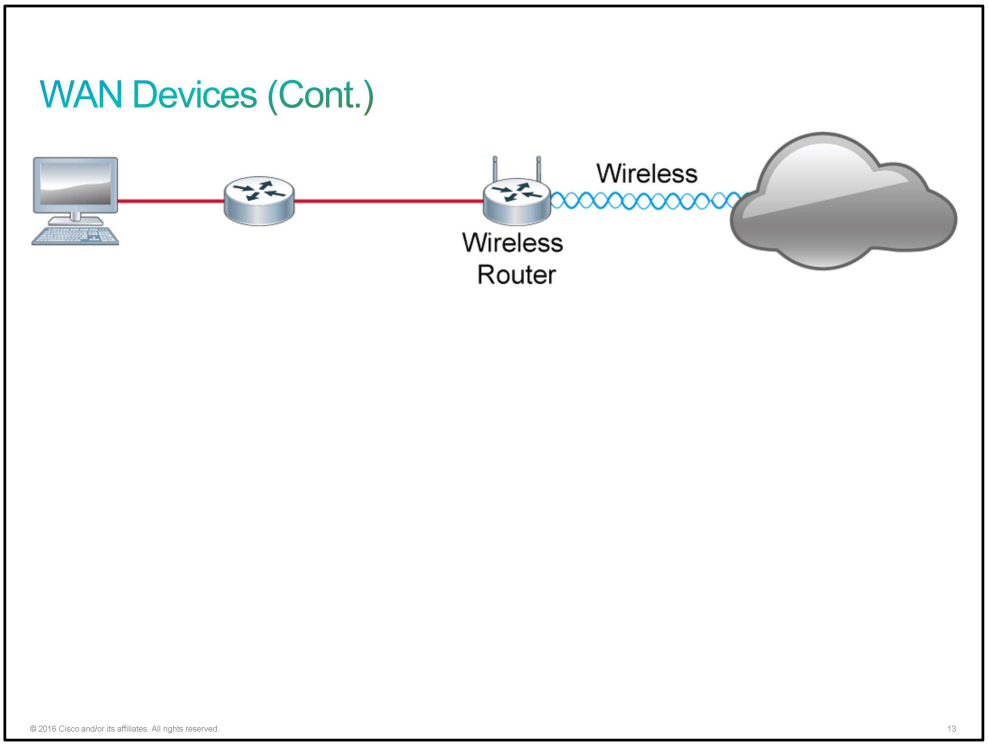
- **CSU/DSU:** A CSU/DSU is a device that is used to connect a DTE to a digital circuit, such as a T1 carrier line. A device is considered DTE if it is either a source or destination for digital data. Examples of DTE include PCs, servers, and routers. In the following figure, the router is considered DTE because it is passing data to the CSU/DSU, which will forward the data to the service provider. Although the CSU/DSU connects to the service provider infrastructure using a telephone or coaxial cable, such as a T1 or E1 line, it connects to the router with a serial cable. A CSU/DSU is actually two devices in one box. The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts the T-carrier line frames into frames that the LAN can interpret and vice versa. You can also implement a CSU/DSU as a module within a router, in which case, a serial cable is not necessary. A CSU/DSU is sometimes referred to as a DCE because it provides a path for communication. DCE is a more general label for devices that provide interfaces for DTE into communication links on the WAN cloud. When the links are digital, the DCE is a CSU/DSU. When analog telephone lines are the communication media, the DCE is a modem.



- **Modem:** A modem is a device that interprets digital and analog signals, enabling data to be transmitted over voice-grade telephone lines. At the source, digital signals are converted to a form that is suitable for transmission over analog communication facilities. At the destination, these analog signals are returned to their digital form. There are various types of modems. In the following figure, a DSL modem (which is used in DSL broadband environments) is connected to a router with an Ethernet cable and is connected to the service provider network with a telephone cable. You can also implement a modem as a router module.



- **Optical fiber converters**: Optical fiber converters are used where a fiber-optic link terminates to convert optical signals into electrical signals and vice versa. You can also implement the converter as a router or switch module.



- **Wireless router**: Wireless routers are used when you are using wireless medium for WAN connectivity. You can also use an access point instead of wireless router.

Challenge

1. Which two statements about WANs are true? (Choose two.)

   A. WANs generally connect devices that are located over a broader geographical area.
   B. WANs generally connect devices that are close to each other.
   C. WAN stands for World Around Networks.
   D. WANs use connections of various types to provide access to bandwidth over large geographical areas.

2. Which WAN topology option provides the highest level of redundancy?

   A. hub-and-spoke
   B. partially meshed
   C. fully meshed
   D. point-to-point

3. Which two VPNs are examples of service provider-managed VPNs? (Choose two.)

   A. remote-access VPNs
   B. Layer 2 MPLS VPN
   C. Layer 3 MPLS VPN
   D. DMVPN

4. Which two technologies are examples of Layer 2 MPLS VPN technologies? (Choose two.)

   A. VPLS
   B. DMVPM
   C. GETVPN
   D. VPWS

5. Which protocol should be used with IPsec to give you the ability to run a routing protocol or IP multicast across the network between two site-to-site VPN peers?

   A. GRE
   B. IPsec tunnel
   C. WAN
   D. MPLS

6. Which protocol provides confidentiality, data integrity, authentication, and antireplay protection?

   A. GRE
   B. IPsec
   C. ISDN
   D. MPLS

7. Which service ensures that data being transmitted has not been changed or altered in any way?

   A. confidentiality
   B. data integrity
   C. authentication
   D. antireplay protection

Answer Key

Challenge

1. A, D
2. C
3. B, C
4. A, D
5. A
6. B
7. B

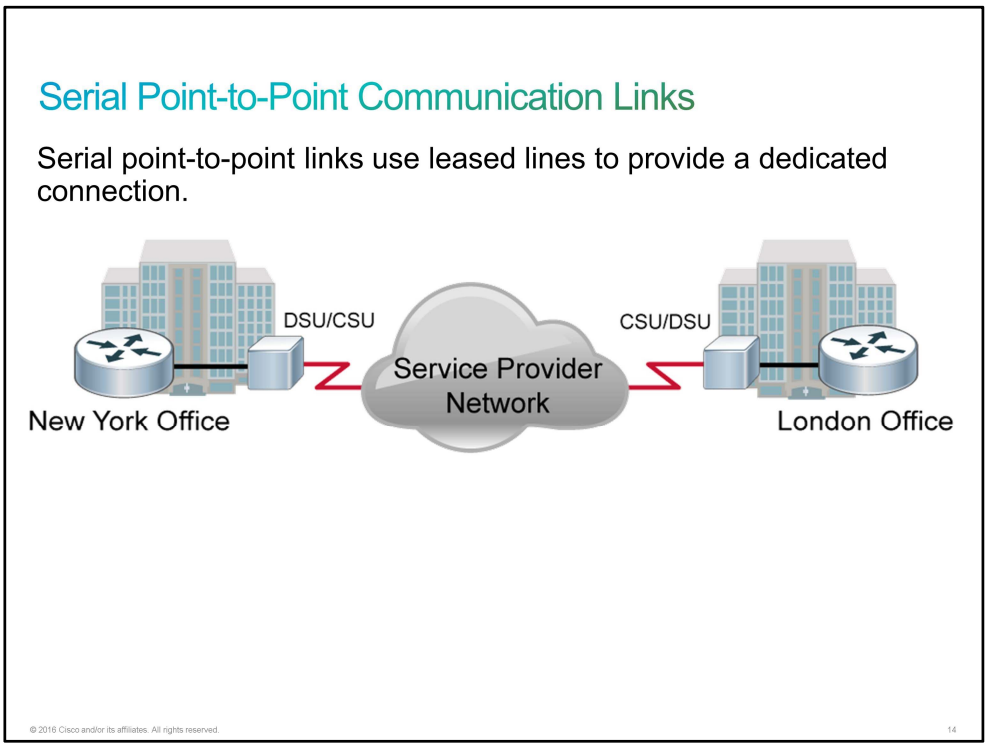
Lesson 2: Understanding Point-to-Point Protocols

Introduction

A CCS customer is adding two new branch offices. At one branch, the customer is running HDLC for the WAN protocol for the connection back to the corporate site. At the other branch, it is running PPPoE. You will be the primary technician for the deployment. Would you like to go on site now to complete the job or study the training before the deployment?

Serial Point-to-Point Communication Links

A point-to-point (or serial) communication link provides a single, established WAN communication path from the customer premises through a carrier network to a remote network.



When permanent dedicated connections are required, a point-to-point link is used to provide a pre-established WAN communications path from the customer premises through the provider network to a remote destination. A serial line can connect two geographically distant sites, such as a corporate office in New York and a regional office in London. Point-to-point lines are usually leased from a carrier and are therefore often called leased lines. For a point-to-point line, the carrier dedicates fixed transport capacity and facility hardware to the line that the customer is leasing. However, the carrier will still use multiplexing technologies within the network.

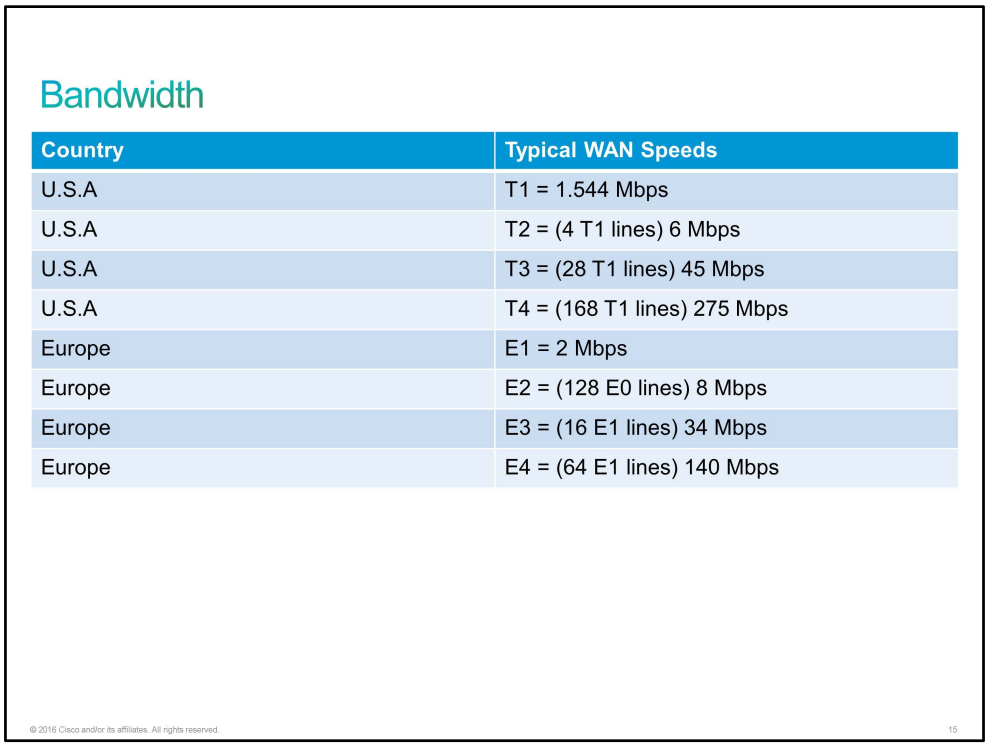
Point-to-point links are usually more expensive than shared services such as Frame Relay. The cost of leased-line solutions can become significant if you use them to connect many sites over increasing distances. However, there are times when the benefits outweigh the cost of the leased line. The dedicated capacity removes latency or jitter between the endpoints. Constant availability is essential for some applications such as VoIP or video over IP.

You need a router serial port for each leased-line connection. If the underlying network is based on the North American (T-carrier) or European (E-carrier) technologies, the leased line connects to the network of the carrier through a CSU/DSU. The purpose of the CSU/DSU is to provide a clocking signal to the customer equipment interface from the DSU and terminate the channelized transport media of the carrier on the CSU. The CSU also provides diagnostic functions such as a loopback test. Most T1 or E1 TDM interfaces on current routers include approved CSU/DSU capabilities.

Leased lines provide permanent dedicated capacity and are used extensively for building WANs. They have been the traditional choice of connection but have several disadvantages. Leased lines have a fixed capacity. However, WAN traffic is often variable and leaves some of the capacity unused. In addition, each endpoint needs a separate physical interface on the router, which increases equipment costs. Any change to the leased line generally requires a site visit by the carrier personnel.

Bandwidth

Bandwidth refers to the rate at which data is transferred over the communication link. The underlying carrier technology depends on the bandwidth that is available. There is a difference in bandwidth points between the North American T-carrier specification and the E-carrier system, as shown in the table.



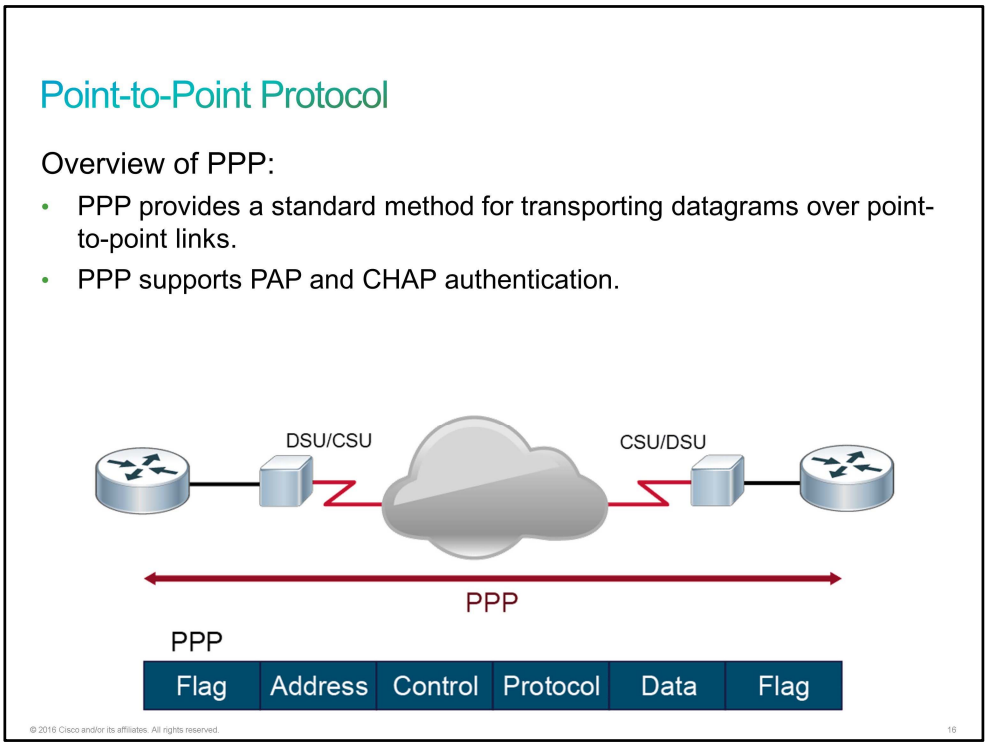
Leased lines are available in different capacities and are generally priced based on the bandwidth that is required and the distance between the two connected points.

Point-to-Point Protocol

PPP originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses, asynchronous (start and stop bit) and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, error detection, and option negotiation for such capabilities as network layer address negotiation and data compression negotiation.

PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits. An example of an asynchronous connection is a dialup connection. An example of a synchronous connection is a leased line.

There are many advantages to using PPP, including the fact that it is not proprietary. Moreover, it includes many features that are not available in HDLC, including the link-quality management feature that monitors the quality of the link. If too many errors are detected, PPP takes down the link. PPP also supports PAP and CHAP authentication.



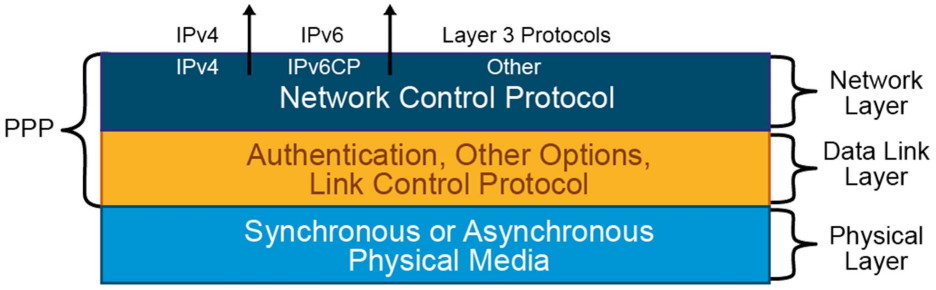
Cisco High-Level Data Link Control (Cisco HDLC) is a data-link layer protocol that can be used on leased lines between two Cisco devices. For communicating with a device from another vendor, synchronous PPP is a better option.

PPP provides a standard method for transporting multiprotocol datagrams (packets) over point-to-point links.

Point-to-Point Protocol (Cont.)

PPP is a layered architecture:

- PPP can carry packets from several protocol suites using NCP.
- PPP controls the setup of several link options using LCP.



PPP includes these three main components:

- A method for encapsulating multiprotocol datagrams.
- Extensible LCP to establish, configure, and test the WAN data-link connection.
- A family of NCPs for establishing and configuring different network layer protocols. PPP allows the simultaneous use of multiple network layer protocols.

LCP provides versatility and portability to a wide variety of environments. LCP is used to automatically determine the encapsulation format option, to manage varying limits on sizes of packets, and to detect a loopback link, and terminate the link. Other optional facilities that LCP provides are authentication of the identity of its peer on the link and the determination of when a link is functioning correctly or failing.

The authentication phase of a PPP session is optional. After the link has been established and the authentication protocol is chosen, the peer can be authenticated. If the authentication option is used, authentication takes place before the network layer protocol configuration phase begins.

Cisco offers CHAP and PAP for PPP authentication.

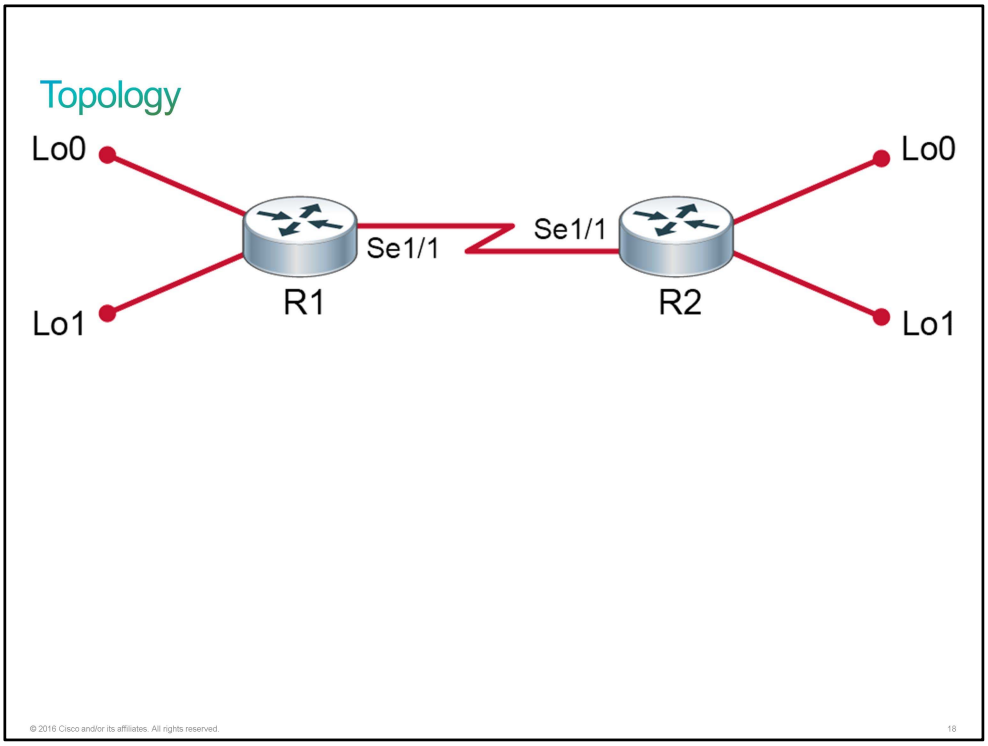
Discovery 47: Configure Serial Interface and PPP

Introduction

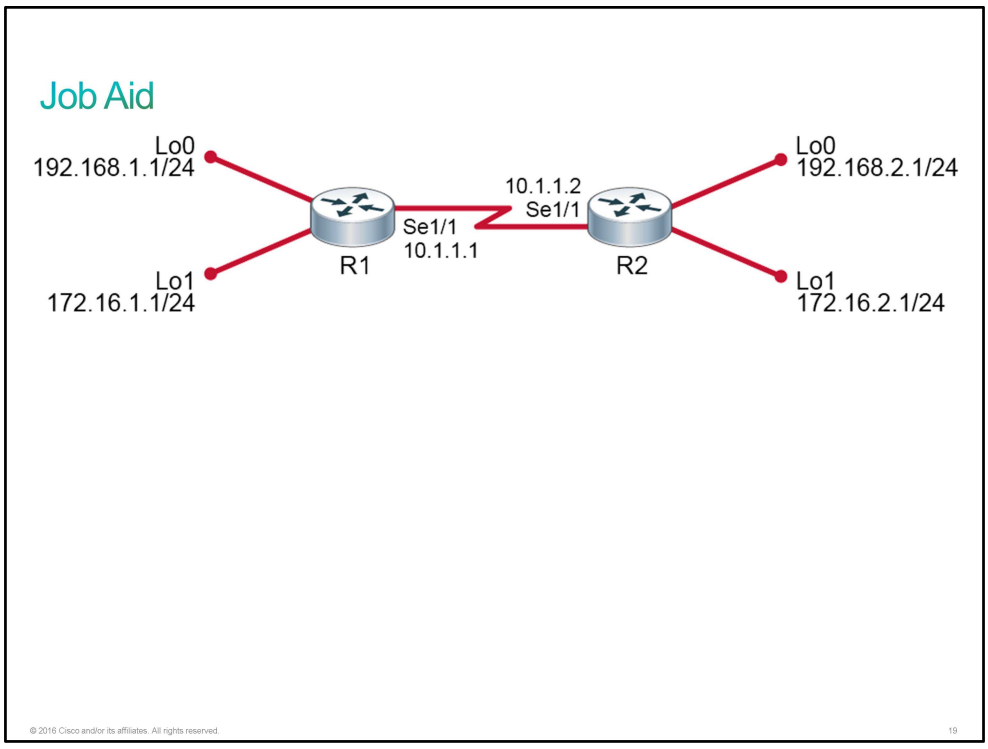
This discovery will guide you through the configuration of the clock rate on the DCE side of a serial link and the configuration of PPP encapsulation on both sides of a serial link between two Cisco IOS routers. The virtual lab is prepared with two routers as depicted in the topology diagram and the connectivity table. R1 has the DCE side of the serial link, while R2 has the DTE side. Both routers have their basic configurations in place, including hostnames, IP addresses, and EIGRP as the routing protocol.

First you will configure and verify a serial interface to use PPP encapsulation, and then you will configure PAP and CHAP authentication for PPP.

Topology



Job Aid



The configuration is as follows:

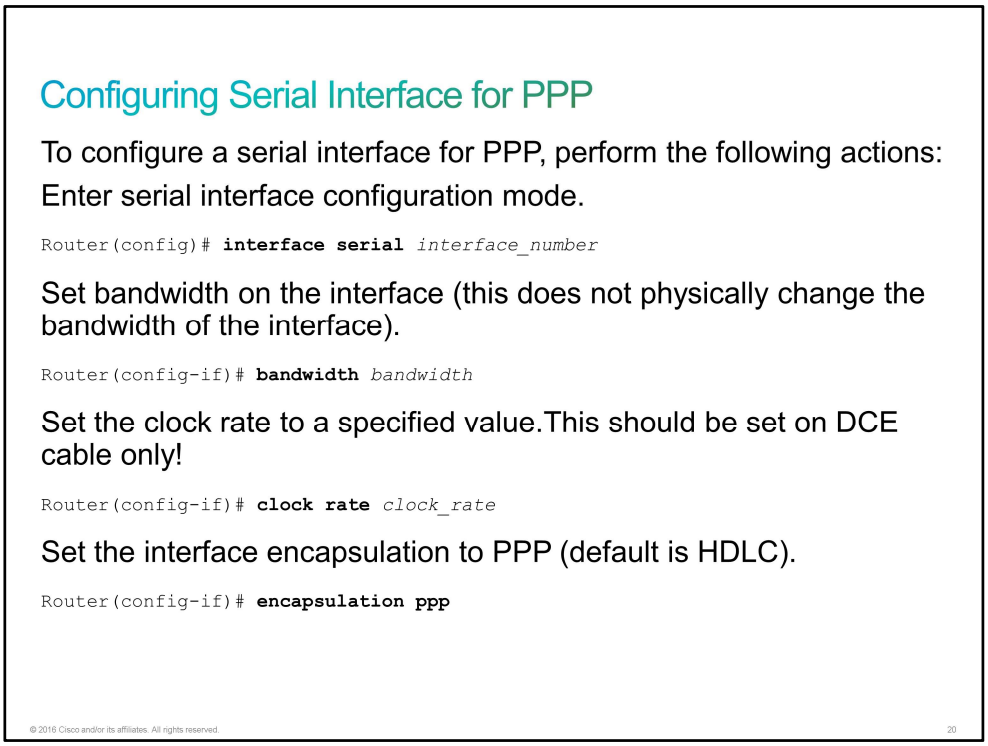
- Both routers have their basic configurations in place, including hostnames and IP addresses.
- EIGRP is configured on both routers, making them aware of each other's loopback interfaces networks.

Device Details

Device	Interface	Neighbor	IP Address
R1	Serial1/1	R2	10.1.1.1/24
R1	Loopback0	—	192.168.1.1/24
R1	Loopback1	—	172.16.1.1/24
R2	Serial1/1	R1	10.1.1.2/24
R2	Loopback0	—	192.168.2.1/24
R2	Loopback1	—	172.16.2.1/24

Task 1: Configure Serial Interface for PPP

Activity



To configure a serial interface, follow these steps:

1. Enter the global configuration mode—use the **configure terminal** command.
2. When in you are in the global configuration mode, enter the interface configuration mode. In this example, you would use the **interface serial 0/0/0** command.
3. If a DCE cable is attached, use the **clock rate** *bps* interface configuration command to configure the clock rate for the hardware connections on serial interfaces, such as network interface modules and interface processors, to an acceptable bit rate. Be sure to enter the complete clock speed. For example, a clock rate of 64000 cannot be abbreviated to 64. On serial links, one side of the link acts as the DCE, and the other side of the link acts as the DTE. By default, Cisco routers are DTE devices, but you can configure them as DCE devices. In a "back-to-back" router configuration in which a modem is not used, you must configure one of the interfaces as the DCE to provide a clocking signal. You must specify the clock rate for each DCE interface that is configured in this type of environment. The clock rates in bits per second are as follows: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, and 4000000.

Note	Some of the routers do not require clock rate configuration anymore.

- Enter the specified bandwidth for the interface. The **bandwidth** *kbps* command overrides the default bandwidth that the **show interfaces** command displays. It is used by some routing protocols, such as the EIGRP, for routing metric calculations. The router also uses the bandwidth for other types of calculations, such as those calculations that are required for the RSVP. The default bandwidth for serial lines is the T1 speed (1.544 Mbps). The entered bandwidth has no effect on the actual speed of the line.

Note	The attached serial cable determines the DTE or DCE mode of the Cisco router. Choose the cable to match the network requirement.

The table provides a description of the commands that you use to configure a serial interface.

Command	Description
interface serial *interface_number*	Enters the serial interface configuration mode for the specified interface.
bandwidth *bandwidth*	Sets the interface bandwidth metric in kilobits per second (kbps).
clock rate *clock_rate*	Sets the interface clock rate in bits per second (bps). You use this command on DCE interfaces only.
encapsulation ppp	Sets the interface encapsulation to PPP.

Note	A common misconception for students that are new to networking and Cisco IOS Software is to assume that the **bandwidth** command changes the physical bandwidth of the link. The bandwidth command modifies only the bandwidth metric that routing protocols such as EIGRP and OSPF use. Sometimes, a network administrator changes the bandwidth value to have more control over the chosen outgoing interface.

The **encapsulation ppp** command has no arguments, but you must first configure the router with an IP routing protocol to use the PPP encapsulation. If you do not configure PPP on a Cisco router, the default encapsulation for serial interfaces is HDLC.

Step 1 Access the console of R1. The Serial1/1 interface on R1 has DCE cable. Configure it for a clock rate of 64,000 bps and define the bandwidth as 64 kbps.

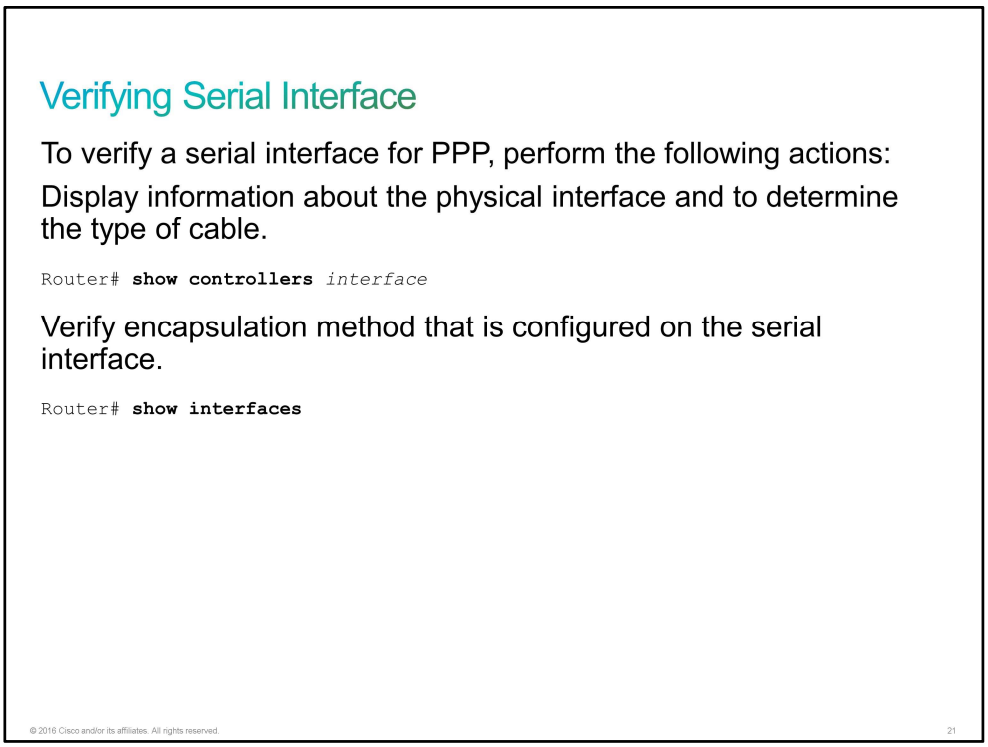
On R1, enter the following commands:

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface Serial1/1
R1(config-if)# clock rate 64000
R1(config-if)# bandwidth 64
R1(config-if)# end
R1#
```

The **clock rate** command controls the actual speed at which the serial link runs. The **bandwidth** command does not affect the running speed of the interface, but instead sets the information which is provided to dynamic routing protocols for determining metrics associated with the link.

The **clock rate** command expects its argument in bits per second, while the **bandwidth** command expects its argument in kilobits per second.

Verifying Serial Interface



The **show controller** command displays information about the physical interface itself. This command is useful with serial interfaces to determine the type of cable that is connected without the need to physically inspect the cable itself.

Use the **show interfaces** command to verify that the proper encapsulation is enabled on the serial interface. The output shows which encapsulation is enabled on the serial interface.

Step 2 Use the **show controllers** command to verify the configuration of Serial1/1 and to verify that the status indicators are all "up."

On R1, enter the following command:


```
R1# show controllers Serial1/1
M4T: show controller:
PAS unit 1, subunit 1, f/w version 1-45, rev ID 0xFFFF, version 1
idb = 0xECF450D8, ds = 0xECF463F0, ssb=0xECF467A8
Clock mux=0x0, ucmd_ctrl=0x1C, port_status=0x3B
Serial config=0x8, line config=0x200
maxdgram=1608, bufpool=78Kb, 120 particles
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
line state: up
cable type : V.11 (X.21) DCE cable, received clockrate 64000
running=1, port id=0x117F0688

base0 registers=0xECF2B038, base1 registers=0xECF2D038
mxt_ds=0xEEAEEEC0, rx ring entries=78, tx ring entries=128
rxring=0xECF46B98, rxr shadow=0xECF46E40, rx_head=73
txring=0xECF47220, txr shadow=0xECF47658, tx_head=101, tx_tail=101, tx_count=0
throttled=0, enabled=0
halted=0, last halt reason=0
Microcode fatal errors=0
rx_no_eop_err=0, rx_no_stp_err=0, rx_no_eop_stp_err=0
rx_no_buf=0, rx_soft_overrun_err=0, dump_err= 0, bogus=0, mxt_flags=0x0
tx_underrun_err=0, tx_soft_underrun_err=0, tx_limited=0(128)
tx_fullring=0, tx_started=1336, mxt_flush_count=0
rx_int_count=1338, tx_int_count=1340
```

Step 3 Use the **show interfaces** command to verify the bandwidth setting that the routing protocols will use, along with the current serial encapsulation method.

On R1, enter the following command:

```
R1# show interfaces Serial1/1
Serial1/1 is up, line protocol is up
  Hardware is M4T
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input 00:00:01, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1399 packets input, 94051 bytes, 0 no buffer
     Received 492 broadcasts (1 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1395 packets output, 93604 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     3 carrier transitions     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Both R1 and R2 are using the default HDLC encapsulation method.

Step 4 EIGRP has been preconfigured on both routers R1 and R2. Verify the content of the routing table on R1.

On R1, enter the following command:

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/24 is directly connected, Serial1/1
L        10.1.1.1/32 is directly connected, Serial1/1
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Loopback1
L        172.16.1.1/32 is directly connected, Loopback1
D        172.16.2.0/24 [90/40640000] via 10.1.1.2, 00:23:31, Serial1/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback0
L        192.168.1.1/32 is directly connected, Loopback0
D     192.168.2.0/24 [90/40640000] via 10.1.1.2, 00:23:31, Serial1/1
```

The marked networks have been learned via the EIGRP protocol.

Step 5 From R1, ping the Loopback0 interface (192.168.2.1) of R2.

On R1, enter the following command:

```
R1# ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 21/21/21 ms
```

The ping should succeed.

Step 6 Set the encapsulation protocol on the R1 Serial1/1 interface to PPP.

On R1, enter the following command:

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface Serial1/1
R1(config-if)# encapsulation ppp
R1(config-if)#
*Dec  3 13:28:08.576: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to down
R1(config-if)#
*Dec  3 13:28:18.198: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.2
(Serial1/1) is down: holding time expired
R1(config-if)# end
R1#
```

Now, R1 is using PPP for encapsulation while R2 is using HDLC. These encapsulation protocols are incompatible, which is why the protocol on the R1 Serial1/1 interface went down and the EIGRP neighbor relationship with R2 has timed out.

Step 7 Display the status of the Serial1/1 interface on R1 with the **show ip interface brief** command.

On R1, enter the following command:

```
R1# show ip interface brief Serial1/1
Interface                  IP-Address      OK? Method Status          Protocol
Serial1/1                  10.1.1.1        YES manual up              down
```

The administrative status of the interface is "up," but the protocol is "down."

Step 8 Access the console of R2. Configure its Serial1/1 interface to use PPP encapsulation and configure its bandwidth setting to 64.

On R2, enter the following command:

```
R2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# interface Serial1/1
R2(config-if)# bandwidth 64
R2(config-if)# encapsulation ppp
R2(config-if)#
*Dec  3 14:45:36.286: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to up
R2(config-if)#
*Dec  3 14:45:42.460: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1
(Serial1/1) is up: new adjacency
R2(config-if)# end
R2#
```

When the encapsulation protocol is compatible with its peer, the line protocol state changes to "up." With the line protocol up, the EIGRP neighbor relationship with R1 is able to re-establish.

You did not need the **clock rate** command on R2 because the router it is connected with the DTE side of the cable.

Step 9 Use the **show interface** command on R2 to verify the serial encapsulation method.

On R2, enter the following command:

```
R2# show interfaces Serial1/1
Serial1/1 is up, line protocol is up
  Hardware is M4T
  Internet address is 10.1.1.2/24
  MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input 00:00:02, output 00:00:03, output hang never
  Last clearing of "show interface" counters 17:57:30
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     28089 packets input, 1493205 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     28090 packets output, 1493281 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Both R1 and R2 are using the PPP encapsulation method.

Step 10 For one last verification of connectivity, from R2, ping the Loopback0 interface (192.168.1.1) of R1.

On R2, enter the following command:

```
R2# ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 33/33/34 ms
```

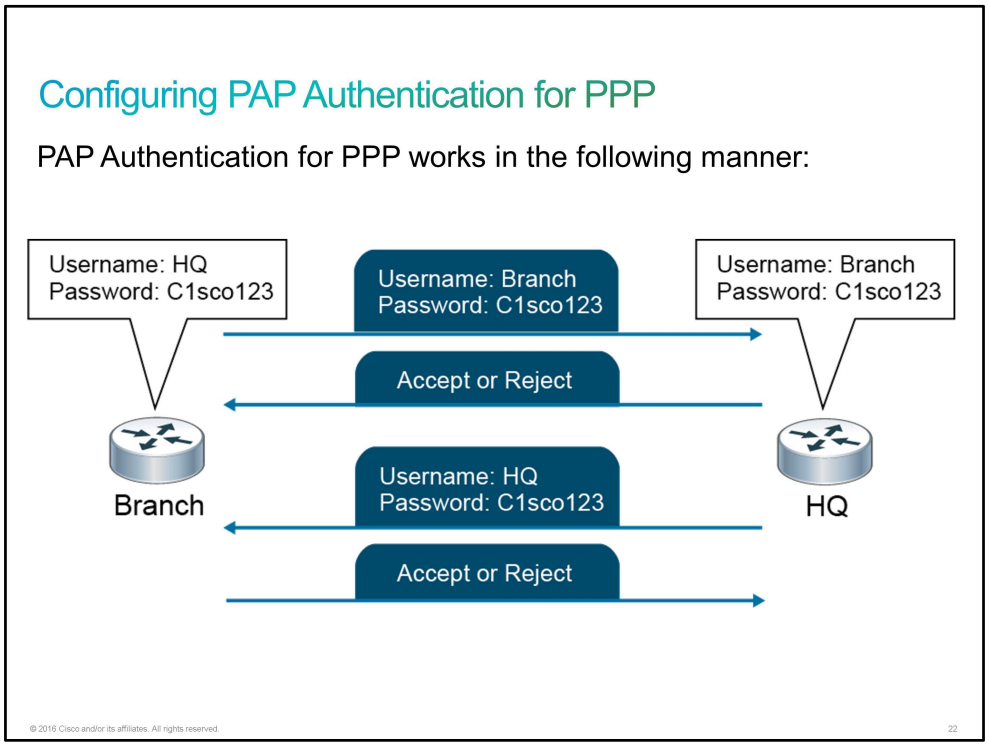
Task 2: Configure PAP Authentication for PPP

Activity

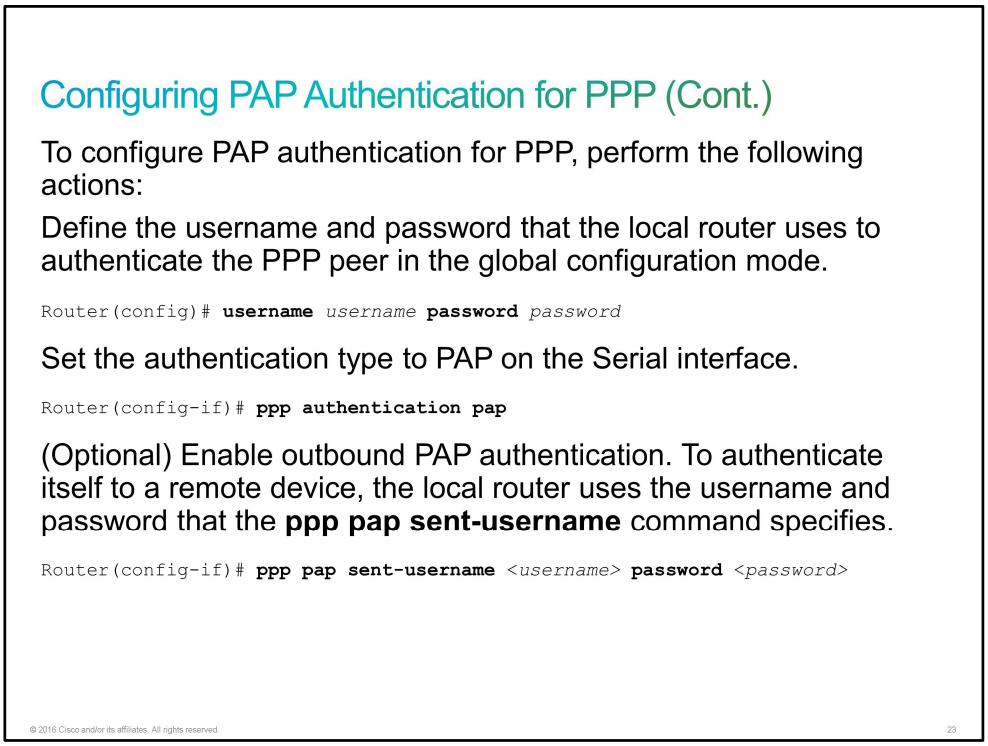
To improve security mitigation, the PPP protocol suite was designed to offer the optional feature of user authentication. Devices that initiate a PPP session must pass a strict identity verification before the link establishment is approved. The link is activated only after the proper credentials have been given and accepted. If PPP authentication fails for any reason, access is denied and the link is promptly terminated. Although you may configure proprietary authentication methods to work with PPP, the two main types of PPP authentication methods are PAP and CHAP.

PAP is a two-way handshake that provides a simple method for a remote node to establish its identity. PAP is performed only upon initial link establishment. There is no encryption. The username and password are sent in plaintext. After the PPP link establishment phase is complete, the remote node repeatedly sends a username and password pair to the router until authentication is acknowledged or the connection is terminated.

PAP is not a strong authentication protocol, but it may be adequate in environments that use token-type passwords that change with each authentication. PPP is not secure in most environments. Also, there is no protection from playback or repeated trial-and-error attacks—the remote node is in control of the frequency and timing of the login attempts.



In the example, the Branch router first sends its PAP username and password to the Headquarter (HQ) router. The HQ router evaluates the Branch router credentials against its local database. If the Branch router credentials match, the HQ router accepts the connection. If not, the HQ router rejects the connection. This is the two-way handshake in which the Branch router authenticates to the HQ router. Then the reverse process occurs with the HQ router authenticating to the Branch router.



The router that the **ppp authentication pap** command is configured on will use PAP to verify the identity of the other side (peer). It means that the other side (peer) must present its username and password to the local device for verification

Usernames and passwords that the local router uses to authenticate the PPP peer are defined using the **username password** command . When the peer sends its PAP username and password, the local router will check whether that username and password are configured locally. If there is a successful match, the peer is authenticated.

The **ppp pap sent-username** <*username*> **password** <*password*> command enables outbound PAP authentication. The local router uses the username and password that the **ppp pap sent-username** command specifies to authenticate itself to a remote device. The other router must have this same username/password configured using the **username** command described above.

Step 1 On R1, define the username "User2" using the "cisco" password.

On R1, enter the following command:

```
R1# conf t
R1(config)# username User2 password cisco
```

The username value is not case-sensitive, but the password value is case-sensitive.

Step 2 On R2, define the username "User1" using the "cisco" password.

On R2, enter the following command:

```
R2# conf t
R2(config)# username User1 password cisco
```


Step 3 Configure PAP authentication on the Serial1/1 interface on R1. Set "User1" as the sent username and "cisco" as the password.

On R1, enter the following commands:

```
R1(config)# interface Serial1/1
R1(config-if)# ppp authentication pap
R1(config-if)#
*Dec  4 14:10:48.834: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to down
*Dec  4 14:10:48.837: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.2
(Serial1/1) is down: interface down
R1(config-if)# ppp pap sent-username User1 password cisco
R1(config-if)# end
R1#
```

The line protocol for interface Serial1/1 goes down because R2 is not configured for PAP authentication yet. The consequence is lost EIGRP neighbor relationship.

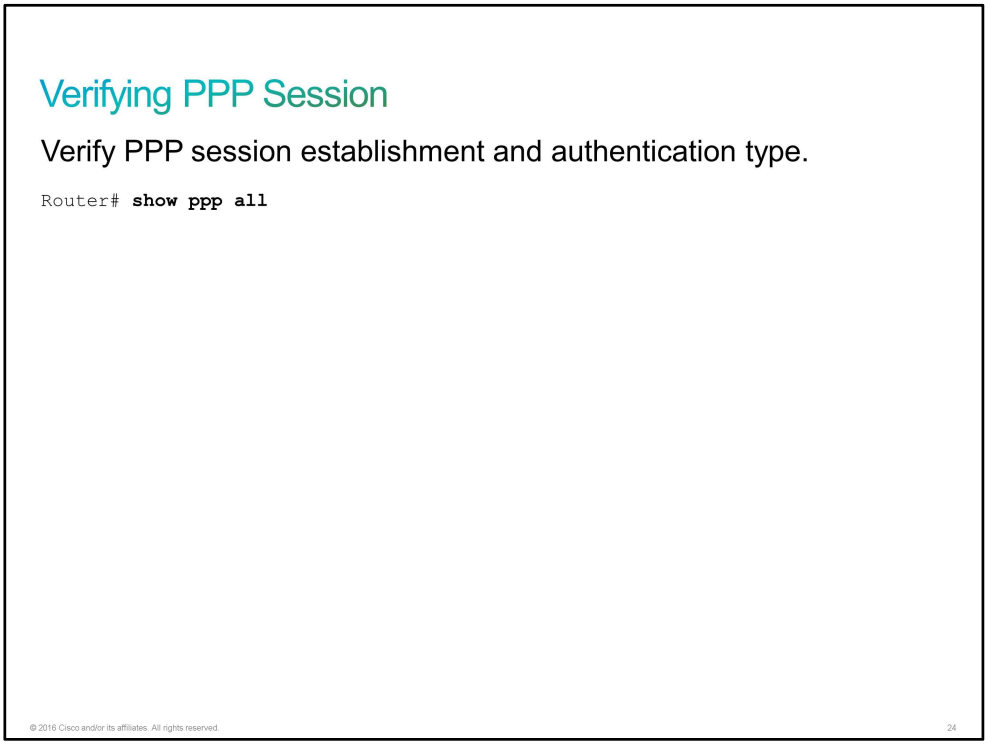
Step 4 Configure PAP authentication on the Serial1/1 interface on R2. Set "User2" as the sent username and "cisco" as the password.

On R2, enter the following command:

```
R2(config)# interface Serial1/1
R2(config-if)# ppp authentication pap
R2(config-if)# ppp pap sent-username User2 password cisco
R2(config-if)#
*Dec  4 14:11:47.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to up
R2(config-if)#
*Dec  4 14:11:48.311: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1
(Serial1/1) is up: new adjacency
R2(config-if)# end
R2#
```

The PPP session gets re-established using PAP authentication. The consequence is that the line protocol on the interface Serial1/1 goes up and the EIGRP neighbor relationship is re-established.

Verifying PPP Session



The **show ppp all** command verifies that the PPP session is established. Is also displays the information of authentication used, peer name, and IP address.

Step 5 On R2, verify that the PPP session is established.

On R2, enter the following command:

```
R2# show ppp all
Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ --------------------- -------- --------------- -------------------
-
Se1/1        LCP+ PAP+ IPCP+ CDPC> LocalT   10.1.1.1        User1
```

The PPP session is established using PAP authentication on the Serial1/1 interface to the peer that is named R1 using the peer IP address 10.1.1.1.

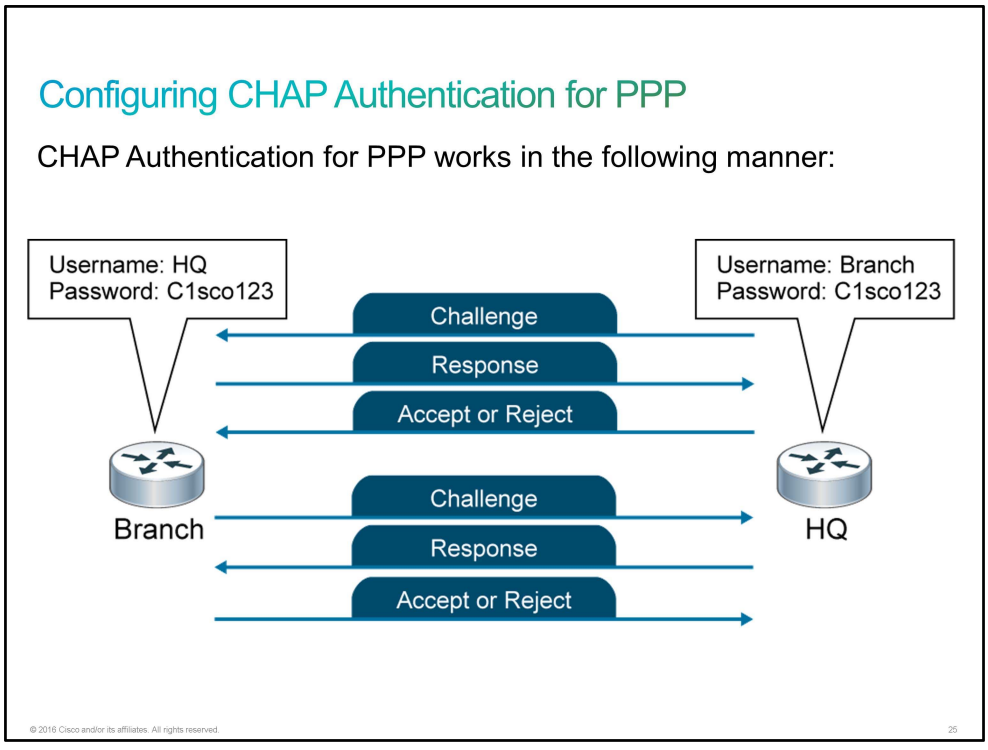
Task 3: Configure CHAP Authentication for PPP

Activity

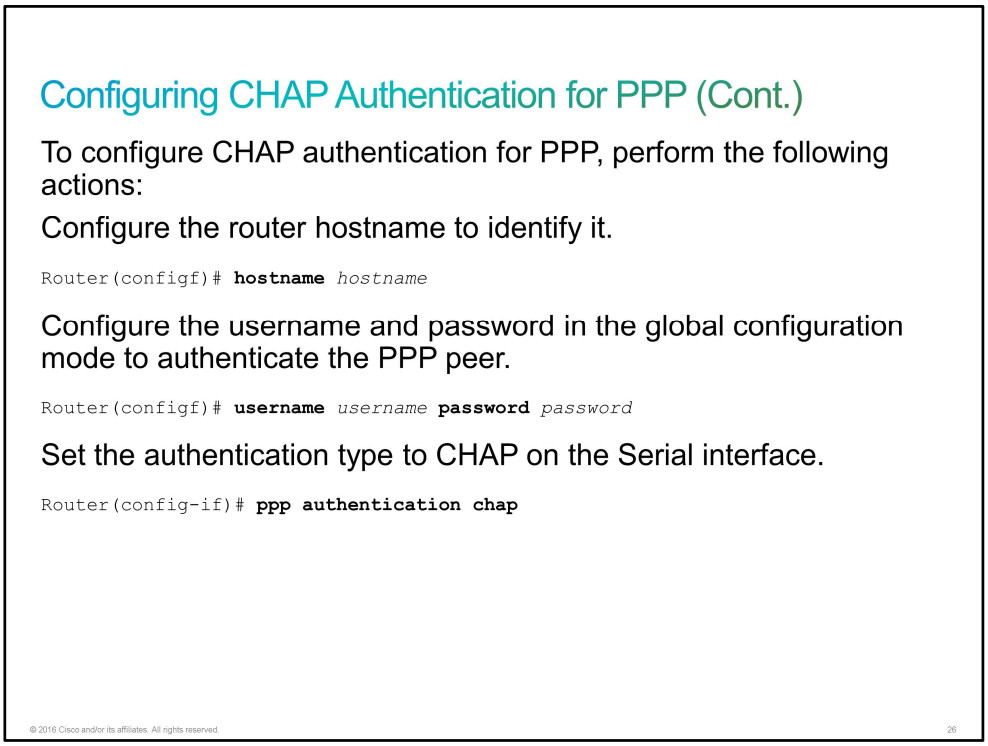
CHAP is the preferred authentication method and is considered superior to PAP. CHAP involves a three-way exchange of a shared secret. When authentication is established with PAP, it essentially stops working, which leaves the network vulnerable to attacks. Unlike PAP, which only authenticates once, CHAP conducts periodic challenges to make sure that the remote node still has a valid password value. CHAP, which uses a three-way handshake, occurs at the startup of a link and periodically thereafter to verify the identity of the remote node.

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, typically MD5, based on the password and challenge message. The local router checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. Otherwise, the connection is terminated immediately.

CHAP provides protection against a playback attack by using a variable challenge value that is unique and unpredictable. Because the challenge is unique and random, the resulting hash value will also be unique and random. The use of repeated challenges is intended to limit exposure to any single attack. The local router or a third-party authentication server is in control of the frequency and timing of the challenges.



In the example, the HQ router sends a challenge message to the Branch router. The Branch router responds to the HQ router by sending its CHAP username and password. The HQ router evaluates the Branch router credentials against its local database. If the credentials match, it accepts the connection. If they do not, it rejects the connection. This process is a three-way handshake of the HQ router authenticating the Branch router. A three-way handshake of the Branch router authenticating the HQ router follows.



To configure PPP authentication, you must configure the interface for PPP encapsulation. Follow these steps to enable CHAP authentication:

- Verify that each router has a hostname assigned to it. To assign a hostname, enter the **hostname** *name* command in the global configuration mode. This name must match the username that the authenticating router expects at the other end of the link.
- On each router, define the username and password to expect from the remote router with the **username** *name* **password** *password* global configuration command. Add a username entry for each remote system that the local router communicates with and that requires authentication. Note that the remote device must have a corresponding username entry for the local router with a matching password.
- Configure PPP authentication with the **ppp authentication {chap | chap pap | pap chap | pap}** interface configuration command.
  - If you configure **ppp authentication chap** on an interface, all incoming PPP sessions on that interface are authenticated using CHAP.
  - Likewise, if you configure **ppp authentication pap**, all incoming PPP sessions on that interface are authenticated using PAP.
  - If you configure **ppp authentication chap pap**, the router attempts to authenticate all incoming PPP sessions using CHAP. If the remote device does not support CHAP, the router tries to authenticate the PPP session using PAP. If the remote device does not support either CHAP or PAP, the authentication fails, and the PPP session is dropped.
  - If you configure **ppp authentication pap chap**, the router attempts to authenticate all incoming PPP sessions using PAP. If the remote device does not support PAP, the router tries to authenticate the PPP session using CHAP. If the remote device does not support either protocol, the authentication fails and the PPP session is dropped.

Note	If you enable both methods, the first method that you specify is requested during link negotiation. If the peer suggests using the second method or refuses the first method, the second method is tried.

The table provides a description of the commands that you use to configure CHAP authentication.

Command	Description
hostname *hostname*	Sets a device hostname.
username *username* **password** *password*	Configures a new user to the device.
interface *interface_name*	Enters the interface configuration mode for the specified interface.
encapsulation ppp	Configures a link with the PPP-type encapsulation.
ppp authentication chap	Enables CHAP authentication on the interface with PPP encapsulation.

Step 1 On R1, define the username "R2" using the "cisco" password.

On R1, enter the following command:

```
R1# conf t
R1(config)# username R2 password cisco
```

The username value is not case-sensitive, but the password value is case-sensitive.

Step 2 On R2, define the username "R1" using the "cisco" password.

On R2, enter the following command:

```
R2# conf t
R2(config)# username R1 password cisco
```

Step 3 Change the PPP authentication type to CHAP on the Serial1/1 interface on R1. You also need to remove all configuration related to PAP authentication.

On R1, enter the following commands:

```
R1# conf t
R1(config)# interface Serial1/1
R1(config-if)# no ppp authentication pap
R1(config-if)# no ppp pap sent-username User1 password cisco
R1(config-if)# ppp athentication chap
R1(config-if)# exit
R1(config)#
```

Step 4 Change the PPP authentication type to CHAP on the Serial1/1 interface on R2. You also need to remove all configuration related to PAP authentication.

On R2, enter the following commands:

```
R2# conf t
R2(config)# interface Serial1/1
R2(config-if)# no ppp authentication pap
R1(config-if)# no ppp pap sent-username User2 password cisco
R2(config-if)# ppp authentication chap
R2(config-if)# exit
R2(config)#
```

Step 5 Enable debugging of PPP authentication on R2. Then disable and reenable the interface Serial1/1 to reinitiate PPP session establishment. Observe the debug messages associated with the CHAP authentication process.

On R2, enter the following commands:

```
R2(config)# interface Serial 1/1
R2(config-if)# do debug ppp authentication
PPP authentication debugging is on
R2(config-if)# shutdown
*Dec  7 09:37:38.093: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1
(Serial1/1) is down: interface down
R2(config-if)#
*Dec  7 09:37:40.093: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to down
*Dec  7 09:37:40.093: %LINK-5-CHANGED: Interface Serial1/1, changed state to
administratively down
R2(config-if)# no shutdown
R2(config-if)#
*Dec  7 09:40:57.897: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
*Dec  7 09:40:57.897: Se1/1 PPP: Using default call direction
*Dec  7 09:40:57.897: Se1/1 PPP: Treating connection as a dedicated line
*Dec  7 09:40:57.897: Se1/1 PPP: Session handle[F000011] Session id[16]
*Dec  7 09:40:57.923: Se1/1 CHAP: O CHALLENGE id 1 len 23 from "R2"
*Dec  7 09:40:57.927: Se1/1 CHAP: I CHALLENGE id 1 len 23 from "R1"
*Dec  7 09:40:57.927: Se1/1 PPP: Sent CHAP SENDAUTH Request
*Dec  7 09:40:57.927: Se1/1 PPP: Received SENDAUTH Response PASS
*Dec  7 09:40:57.927: Se1/1 CHAP: Using hostname from configured hostname
*Dec  7 09:40:57.927: Se1/1 CHAP: Using password from AAA
*Dec  7 09:40:57.927: Se1/1 CHAP: O RESPONSE id 1 len 23 from "R2"
*Dec  7 09:40:57.933: Se1/1 CHAP: I RESPONSE id 1 len 23 from "R1"
*Dec  7 09:40:57.933: Se1/1 PPP: Sent CHAP LOGIN Request
*Dec  7 09:40:57.933: Se1/1 PPP: Received LOGIN Response PASS
*Dec  7 09:40:57.938: Se1/1 CHAP: O SUCCESS id 1 len 4
*Dec  7 09:40:57.943: Se1/1 CHAP: I SUCCESS id 1 len 4
R2(config-if)#
*Dec  7 09:40:57.943: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to up
R2(config-if)#
*Dec  7 09:41:01.348: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1
(Serial1/1) is up: new adjacency
R2(config-if)# end
R2#
```

The debug output shows the bidirectional CHAP authentication procedure. Both sides challenge each other, respond to each other, and pass each other. After successful authentication, the line protocol comes back up and EIGRP neighbor relationship gets established.

Step 6 For one last verification of connectivity, from R2, ping the R1 Loopback0 interface (192.168.1.1).

On R2, enter the following command:

```
R2# ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 33/33/34 ms
```

Step 7 On R2, verify that the PPP session gets established.

On R2, enter the following command:

```
R2# show ppp all
Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ --------------------- -------- --------------- -------------------
-
Se1/1        LCP+ CHAP+ IPCP+ CDP> LocalT   10.1.1.1        R1
```

The PPP session is established using the CHAP authentication method on the Serial1/1 interface to the peer that is named R1 using the peer IP address 10.1.1.1.

This is the end of the discovery lab.

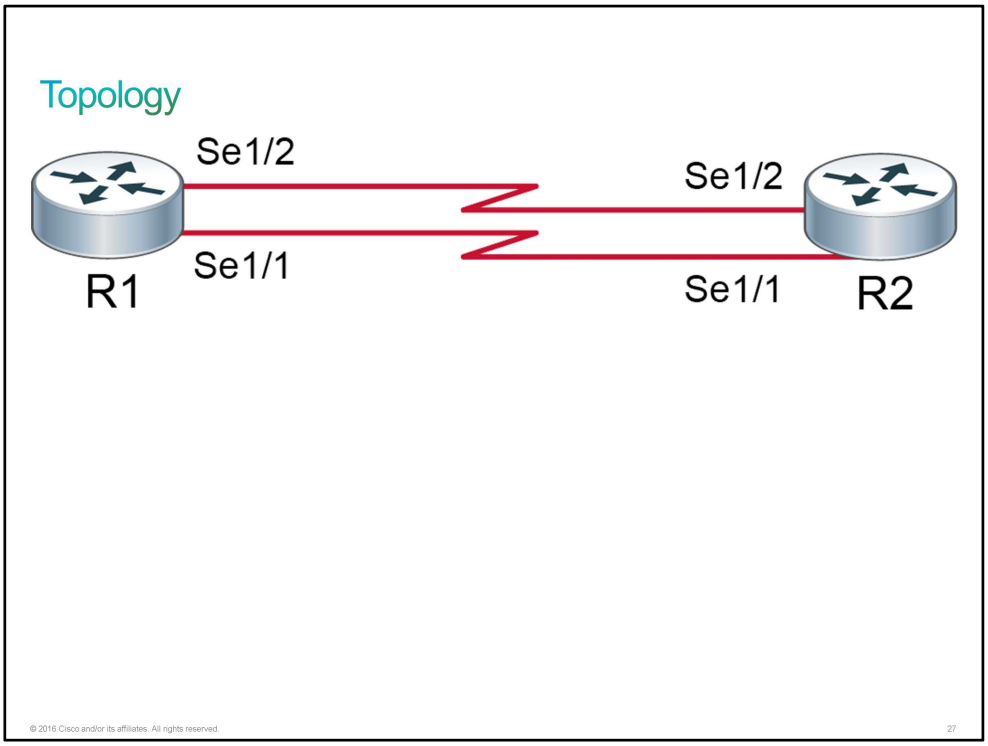
Discovery 48: Configure and Verify MLP

Introduction

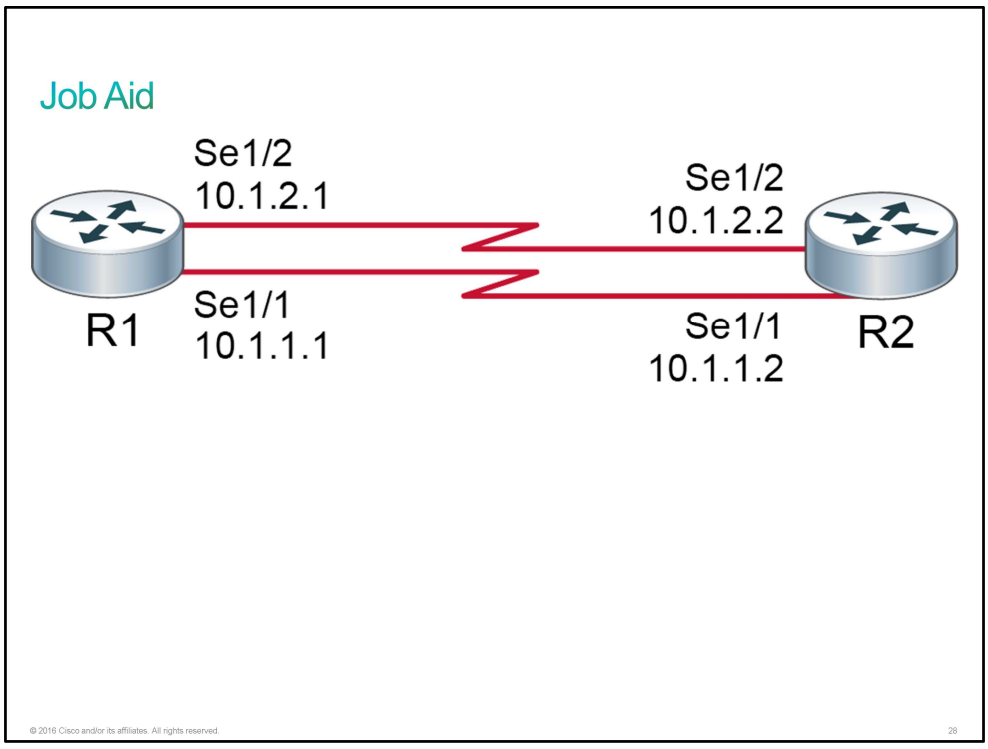
This discovery will guide you through the configuration of the Multilink PPP, also known as MLP. MLP provides a method for spreading traffic across multiple distinct PPP connections. You can use it, for example, to connect a home computer to an Internet Service Provider using two traditional modems, or to connect a company through two leased lines.

You will configure an MLP bundle on the R1 and R2 routers, which are connected using two serial interfaces.

Topology



Job Aid



The configuration is as follows:

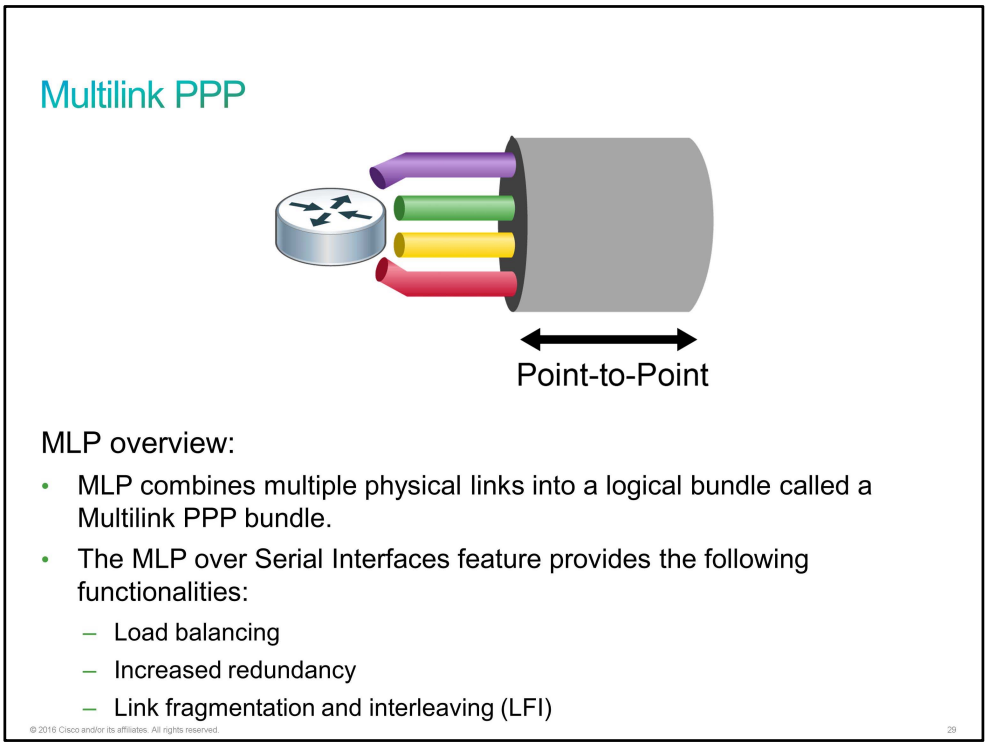
- Both routers have their basic configurations in place, including hostnames and IP addresses.
- PPP encapsulation is configured on all Serial interfaces.

Device Details

Device	Interface	Neighbor	IP Address
R1	Serial1/1	R2	10.1.1.1/24
R1	Serial1/2	R2	10.1.2.1/24
R1	Loopback0	—	192.168.1.1/24
R1	Loopback1	—	172.16.1.1/24
R2	Serial1/1	R1	10.1.1.2/24
R2	Serial1/2	R1	10.1.2.2/24
R2	Loopback0	—	192.168.2.1/24
R2	Loopback1	—	172.16.2.1/24

Task 1: Configure and Verify MLP

Activity



The MLP feature provides a load-balancing functionality over multiple WAN links while providing multivendor interoperability and support for packet fragmentation, proper sequencing, and load calculation on both inbound and outbound traffic. The MLP feature supports the fragmentation and packet sequencing specifications that are described in RFC 1990.

MLP allows packets to be fragmented and fragments to be sent at the same time over multiple point-to-point links to the same remote address. Multiple links come up in response to a defined dialer load threshold. The load can be calculated on inbound or outbound traffic, as required, for the traffic between specific sites. MLP provides bandwidth on demand and reduces transmission latency across WAN links.

MLP can work over synchronous and asynchronous serial types of single or multiple interfaces that have been configured to support both dial-on-demand rotary groups and PPP encapsulation.

MLP combines multiple physical links into a logical bundle that is called an MLP bundle. An MLP bundle is a single, virtual interface that connects to the peer system. Having a single interface (MLP bundle interface) provides a single point to apply hierarchical queueing, shaping, and policing to traffic flows. Individual links in a bundle do not perform any hierarchical queueing. None of the links have any knowledge about the traffic on parallel links. Hierarchical queueing and QoS cannot be applied uniformly to the entire aggregate traffic between a system and its peer system. A single, virtual interface also simplifies the task of monitoring traffic to the peer system (for example, all traffic statistics run on one interface).

MLP works with fully functional PPP interfaces. An MLP bundle can have multiple links connecting peer devices. These links can be serial links or broadband links (Ethernet or ATM). As long as each link behaves like a standard serial interface, mixed links work properly in a bundle.

The MLP over serial interfaces feature enables you to bundle interfaces into a single, logical connection called an MLP bundle. The MLP over serial interfaces feature also provides the following functionalities:

- **Load balancing:** MLP provides bandwidth on demand and uses load balancing across all member links (up to ten) to transmit packets and packet fragments. MLP mechanisms calculate the load on inbound or outbound traffic between specific sites. Because MLP splits packets and fragments across all member links during transmission, MLP reduces transmission latency across WAN links. Ideally, all member links in a bundle would be of the same bandwidth (for example, T1s). Load balancing and fragmentation and interleaving also allow for a mix of unequal cost member links for situations where a small increment in the bundle bandwidth is required.
- **Increased redundancy:** MLP allows traffic to flow over remaining member links when a port fails. When you configure an MLP bundle that consists of T1 lines from more than one line card and if one line card stops operating, a part of the bundle on other line cards continues to operate.
- **Link fragmentation and interleaving**: The MLP fragmenting mechanism fragments large, nonreal-time packets and sends fragments at the same time over multiple point-to-point links to the same remote address. Smaller, real-time packets remain intact. The MLP interleaving mechanism sends real-time packets between fragments of nonreal-time packets, thus reducing real-time packet delay.

Step 1 Access the console of R1 and verify the status of serial interfaces that are connected to R2.

On R1, enter the following commands:

```
R1# show interfaces Serial1/1
Serial1/1 is up, line protocol is up
  Hardware is M4T
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, crc 16, loopback not set


R1# show interfaces Serial1/2
Serial1/2 is up, line protocol is up
  Hardware is M4T
  Internet address is 10.1.2.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, crc 16, loopback not set
```

Interfaces Serial1/1 and Serial1/2 are connected to R2. Both interfaces are "up" and have an IP addresses assigned. Encapsulation is set to PPP on serial interfaces connecting R1 and R2.

Step 2 EIGRP has been preconfigured on both routers R1 and R2. Verify the content of the routing table on R1.

On R1, enter the following command:

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.1.1.0/24 is directly connected, Serial1/1
L        10.1.1.1/32 is directly connected, Serial1/1
C        10.1.1.2/32 is directly connected, Serial1/1
C        10.1.2.0/24 is directly connected, Serial1/2
L        10.1.2.1/32 is directly connected, Serial1/2
C        10.1.2.2/32 is directly connected, Serial1/2
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Loopback1
L        172.16.1.1/32 is directly connected, Loopback1
D        172.16.2.0/24 [90/2297856] via 10.1.2.2, 20:06:22, Serial1/2
                       [90/2297856] via 10.1.1.2, 20:06:22, Serial1/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback0
L        192.168.1.1/32 is directly connected, Loopback0
D     192.168.2.0/24 [90/2297856] via 10.1.2.2, 20:06:22, Serial1/2
                     [90/2297856] via 10.1.1.2, 20:06:22, Serial1/1
```

The marked networks have been learned via EIGRP. Traffic to these networks is load-balanced via Serial1/1 and Serial1/2 links.

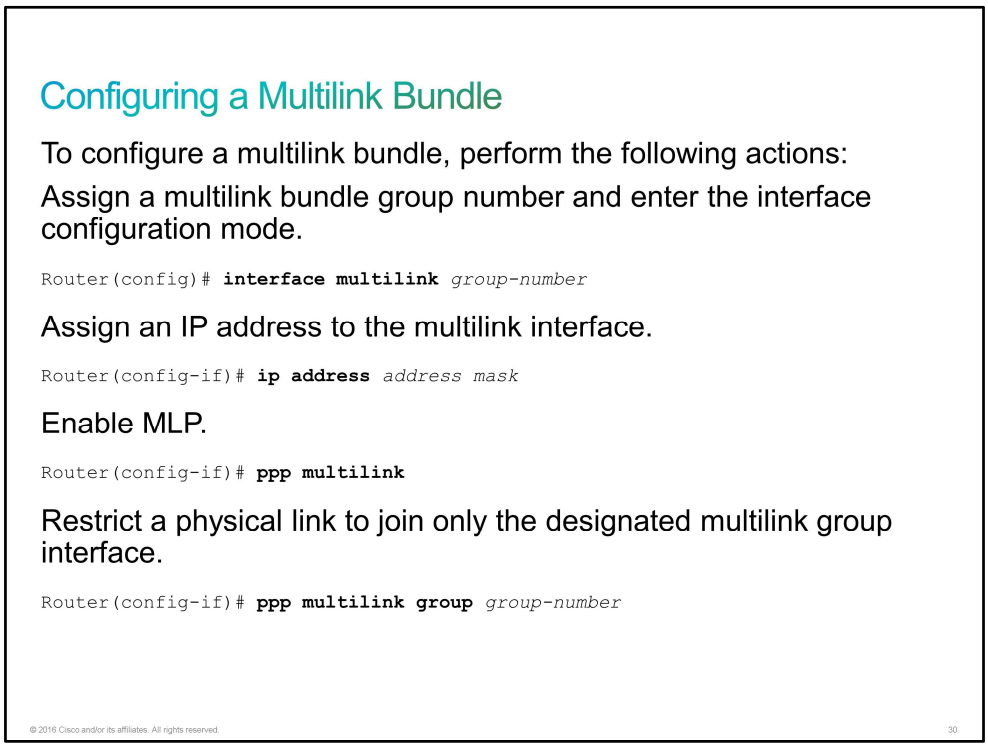
Step 3 From R1, ping the Loopback0 interface (192.168.2.1) on R2.

On R1, enter the following command:

```
R1# ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 21/21/21 ms
```

The ping should be successful.

Configuring a Multilink Bundle



When configuring MLP, you need to first configure a multilink bundle by creating a multilink interface. You need to assign an IP address to this multilink interface, enable the MLP feature, and restrict a physical link to join only the designated multilink group interface.

Step 4 Create a multilink interface on R1 with the following specified characteristics:

- Group number: 1
- IP address: 10.1.1.1/24
- Enable the MLP feature.
- Restrict physical links with the multilink group 1 only to join this bundle.

On R1, enter the following commands:

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface Multilink1
R1(config-if)#
*Dec  9 10:28:40.548: %LINK-3-UPDOWN: Interface Multilink1, changed state to
down
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# ppp multilink
R1(config-if)# ppp multilink group 1
R1(config-if)# end
R1#
```

Step 5 Create a multilink interface on R2 with the following specified characteristics.

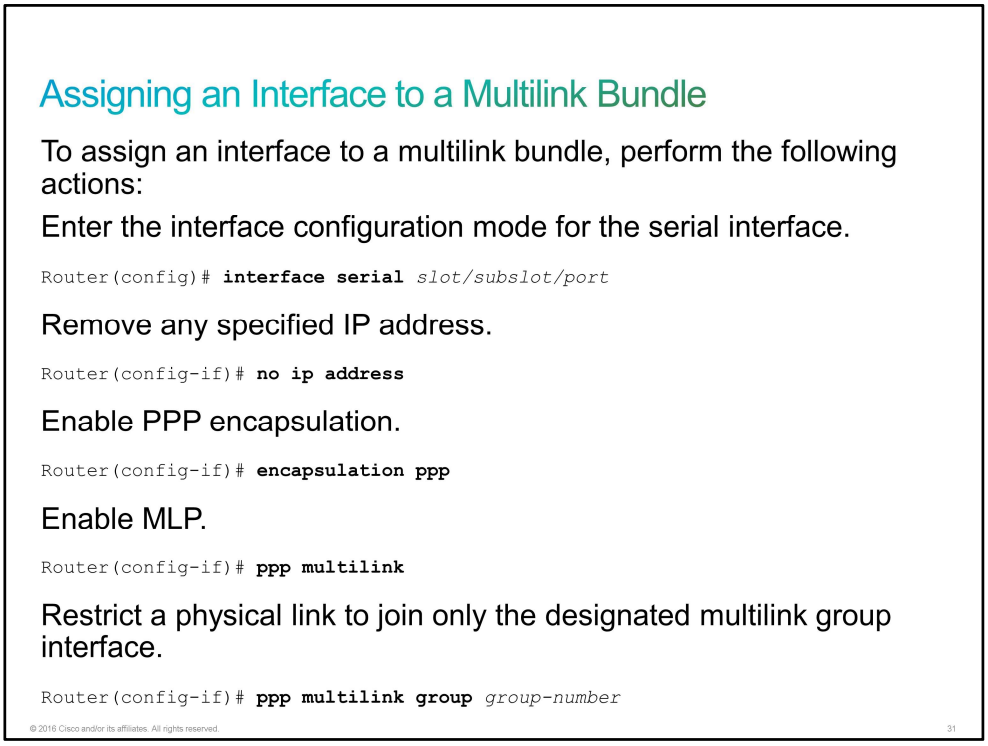
- Group number: 1

- IP address: 10.1.1.2/24
- Enable the MLP feature.
- Restrict physical links with the multilink group 1 only to join this bundle.

On R2, enter the following commands:

```
R2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# interface Multilink1
R2(config-if)#
*Dec  9 10:31:38.411: %LINK-3-UPDOWN: Interface Multilink1, changed state to
down
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# ppp multilink
R2(config-if)# ppp multilink group 1
R2(config-if)# end
R2#
```

Assigning an Interface to a Multilink Bundle



After you have created the multilink interface, you need to assign a serial interface to a multilink interface.

To designate a link to a specified bundle, use the **ppp multilink group** command for configuring the link. This command restricts the link to join only the specified bundle. When a link negotiates to join an MLP bundle, the link must provide proper identification that is associated with the MLP bundle. If the negotiation is successful, the link is assigned to the requested MLP bundle. If the link provides identification that coincides with the identification that is associated with a different MLP bundle in the system or if the link fails to match the identity of an MLP bundle that is already active on the multilink group interface, the connection terminates.

A link joins an MLP bundle only if it negotiates to use the bundle when a connection is established and the identification information that is exchanged matches that of an existing bundle.

When you configure the **ppp multilink group** command on a link, the command applies the following restrictions on the link:

- The link is not allowed to join any bundle other than the indicated group interface.
- The PPP session must be terminated if the peer device attempts to join a different bundle.

Step 6 Remove the IP addresses from Serial1/1 and Serial1/2 interfaces on both R1 and R2.

On R1 and R2, enter the following commands:

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface Serial1/1
R1(config-if)# no ip address
R1(config-if)#
*Dec  9 10:21:57.098: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.2
(Serial1/1) is down: interface down
R1(config-if)# exit
R1(config)# interface Serial1/2
R1(config-if)# no ip address
R1(config-if)#
*Dec  9 10:22:13.474: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.2.2
(Serial1/2) is down: interface down
R1(config-if)# end
R1#


R2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# interface Serial1/1
R2(config-if)# no ip address
R2(config-if)# exit
R2(config)# interface Serial1/2
R2(config-if)# no ip address
R2(config-if)# end
R1#
```

Immediately after you remove the IP address from the interfaces on R1 router, the EIGRP neighbor goes down.

Step 7 Assign interfaces Serial1/1 and Serial1/2 to the interface Multilink1 on R1.

On R1, enter the following command:

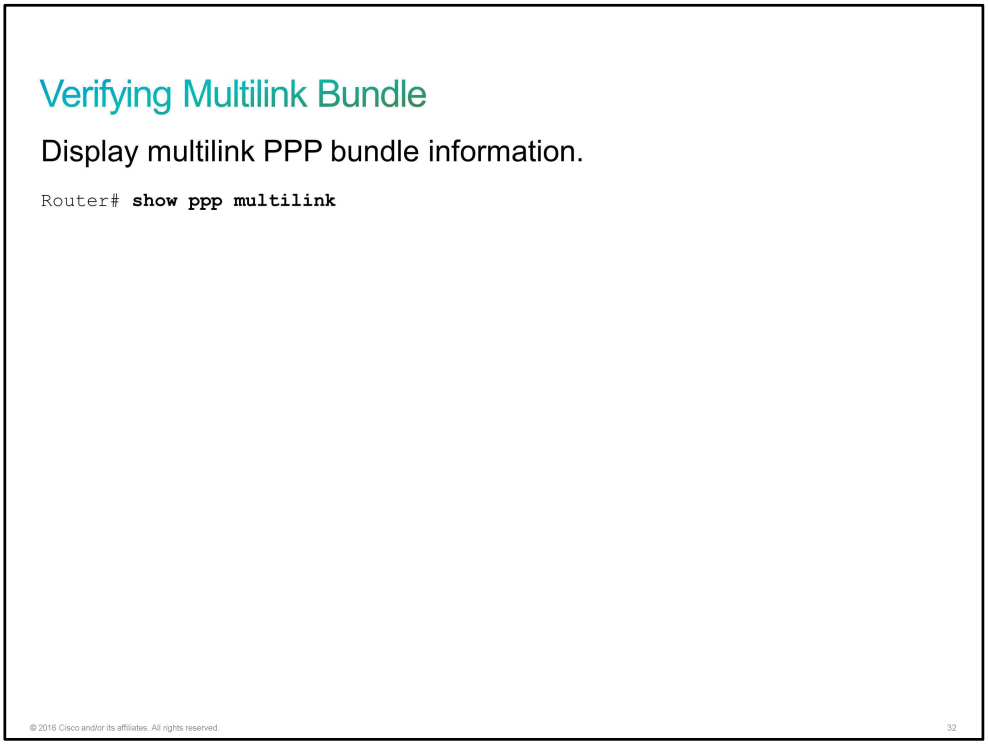
```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface Serial1/1
R1(config-if)# ppp multilink
*Dec  9 10:33:52.141: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to down
*Dec  9 10:33:52.176: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to up
R1(config-if)# ppp multilink group 1
R1(config-if)#
*Dec  9 10:34:05.996: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to down
*Dec  9 10:34:06.031: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to up
R1(config-if)# exit
R1(config)# interface Serial1/2
R1(config-if)# ppp multilink
R1(config-if)#
*Dec  9 10:34:26.927: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/2, changed state to down
*Dec  9 10:34:26.954: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/2, changed state to up
R1(config-if)# ppp multilink group 1
R1(config-if)#
*Dec  9 10:34:33.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/2, changed state to down
*Dec  9 10:34:33.965: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/2, changed state to up
R1(config-if)# end
R1#
```

Step 8 Assign interfaces Serial1/1 and Serial1/2 to the interface Multilink1 on R2.

On R2, enter the following command:


```
R2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# interface Serial1/1
R2(config-if)# ppp multilink
*Dec  9 10:35:13.501: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to down
*Dec  9 10:35:13.540: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to up
*Dec  9 10:35:13.555: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state
to up
*Dec  9 10:35:13.555: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-
Access1, changed state to up
R2(config-if)# ppp multilink group 1
R2(config-if)#
*Dec  9 10:35:31.049: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to down
*Dec  9 10:35:31.050: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-
Access1, changed state to down
*Dec  9 10:35:31.051: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state
to down
*Dec  9 10:35:31.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/2, changed state to down
*Dec  9 10:35:31.073: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to up
*Dec  9 10:35:31.087: %LINK-3-UPDOWN: Interface Multilink1, changed state to up
R2(config-if)#
*Dec  9 10:35:31.087: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Multilink1, changed state to up
*Dec  9 10:35:31.104: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/2, changed state to up
*Dec  9 10:35:31.316: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1
(Multilink1) is up: new adjacency
R2(config-if)# exit
R2(config)# interface Serial1/2
R2(config-if)# ppp multilink
*Dec  9 10:35:56.861: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/2, changed state to down
*Dec  9 10:35:56.902: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/2, changed state to up
*Dec  9 10:35:56.912: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/2, changed state to down
R2(config-if)# ppp multilink group 1
*Dec  9 10:36:00.966: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/2, changed state to up
*Dec  9 10:36:00.975: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/2, changed state to down
*Dec  9 10:36:05.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/2, changed state to up
```

Verifying Multilink Bundle



The **show ppp multilink** command verifies that all the desired interfaces are bundled into multilink PPP bundle.

Step 9 Verify the multilink PPP bundle information using the **show ppp multilink** command on R1.

On R1, enter the following command:

```
R1# show ppp multilink

Multilink1
  Bundle name: R2
  Remote Endpoint Discriminator: [1] R2
  Local Endpoint Discriminator: [1] R1
  Bundle up for 01:32:05, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 53 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x56E received sequence, 0x572 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
    Se1/1, since 01:32:05
    Se1/2, since 01:31:31
No inactive multilink interfaces
```

The physical interfaces Serial1/1 and Serial1/2 are members of the logical interface bundle Multilink 1.

Step 10 Shut down the interface Serial1/1 on R1 to simulate a failure on this link.

On R1, enter the following command:


```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface Serial1/1
R1(config-if)# shutdown
*Dec  9 13:13:34.223: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/1, changed state to down
*Dec  9 13:13:34.223: %LINK-5-CHANGED: Interface Serial1/1, changed state to
administratively down
R1(config-if)# end
R1#
```

Step 11 Verify the status of the interface Multilink1 on R1 router.

On R1, enter the following command:

```
R1# show interfaces Multilink1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open, multilink Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
<... output omitted ...>
```

The logical interface Multilink1 is still up, even though one of the members of the bundle was shut down.

Step 12 Verify the content of the routing table on R1 again.

On R1, enter the following command:

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/24 is directly connected, Multilink1
L        10.1.1.1/32 is directly connected, Multilink1
C        10.1.1.2/32 is directly connected, Multilink1
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Loopback1
L        172.16.1.1/32 is directly connected, Loopback1
D        172.16.2.0/24 [90/2297856] via 10.1.1.2, 00:14:24, Multilink1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback0
L        192.168.1.1/32 is directly connected, Loopback0
D     192.168.2.0/24 [90/2297856] via 10.1.1.2, 00:14:24, Multilink1
```

The outgoing interface in the routing table for networks learned via EIGRP points to the logical interface Multilink 1.

Step 13 From R1, ping the Loopback0 interface (192.168.2.1) on R2.

On R1, enter the following command:

```
R1# ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 21/21/21 ms
```

The ping should be successful despite the interface Serial1/1 on R1 being shut down. **Note**: You may have to wait couple of seconds, for a ping to work.

This is the end of the discovery lab.

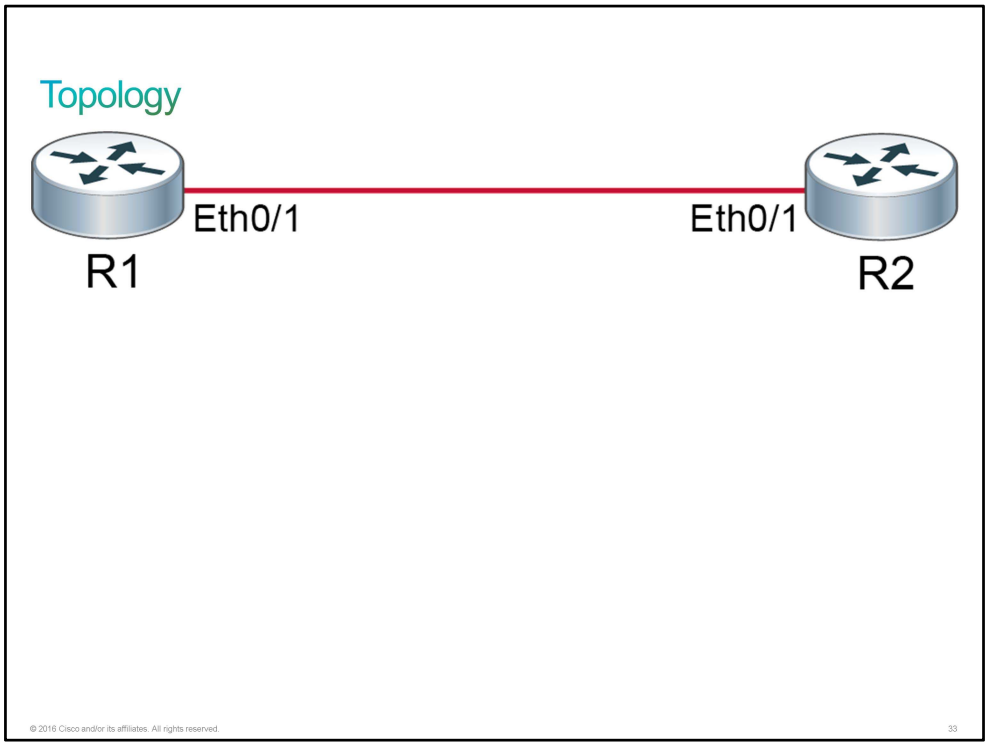
Discovery 49: Configure and Verify PPPoE Client

Introduction

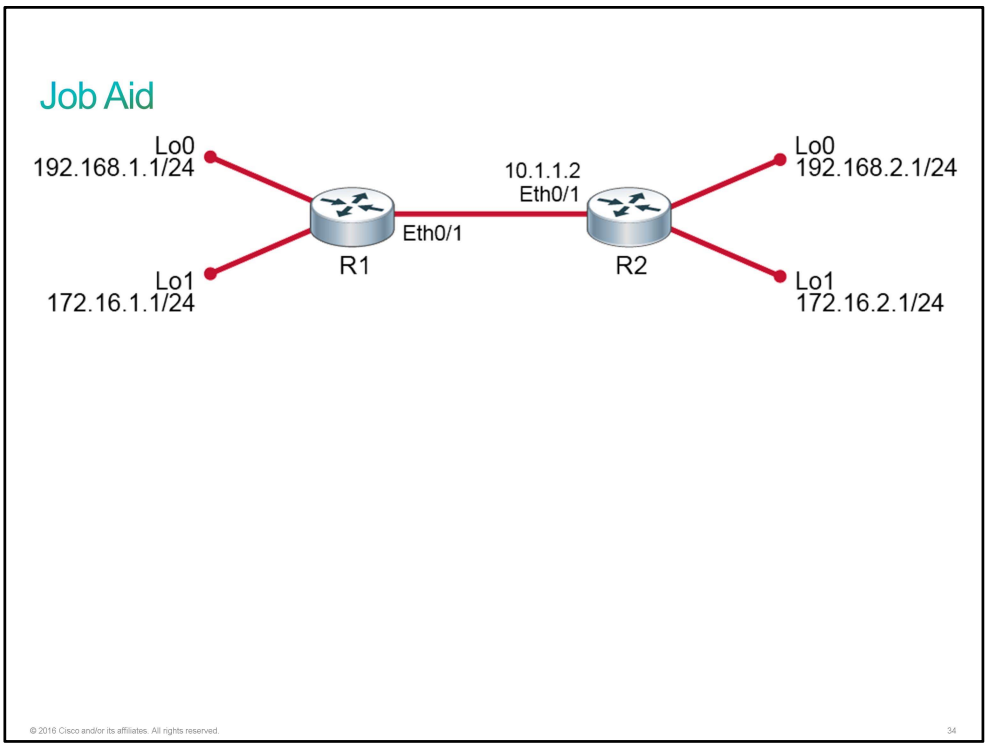
This discovery will guide you through the configuration of PPPoE client. PPoE provides an emulated (and optionally authenticated) point-to-point link across a shared medium, typically a broadband aggregation network such as the ones that you can find in DSL service providers. A very common scenario is to run a PPPoE client on the customer side, which connects to and obtains its configuration from the PPPoE server (head-end router) at the ISP side.

You will configure R1 as PPPoE client, while the R2 has been preconfigured as the PPPoE server.

Topology



Job Aid



The configuration is as follows:

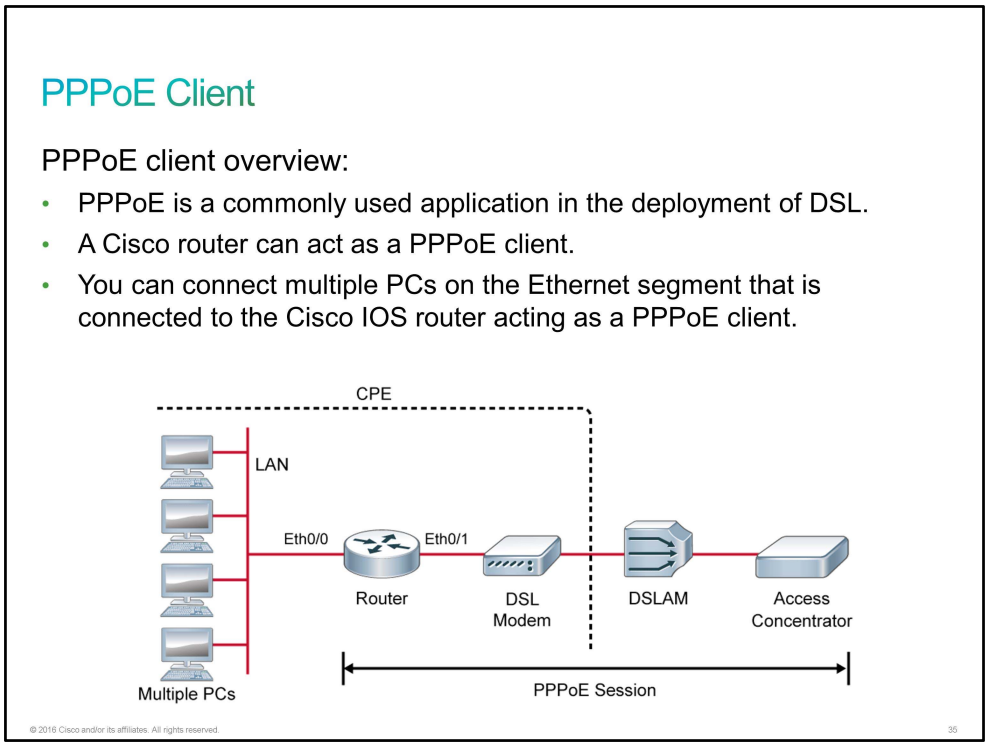
- Both routers have their basic configurations in place, including hostnames and IP addresses.
- R2 has been preconfigured as the PPPoE server.

Device Details

Device	Interface	Neighbor	IP Address
R1	Ethernet0/1	R2	—
R1	Loopback0	—	192.168.1.1/24
R1	Loopback1	—	172.16.1.1/24
R2	Ethernet0/1	R1	10.1.1.2/24
R2	Loopback0	—	192.168.2.1/24
R2	Loopback1	—	172.16.2.1/24

Task 1: Configure and Verify PPPoE Client

Activity



The PPPoE client feature provides PPPoE client support on routers on customer premises. Before the introduction of this feature, Cisco IOS software supported PPPoE on the access server side only. The figure shows a typical network topology for PPPoE client deployment.

PPPoE is a commonly used application in the deployment of DSL. The PPPoE client feature expands the PPPoE functionality by providing support for PPPoE on both the client and on the server.

ISPs often provide their customers with a DSL modem that has one Ethernet interface to connect to the customer Ethernet segment, and another interface for DSL line connectivity. ATM is typically run between the customer's modem and the DSLAM. In such a case, the DSL modem acts only as a bridge if the CPE is not configurable for any IP connectivity or enhanced features over DSL. This situation limits your connectivity to only one PPPoE client PC. With the addition of a Cisco IOS router that connects to the Ethernet of the DSL modem, you can run the PPPoE client IOS feature on the Cisco router. This way, you can connect multiple PCs on the Ethernet segment that is connected to the Cisco IOS router. With the use of the Cisco IOS router, you can enhance your DSL connectivities and all IOS features, such as Security, NAT, and DHCP to internal hosts.

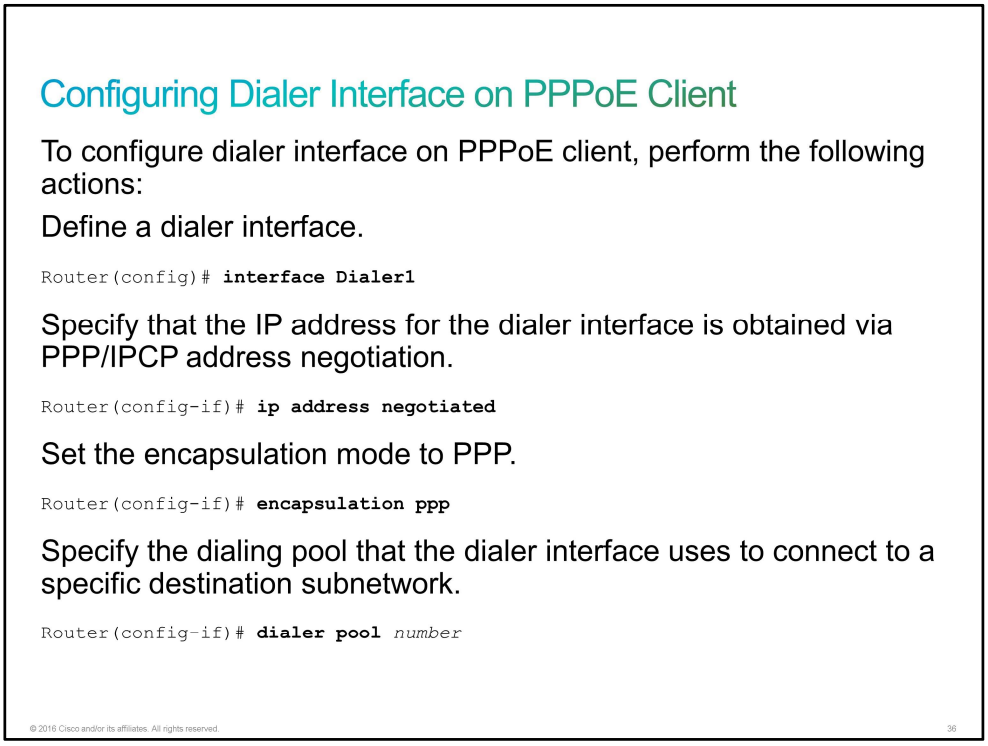
The PPPoE client initiates a PPPoE session. If the session has a timeout or is disconnected, the PPPoE client will immediately attempt to re-establish the session. The following four steps describe the exchange of packets that occurs when a PPPoE client initiates a PPPoE session:

1. The client broadcasts a PADI packet.
2. When the access concentrator receives a PADI that it can serve, it replies by sending a PADO packet to the client.

3. Because the PADI was broadcast, the host may receive more than one PADO packet. The host looks through the PADO packets that it receives and chooses one. The choice can be based on the access concentrator name or on the services that are offered. The host then sends a single PADR packet to the access concentrator that it has chosen.
4. The access concentrator responds to the PADR by sending a PADS packet. At this point, a virtual access interface is created that will then negotiate the PPP, and the PPPoE session will run on this virtual access.

If a client does not receive a PADO for a preceding PADI, the client sends out a PADI at predetermined intervals. That interval length is doubled for every successive PADI that does not evoke a response, until the interval reaches a configured maximum. If PPP negotiation fails or the PPP line protocol is brought down for any reason, the PPPoE session and the virtual access will be brought down. When the PPPoE session is brought down, the client waits for a predetermined number of seconds before trying again to establish a PPPoE.

Configuring Dialer Interface on PPPoE Client



The PPPoE client configuration is relatively simple. You need to create a dialer interface to handle the PPPoE connection, and tie it later to a physical interface that provides the transport.

To create a dialer interface and to enter the interface configuration mode, use the **interface dialer** *number* command. When you are in the interface configuration mode, you need to specify that the IP address for a dialer interface is obtained via PPP/IPCP address negotiation. Also, set the encapsulation mode to PPP. The last task requires of you to specify the dialing pool that the dialer interface uses to connect to a specific destination subnetwork.

Step 1 Create a dialer interface to handle the PPPoE connection:

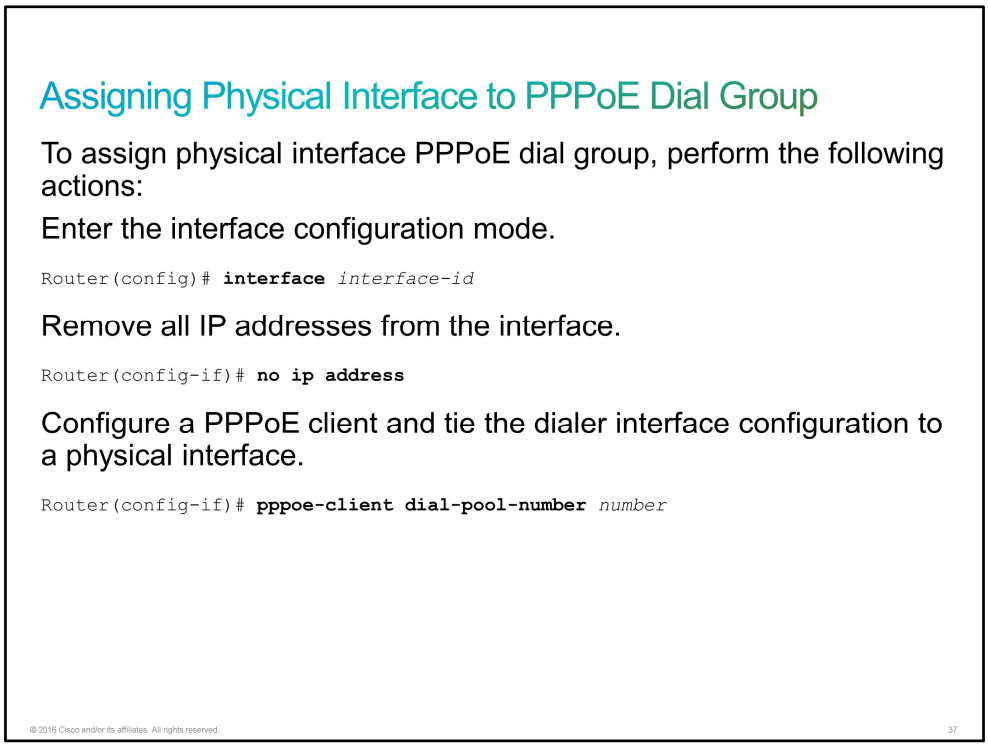
- Instruct the client to use an IP address provided by the PPPoE server.

- Set the encapsulation type to PPP.
- Specify the dialing pool that the dialer interface uses to connect to a specific destination subnetwork to "1."

On R1, enter the following command:

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface Dialer1
R1(config-if)# ip address negotiated
R1(config-if)# encapsulation ppp
R1(config-if)# dialer pool 1
R1(config-if)# end
R1#
```

Assigning Physical Interface to PPPoE Dial Group



You need to tie the dialer interface configuration to a physical interface using the **pppoe-client dial-pool-number** *number* command. You also need to make sure that no IP address is manually assigned to the physical interface.

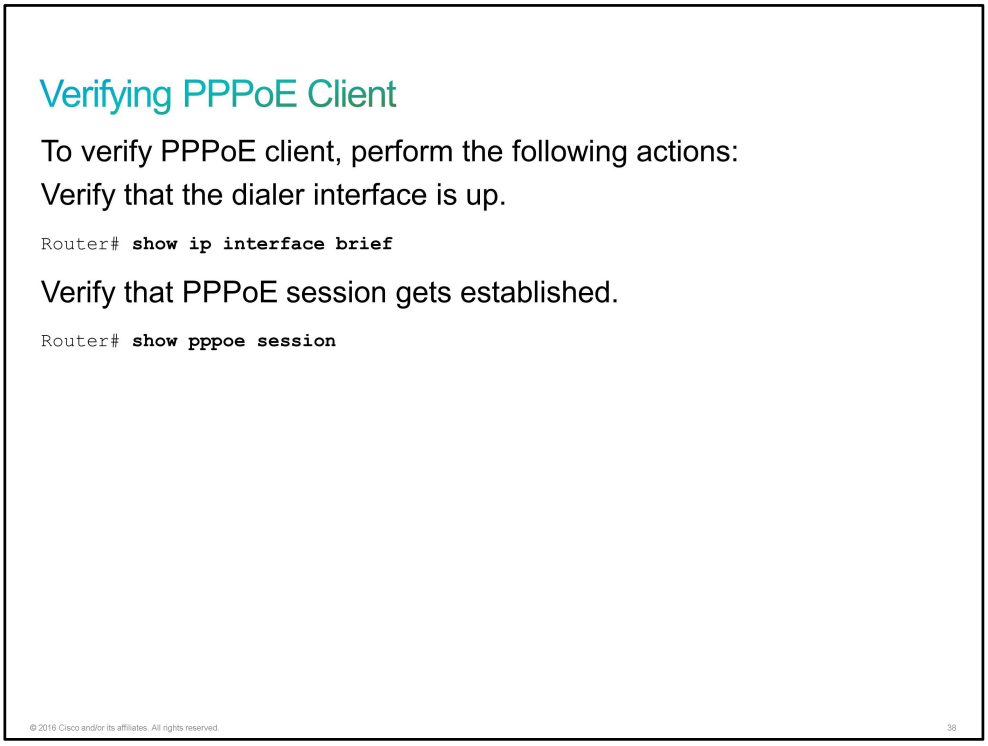
Step 2 Assign the interface Ethernet0/1 to a newly created PPPoE dial group 1. Also make sure that no IP address is manually assigned to the Ethernet0/1 interface.

On R1, enter the following command:

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface Ethernet0/1
R1(config-if)# no ip address
R1(config-if)# pppoe-client dial-pool-number 1
*Dec 11 12:49:17.540: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Dec 11 12:49:17.541: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state
to up
R1(config-if)#
*Dec 11 12:49:17.550: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-
Access2, changed state to up
*Dec 11 12:49:17.593: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.10.10.2
(Dialer1) is up: new adjacency
R1(config-if)# end
R1#
```

You should see a notification indicating the PPPoE session has successfully formed. EIGRP neighbor relationship also gets established between R1 and R2 immediately after an IP address is assigned to the R1 router (PPPoE client) from R2 router (PPPoE server).

Verifying PPPoE Client



When verifying a PPPoE client, first make sure that Dialer interface is up and running. Then also make sure that the PPPoE session gets established using the **show pppoe session** command.

Step 3 On R1, verify that the interface Dialer1 has negotiated an IP address from R2.

On R1, enter the following command:

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
Ethernet0/0                unassigned      YES NVRAM  up                    up
Ethernet0/1                unassigned      YES NVRAM  up                    up
<... output omitted ...>
Dialer1                    10.10.10.3      YES IPCP   up                    up
Loopback0                  192.168.1.1     YES NVRAM  up                    up
Loopback1                  172.16.1.1      YES NVRAM  up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  up                    up
```

R1 gets the IP address from PPPoE server R2, from the pool of IP addresses starting with 10.10.10.3 and ending with 10.10.10.10. Notice that the IP address is on the dialer interface, not the physical, Etheernet0/1 interface.

Step 4 Verify that PPPoE session gets established on R1.

On R1, enter the following command:

```
R1# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC          Port                 VT  VA         State
           SID  LocMAC                               VA-st      Type
    N/A      4  aabb.cc00.2010  Et0/1                Di1 Vi2        UP
                aabb.cc00.1f10                           UP
```

You should see that the PPPoE session gets established on the interface Ethernet0/1.

Note: The MAC addresses in your output may be different.

Step 5 From R1, ping the Loopback0 interface (192.168.1.2) on R2.

On R1, enter the following command:

```
R1# ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

The ping should be successful because EIGRP has been preconfigured on both routers.

This is the end of the discovery lab.

Challenge

1. Which of the following PPP authentication protocols authenticates a device on the other end of a link with an encrypted password?

   A. MD5
   B. PAP
   C. CHAP
   D. DES

2. Which two commands are the minimum that must be configured on two routers that have their serial links directly connected using DTE and DCE cables to ping each other? (Choose two.)

   A. **encapsulation ppp**
   B. **ip address**
   C. **clockrate**
   D. **no encapsulation hdlc**

3. Which of the following PPP protocols controls the layer 2 operation of PPP?

   A. IPCP
   B. LCP
   C. CDPCP
   D. IPXCP

4. Two routers, R1 and R2, have a leased line between them. Each router had its configuration erased and was then reloaded. R1 was then configured with the commands shown below:

```
R1(conf)# hostname R1
R1(conf)# interface s0/0
R1(config-if)# encapsulation ppp
R1(config-if)# ppp authentication chap
```

   Which configuration command can complete the configuration on R1 so that CHAP can work correctly? Assume that R2 has been configured correctly and that the password is "fred."

   A. No other configuration is needed.
   B. **ppp chap** (global command)
   C. **username R1 password fred**
   D. **username R2 password fred**
   E. **ppp chap password fred**

5. Shown below is the output of a show command. Which two statements about this router's S0/0/1 interface are true? (Choose two.)

```
R1# show interfaces serial 0/0/1
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
Internet address is 10.0.1.1/30
    MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP,CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
<Output omitted for brevity>
```

6. A. The interface is using HDLC.
   B. The interface is using PPP.
   C. The link should be able to pass PPP frames.
   D. The interface currently cannot pass IPv4 traffic.

```
R1# show interfaces serial 0/0/1
Serial0/0/0 is up, line protocol is down
  Hardware is GT96K Serial
Internet address is 10.0.1.1/30
```

Shown above is excerpt from the output of a show interfaces command on an interface that is configured to use PPP. A ping of the IP address on the other end of the link fails. Which two of the following are reasons for the failure, assuming that the problem that is listed in that answer is the only problem with the link? (Choose two.)

A. The CSU/DSU connected to the other router is not powered on.
B. The IP address on the router at the other end of the link is not in subnet 192.168.2.0/24.
C. CHAP authentication failed.
D. The router on the other end of the link has been configured to use HDLC.

7. Which username must be configured on routers for PPP CHAP authentication?

   A. a username that matches the hostname of the local router
   B. a username that matches the hostname of the remote router
   C. a username that matches neither hostname
   D. There is no restriction on usernames.

Answer Key

Challenge

1. C
2. A, B
3. B
4. D
5. B, C
6. C, D
7. B

Lesson 3: Configuring GRE Tunnels

Introduction

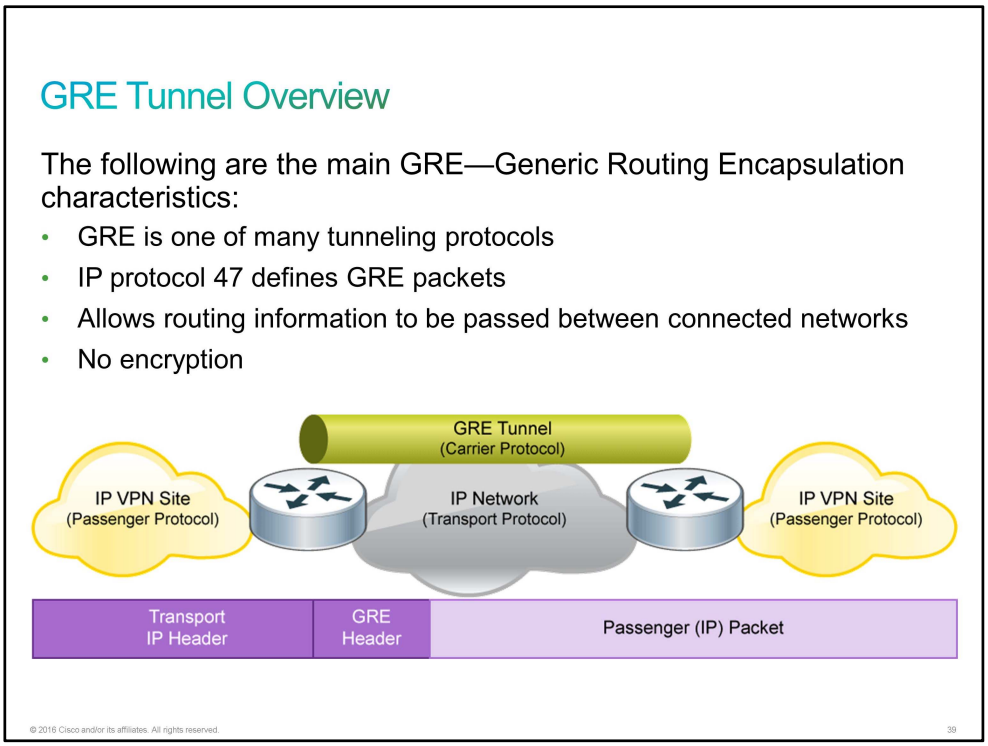
A customer wants to connect a branch office to its headquarters. Because the connection is over the Internet and running a routing protocol, CCS has determined that the customer needs a GRE tunnel. You are the technician who is assigned to do the deployment and need to know how to establish a GRE tunnel and verify its proper operation. Would you like to go onsite now to complete the job or study the training "Configuring GRE Tunnels"?

GRE Tunnel Overview

Generic Routing Encapsulation, also known as GRE, is a tunneling protocol which provides a secure path for transporting packets over a public network by encapsulating packets inside a transport protocol. GRE supports multiple Layer 3 protocols such as IP, IPX, and AppleTalk. It also enables the use of multicast routing protocols across the tunnel.

GRE adds a 20-byte IP header and a 4-byte GRE header, hiding the existing packet headers. The GRE header contains a flag field and a protocol type field to identify the Layer 3 protocol being transported. It may contain a tunnel checksum, tunnel key, and tunnel sequence number. GRE does not encrypt traffic or use any strong security measures to protect the traffic.

GRE can be used along with IPsec to provide data source authentication and data confidentiality and ensure data integrity. GRE over IPsec tunnels are typically configured in a hub-and-spoke topology over an untrusted WAN to minimize the number of tunnels that each router must maintain.



Note	GRE, developed by Cisco, is designed to encapsulate arbitrary types of network layer packets inside arbitrary types of network layer packets, as defined in RFC 1701, *Generic Routing Encapsulation (GRE)*; RFC 1702, *Generic Routing Encapsulation over IPv4 Networks*; and RFC 2784, *Generic Routing Encapsulation (GRE)*.

A tunnel interface supports a header for each of the following:

- A passenger protocol or encapsulated protocol such as IPv4 or IPv6. This protocol is the one that is being encapsulated.
- A carrier or encapsulation protocol (GRE, in this case).
- A transport delivery protocol, such as IP, which is the protocol that carries the encapsulated protocol.

GRE has these characteristics:

- It uses a protocol-type field in the GRE header to support the encapsulation of any OSI Layer 3 protocol.
- It is stateless. It does not include any flow-control mechanisms, by default.
- It does not include any strong security mechanisms to protect its payload.
- The GRE header, together with the tunneling IP header, creates at least 24 bytes of additional overhead for tunneled packets.

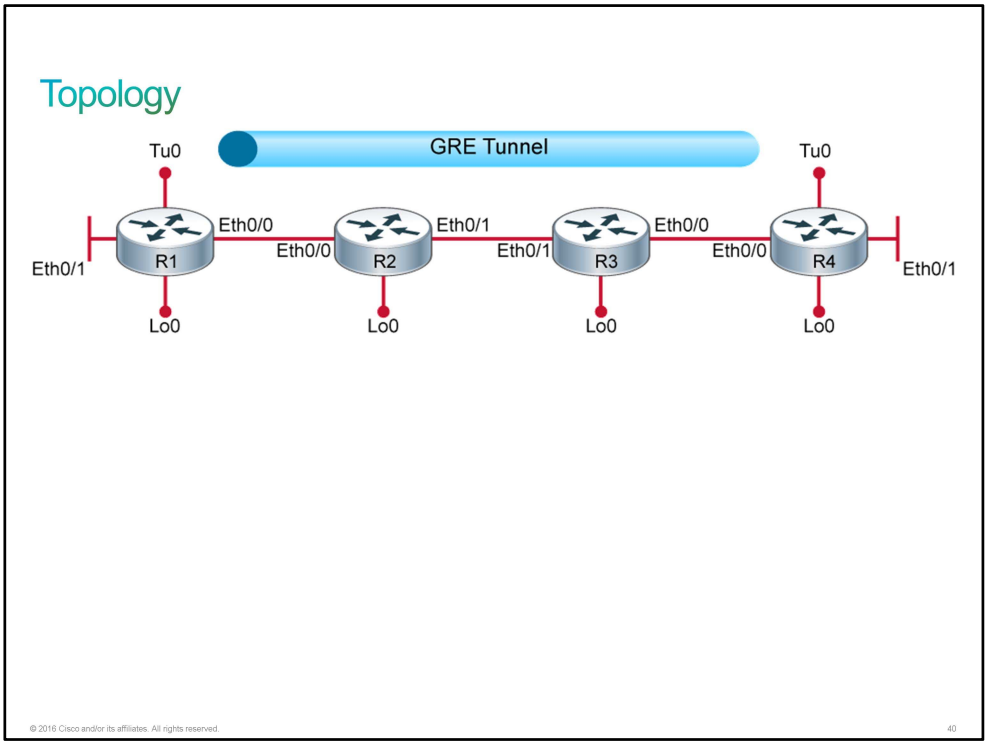
Note	You may have to adjust MTU on GRE tunnels, using **ip mtu** interface configuration command. This MTU must match on both sides.

Discovery 50: Configure and Verify GRE Tunnel

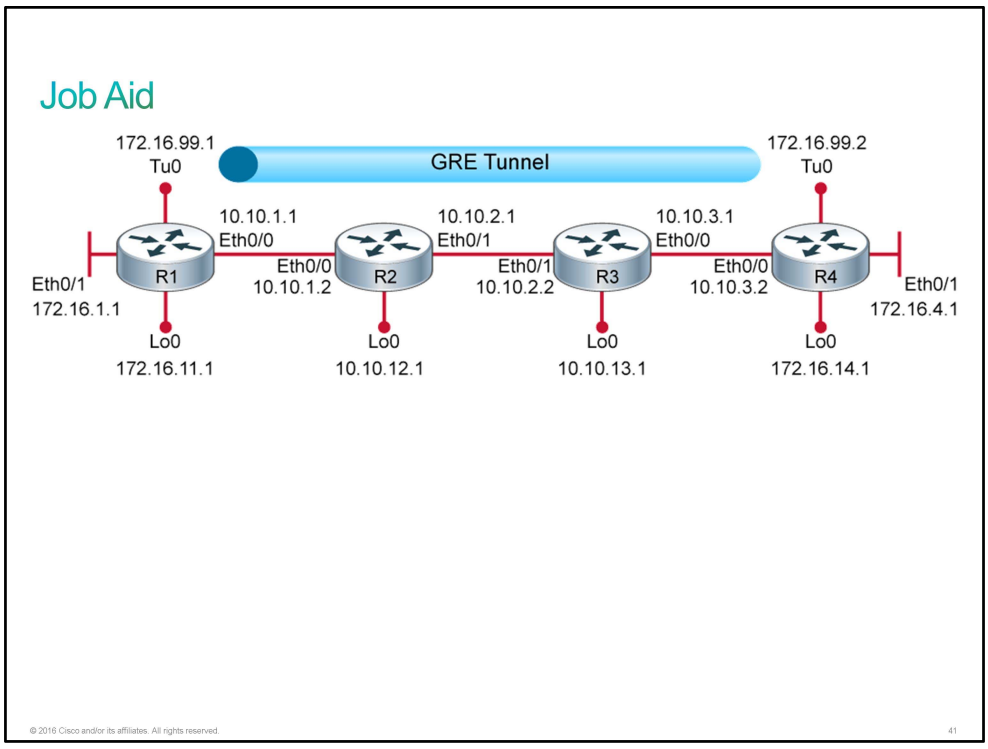
Introduction

This discovery will guide you through the configuration, verification, and usage of a GRE tunnel to connect IP networks using a completely different IP network as a transit link. The live virtual lab is prepared with the devices represented in the topology diagram and the connectivity table. All devices have their basic configurations in place, including hostnames and IP addresses on the Ethernet and loopback interfaces. EIGRP has been configured on R2 and R3 for the 10.0.0.0/8 network. R2 and R3 are not aware of any of the 172.16.0.0/16 networks that exist on R1 and R4. The tunnel interfaces have not yet been configured. Configuring them is one of your tasks during this discovery. Once the tunnel interfaces are up and operational, you will verify connectivity between the 172.16.0.0/16 networks through the GRE tunnel.

Topology



Job Aid



The configuration is as follows:

- All devices have their basic configurations in place, including hostnames and IP addresses.
- EIGRP is configured on R2 and R3.
- A static route is configured for 10.0.0.0/8 on R1 and R4.
- OSPF is configured on R1 and R4 after the tunnel is configured.

Device Information

Device Details

Device	Interface	Neighbor	IP Address
R1	Ethernet 0/0	R2	10.10.1.1/24
R1	Ethernet 0/1	—	172.16.1.1/24
R1	Loopback 0	—	172.16.11.1/24
R1	Tunnel 0	R4	172.16.99.1
R2	Ethernet 0/0	R1	10.10.1.2/24
R2	Ethernet 0/1	R3	10.10.2.1/24

Device	Interface	Neighbor	IP Address
R2	Loopback	—	10.10.12.1/24
R3	Ethernet 0/0	R4	10.10.3.1/24
R3	Ethernet 0/1	R2	10.10.2.2/24
R3	Loopback 0	—	10.10.13.1/24
R4	Ethernet 0/0	R3	10.10.3.2/24
R4	Ethernet 0/1	—	172.16.4.1/24
R4	Loopback 0	—	172.16.14.1/24
R4	Tunnel 0	R1	172.16.99.2

Task 1: Configure and Verify GRE Tunnel

Activity

Complete the following steps:

Step 1 In the first few steps of this discovery, you will verify the status of the network as it has been prepared. Start by accessing the console of R1 and displaying its routing table.

Enter this command on the R1 router:

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
S        10.0.0.0/8 [1/0] via 10.10.1.2
C        10.10.1.0/24 is directly connected, Ethernet0/0
L        10.10.1.1/32 is directly connected, Ethernet0/0
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/1
L        172.16.1.1/32 is directly connected, Ethernet0/1
C        172.16.11.0/24 is directly connected, Loopback0
L        172.16.11.1/32 is directly connected, Loopback0
```

R1 is not running any dynamic routing protocols. Other than the locally connected routes, the only other route is a static route for the 10.0.0.0/8 network. R4 is configured in a similar fashion.

Step 2 Verify that R1 can ping the R4 Ethernet0/0 interface (10.10.3.2).

Enter this command on the R1 router:

```
R1# ping 10.10.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

R1 and R4 can reach each other using the 10.0.0.0/8 network.

Step 3 Access the console of R2 and display its routing table.

Enter this command on the R2 router:

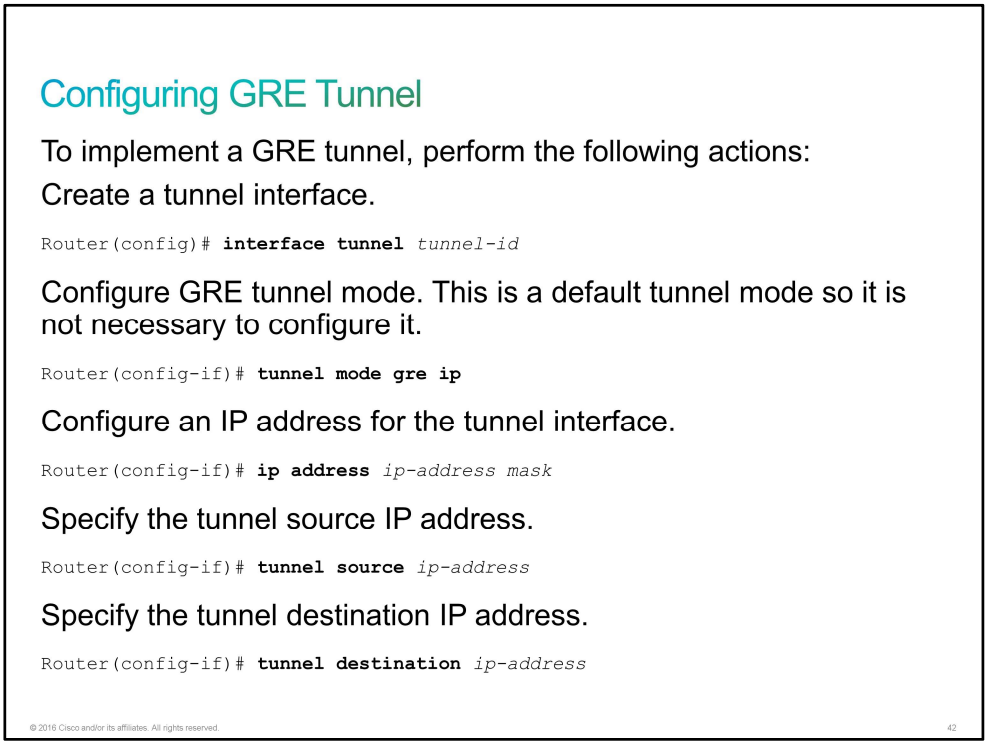
```
R2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C        10.10.1.0/24 is directly connected, Ethernet0/0
L        10.10.1.2/32 is directly connected, Ethernet0/0
C        10.10.2.0/24 is directly connected, Ethernet0/1
L        10.10.2.1/32 is directly connected, Ethernet0/1
D        10.10.3.0/24 [90/307200] via 10.10.2.2, 21:40:41, Ethernet0/1
C        10.10.12.0/24 is directly connected, Loopback0
L        10.10.12.1/32 is directly connected, Loopback0
D        10.10.13.0/24 [90/409600] via 10.10.2.2, 21:40:41, Ethernet0/1
```

R2 is running EIGRP and is peering with R3. Between them, they are aware of the entire 10.0.0.0/8 address space within the topology. R2 has no awareness of the 172.16.0.0/16 address space that is behind R1 and R4. Neither does R3.

Configuring GRE Tunnel



The minimum GRE tunnel configuration requires specification of the tunnel source and destination addresses. You must also configure an IP subnet to provide IP connectivity across the tunnel link.

Note	At each end of the tunnel, you must use symmetrical, reachable addresses. You can use loopback addresses if they are reachable.

Command	Description
tunnel source *ip-address*	Specifies the tunnel source IP address in interface tunnel configuration mode. This IP address is the one that is assigned to the local interface.
tunnel destination *ip-address*	Specifies the tunnel destination IP address in interface tunnel configuration mode. This IP address is the one that is assigned to the local interface or the remote router.
ip address *ip-address mask*	Specifies the IP address of the tunnel interface.
tunnel mode gre ip	Specifies the GRE tunnel mode as the tunnel interface mode in interface tunnel configuration mode. The GRE tunnel mode is the default tunnel mode on Cisco routers, so you do not need to enter this command.

Step 4 Access the console of R1 and define the interface Tunnel0. Assign it the IP address 172.16.99.1/24. The R1 Ethernet0/0 interface (10.10.1.1) should be the source and the R4 Ethernet 0/0 interface (10.10.3.2) should be the destination.

Enter this command on the R1 router:

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface tunnel0
R1(config-if)#
*Nov  3 14:14:43.002: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to down
R1(config-if)# ip address 172.16.99.1 255.255.255.0
R1(config-if)# tunnel source 10.10.1.1
R1(config-if)# tunnel destination 10.10.3.2
R1(config-if)#
*Nov  3 14:15:12.555: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up
R1(config-if)# end
R1#
```

The Tunnel0 interface was administratively up immediately after being defined, and its line protocol came up immediately after being fully configured.

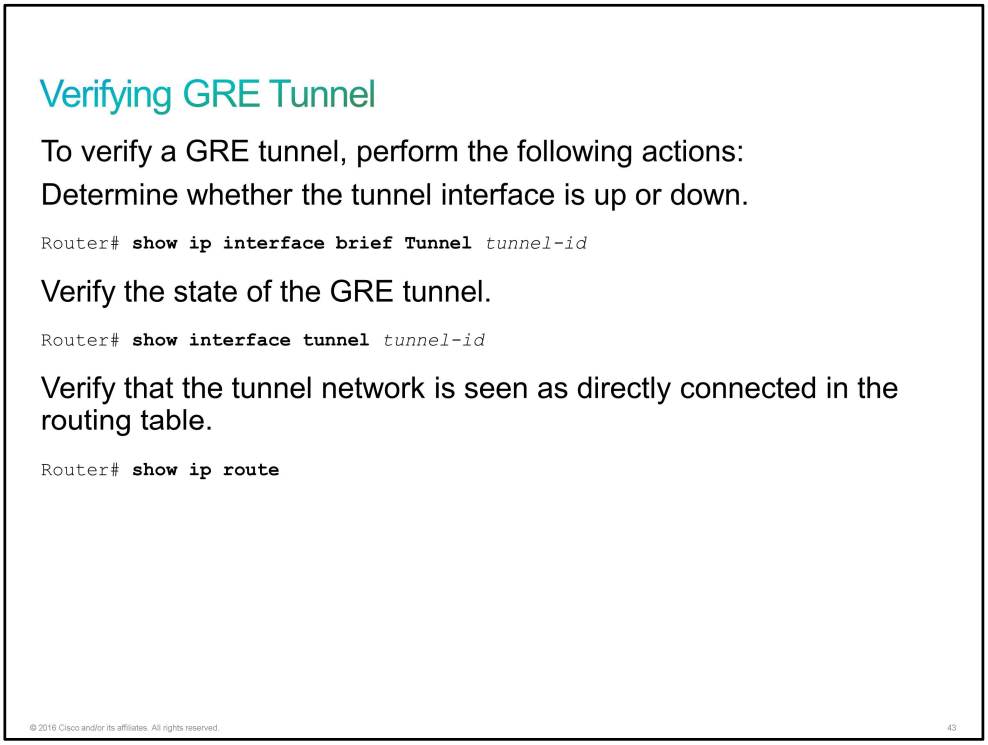
Step 5 Access the console of R4 and define the peer Tunnel0 interface. Assign it the IP address 172.16.99.2/24. The R4 Ethernet0/0 interface (10.10.3.2) should be the source and the R1 Ethernet 0/0 interface (10.10.1.1) should be the destination..

Enter this command on the R4 router:

```
R4# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)# interface tunnel0
R4(config-if)#
*Nov  3 14:24:00.594: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to down
R4(config-if)# ip address 172.16.99.2 255.255.255.0
R4(config-if)# tunnel source 10.10.3.2
R4(config-if)# tunnel destination 10.10.1.1
R4(config-if)#
*Nov  3 14:24:29.749: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up
R4(config-if)# end
R4#
```

Again, the Tunnel0 interface was administratively up immediately after being defined, and its line protocol came up immediately after being fully configured.

Verifying GRE Tunnel



To determine whether the tunnel interface is up or down, use the **show ip interface brief** command.

You can verify the state of a GRE tunnel by using the **show interface tunnel** command. The line protocol on a GRE tunnel interface is up as long as there is a route to the tunnel destination.

By issuing the **show ip route** command, you can identify the route between the GRE-tunnel-enabled routers. Because a tunnel is established between the two routers, the path is seen as directly connected.

Step 6 Verify that the Tunnel0 interface on R1 is up.

Enter this command on the R1 router:

```
R1# show ip interface brief Tunnel 0
Interface                  IP-Address      OK? Method Status
Protocol
Tunnel0                    172.16.99.1     YES manual up                    up
```

The status and line protocol for the Tunnel0 interface are "up."

Step 7 Verify that the Tunnel0 interface on R4 is up.

Instead of using **show ip interface brief** command on R4, use **show interface** command:


```
R4# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.99.2/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.10.3.2, destination 10.10.1.1
  Tunnel protocol/transport GRE/IP
<... output omitted ...>
```

The status and line protocol for the Tunnel0 interface are "up." You can also see the IP address of the tunnel interface, source and destination IP address, as well as tunnel mode.

Step 8 Display the routing table on the R1 router.

Enter this command on the R1 router:

```
R1# show ip route

<... output omitted ...>
      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
S        10.0.0.0/8 [1/0] via 10.10.1.2
C        10.10.1.0/24 is directly connected, Ethernet0/0
L        10.10.1.1/32 is directly connected, Ethernet0/0
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/1
L        172.16.1.1/32 is directly connected, Ethernet0/1
C        172.16.11.0/24 is directly connected, Loopback0
L        172.16.11.1/32 is directly connected, Loopback0
C        172.16.99.0/24 is directly connected, Tunnel0
L        172.16.99.1/32 is directly connected, Tunnel0
```

As you can see, the traffic that is destined for 172.16.99.0/24 enters the GRE tunnel interface.

Step 9 Ping the IP address of the R4 Tunnel0 interface from R1.

Enter this command on the R1 router:

```
R1# ping 172.16.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

The ping was successful through the GRE tunnel. The ICMP echo and echo reply packets were encapsulated in the GRE tunnel. That is, from R1 to R4, the IP packet sourced from 172.16.99.1 and destined for 172.16.99.2 was encapsulated with a second IP header sourced from 10.10.1.1 and destined to 10.10.3.2. This packet was sent out the R1 Ethernet 0/0 interface and was forwarded by R2 and R3 to the R4 Ethernet0/0 interface. R4 then stripped the outer IP header to reveal the encapsulated IP packet that is destined for 172.16.99.2.

R3 and R2 did not know that that other IP packets were embedded in the packets that they forwarded. The 10.0.0.0/8 network was used to forward packets for 172.16.0.0/16 even though the transit routers had no awareness of 172.16.0.0/16.

Step 10 Being able to forward packets between the two tunnel interfaces is good. But you can also run dynamic routing protocol through the tunnel. Configure OSPF process ID 1 on R4. Assign R4 the router ID 0.0.0.4. Include the network 172.16.0.0/16 (which includes the interfaces Ethernet0/1, Loopback0, and Tunnel0) in Area 0.

Enter these commands on the R4 router:

```
R4# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)# router ospf 1
R4(config-router)# router-id 0.0.0.4
R4(config-router)# network 172.16.0.0 0.0.255.255 area 0
R4(config-router)# end
R4#
```

Step 11 Access the console of R1 to configure it for OSPF. Configure OSPF process ID 1. Assign the router ID 0.0.0.1. Include the network 172.16.0.0/16 (which includes the interfaces Ethernet0/1, Loopback0, and Tunnel0) in Area 0.

Enter these commands on the R1 router:

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# router ospf 1
R1(config-router)# router-id 0.0.0.1
R1(config-router)# network 172.16.0.0 0.0.255.255 area 0
R1(config-router)#
*Nov  4 11:41:51.093: %OSPF-5-ADJCHG: Process 1, Nbr 0.0.0.4 on Tunnel0 from
LOADING to FULL, Loading Done
R1(config-router)# end
```

Step 12 Display the routing table on the R1 router.

Enter this command on the R1 router:

```
R1# show ip route

<... output omitted ...>
      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
S        10.0.0.0/8 [1/0] via 10.10.1.2
C        10.10.1.0/24 is directly connected, Ethernet0/0
L        10.10.1.1/32 is directly connected, Ethernet0/0
      172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/1
L        172.16.1.1/32 is directly connected, Ethernet0/1
O        172.16.4.0/24 [110/1010] via 172.16.99.2, 00:19:23, Tunnel0
C        172.16.11.0/24 is directly connected, Loopback0
L        172.16.11.1/32 is directly connected, Loopback0
O        172.16.14.1/32 [110/1001] via 172.16.99.2, 00:19:23, Tunnel0
C        172.16.99.0/24 is directly connected, Tunnel0
L        172.16.99.1/32 is directly connected, Tunnel0
```

R1 has learned about the networks running behind the R4 Loopback0 and Ethernet0/1 interfaces via OSPF routing protocol. The traffic that is destined to the R4 Loopback0 and Ethernet0/1 interfaces will enter the GRE Tunnel0 interface.

Step 13 Ping the R4 Ethernet0/1 interface (172.16.4.1) from R1.

Enter this command on the R1 router:

```
R1# ping 172.16.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Again, this traffic and all other 172.16.0.0/16 traffic between R1 and R4 traverses the GRE tunnel. This traffic is forwarded by R2 and R3, but they are unaware of it. They see it as traffic between the R1 Ethernet0/0 interface (10.10.1.1) and the R4 Ethernet0/0 interface (10.10.3.2).

Step 14 Display the OSPF neighbors of R1.

Enter this command on the R1 router:

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
0.0.0.4           0   FULL/  -        00:00:37    172.16.99.2     Tunnel0
```

R4 is an OSPF neighbor of R1, using the GRE tunnel.

This is the end of the discovery lab.

Challenge

1. GRE tunnel mode is the default tunnel interface mode in Cisco IOS Software. True or False ?

   A. True
   B. False

2. Which two of the following are GRE characteristics? (Choose two.)

   A. GRE encapsulation uses a protocol-type field in the GRE header to support the encapsulation of any OSI Layer 3 protocol.
   B. GRE itself is stateful. It includes flow-control mechanisms, by default.
   C. GRE includes strong security mechanisms to protect its payload.
   D. The GRE header, together with the tunneling IP header, creates at least 24 bytes of additional overhead for tunneled packets.

3. GRE tunnel is flapping with the following error message below:

```
01:11:39: %LINEPROTO-5-UPDOWN:
          Line protocol on Interface Tunnel0, changed state to up
01:11:48: %TUN-5-RECURDOWN:
          Tunnel0 temporarily disabled due to recursive routing
01:11:49: %LINEPROTO-5-UPDOWN:
          Line protocol on Interface Tunnel0, changed state to down
01:12:49: %LINEPROTO-5-UPDOWN:
```

   What could be the reason for the tunnel flapping ?

   A. IP routing has not been enabled on tunnel interface.
   B. MTU issue on the tunnel interface.
   C. The router is trying to route to the tunnel destination address using the tunnel interface itself.
   D. Access-list blocking traffic on the tunnel interface.

4. Is GRE tunnel considered secure ?

   A. Yes
   B. No

5. Which of the following commands will not tell you if the GRE tunnel X is in "up/up" state ?

   A. **show ip interface brief**
   B. **show interface tunnel X**
   C. **show ip interface tunnel X**
   D. **show run interface tunnel X**

6. Can you have a Loopback address as the tunnel source IP address ?

   A. Yes
   B. No

7. Does GRE tunnel support multicast ?

   A. No
   B. Yes

Answer Key

Challenge

1. A
2. A, D
3. C
4. B
5. D
6. A
7. B

Lesson 4: Configuring Single-Homed EBGP

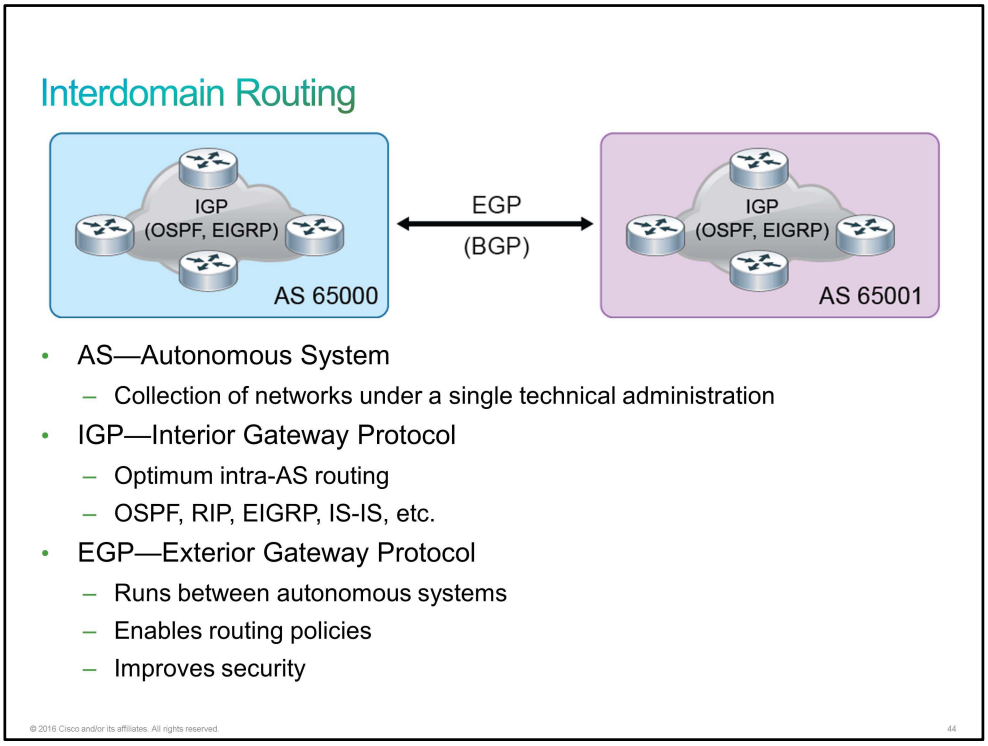
Introduction

BGP is the routing protocol that is one of the underlying foundations of the Internet. This protocol is complex and scalable, but it is also reliable and secure. EBGP is a part of the BGP that you use for exchanging routes between different autonomous systems.

Interdomain Routing

The Internet is a collection of autonomous systems that are interconnected to allow communication between them. An autonomous system is by definition a collection of networks under a single technical administration domain. BGP provides the routing between these autonomous systems.

To understand BGP, you must first understand how it differs from other routing protocols.

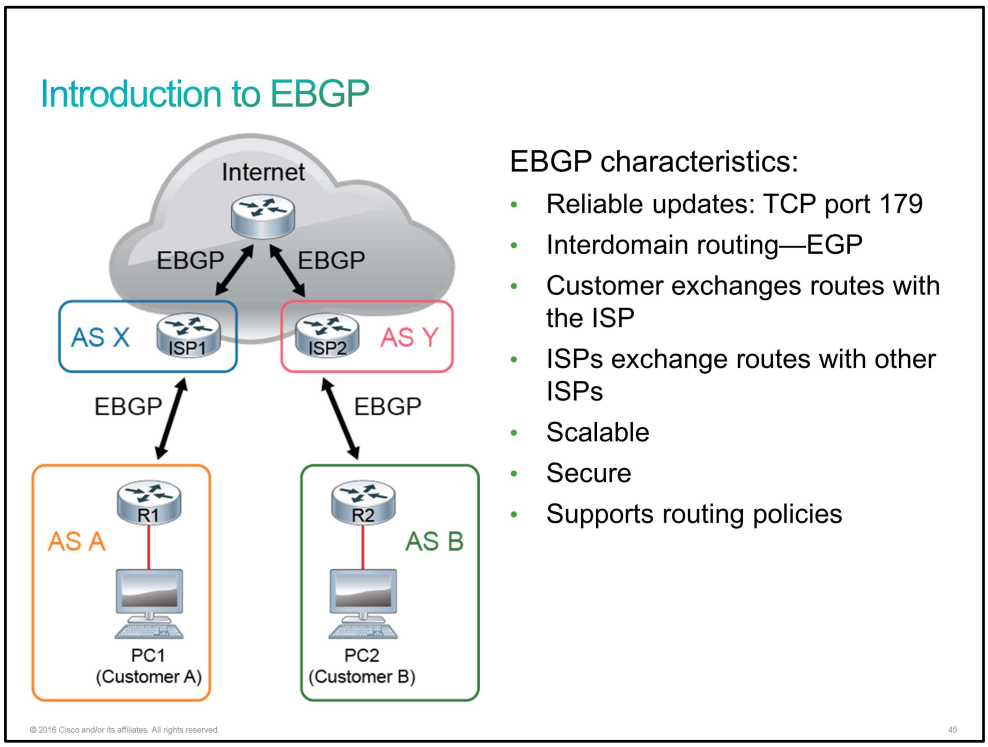


One way you can categorize routing protocols is whether they are interior or exterior.

- IGP is a routing protocol that exchanges routing information within an AS. RIP, OSPF, and EIGRP are examples of IGPs.
- EGP is a routing protocol that exchanges routing information between different autonomous systems. BGP is an example of an EGP.

Introduction to EBGP

BGP is an important building block of the Internet as you know it today. The Internet is a set of many autonomous systems and a set of an even higher number of routes that have to be reachable any time.



BGP uses TCP as the transport mechanism, which provides reliable connection-oriented delivery. BGP uses TCP port 179. Two routers that are using BGP form a TCP connection with one another. These two BGP routers are called "peer routers," or "neighbors."

When BGP is running between routers in different autonomous systems, it is called EBGP. When BGP is running between routers in the same autonomous system, it is called IBGP. IBGP is used between routers in the same autonomous system mostly for redundancy and load balancing purposes.

Different customers are using EBGP for route exchange between their local environments and their ISPs. The IANA is responsible for the global coordination and assignment of AS numbers and public IP addresses (usually through a local ISP). Each customer has to place a request for their AS number and a set of public space IP prefixes. The customer then establishes an EBGP session with its ISP and they exchange routing information.

Internet Service Providers are also interconnected. Each ISP has his own AS number. ISPs can communicate directly or they can use IXP for route distribution.

The Internet is expanding with high speed and the size of all routing information is extremely large. In 2015, more than 570,000 routes exist in full BGP table and the number of routes is still expending greatly. Therefore, scalability is a very important feature of BGP. BGP enables reliable information exchange and is capable of batching the routing updates. These two characteristics allow BGP to scale to large, Internet-sized networks.

BGP also has security features. You can configure peer authentication and route filtering.

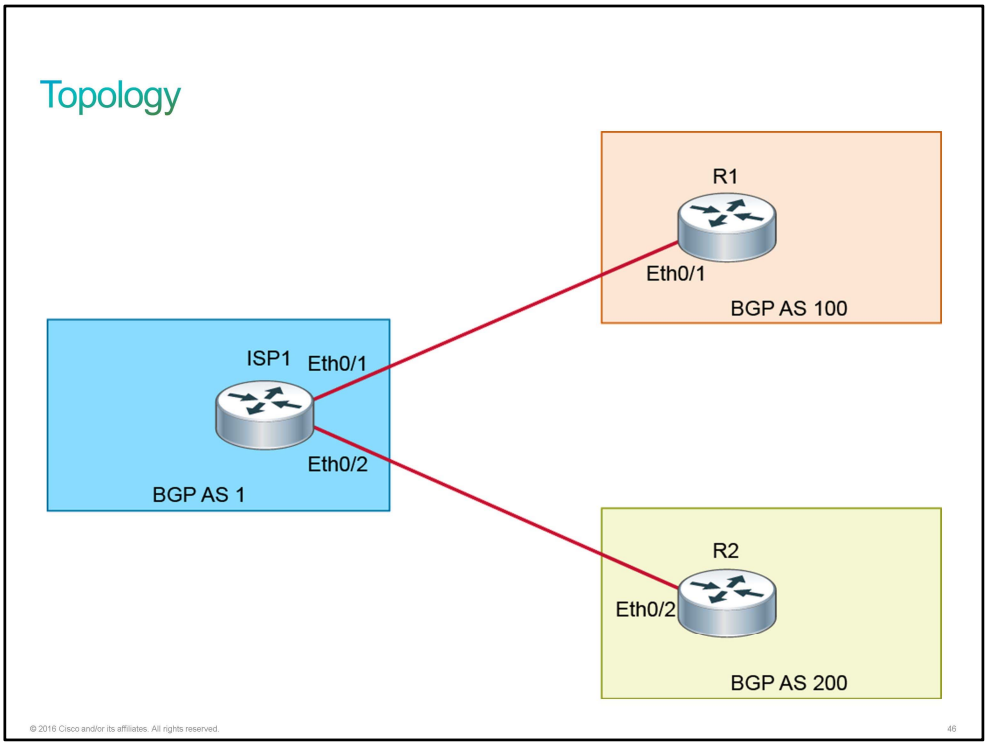
For more advanced networks, BGP also provides routing policies for route update manipulations.

Discovery 51: Configure and Verify Single Homed EBGP

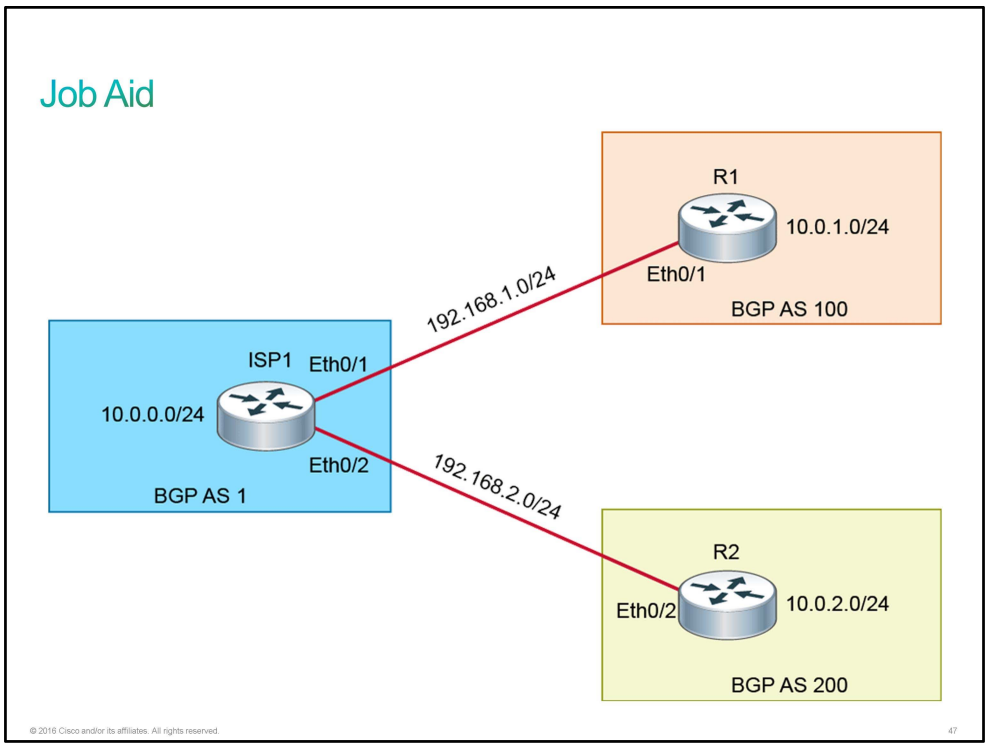
Introduction

In this discovery, you will learn how to configure external BGP between the service provider and customer. The service provider (ISP1 router) has two different customers (R1 and R2 routers). It has to establish a separate EBGP session with each of the customers. All devices have their basic configurations in place, including hostnames and IP addresses. R1 and R2 have also been preconfigured with BGP.

Topology



Job Aid



The configuration is as follows:

- All devices have their basic configurations in place, including hostnames and IP addresses.
- R1 and R2 have been preconfigured with BGP:
  - R1 has BGP AS 100.
  - R2 has BGP AS 200.
  - Both routers are announcing Loopback interface network.

Device Information

Device Details

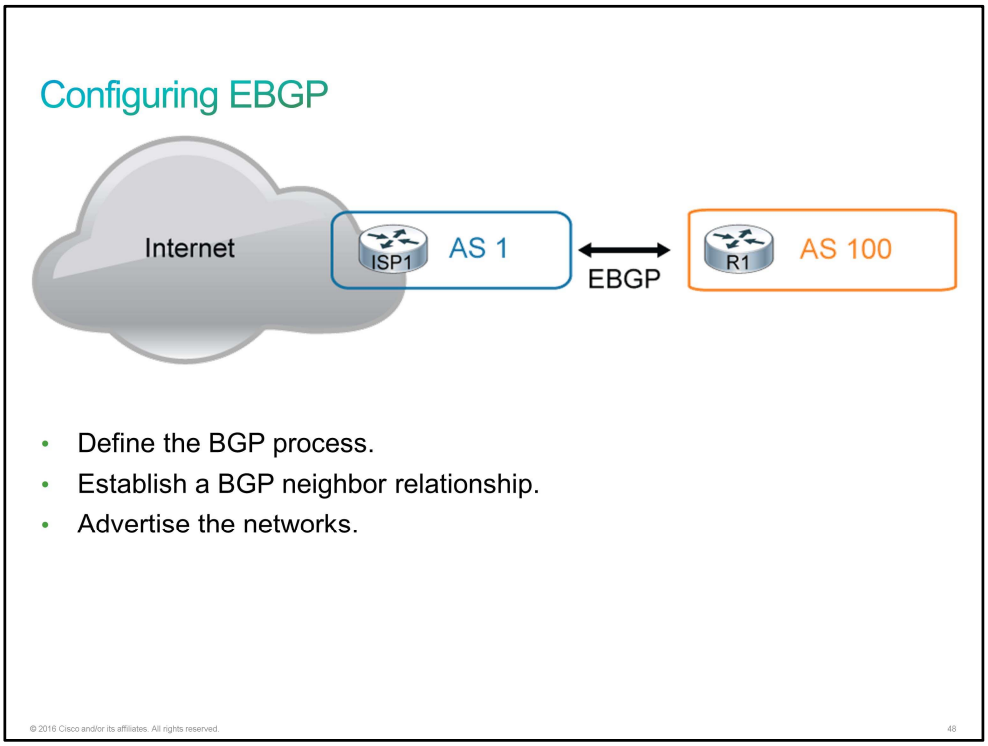
Device	Interface	IP Address	Description
ISP1	Ethernet0/1	192.168.1.10/24	Connection to R1
ISP1	Ethernet0/2	192.168.2.10/24	Connection to R2
ISP1	Loopback0	10.0.0.1/24	Loopbacks simulate LAN networks
R1	Ethernet0/1	192.168.1.11/24	Connection to ISP1
R1	Loopback0	10.0.1.1/24	Loopbacks simulate LAN networks

Device	Interface	IP Address	Description
R2	Ethernet0/2	192.168.2.11/24	Connection to ISP1
R2	Loopback0	10.0.2.1/24	Loopbacks simulate LAN networks

Device AS Information

Device	AS Number
ISP1	AS 1
R1	AS 100
R2	AS 200

Task 1: Configure and Verify Single Homed EBGP



The requirements to configure basic EBGP include the following details:

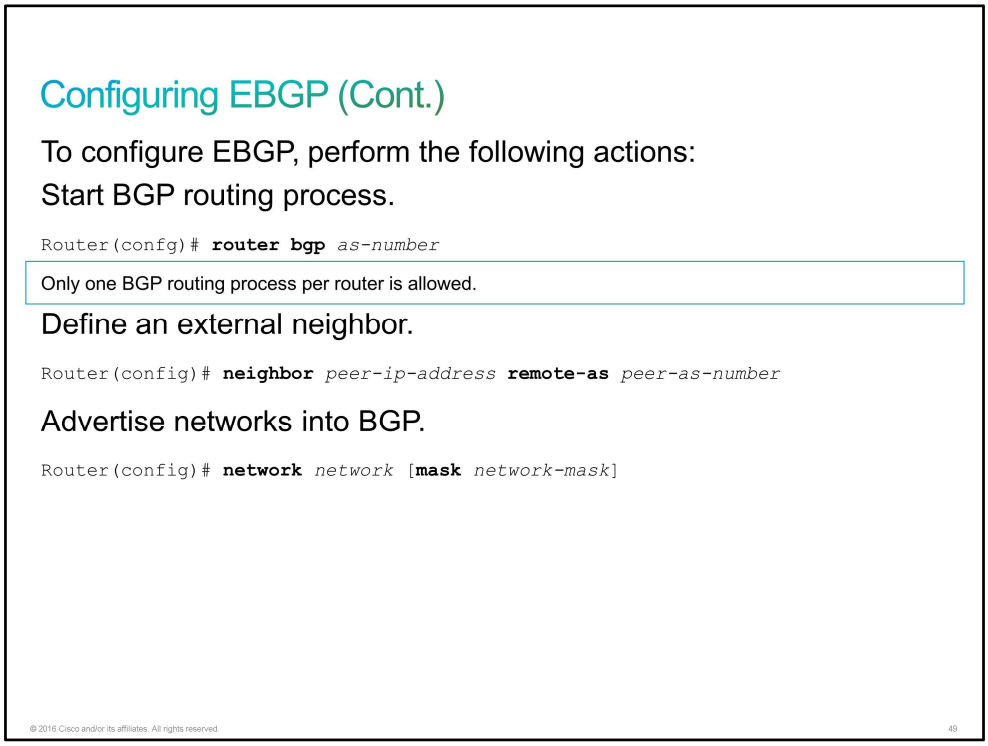
- AS numbers (your own and all remote AS numbers, which must be different)
- All the neighbors (peers) that are involved in BGP, and IP addressing that is used among the BGP neighbors
- Networks that need to be advertised into BGP

Note	IGP is the routing protocol that runs inside an AS. An IGP is not run between the EBGP neighbors that are residing in different autonomous systems. Therefore, the IP address that is used in the BGP neighbor command must be reachable without using an IGP, which can be accomplished by pointing at an address that is reachable through a directly connected network or by using static routes to that IP address.

A typical BGP configuration involves configuring BGP between a customer network and an ISP. This process is called EBGP.

The basic BGP configuration requires three main steps:

1. Define the BGP process.
2. Establish one or more neighbor relationships.
3. Advertise the networks into BGP.



1. To start BGP process on a router, use the **router bgp** command. Each process must be assigned the local AS number. There can be, at most, one BGP process in a router which means that each router can only be in one AS at any given time.

Note	AS number is a 16-bit integer in the range from 1 to 65,534. When the AS-number pool from IANA approached exhaustion, also new 32-bit AS numbers were created.

2. Since BGP does not automatically discover neighbors like other routing protocols do, you have to explicitly configure them using the **neighbor** *peer-ip-address* **remote-as** *peer-as-number* command. The external neighbor has to be reachable on the indicated IP address.
3. To specify the networks to advertise into BGP, you can use the **network** command with the optional **mask** keyword and the subnet mask specified. If an exact match of the advertised network is not found in the IP routing table, the network will not be advertised.

Note	The **network** command with no mask option uses the classful approach to insert a major network into the BGP table.

If you have, for example, a 10.10.10.0/24 network on the router that you want to announce it in the BGP, you have to announce it using the **mask** keyword (**network 10.10.10.10 255.255.255.0**). If you do not specify the mask, BGP will take the whole Class A network (10.0.0.0/8) to announce it. Because this exact class A network cannot be found in the routing table, it cannot be announced in the BGP.

Note	The meaning of the **network** command in BGP is radically different from the meaning of this command in other routing protocols. In all other routing protocols, the **network** command indicates interfaces over which the routing protocol will be run. In BGP, it indicates only which routes should be injected into the BGP table on the local router.

Activity

Complete the following steps:

Step 1 BGP has been preconfigured on the customers side. Access the console of R1 and display the BGP configuration.

```
R1# show running-config | section bgp
router bgp 100
 bgp log-neighbor-changes
 network 10.0.1.0 mask 255.255.255.0
 neighbor 192.168.1.10 remote-as 1
```

- R1 has been configured in the BGP AS 100.
- Network 10.0.1.0/24 has been announced to all configured BGP neighbors.
- The external neighbor with IP address 192.168.1.10 has been configured. Note that this IP address belongs to the ISP1 router.

You will find a similar configuration on the R2 router.

Step 2 For a BGP session to be established, both sites have to be configured. Configure the service provider site.

Enable BGP routing process on ISP1 and configure both external neighbors, the R1 and R2 routers. Use the following information:

- ISP1 is in AS 1.

- R1 is in AS 100 and has IP address 192.168.1.11.
- R2 is in AS 200 and has IP address 192.168.2.11.

```
ISP1# conf t
ISP1(config)# router bgp 1
ISP1(config-router)# neighbor 192.168.1.11 remote-as 100
ISP1(config-router)# neighbor 192.168.2.11 remote-as 200
ISP1(config-router)# end
```

After you configure the external BGP neighbors on ISP1, you will see that external BGP sessions between R1 and ISP1, and R2 and ISP1 are successfully established.

```
*Oct  6 11:36:01.393: %BGP-5-ADJCHANGE: neighbor 192.168.1.11 Up
*Oct  6 11:36:12.364: %BGP-5-ADJCHANGE: neighbor 192.168.2.11 Up
```

Step 3 You will now announce ISP1 Loopback0 network with the IP address 10.0.0.0/24 in the BGP. Before advertising it, verify that there is an exact match of this network in the ISP1 routing table.

```
ISP1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Loopback0
L        10.0.0.1/32 is directly connected, Loopback0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Ethernet0/1
L        192.168.1.10/32 is directly connected, Ethernet0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Ethernet0/2
L        192.168.2.10/32 is directly connected, Ethernet0/2
```

If the route was missing from the routing table, it would not be advertised into the BGP.

Step 4 Configure ISP1 to announce the Loopback0 network with the IP address 10.0.0.0/24 in the BGP process.

Use the **network** router configuration command to announce the network.

```
ISP1# conf t
ISP1(config)# router bgp 1
ISP1(config-router)# network 10.0.0.0 mask 255.255.255.0
ISP1(config-router)# end
```

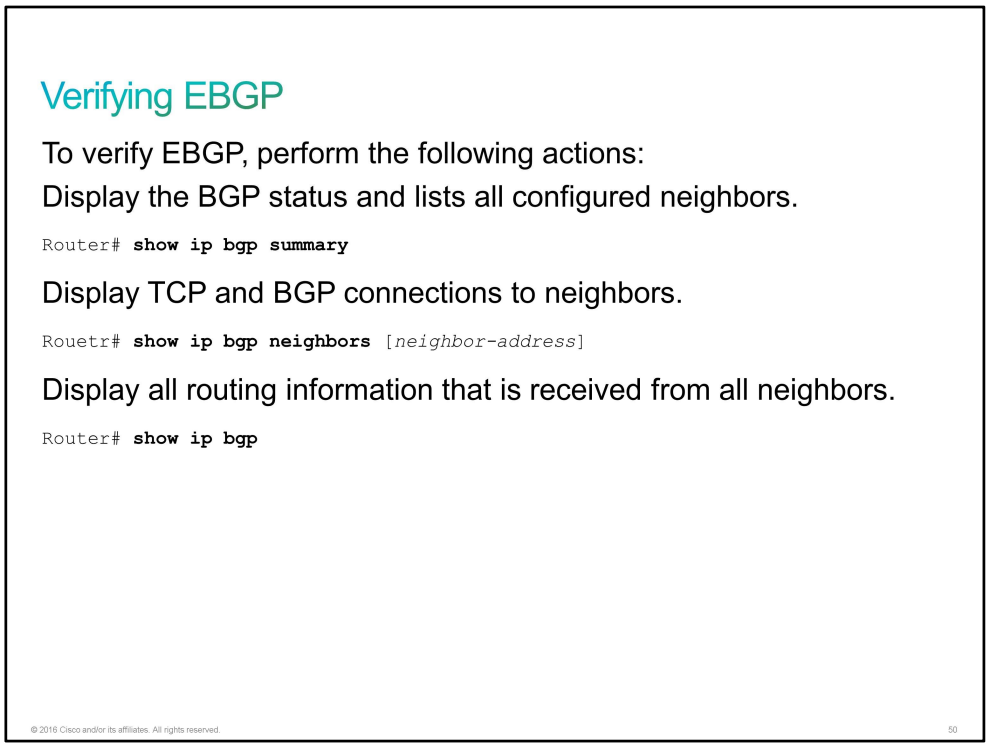
Verifying EBGP

The **show ip bgp summary** command gives you an overview of the BGP status. Each configured neighbor is listed in the output of the command. The output will display the IP address and AS number of the neighbor, along with the status of the session. You can use this information to verify that BGP sessions are up and established, or to verify the IP address and AS number of the configured BGP neighbor.

The **show ip bgp neighbors** command supplies additional information about BGP connections to neighbors. This command can be used for two purposes. First one is to get information about the TCP sessions and the BGP parameters of the sessions. All BGP session parameters are displayed. In addition, TCP timers and counters are also displayed.

To display the entire BGP table, use the **show ip bgp** command. This command gives you an overview of all routing information that is received from all neighbors. It displays basic information about each route on a single link.

Note	If multiple paths to reach the same network exist, all are displayed. The router selects only one of the alternatives as the best path toward the destination and marks it with the ">" sign.



Step 5 On the ISP1 router, verify the state of BGP session.

Use the **show ip bgp summary** command to examine the external BGP sessions.

```
ISP1# show ip bgp summary
BGP router identifier 10.0.0.1, local AS number 1
BGP table version is 3, main routing table version 3
2 network entries using 296 bytes of memory
2 path entries using 128 bytes of memory
3/2 BGP path/bestpath attribute entries using 408 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 880 total bytes of memory
BGP activity 5/3 prefixes, 5/3 paths, scan interval 60 secs

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
192.168.1.11    4        100       5       6        3    0    0 00:00:10        1
192.168.2.11    4        200       5       6        3    0    0 00:00:10        1
```

The first section of the **show ip bgp summary** command output describes the BGP table and its content:

- The router ID of the router and local AS number
- The BGP table version is the version number of the local BGP table. This number is increased every time that the table is changed

The second section of the **show ip bgp summary** command output is a table in which the current neighbor statuses are shown. There is one line of text for each neighbor that has been configured. The information that is displayed:

- IP address of the neighbor.
- BGP version number that is used by the router when communicating with the neighbor
- AS number of the remote neighbor.
- Number of messages and updates that have been received from the neighbor since the session was established
- Number of messages and updates that have been sent to the neighbor since the session was established
- Version number of the local BGP table that has been included in the most recent update to the neighbor
- Number of messages that are waiting to be processed in the incoming queue from this neighbor
- Number of messages that are waiting in the outgoing queue for transmission to the neighbor
- How long the neighbor has been in the current state and the name of the current state (the state "Established" is not printed out, so no state name indicates "Established")
- Number of received prefixes from the neighbor.

ISP1 has two established sessions with the following neighbors:

- 192.168.1.11, which is the IP address of R1 router and is in AS 100.
- 192.168.2.11, which is the IP address of R2 router and is in AS 200.

From each of the neighbors, ISP1 has received one prefix (one network).

Step 6 On ISP1, use the **show ip bgp neighbors** command to verify that BGP state is established with both neighbors.

Optionally you can add the IP address of the neighbor at the end of the command.

```
ISP1# show ip bgp neighbors 192.168.1.11
BGP neighbor is 192.168.1.11,  remote AS 100, external link
  BGP version 4, remote router ID 10.0.1.1
  BGP state = Established, up for 00:01:16
  Last read 00:00:24, last write 00:00:05, hold time is 180, keepalive interval
is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  <... output omitted ...>


ISP1# show ip bgp neighbors 192.168.2.11
BGP neighbor is 192.168.2.11,  remote AS 200, external link
  BGP version 4, remote router ID 10.0.2.1
  BGP state = Established, up for 00:02:31
  Last read 00:00:42, last write 00:00:11, hold time is 180, keepalive interval
is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
<... output omitted ...>
```

Notice that the external BGP connection is identified as an external link in the **show ip bgp neighbor** command output.

Step 7 On ISP1 router, verify the received prefixes.

Use the **show ip bgp** command, that will display all the routing information.

```
ISP1# show ip bgp
BGP table version is 4, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.0.0.0/24      0.0.0.0                  0         32768 i
 *>  10.0.1.0/24      192.168.1.11             0             0 100 i
 *>  10.0.2.0/24      192.168.2.11             0             0 200 i
```


With the **show ip bgp** command, the entire BGP table is displayed. An abbreviated list of information about each route is displayed, one line per prefix. The output is sorted in network number order. Therefore, if the BGP table contains more than one route to the same network, the alternative routes are displayed on successive lines. The network number is printed on the first of these lines only. The following lines, which refer to the same network, have the network number field left blank. Also some, but not all, of the BGP attributes that are associated with the route are displayed on the line.

The BGP path selection process selects one of the available routes to each of the networks as the best. This route is pointed out by the ">" character in the left column.

ISP1 has the following networks in the BGP table:

- 10.0.0.0/24, which has been locally configured on ISP1.
- 10.0.1.0/24, which has been announced from 192.168.1.11 (R1) neighbor.
- 10.0.2.0/24, which has been announced from 192.168.2.11 (R2) neighbor.

Since the command displays all routing information, note that also network 10.0.0.0/24, with the next hop attribute set to 0.0.0.0, is displayed. The next hop attribute is set to 0.0.0.0 when you view the BGP table on the router that originates the route in BGP. The 10.0.0.0/24 network is the network that you locally announced on ISP1 into BGP.

Note that each path is marked as the best path, since there is only one path to each of the networks.

This is the end of the discovery lab.

Challenge

1. Which of the following are an Exterior Gateway Protocol ?

   A. EIGRP
   B. OSPF
   C. RIP
   D. BGP

2. When BGP runs between two peers in the same autonomous system (AS), it is referred to as External BGP (EBGP).

   A. True
   B. False

3. In the following command, the AS number, 65200 is for which router ?

```
R1(config-router)# neighbor 10.108.200.1 remote-as 65200
```

   A. The local router R1
   B. The neighbor router with IP address 10.108.200.1.
   C. Both
   D. None of the above

4. Which TCP port does BGP use to establish BGP session.

   A. 179
   B. 21
   C. 81
   D. 441

5. Refer to the output below. Is the BGP session established between the peers ?

```
R1#show ip bgp summary
BGP router identifier 10.1.1.1, local AS number 64
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.5.70   4 64       0       0        0    0    0 never    Active
```

   A. Yes
   B. No

6. Which command can you use to know the hold time on the two BGP peers ?

   A. **show ip bgp**
   B. **show ip bgp summary**
   C. **show ip bgp all**
   D. **show ip bgp neighbor**

7. What does a next hop of 0.0.0.0 mean in the **show ip bgp** command output?

```
Router# show ip bgp

 For address family: IPv4 Unicast   *****
 BGP table version is 27, local router ID is 1.1.1.1
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure
 Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf Weight Path
 *> 10.1.1.0/24      0.0.0.0                  0         32768 ?
 *> 10.13.13.0/24    0.0.0.0                  0         32768 ?
 *> 10.15.15.0/24    0.0.0.0                  0         32768 ?
```

A. The router does not know the next hop.
B. Network is locally originated via **network** command in BGP.
C. It is not a valid network.
D. The next hop is not reachable.

Answer Key

Challenge

1. D
2. B
3. B
4. A
5. B
6. D
7. B

Module 12: Network Device Management

Introduction

The network staff is responsible for managing each device on the network according to industry best practices and in an effort to reduce device downtime. This module describes the commands and processes to determine network operational status, gather information about remote devices, and manage Cisco IOS Software images, configuration files, and devices on a network. The module also explains how to enable Cisco IOS Software feature sets by obtaining and validating a Cisco software license.

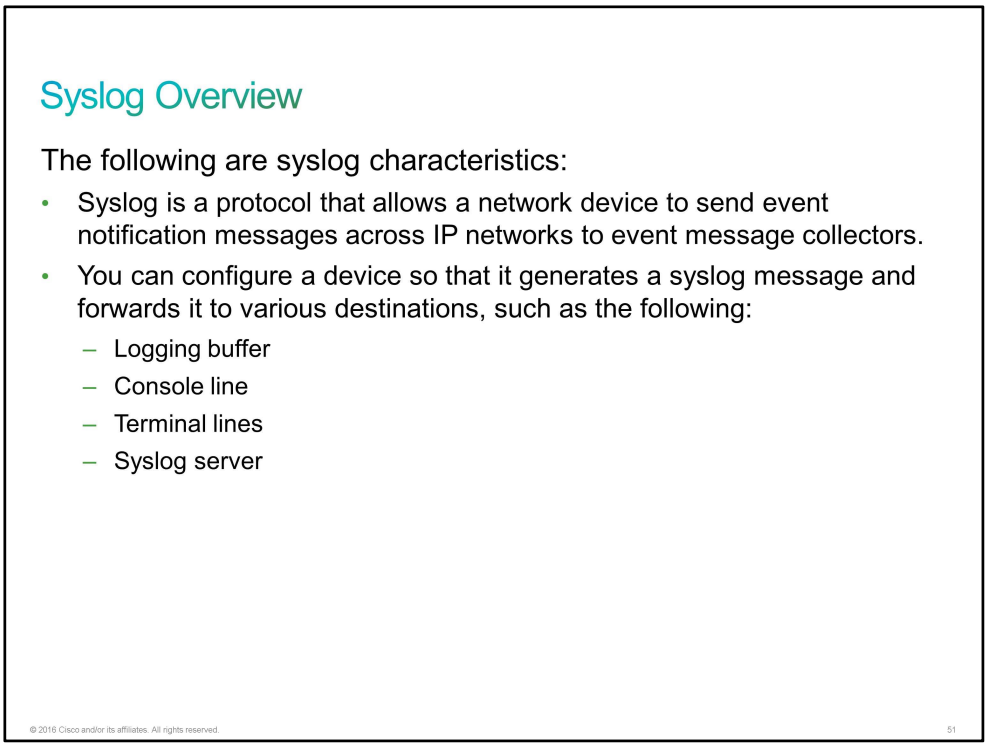
Lesson 1: Implementing Basic Network Device Management

Introduction

Your boss sends you to your customer to enable device management using system logging and SNMP. You will need to explain to the customer how to configure and verify syslog and SNMP.

Introducing Syslog

Syslog is a protocol that allows a machine to send event notification messages across IP networks to event message collectors. By default, a network device sends the output from system messages and debug privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a syslog server, depending on your configuration. The process also sends messages to the console. Logging services provide a means to gather logging information for monitoring and troubleshooting, to select the type of logging information that is captured, and to specify the destinations of captured syslog messages.



You can set the severity level of the messages to control the type of messages that the consoles display and each of the destinations. You can time-stamp log messages or set the syslog source address to enhance real-time debugging and management.

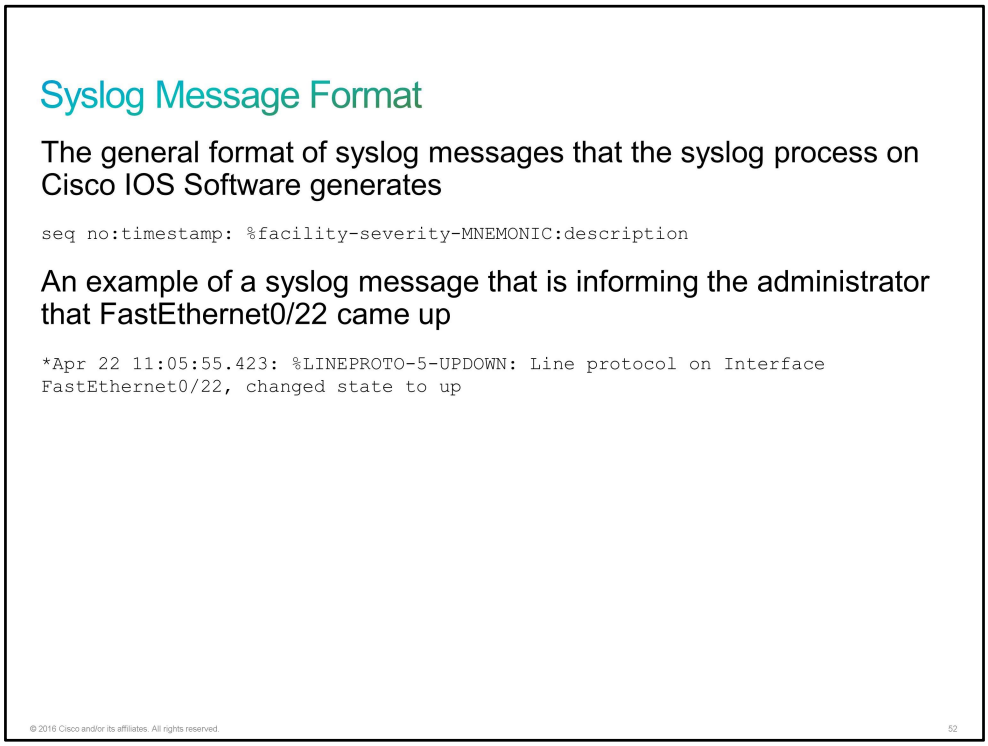
You can access logged system messages by using the device CLI or by saving them to a correctly configured syslog server. The switch or router software saves syslog messages in an internal buffer.

You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the device through Telnet, SSH, or through the console port.

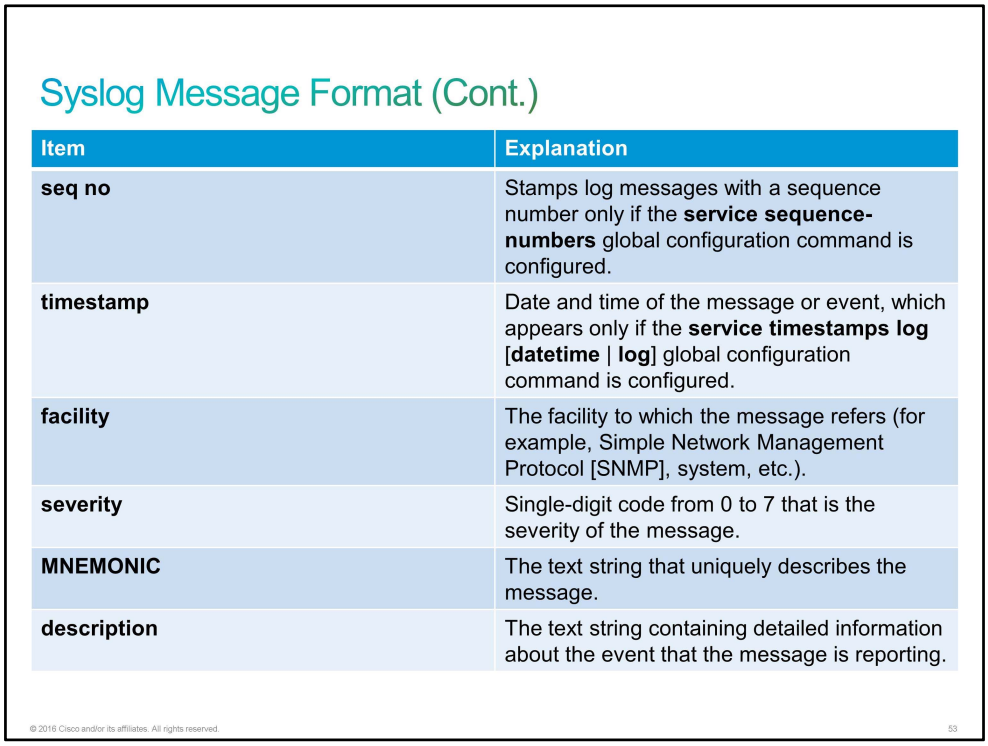
Syslog Message Format

The following is the general format of syslog messages that the syslog process on the Cisco IOS Software generates by default:

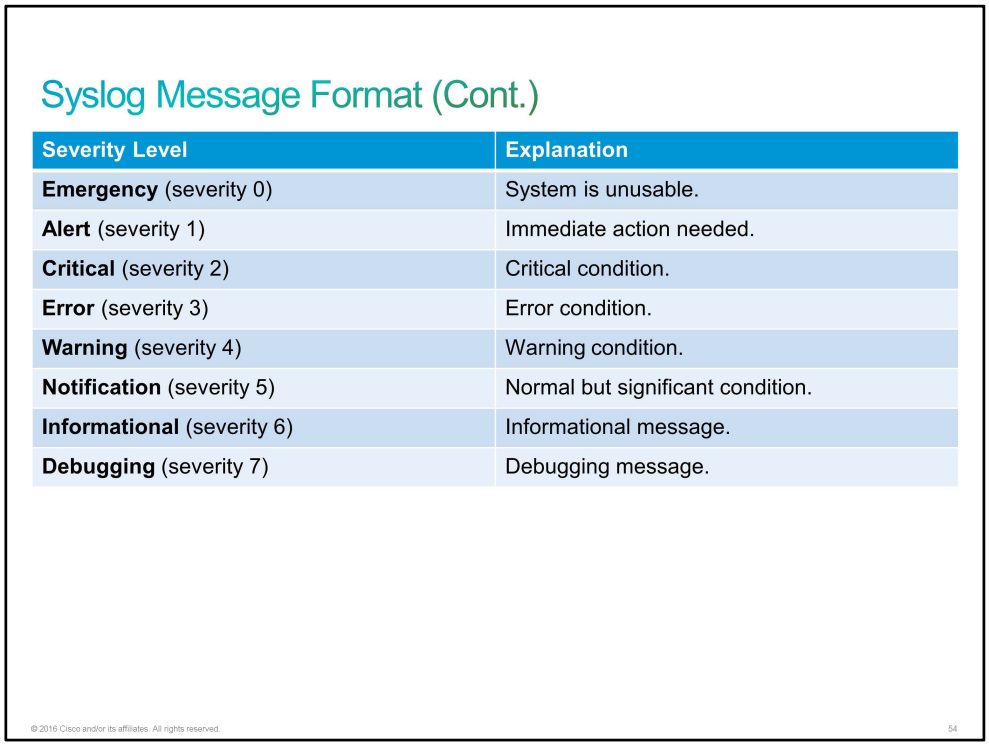
```
seq no:timestamp: %facility-severity-MNEMONIC:description
```



This table explains the items that Cisco IOS Software syslog message contains.



This table explains the eight message severity levels from the most severe level to the least severe level.

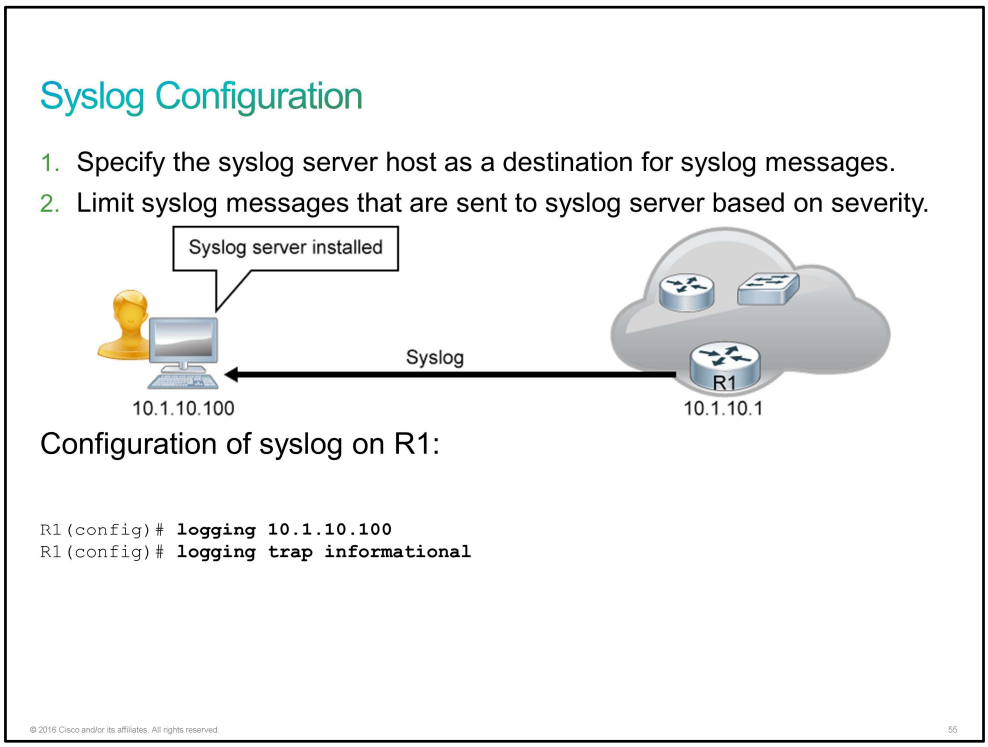


If severity level 0 is configured, it means that only emergency-level messages will be displayed. For example, if severity level 4 is configured, all messages with severity levels up to 4 will be displayed (**Emergency**, **Alert**, **Critical**, **Error**, and **Warning**).

The highest severity level is level 7, which is the debugging-level message. Much information can be displayed at this level, and it can even hamper the performance of your network. Use it with caution.

Syslog Configuration

To implement a syslog configuration, specify a syslog server host as a destination for syslog messages and limit the syslog messages that are sent to the syslog server based on the severity.



Configuration of syslog is based on the commands that the following table describes.

Command	Description
logging {*hostname* | *ip-address*}	Identifies a syslog server host to receive logging messages.
logging trap *severity*	Limits the syslog messages that are sent to the syslog server. It limits the messages based on severity.

The figure shows configurations for logging syslog messages to a syslog server with the IP address 10.1.10.100, where you can observe syslog messages.

The **logging** command identifies a syslog server host to receive logging messages. By issuing this command more than once, you build a list of syslog servers that receive logging messages. You can limit the syslog messages that are sent to the syslog server based on severity, using the **logging trap** command.

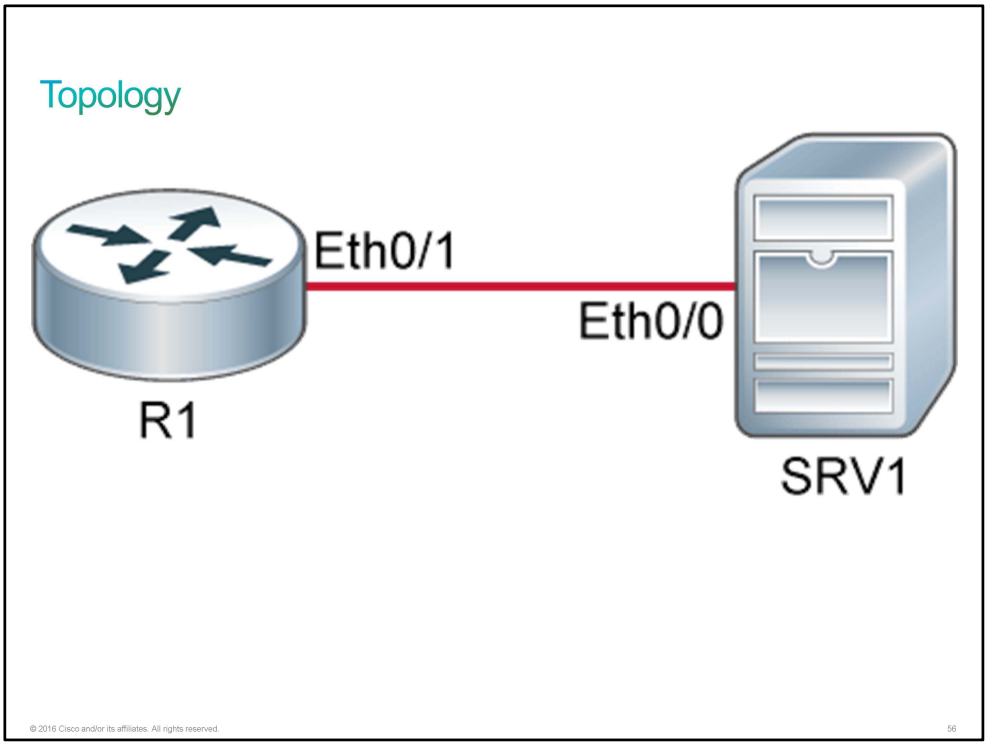
Discovery 52: Configure Syslog

Introduction

The objective of this discovery lab is to provide you with some experience with the syntax of basic syslog configuration to facilitate the management of Cisco IOS devices. This lab is prepared with the router and server that are represented in the topology diagram and the connectivity table. The devices have their basic configurations in place, including hostnames and IP addresses.

In the discovery lab, you will configure the syslog server address of the router and set the severity threshold for messages that are forwarded to the server. You will also use show commands to verify the syslog configuration and examine the syslog messages in the local logging buffer of the router.

Topology



Job Aid

Device Information

Device Information Table

Device	Characteristic	Value
SRV1	Hostname	SRV1
SRV1	IP address	10.1.1.10/24
R1	Hostname	R1

Device	Characteristic	Value
R1	Ethernet0/1 description	Link to SRV1
R1	Ethernet0/1 IP address	10.1.1.1/24

SRV in the virtual lab environment is simulated as router, so you should use Cisco IOS commands to configure it or make verifications.

Task 1: Configure Syslog

Activity

Step 1 Access the R1 console. Define SRV1 (10.1.1.10) as the R1 syslog server.

On R1, enter the following commands:

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# logging 10.1.1.10
```

The most commonly used commands are abbreviated in this guided discovery. For example, you use **conf t** for **configure terminal**. If there is any confusion, you can perform tab completion of commands to see the full commands during the discovery execution. For example, **conf<tab> t<tab>** would expand to **configure terminal**.

Step 2 Set "informational" as the threshold for the minimum severity level for messages to send to syslog servers.

On R1, enter the following commands:

```
R1(config)# logging trap informational
R1(config)# end
R1#
*Dec  1 08:04:49.998: %SYS-5-CONFIG_I: Configured from console by console
R1#
*Dec  1 08:04:51.027: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.1.1.10
port 514 started - CLI initiated
```

There is a syslog message that is displayed to the console indicating that logging has started to the server at 10.1.1.10. The first message is of severity 5 (Notification), and the second message is of severity 6 (Informational). Setting the threshold to "informational" means that messages of severity 0 through 6 will be forwarded to the syslog server. Both these messages are forwarded.

Step 3 Enter the **show logging** command to display the syslog status and the local logging buffer.

On R1, enter the following command:

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0
flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 32 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 32 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 35 message lines logged
        Logging to 10.1.1.10  (udp port 514, audit disabled,
              link up),
              2 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:

Log Buffer (4096 bytes):

*Dec  1 07:49:59.944: %IFMGR-7-NO_IFINDEX_FILE: Unable to open nvram:/ifIndex-
table No such file or directory
<... output omitted ...>
*Dec  1 08:04:49.998: %SYS-5-CONFIG_I: Configured from console by console
*Dec  1 08:04:51.027: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.1.1.10
port 514 started - CLI initiated
```

The output indicates that R1 is now sending syslog messages to 10.1.1.10 with the minimum severity threshold set to "informational." The output also indicates that two messages have been sent to the syslog server. Syslog uses UDP for transport and is inherently not reliable. If these two messages are lost somewhere in the transport path, there is no mechanism to recognize the lost message or to request a retransmission.

There is a local logging buffer. It is in its default state, with a severity threshold of "debugging" (Severity 7) and sized at 4096 bytes. In the sample transcript, 32 messages have been logged in the local buffer. The end of the **show logging** command output displays the contents of the buffer. At this point in the discovery, the buffer is mostly filled with the messages that were produced when R1 booted. At the end of the buffer, however, are the two syslog messages that were produced as a result of the syslog configuration activity.

Step 4 The output of the **show logging** command documents that two messages were sent to 10.1.1.10. Initiate some activity that will generate more syslog messages on R1. Enter the configuration mode, enable the interface Ethernet0/3, then disable the interface back down, and leave configuration mode.

On R1, enter the following commands:


```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# int e 0/3
R1(config-if)# no shut
R1(config-if)#
*Dec  1 08:10:54.261: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to
up
*Dec  1 08:10:55.265: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet0/3, changed state to up
R1(config-if)# shutdown
R1(config-if)#
*Dec  1 08:11:02.057: %LINK-5-CHANGED: Interface Ethernet0/3, changed state to
administratively down
*Dec  1 08:11:03.061: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet0/3, changed state to down
R1(config-if)# end
R1#
*Dec  1 08:11:06.063: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

This sample activity caused the generation of five syslog messages.

Step 5 Display the logging status and the local logging buffer.

On R1, enter the following command:

```
R1# show logging
<... output omitted ...>
    Console logging: level debugging, 37 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 37 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 40 message lines logged
        Logging to 10.1.1.10  (udp port 514, audit disabled,
              link up),
<... output omitted ...>
*Dec  1 08:10:54.261: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to
up
*Dec  1 08:10:55.265: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet0/3, changed state to up
*Dec  1 08:11:02.057: %LINK-5-CHANGED: Interface Ethernet0/3, changed state to
administratively down
*Dec  1 08:11:03.061: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet0/3, changed state to down
*Dec  1 08:11:06.063: %SYS-5-CONFIG_I: Configured from console by console
```

Additional messages were logged to 10.1.1.10.

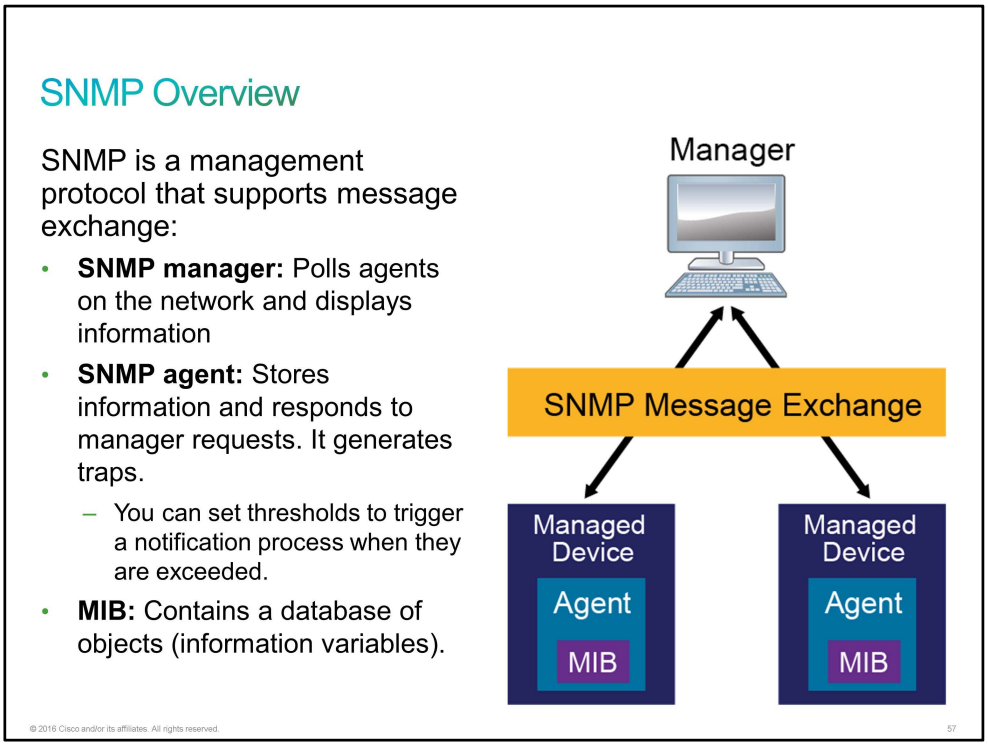
The five syslog messages that were produced in response to your previous activity are at the end of the local logging buffer.

This is the end of the discovery lab.

Introducing SNMP

In the complex network of routers, switches, and servers today, it can seem like a daunting task to manage all devices on your network and make sure that they are not only up and running but also performing optimally. This area is where SNMP can help. SNMP was introduced to meet the growing need for a standard of managing IP devices.

SNMP exposes environment and performance parameters of a network device, allowing an NMS to collect and process data.



SNMP is an application layer protocol that defines how SNMP managers and SNMP agents exchange management information. SNMP uses the UDP transport mechanism to retrieve and send management information, such as MIB variables.

SNMP is broken down into these three components:

- **SNMP manager:** Periodically polls the SNMP agents on managed devices by querying the device for data. The SNMP manager can be part of an NMS such as Cisco Prime Infrastructure.
- **SNMP agent:** Runs directly on managed devices, collects device information, and translates it into a compatible SNMP format according to the MIB.
- **MIB:** Represents a virtual information storage location that contains collections of managed objects. Within the MIB, there are objects that relate to different defined MIB modules (for example, the interface module).

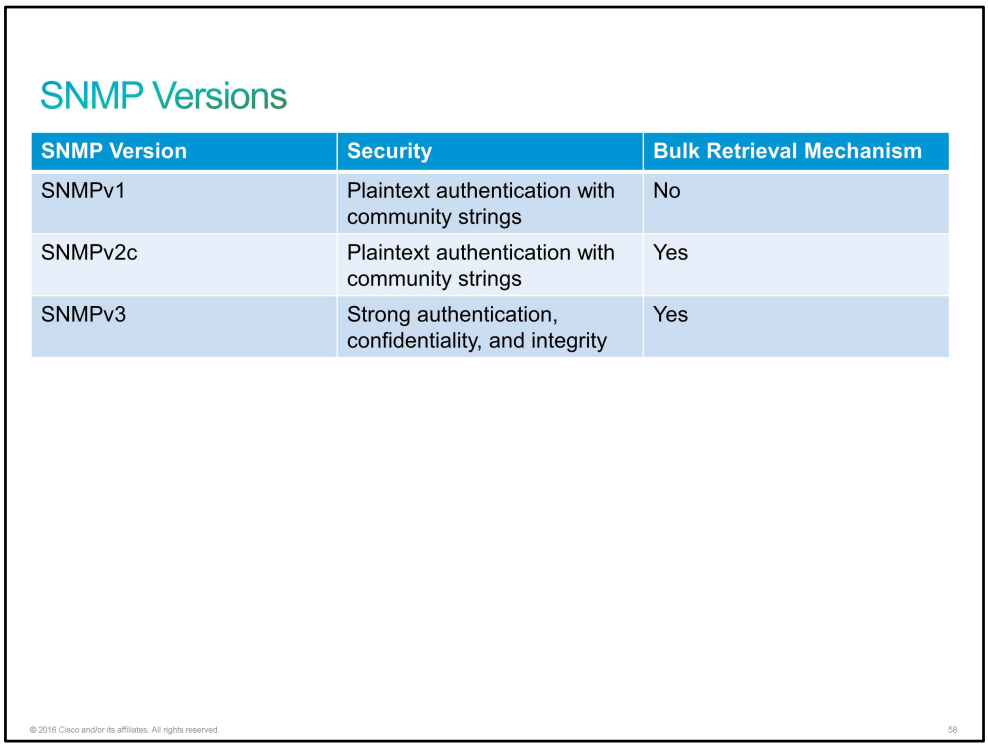
Routers and other network devices keep statistics about the information of their processes and interfaces locally. SNMP on a device runs a special process that is called an agent. This agent can be queried, using SNMP. SNMP is typically used to gather environment and performance data such as device CPU usage, memory usage, interface traffic, interface error rate, and so on. By periodically querying or "polling" the SNMP agent on a device, an NMS can gather or collect statistics over time. The NMS polls devices periodically to obtain the values of the MIB objects that it is set up to collect. It then offers a look into historical data and anticipated trends. Based on SNMP values, NMS triggers alarms to notify network operators.

To obtain information from the MIB on the SNMP agent, you can use several different operations:

- **Get:** This operation is used to get information from the MIB to an SNMP agent.
- **Get-next:** This operation is used to get the next object from the MIB to and SNMP agent.
- **Get-bulk**: This operation allows a management application to retrive a large section of a table at once.
- **Set:** This operation is used to get information to the MIB from an SNMP manager.
- **Trap:** This operation is used by the SNMP agent to send a triggered piece of information to the SNMP manager.
- **Inform:** This operation is the same as a trap, but it adds an acknowledgment that a trap does not provide.

SNMP Versions

New functionalities were added to SNMP through time. There are currently three versions of SNMP.



The following are different versions of SNMP:

- **SNMP Version 1:** SNMPv1 is the initial version of SNMP. SNMPv1 security is based on communities that are nothing more than passwords: plaintext strings that allow any SNMP-based application that knows the strings to gain access to the management information of a device. There are typically three communities in SNMPv1: read-only, read-write, and trap.

  A key security flaw in SNMPv1 is that the only authentication available is through a community string. Anyone who knows the community string is allowed access. Adding to this problem is the fact that all SNMPv1 packets pass across the network unencrypted. Therefore, anyone who can sniff a single SNMP packet now has the community string that is needed to get access.

- **SNMP Version 2c:** SNMPv2 was the first attempt to fix SNMPv1 security flaws. However, SNMPv2 never really took off. The only prevalent version of SNMPv2 today is SNMPv2c, which contains SNMPv2 protocol enhancements but leaves out the security features that no one could agree on. The "c" designates v2c as being "community based," which means that it uses the same authentication mechanism as v1—community strings.

- **SNMP Version 3:** SNMPv3 is the latest version of SNMP. It adds support for strong authentication and private communication between managed entities. You can define a secure policy for each group, and optionally limit IP addresses to which its members can belong. You have to define encryption and hashing algorithms and passwords for each user. The key security additions to SNMPv3 are as follows:
  - Can use MD5 or SHA hashes for authentication
  - Can encrypt the entire packet
  - Can guarantee message integrity

SNMPv3 introduces three levels of security:

- **noAuthNoPriv:** No authentication is required, and no privacy (encryption) is provided.
- **authNoPriv:** Authentication is required, but no encryption is provided.
- **authPriv:** In addition to authentication, encryption is also used.

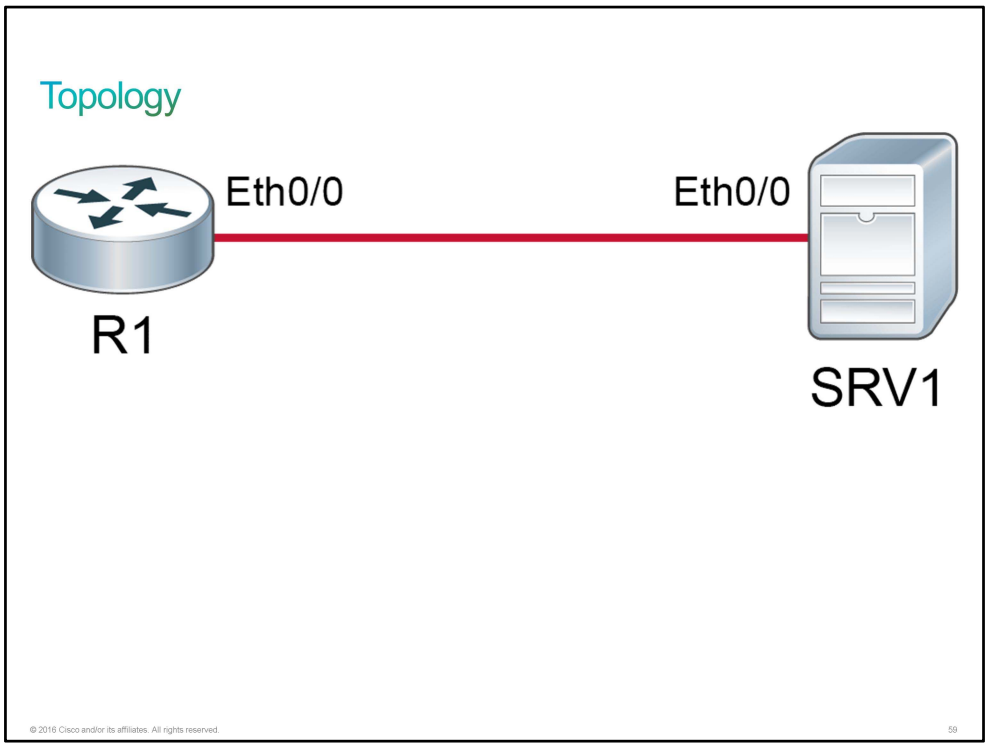
Note	Neither SNMPv1 nor SNMPv2c offer security features. Specifically, SNMPv1 and SNMPv2c can neither authenticate the source of a management message nor provide encryption.

Discovery 53: Configure SNMP

Introduction

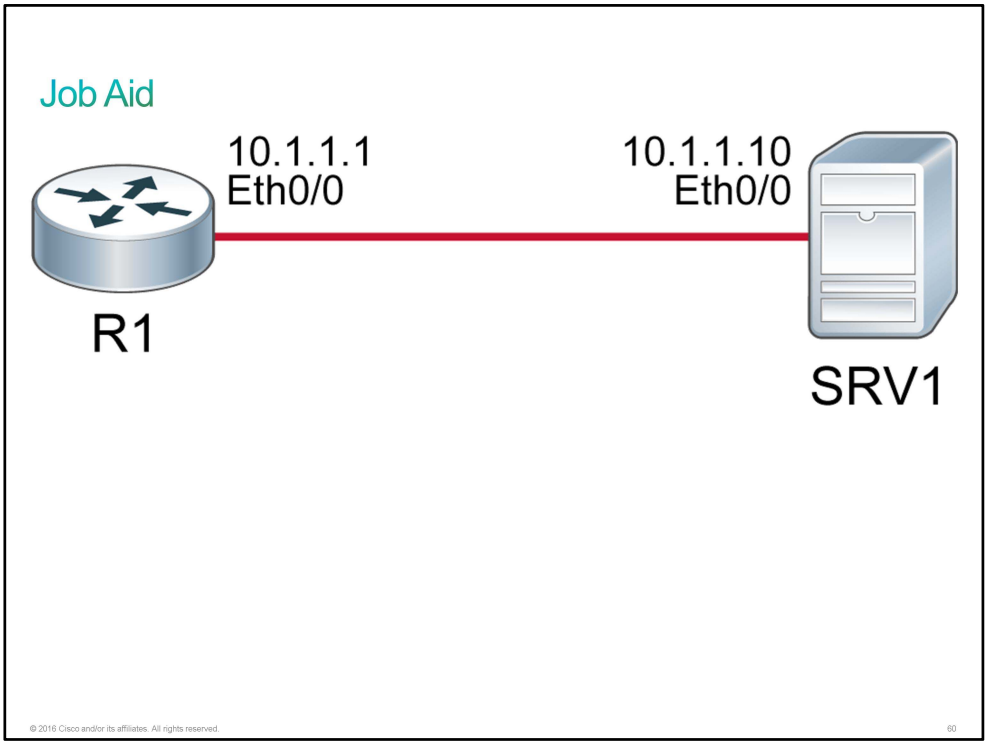
This discovery will provide you with some experience with the syntax of basic SNMP configuration facilitating the management of Cisco IOS devices. The live virtual lab is prepared with the router and server that are represented in the topology diagram and the connectivity table. The devices have their basic configurations in place, including hostnames and IP addresses. In the discovery, you will configure the router SNMP system contact and location variables. You will also define a read-only and a read-write community string and an SNMP server as the destination for SNMP traps.

Topology



Job Aid

Device Information



The configuration is as follows:

- All devices have their basic configurations in place, including hostnames and IP addresses.

Device Details

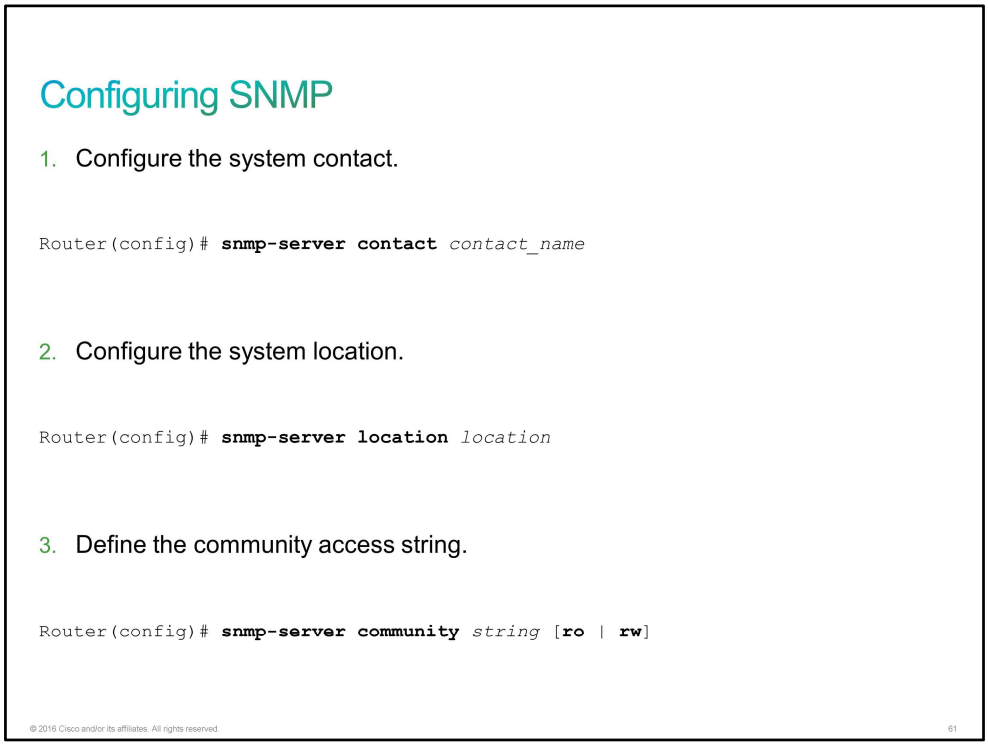
Device	Interface	Neighbor	IP Address
R1	Ethernet0/0	SRV1	10.1.1.1/24
SRV1	Ethernet0/0	R1	10.1.1.10/24

Note	PC and SRV in the virtual lab environment are simulated as routers, so you should use Cisco IOS commands to configure them or make verifications.

Task 1: Configure SNMP

To implement SNMP access to the router, you must do the following:

- On the router, set the system contact and location of the SNMP agent on the router.
- Configure a community access string with a read-write privilege to permit access to the SNMP.



Configuration of SNMP is based on the steps that are described in the table.

Command	Description
snmp-server contact *contact_name*	Sets the system contact string.
snmp-server location *location*	Sets the system location string.
snmp-server community *string* [**ro** | **rw**]	Defines the community access string with a read-only or read-write privilege.

Note	The first **snmp-server** command that you issue enables SNMP on the device.

A community string authenticates access to MIB objects and can have one of these attributes:

- **Read-only:** Gives read access to authorized management stations to all objects in the MIB, except the community strings, but it does not allow write access.
- **Read-write:** Gives read and write access to authorized management stations to all objects in the MIB, but it does not allow access to the community strings.

The system contact and the location of the SNMP agent is also set on the router so that you can access these descriptions through the configuration file. Configuring the basic information is recommended because it may be useful when troubleshooting your configuration.

Activity

Step 1 Access the R1 console. Set the R1 SNMP system contact to "admin@icnd2.lab" and set the R1 SNMP system location to Remote Lab Facility."

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# snmp-server contact admin@icnd2.lab
R1(config)# snmp-server location Remote Lab Facility
```

Note: All devices that support SNMP management must support MIB-2. MIB-2 stores data that is generically applicable to all IP devices. The three basic objects in MIB-2 are the system name, system contact, and system location. You just defined the latter two. The SNMP system name automatically inherits the value of the hostname setting on a Cisco IOS device, so the R1 SNMP system name was already R1.

Step 2 Define "Cisco1" as a read-only community string and "Cisco2" as a read-write community string.

```
R1(config)# snmp-server community Cisco1 ro
R1(config)# snmp-server community Cisco2 rw
```

SNMP community strings should be treated with the same care as passwords. The read-only community string has privileges that are similar to a login password, and the read-write community string has privileges that are similar to the enable secret. The strings that are used in this example are too easy to guess to use in a production environment.

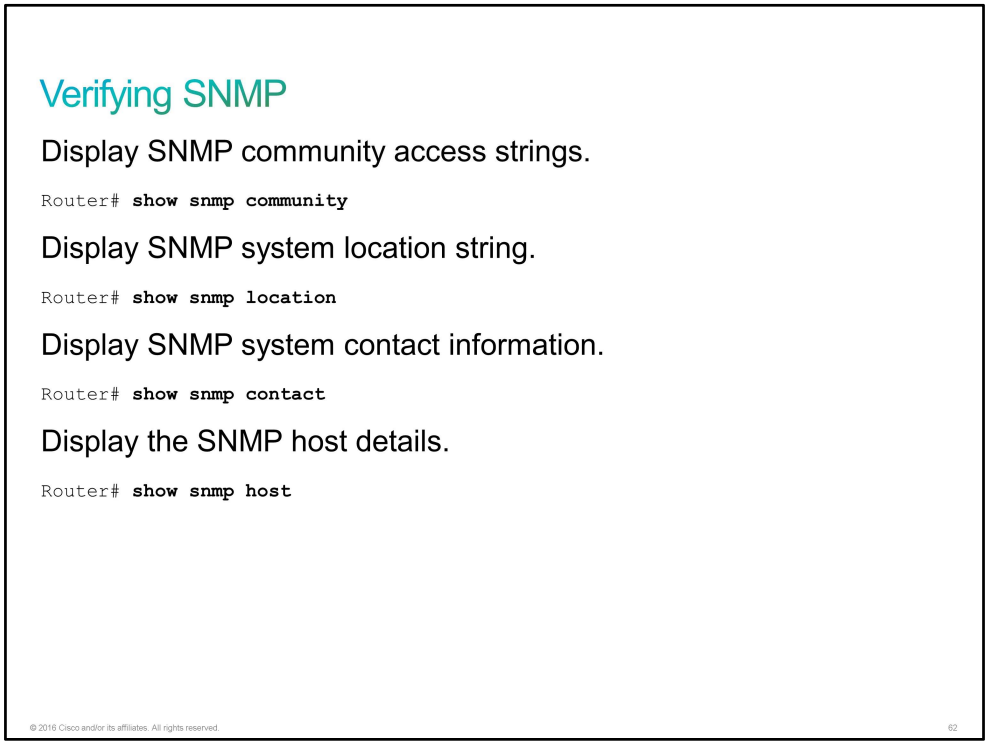
Step 3 Define SRV1 (10.1.1.10) as the SNMP destination for traps that R1 generates. Specify "Cisco3" as the community string to be included in the traps.

To specify the recipient of the SNMP notification operation, use the **snmp-server host** *ip-address community* command.

```
R1(config)# snmp-server host 10.1.1.10 Cisco3
R1(config)# exit
```

Traps provide the facility for the managed device to send unsolicited alerts to the SNMP system. It allows for faster response times than would be practical with periodic polling by the management system.

Verifying SNMP



The following tables represents the commands used to verify SNMP.

Command	Description
show snmp community	Displays SNMP community access strings.
show snmp location	Displays SNMP system location string.
show snmp contact	Displays SNMP system contact information.
show snmp host	Displays the recipient details for SNMP notification operations.

Step 4 Use the **show snmp community** command to verify that the three community strings that you just defined are active.

```
R1# show snmp community

Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only  active


Community name: Cisco1
Community Index: cisco1
Community SecurityName: Cisco1
storage-type: nonvolatile        active


Community name: Cisco2
Community Index: cisco2
Community SecurityName: Cisco2
storage-type: nonvolatile        active


Community name: Cisco3
Community Index: cisco3
Community SecurityName: Cisco3
storage-type: nonvolatile        active
```

The ILMI community string is defined within Cisco IOS Software. You cannot not configure it. It is a read-only community string that is associated with the LMI protocol running between a router and an ATM switch.

Challenge

1. How can you access the syslog of a router?

   A. On a remote router that is receiving the syslog
   B. On a router that is placed between the router that is sending the syslog messages and a syslog server that is receiving the log messages
   C. On a syslog server that is receiving the syslog
   D. On a remote switch that is receiving the syslog

2. This is the format of a syslog message:

   seq no: timestamp: %facility-severity-MNEMONIC:description
   What is the MNEMONIC?

   A. The text string or code that uniquely describes the message.
   B. The text that is a full sentence-like description of the event.
   C. A way of remembering previous events.
   D. A number that is part event number and part MAC Address.

3. You want to control the severity of the event that determines when a syslog should be sent. Which command do you use?

   A. **logging *{hostname | ip address}***
   B. **logging trap *severity***
   C. **logging severity**
   D. **logging level *severity***

4. Which of the following severity levels is used when a system is unusable?

   A. Emergency
   B. Alert
   C. Critical
   D. Error

5. Severity level "Emergency" has which number assigned to it?

   A. 0
   B. 1
   C. 6
   D. 7

6. A router is configured with the **snmp-server community Cisco RO** command. An NMS is trying to communicate to this router via SNMP. Which actions can be performed by the NMS?

   A. The NMS can only read obtained results.
   B. The NMS can read obtained results and change the hostname of the router.
   C. The NMS can only change the hostname of the router.
   D. None of the above is correct.

7. Match the operations used by SNMP agent to their explanation.

Set	This operation is used to get information from the MIB to an SNMP agent
Trap	This operation is used by the SNMP agent to send a triggered piece of information to the SNMP manager.
Inform	This operation is used to get information to the MIB from an SNMP manager.
Get	This operation is the same as a trap, but it adds an acknowledgment that a trap does not provide.

Answer Key

Challenge

1. C
2. A
3. B
4. A
5. A
6. A
7.

Get	This operation is used to get information from the MIB to an SNMP agent
Trap	This operation is used by the SNMP agent to send a triggered piece of information to the SNMP manager.
Set	This operation is used to get information to the MIB from an SNMP manager.
Inform	This operation is the same as a trap, but it adds an acknowledgment that a trap does not provide.

Lesson 2: Evolution of Intelligent Networks

Introduction

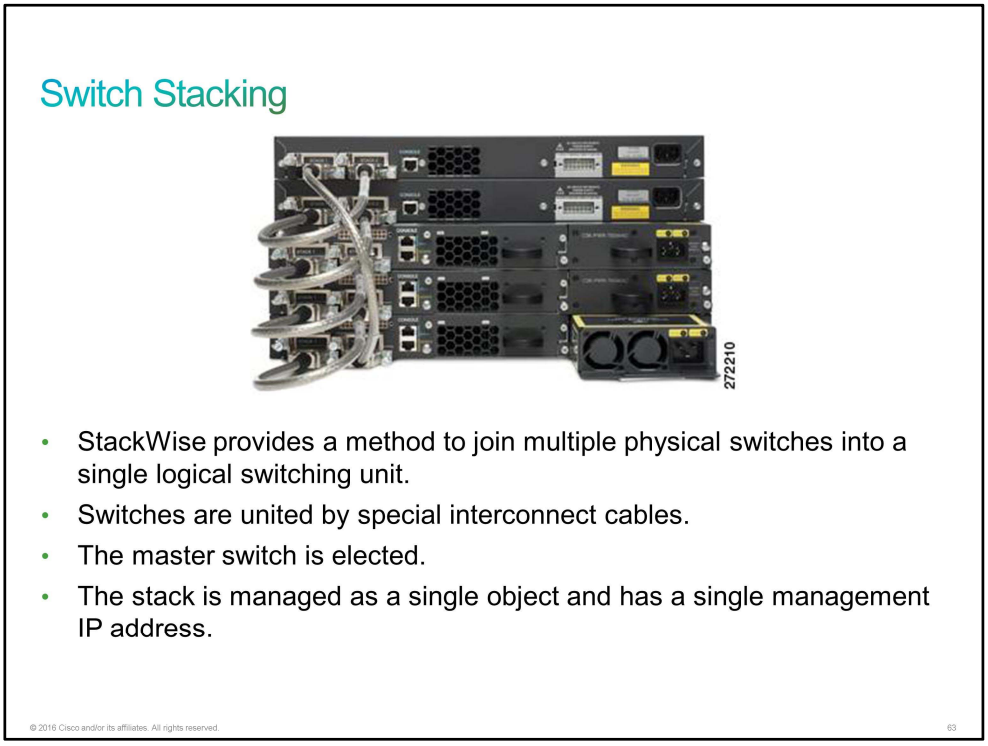
Bob, the senior engineer at CSS, came to you and asked you for a favor. He is really busy this week, so he would like you to explain to one of the customers what switch stacking is and how they would benefit from it. Bob also informs you that the management heard that intelligent networks are becoming increasingly popular, so they are wondering if you can use them in the corporate networks. Bob asks you to sit down with the manager and explain to them what the intelligent network really means—including cloud computing, SDN, and IWAN.

You can decide when during this week you will finish these two tasks—you can either do it today, or you can first do some research about the topics that are about to be discussed.

Switch Stacking

A typical switch topology on the access and the distribution layers has two (or more) access switches that are placed next to each other in the same rack to provide enough access ports for all network devices. Each access switch has two redundant connections to each of the distribution switches. This topology introduces certain overhead in terms of management, resiliency, and performance.

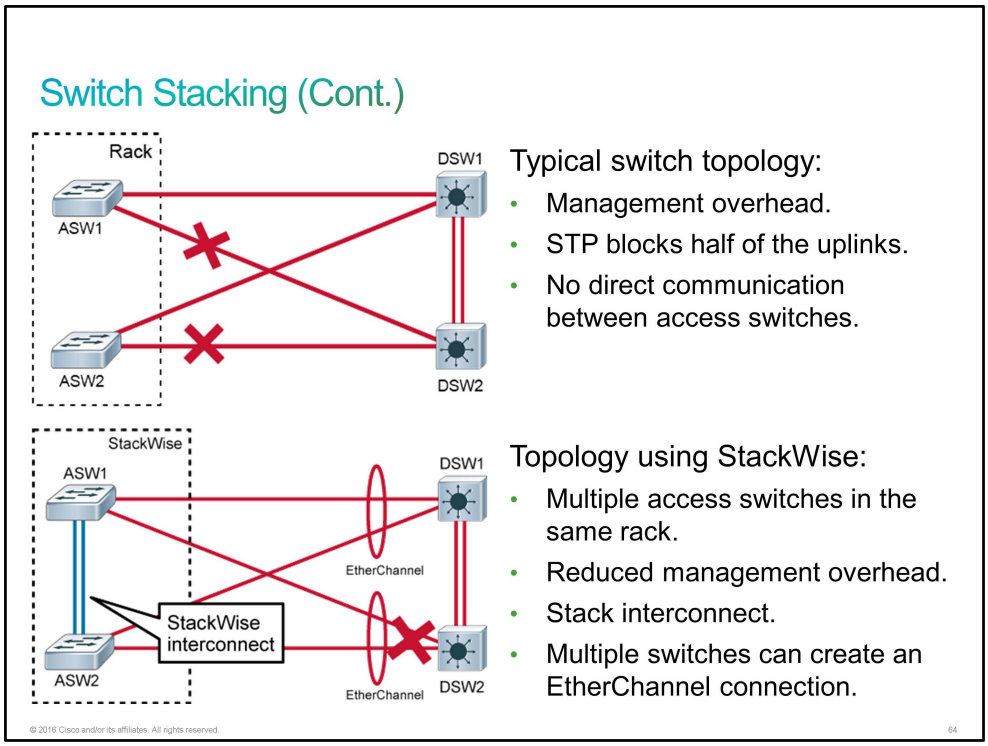
The Cisco StackWise technology is typically used to unite access switches that are mounted in the same rack. Multiple switches are used to provide enough access ports. The stack, which consists of up to nine switches, is managed as a single unit, reducing the number of units you have to manage in your network. All switches in the stack share configuration and routing information, creating a single switching unit. You can add switches to and deleted them from a working stack without affecting the performance.



You unite switches into a single logical unit using special stack interconnect cables that create a bidirectional closed-loop path. The network topology and routing information are updated continuously through the stack interconnect. All stack members have full access to the stack interconnect bandwidth. A master switch manages the stack as a single unit. The master switch is elected from one of the stack member switches. You can join up to nine separate switches.

Each stack of switches has a single IP address and is managed as a single object. This single IP management applies to activities such as fault detection, VLAN creation and modification, security, and QoS controls. Each stack has only one configuration file, which is distributed to each member in the stack.

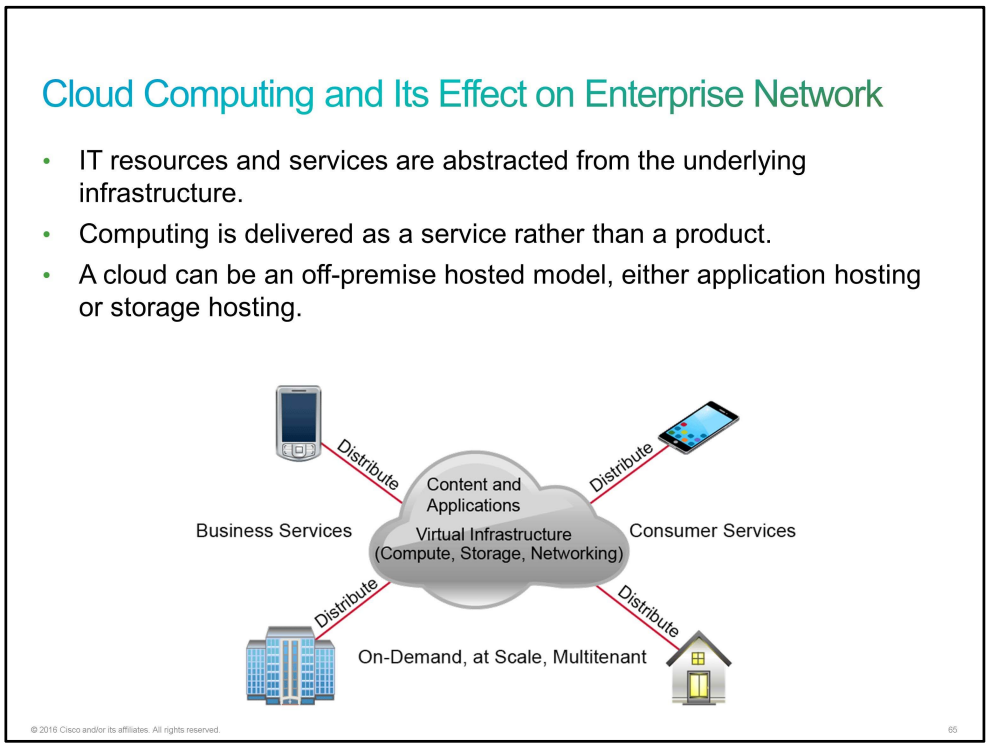
When you add a new switch to the stack, the master switch automatically configures the unit with the currently running IOS image and the configuration of the stack. You do not have to do anything to bring up the switch before it is ready to operate.



Multiple switches in a stack can create an EtherChannel connection. You might therefore avoid STP, doubling the available bandwidth of the uplinks of the existing distribution switches.

Cloud Computing and Its Effect on Enterprise Network

Cloud computing is a general term that describes a way of using resources: processing, storage, network, and so on. The term "cloud" and its deployment are somewhat new concepts, but the base concepts have been used for decades.



Deploying a cloud means deploying a computer system, or a network of systems, from which computing resources are offered to remote users. Therefore, from a user perspective, the resources are transparently available, regardless of the user point of entry. For example, a user can use a personal computer at home, an office computer at work, a borrowed computer, or a computer on a school campus. When accessing cloud resources, these resources will seem the same. Also, the data that the user stores is always available when users are connected to the cloud.

The cloud is available remotely via network connectivity, usually through the Internet. You can also use virtual private networks—also running over the Internet—or cloud-dedicated physical networks.

Computer resources that a cloud offers can vary greatly. The resources can include storage resources, computing resources, or applications. The user experience of using remote resources might be somewhat different than using local resources. The user experience depends on the capacity of the network access that is used to connect to the cloud. Therefore, a low-capacity network link might be sufficient only for services that require minimal data transfer or are not interactive, while high-capacity links could, theoretically, allow remote graphic rendering.

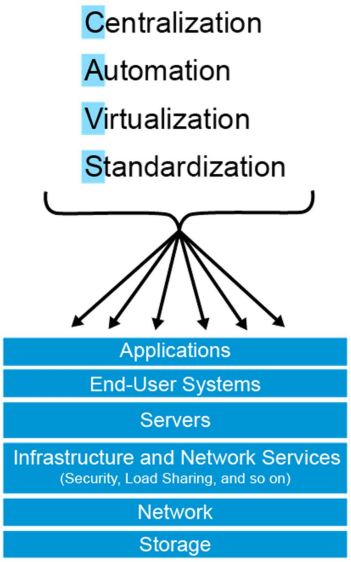
Cloud Computing and Its Effect on Enterprise Network (Cont.)

Advantages to the cloud service builder or provider:

- Cost reduction from standardization and automation
- High utilization through virtualized, shared resources
- Easier administration
- Fail-in-place operations model

Advantages to cloud users:

- On-demand, self-service resource provisioning
- Centralized appearance of resources
- Highly available, horizontally scaled application architectures
- No local backups



Cloud computing has several advantages over the traditional use of computer resources.

First, for operators, the way that clouds are deployed provides several advantages. Consolidation, virtualization, and automation are often mentioned in the context of cloud computing. These concepts, while very good for IT and data center management, do not necessarily apply to all cloud deployments.

Even if a company does not plan to deploy a cloud, consolidation, virtualization, and automation will improve the company data center setup.

With consolidation and virtualization, resources are used more efficiently. A classic example is the virtualization of servers. Two physical servers will use twice the amount of electricity as one server. With virtualization, however, one physical server can usually host two virtual machines. If there is a demand for more CPU power, you can, for example, invest in a new CPU. The other components—memory, storage, network interface, data bus, peripherals, and so on—can now be shared more efficiently.

A more efficient use of resources has a cost benefit, as less physical equipment means less cost. What minimizes the spending is the fact that the customer pays only for the services or infrastructure that the customer uses. From another side, the customer is offered a fixed price for each service that the customer uses. This fixed price means that the customer is now able to plan any future spending. Certainly, additional staff or staff education will cost more, but with added automation, staff increases may not be necessary. Administration will be easier and less complex, which will free staff to do other tasks.

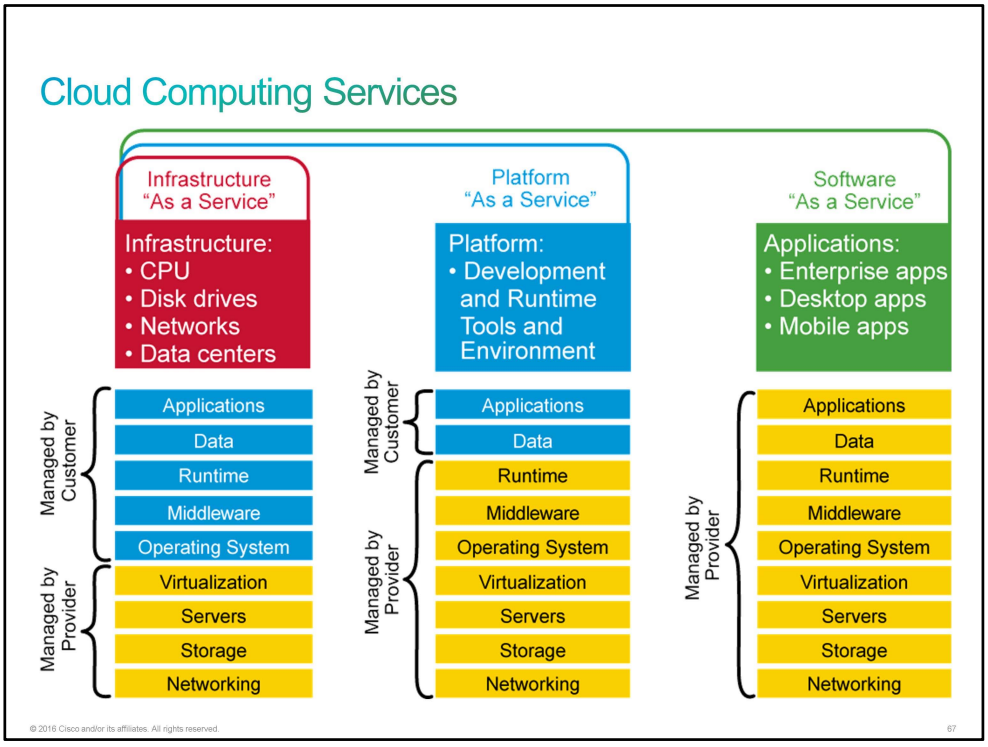
Second, there are benefits for users of cloud services. The obvious benefit is the centralization of resources. Although you do not need to centralize resources—you can and should distribute resources for better resiliency—, the resources will appear centralized to the cloud user. This benefit means that a user can move from computer to computer and always experience a familiar environment.

All data that the cloud stores will always be available. This availability means that users do not need to back up their data. Before the cloud, users could lose important documents because of an accidental deletion, misplacement, or computer breakdown. In the cloud, backups and data management are centralized, so users and IT staff no longer need to be concerned about backing up data on individual computers. If a computer fails, you can replace it with a generic system. As long as the cloud is up and running, the data is available.

If cloud computing offers CPU- or memory-intensive services as part of the cloud, you manage these resources at the data center. User computers may not need as many resources as before the introduction of cloud services, which may cut equipment costs. Also, resources are now managed in the data center rather than at each workstation, so performance of an application is not subject to a user workstation configuration.

Cloud Computing Services

The cloud offers various resources. For example, resources can be storage resources, computing resources, network resources, applications, and so on. The cloud service models define which services the cloud service providers offer.



Depending on which types of service you can get from a cloud, the following three service models exist:

- **Infrastructure as a Service (IaaS):** Provides only the network.
  - Delivers computer infrastructure (platform virtualization environment).
- **Platform as a Service (PaaS):** Provides the operating system and the network.
  - Delivers a computing platform and solution stack.
- **Software as a Service (SaaS):** Provides the required software, operating system, and network.
  - Provides ready-to-use applications or software

Also, service providers have an important building block for delivering IT as a service. Service providers offer resources, such and broadband network traffic, public IP addresses, and other services—for example, DHCP, NAT, and firewalls.

There are other "as-a-service" offerings from various cloud providers on the market, but those services focus on specific applications or platforms—such offerings can be classified under one of the three major "as-a-service" models.

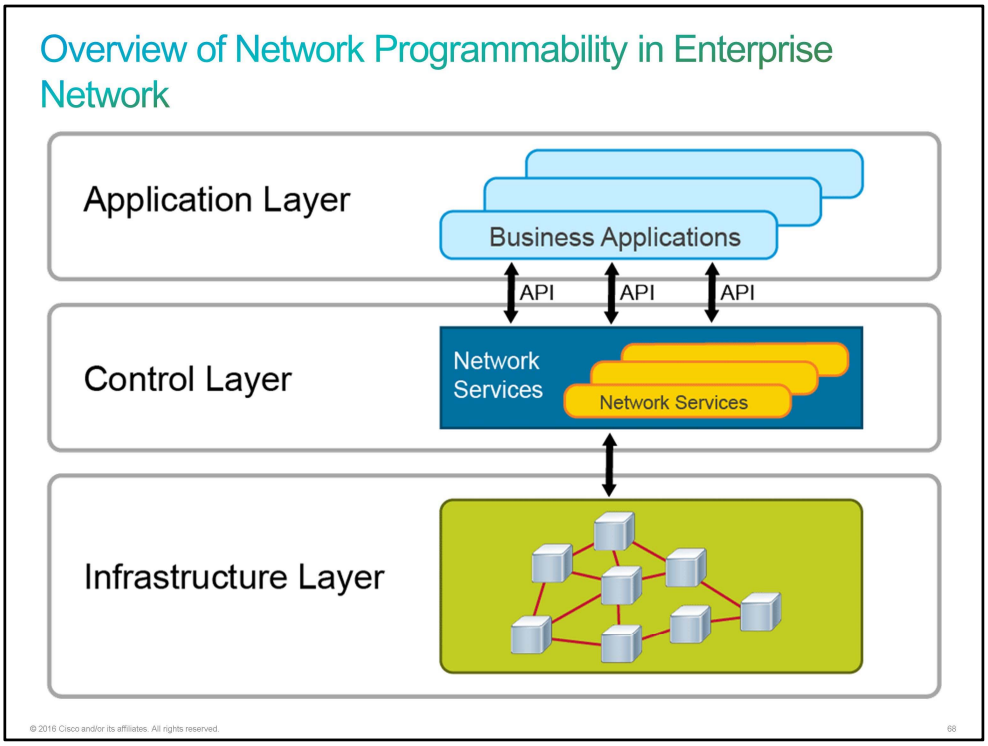
Note	Some examples of cloud computing are Google Docs, Salesforce, Amazon Web Services, Microsoft Office 365, British Telecom, Hosting provider, and so on. Some of these examples are services that providers offer to meet different business needs. Others are designed mainly for private use (such as Microsoft OneDrive, Google Docs, and so on). It does not matter if the cloud services are targeted towards companies or individuals, they are still cloud services.

Overview of Network Programmability in Enterprise Network

Traditional networks comprise several devices (for example, routers and switches) that are equipped with software and networking functionality:

- The data (or forwarding) plane is responsible for the forwarding of frames or packets.
- The control plane is responsible for controlling the forwarding tables that the data plane uses.

The SDN architecture changes the networking paradigm by removing "intelligence" from individual devices and transferring it to a central controller and enabling management of networks through software.



SDN separates the control plane of the network from the forwarding plane. It automates processes such as provisioning, configuration, and remediation allowing for flexibility, agility, and scalability.

SDN offers a centralized view of the network, giving an SDN controller the ability to act as the "brains" of the network. The control layer of the SDN is usually a software solution that is called the SDN controller. Using APIs, business applications tell the SDN controller what they need from the network. Then the controller uses the APIs to pass instructions to network devices, such as routers and switches. However, those two sets of APIs are very different. The controller uses southbound API to control individual devices and provide an abstracted network view to upstream applications using a northbound API.

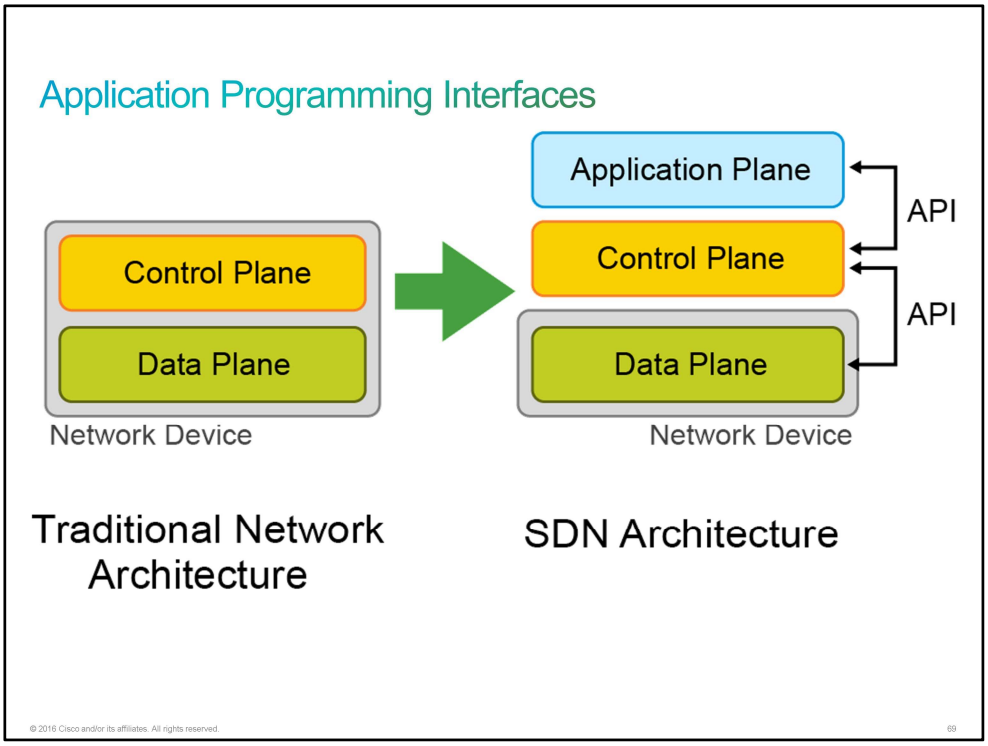
Note	SDN is not NFV. Researchers created SDN to easily test and implement new technologies and concepts in networking, but a consortium of service providers created NFV. Their main motivation was to speed up deployment of new services, and reduce costs. NFV accomplishes these facts by virtualizing network devices that were previously sold only as a separate box (such as the switch, router, firewall, and IPS) and by enabling them to run on any server. It is perfectly possible to use both technologies at the same time to complement each other. In other words, SDN decouples the control plane and data plane of network devices, and NFV decouples network functions from proprietary hardware appliances.

Application Programming Interfaces

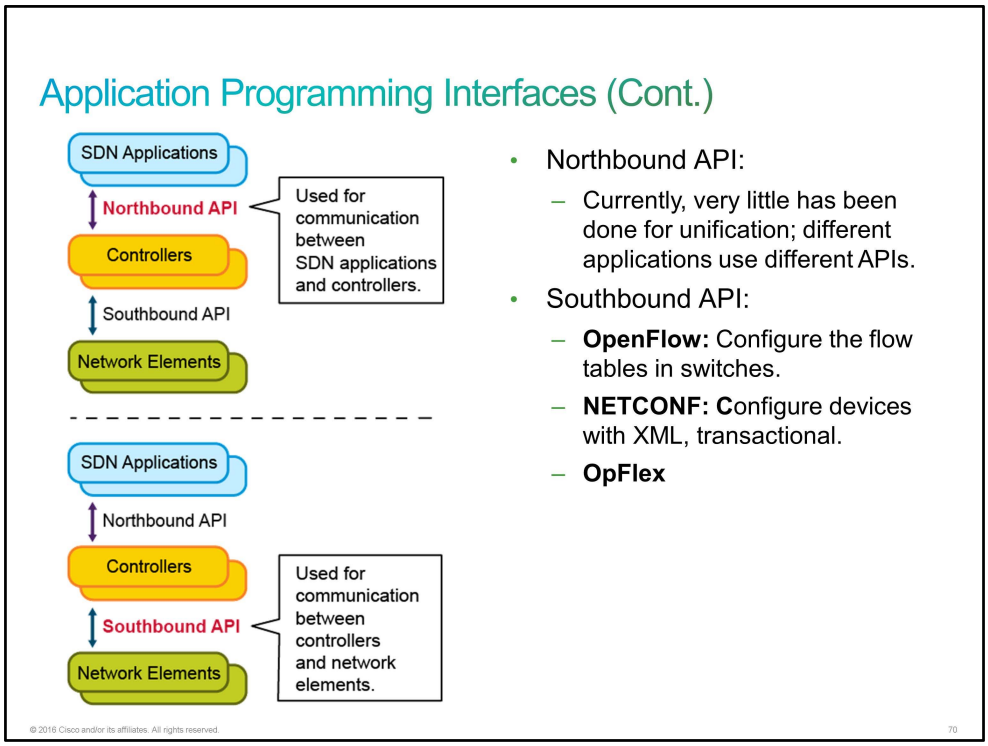
The SDN architecture slightly differs from the architecture of traditional networks. It comprises three stacked layers (from the bottom up):

- **Data (or forwarding) plane:** Contains network elements (any physical or virtual device that deals with customer traffic)
- **Control plane:** Represents the core layer of the SDN architecture. It contains SDN controllers, which provide centralized control of the devices in the data plane.
- **Application plane:** Contains SDN applications that communicate their network requirements toward the controller.

The SDN controller uses APIs to communicate with the application and data plane.



Communication with the data plane is defined with southbound interfaces, while services are offered to the application plane using the northbound interface.



Southbound APIs

Southbound APIs (or device-to-control-plane interfaces) are used for communication between the controllers and network devices.

- **OpenFlow:** Describes an industry-standard API, which the ONF defines. It configures white label switches, and as a result defines the flow path through the network. The actual configuration of the devices is accomplished with the use of NETCONF.
- **NETCONF:** It is a network management protocol that the IETF standardized. It provides mechanisms to install, manipulate, and delete the configuration of network devices via RPC mechanisms. The messages are encoded by using XML. Not all devices support NETCONF, the ones that do, advertise their capabilities via the interface.
- **OpFlex:** It is an open-standard protocol that provides a distributed control system that is based on a declarative policy information model. The big difference between OpFlex and OpenFlow lies with their respective SDN models. OpenFlow uses an imperative SDN model, where a centralized controller sends detailed and complex instructions to the control plane of the network elements in order to implement a new application policy. In contrast, OpFlex uses a declarative SDN model. The controller, which, in this case, is called by its marketing name APIC, sends a more abstract policy to the network elements. The controller trusts the network elements to implement the required changes using their own control planes.

Note	NETCONF is a protocol that allows you to modify the configuration of a networking device, whereas OpenFlow is a protocol that allows you to modify its forwarding table. If you need to reconfigure a device, NETCONF is the way to go. If you want to implement a new functionality that is not easily configurable within the software that your networking device is running, you should be able to modify the forwarding plane directly using OpenFlow.

Northbound APIs

Northbound APIs or northbound interfaces are responsible for the communication between the SDN controller and the services running over the network. Northbound APIs enable your applications to manage and control the network. So rather than adjusting and tweaking your network repeatedly to get a service or application running correctly, you can set up a framework that allows the application to demand the network setup that it needs. These applications range from network virtualization and dynamic virtual network provisioning to more granular firewall monitoring, user identity management, and access policy control.

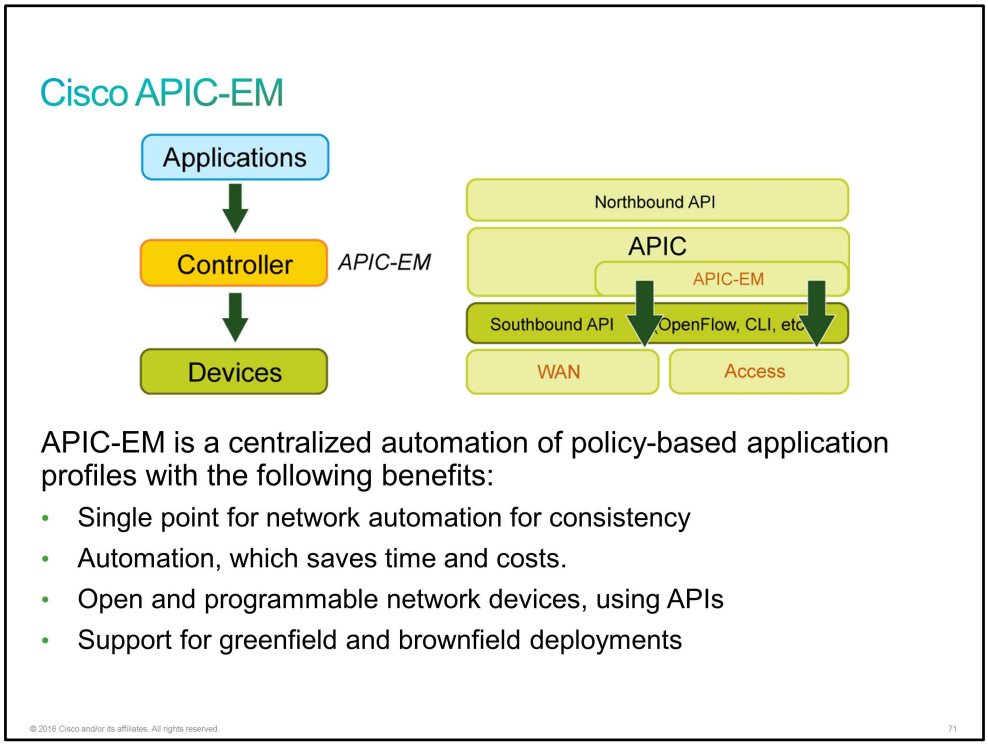
Unfortunately, currently there is no single northbound interface that you can use for communication between the controller and all applications. Instead, you use various different northbound APIs, each working only with a specific set of applications.

Cisco APIC-EM

Lately, many different SDN controller platforms have emerged. Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) is one of them. It is a Cisco SDN controller for enterprise networks—access, campus, and WAN.

Note	With Cisco APIC-EM, you can program the network in an automated fashion that is based on the application requirements. The policies are applied with the use of OpFlex, OpenFlow, or, NETCONF. Besides APIC-EM, there is also a controller for the data center environment (Cisco Application Policy Infrastructure Controller Data Center [Cisco APIC-DC]).

With Cisco APIC-EM, you can use open programmability APIs for policy-based management and security through a single controller. It provides you with abstraction of the network, further simplifying the management of network services. This approach automates what has typically been a tedious manual configuration.

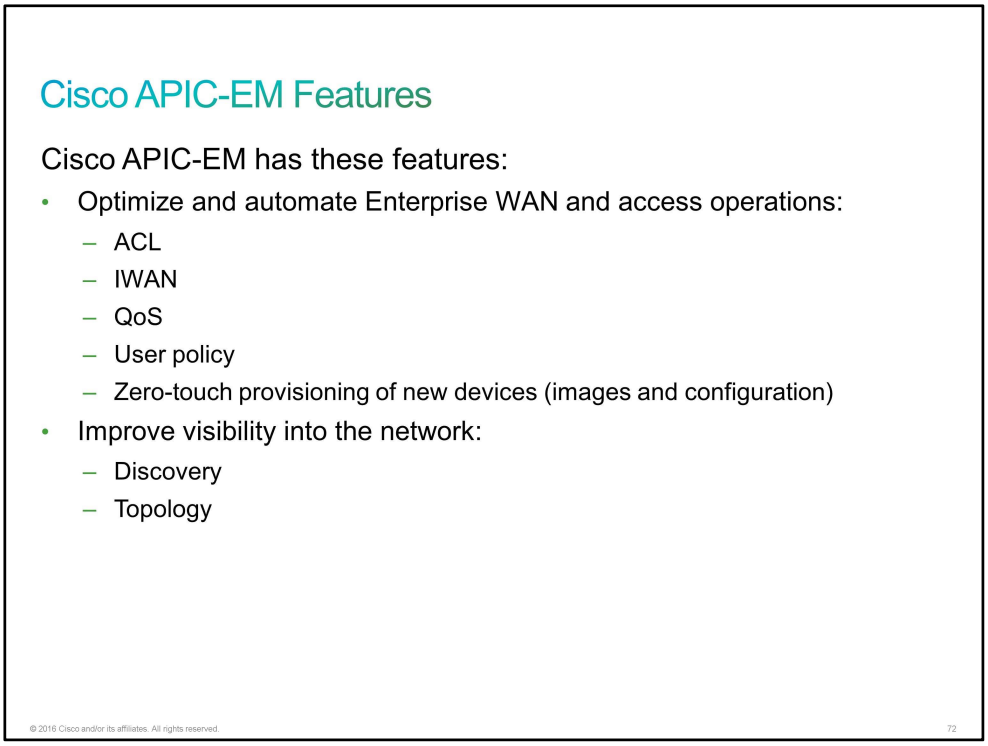


The controller provisions network services consistently and provides rich network information and analytics across all network resources: both LAN and WAN, wired and wireless, and physical and virtual infrastructures. This visibility allows you to optimize services and support new applications and business models. The controller bridges the gap between open, programmable network elements and the applications that communicate with them, automating the provisioning of the entire end-to-end infrastructure.

Cisco APIC-EM simplifies and streamlines network operations while also reducing cost. It frees the IT department to focus on business innovation by deploying new network devices and applications rapidly. The following are some of the benefits of Cisco APIC-EM:

- Consistency across the enterprise network keeps downtime to a minimum and lowers operational complexity and associated cost.
- Automated end-to-end provisioning and configuration enable rapid deployment of applications and services. Provisioning times drop from months to hours.
- Open and programmable network devices, policy, data, and analytics drive business innovation by providing easy access to network intelligence.
- Support for greenfield and brownfield deployments lets you implement programmability and automation with the infrastructure that you already have.

Cisco APIC-EM Features



The following are some features of Cisco APIC-EM:

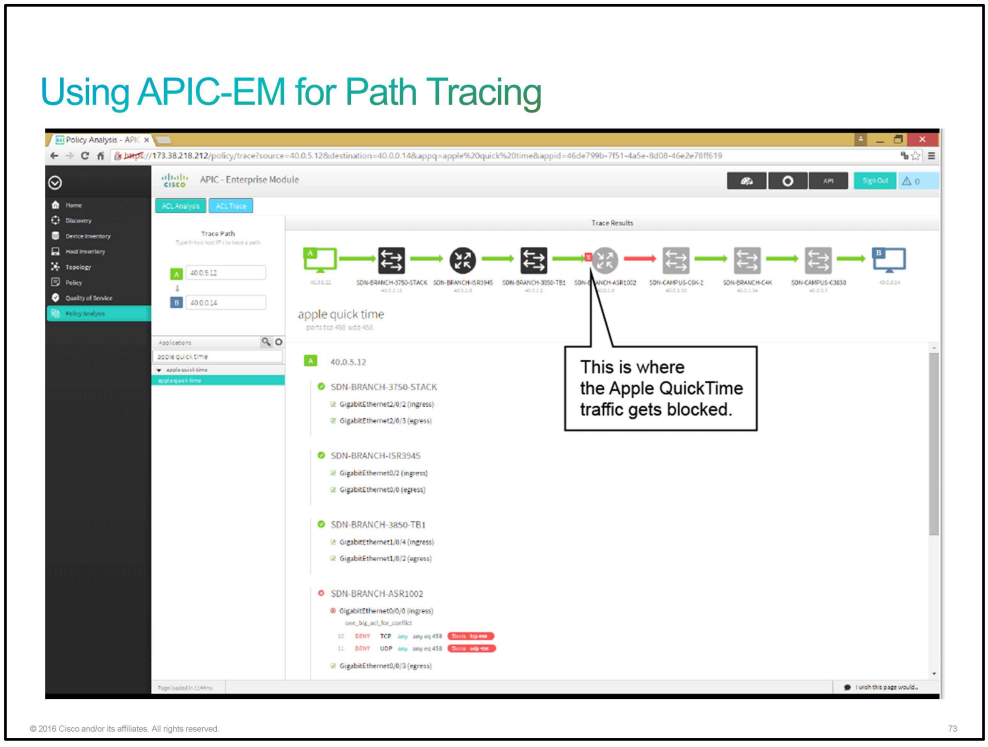
- **Network Information Database**: Scans the network and provides the inventory, including all network devices.
- **Network topology visualization**: Autodiscovers and maps network devices to a physical topology with detailed device-level data (including the discovered hosts).
- **Zero-touch deployment**: When the controller scanner discovers a new network device, it creates a network information database entry for it and then automatically configures it.
- **Identity Manager**: You can track user identities and endpoints by exchanging the information with the Cisco Identity Service Engine (Cisco ISE).
- **Policy Manager**: The controller translates a business policy into a network device-level policy. It can enforce the policy for a specific user at various times of the day, across wired and wireless network.

- **ACL analysis:** Accelerates ACL management by querying and analyzing ACLs on each network device. It can quickly identify ACL misconfiguration.
- **QoS deployment and change management**: You can quickly set and enforce QoS priority policies.
- **Cisco Intelligent WAN application**: Simplifies the provisioning of IWAN network profiles with simple business policies.

Using APIC-EM for Path Tracing

Using the path trace service of ACL analysis allows you to examine the path that a specific type of packet travels as it makes its way across the network from a source to a destination node.

The path takes into account not only the source and destination IP addresses, but it can also consider the TCP or UDP source and destination ports. This way, if there are specific configuration settings that are related to these packet fields that would impact forwarding behavior, then APIC-EM will take these factors into account (for example, by showing where the specific traffic gets blocked).
The result of a path trace will be a visual and textual representation of the path that a packet takes across all the devices and links between the source and destination.



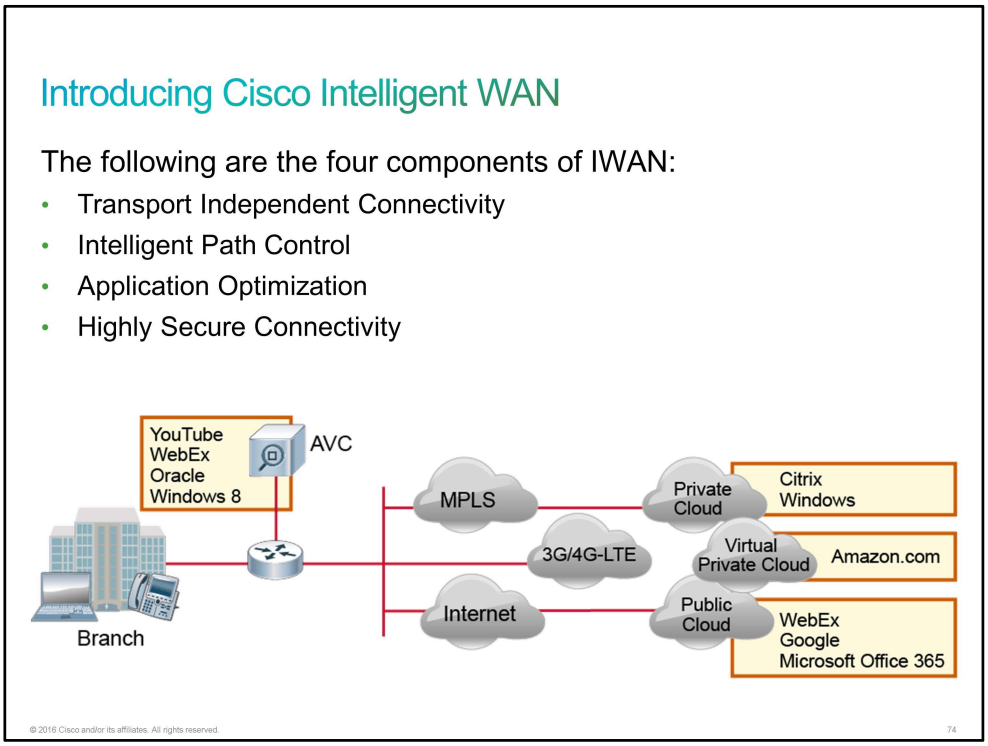
When you fill in the fields for the source, destination, and optionally the application, the path trace is initiated. The output for a path trace consists of two elements:

- The graphical display of the path between the hosts
- The list of each device along the path, with details about the interfaces.

In the example, you can see that the traffic for the Apple QuickTime application gets blocked on the SDN-BRANCH-ASR1002 router in the ingress direction.

Introducing Cisco Intelligent WAN

Media-rich applications, an increased number of devices connecting to the network, guest access, IoT, and other factors are causing a higher demand for bandwidth at the branch location. Cheaper Internet connections have become more reliable, and they are more economical compared to dedicated links. The Cisco Intelligent WAN (Cisco IWAN) solution gives you a way to take advantage of cheaper bandwidth at branch locations, without compromising application performance, availability, or security.



Cisco IWAN enables organizations to deliver an uncompromised experience over any connection. With Cisco IWAN, IT organizations can provide more bandwidth to their branch office connections by using less expensive WAN transport options without affecting performance, security, or reliability. With the Cisco IWAN solution, traffic is dynamically routed based on the application SLA, endpoint type, and network conditions in order to deliver the best-quality experience. The realized savings from Cisco IWAN not only pay for the infrastructure upgrades, but also free resources for business innovation.

The following are the components of Cisco IWAN:

- **Transport Independent Connectivity**: Cisco IWAN provides a DMVPN-based overlay across all available connectivity. This solution provides one network with a single routing domain. You can easily multihome the network across different types of connections including MPLS, broadband, and cellular. You gain the flexibility to use any available connectivity and to add or replace network connections without having to modify your network architecture.
- **Intelligent Path Control**: By using Cisco Performance Routing (Cisco PfR), Cisco IWAN improves delivery and WAN efficiency of applications. Cisco PfR dynamically controls data packet forwarding decisions by looking at the application type, performance, policies, and path status.

- **Application Optimization**: Cisco Application Visibility and Control (Cisco AVC) and Cisco Wide Area Application Services (Cisco WAAS) give you the visibility of and help you optimize application performance over WAN links.
- **Highly Secure Connectivity**: When traffic is sent over the public Internet, you must make sure that it is secure. By taking advantage of the varying VPN, firewall, network segmentation, and security features, Cisco IWAN helps make sure that the solution provides the security you need.

Challenge

1. Match the switch stacking terms with their descriptions.

StackWise	used to connect the switches to create a bidirectional closed-loop path
StackWise interconnect cable	up to 9 individual switches joined in a single logical switching unit

2. How is cloud computing defined?

   A. a classic data center
   B. an on-demand computing model
   C. a computing model with data at the service provider
   D. a computing model with data in a local data center

3. In which cloud service model is the customer responsible for managing the operating system, software, platforms, and applications?

   A. PaaS
   B. SaaS
   C. IaaS
   D. applications

4. Which three layers are part of the SDN architecture? (Choose three.)

   A. data
   B. control
   C. presentation
   D. session
   E. application
   F. transport

5. Between which two planes are SDN southbound interfaces used?

   A. control plane
   B. switching plane
   C. data plane
   D. routing plane
   E. application plane
   F. OpenFlow

6. What does using SDN in your network mean?

   A. Network engineers will be out of a job because everything will be automated.
   B. You will have to replace all existing software.
   C. You will have to replace all existing hardware.
   D. You will be able to react faster when a new business requirement arises.

7. Which statement about IWAN is correct?

   A. The IWAN allows transport-independent connectivity.
   B. The IWAN allows only static routing.
   C. The IWAN does not provide application visibility because only encrypted traffic is transported.
   D. The IWAN needs special encrypting devices to provide an acceptable security level.

Answer Key

Challenge

1.

StackWise interconnect cable	used to connect the switches to create a bidirectional closed-loop path
StackWise	up to 9 individual switches joined in a single logical switching unit

2. B
3. C
4. A, B, E
5. A, C
6. D
7. A

Lesson 3: Introducing QoS

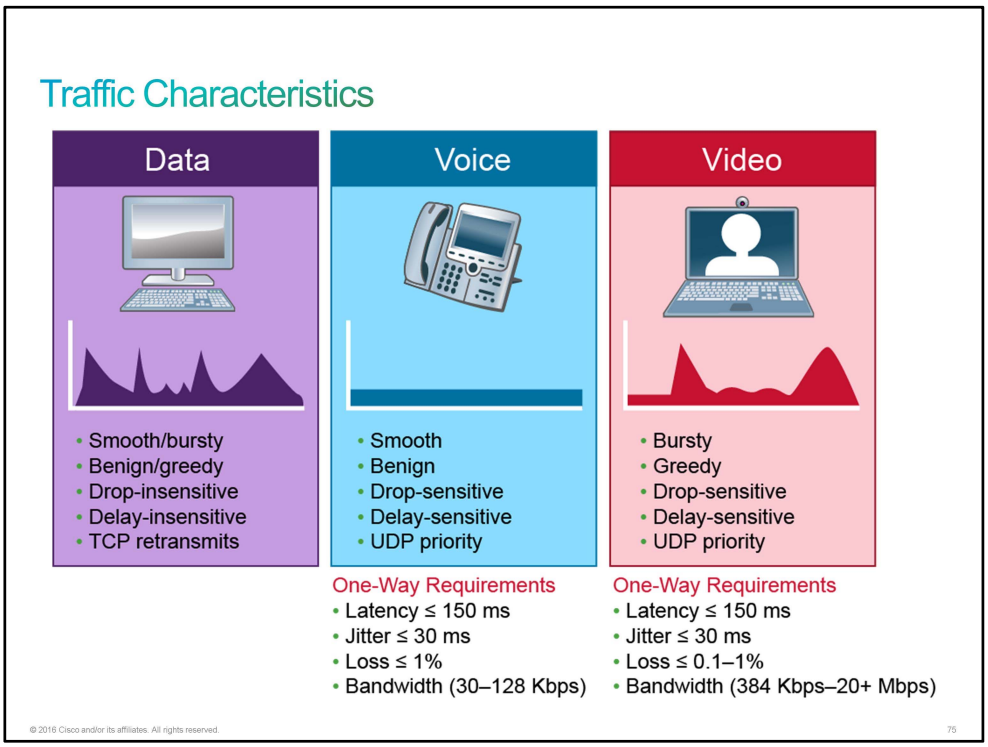
Introduction

QoS can be defined as the measure of transmission quality and service availability of a network (or internetwork). Another definition of QoS is that it refers to the ability of a network to provide improved service to the selected network traffic over various underlying technologies. The common theme here is that QoS ensures quality service to network traffic.

A network where no QoS strategy, tools, or techniques have been implemented, treats all traffic the same way. This kind of network offers a best-effort service. It does its best to send all packets and treats all packets equally. If a company CEO is on a voice call with an important client and someone starts to download a movie to watch over the weekend, the network treats both types of traffic equally. The network does not consider voice traffic any differently if contention for network resources exists. This experience is probably not how the CEO imagined that the network should work.

Traffic Characteristics

In today's networks, you will find a mix of data, voice, and video traffic. Each traffic type has different properties.



Data traffic is not real-time traffic. It comprises bursty (or unpredictable) and widely varying packet arrival times. Many types of application data exist within an organization. For example, some are relatively noninteractive and therefore not delay-sensitive (such as email). Other applications involve users entering data and waiting for responses (such as database applications) and are therefore very delay-sensitive. You can also classify data according to its importance to the overall corporate business objectives. For example, a company that provides interactive, live e-learning sessions to its customers would consider that traffic to be mission-critical. On the other hand, a manufacturing company might consider that same traffic important, but not critical to its operations.

Voice traffic is real-time traffic and comprises constant and predictable bandwidth and packet arrival times.

Video traffic comprises several traffic subtypes, including passive streaming video, real-time interactive video, and video conferences. Video traffic can be real time, but not always. Video has varied bandwidth requirements, and comprises different types of packets with different delay and tolerance for loss within the same session.

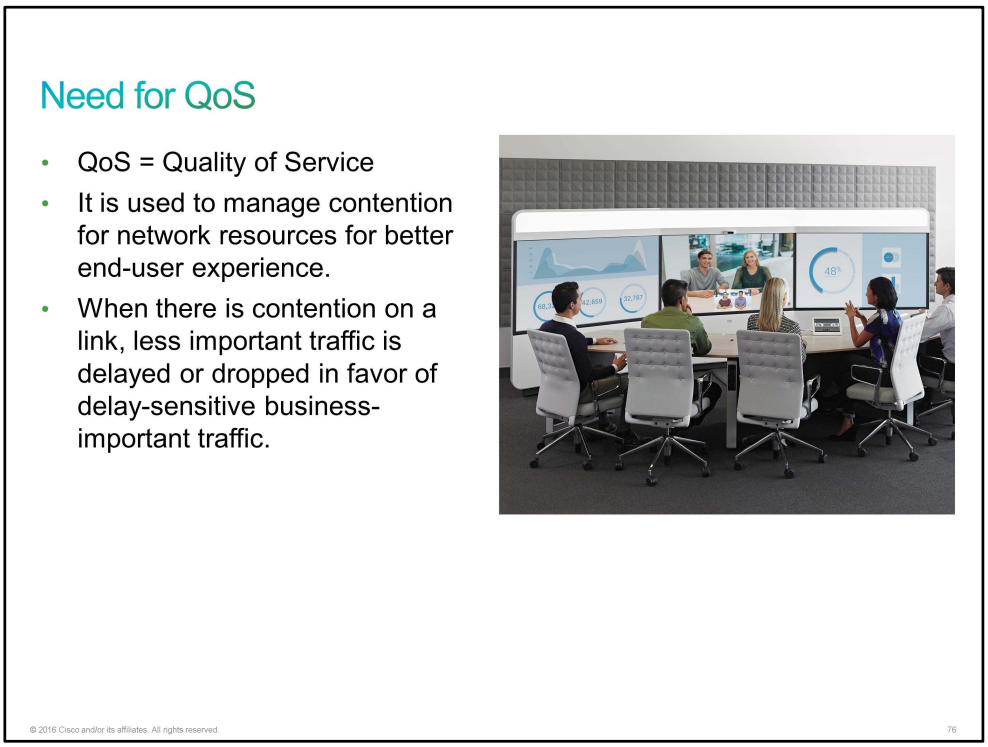
Interactive video, or video conferencing, has the same delay, jitter, and packet loss requirements as voice traffic. The difference is the bandwidth requirements—voice packets are small while video conferencing packet sizes can vary, as can the data rate. A general guideline for overhead is to provide 20 percent more bandwidth than the data currently requires. Streaming video has different requirements than interactive video. An example of the use of streaming video is when an employee views an online video during an e-learning session. As such, this video stream is not nearly as sensitive to delay or loss as interactive video is. Requirements for streaming video include a loss of no more than 5 percent and a delay of no more than 4 to 5 seconds. Depending on how important this traffic is to the organization, it can be given precedence over other traffic.

When you start watching a recording on the Internet, you might see messages such as "Buffering 50%" before the video starts in the application that you are running. This buffering is to compensate for any transmission delays that might occur.

Note	You must also consider the traffic that is related to the operation of the network itself. One example of this type of traffic is routing protocol messages—the size and frequency of these messages vary, depending on the specific protocol that the network uses and the stability of the network. Network management data is another example, including SNMP traffic between network devices and the network management station.

Need for QoS

The fundamental purpose of QoS is to manage contention for network resources to maximize the end-user experience of a session. Because not all packets are equal, you should not treat them equally.



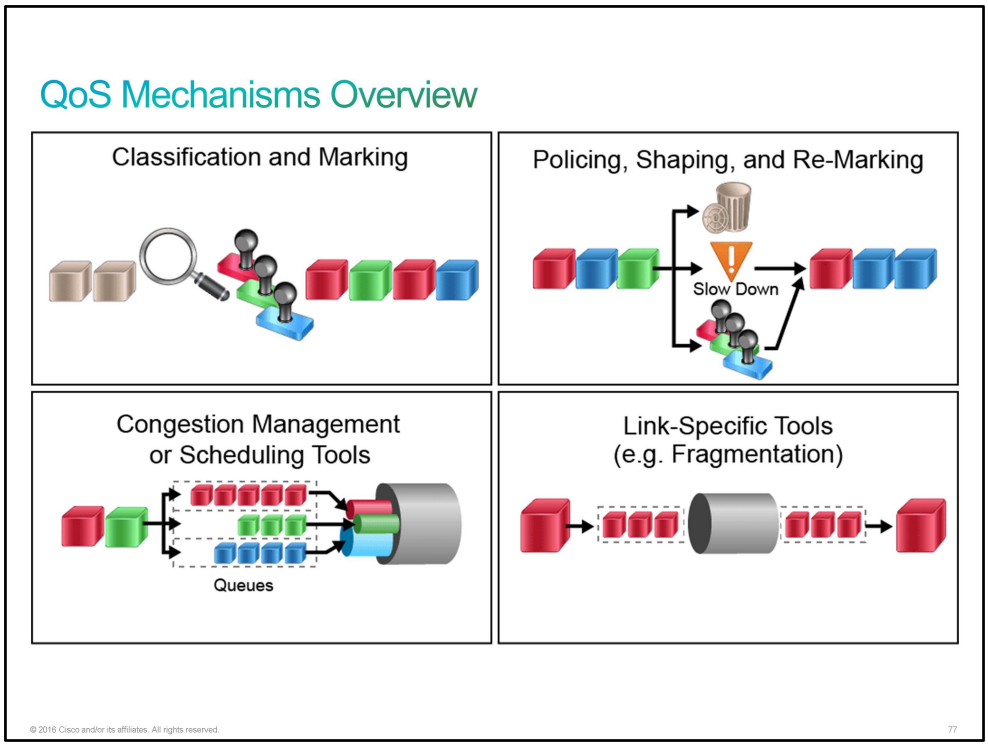
QoS gives priority to some sessions over other sessions. Packets of delay-sensitive sessions bypass queues of packets belonging to non-delay-sensitive sessions. When queue buffers overflow, packets are dropped on the session that can recover from the loss or those sessions that can be eliminated with minimal business impact.

In order to make space for applications that are important and cannot tolerate loss without affecting the end-user experience, QoS *manages* other sessions based on QoS policy decisions that you implemented in the network. *Managing* refers to selectively delaying or dropping packets when contention arises.

Note	QoS describes technical network performance and you can measure QoS. Measurements are numerical: jitter, latency, bandwidth, and so on. QoE measures end-user perception of the network performance. QoE is not a technical metric, it is a subjective metric. You deploy QoS features to maximize QoE for the end user. When you have a session between two users, QoE is what these two users experience, regardless of how the network between them works. QoS is almost meaningless when you implement it on only a segment of your network, because the QoE perception is equal to the impairment that is imposed by the worst-performing segment of the network.

Introducing QoS Mechanisms

Generally, you can place QoS tools into different categories as presented in the figure.



Classification and marking tools: These tools analyze sessions to determine which traffic class they belong to and therefore which treatment the packets in the session should be given. Classification should happen as few times as possible, because it takes time and uses up resources. For that reason, packets are marked after classification, usually at the ingress edge of a network. A packet might travel across different networks to its destination. Reclassification and re-marking are common at the hand-off points upon entry to a new network.

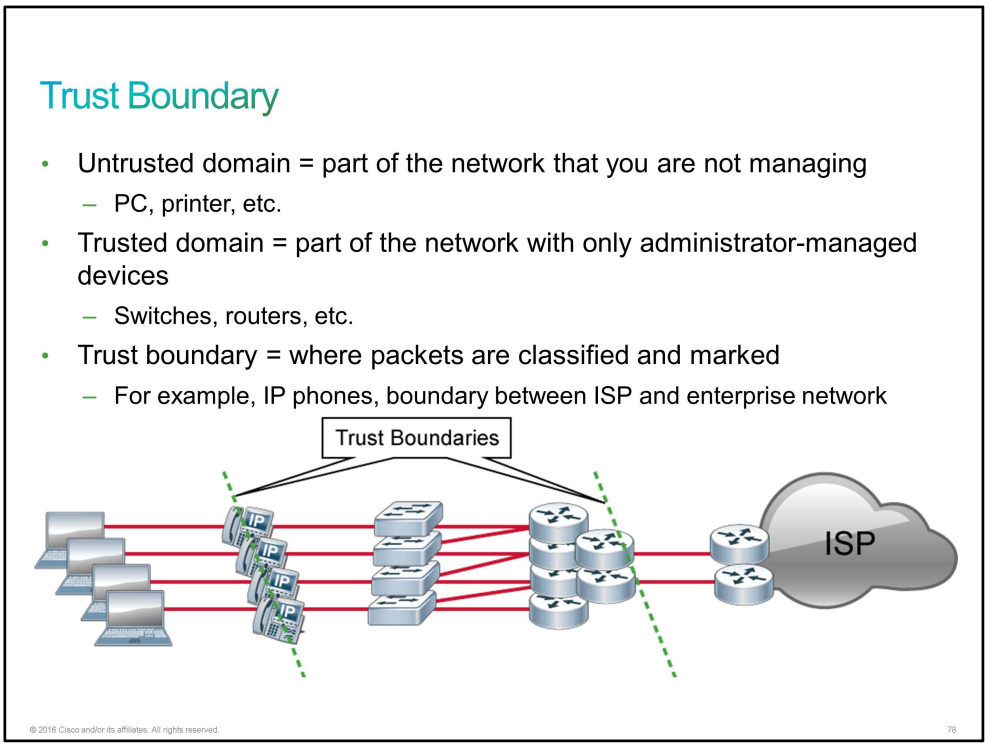
Policing, shaping, and re-marking tools: These tools assign different classes of traffic to certain portions of network resources. When traffic exceeds available resources, some traffic might be dropped, delayed, or re-marked in order to avoid a congestion on a link. Each session is monitored to ensure that it does not use more than the allotted bandwidth. If a session uses more than the allotted bandwidth, traffic is dropped (policing), slowed down (shaped), or re-marked (markdown) to conform.

Congestion management or scheduling tools: When traffic exceeds network resources that are available, traffic is queued. Queued traffic will await available resources. Traffic classes that do not handle delay well are better off being dropped unless there is delay-free guaranteed bandwidth for that traffic class.

Link-specific tools: There are certain types of connections such as WAN links, that can be provisioned with special traffic handling tools. One such example is fragmentation.

Trust Boundary

The trust boundary is a point in the network where packet markings are not necessarily trusted. You can create, remove, or rewrite markings at that point. The borders of a trust domain are the network locations where packet markings are accepted and acted upon.



Untrusted domains are usually devices with user access—such as PCs and printers. The trusted part of the network includes devices that only the network administrators have access to, such as routers and switches.

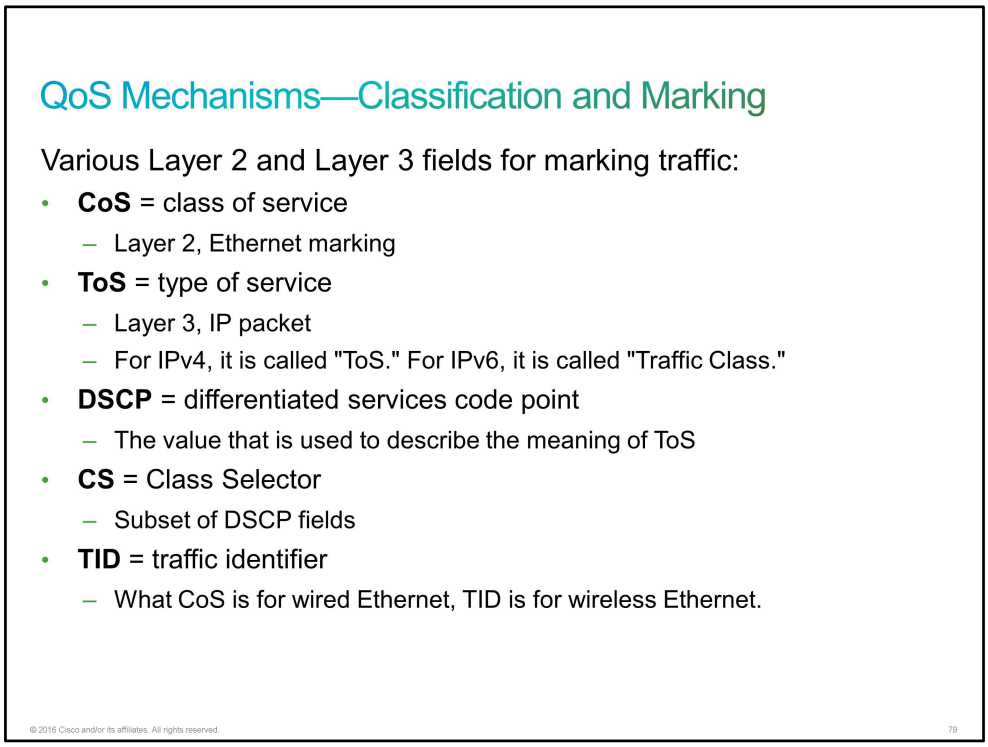
A trust boundary may also be established between an enterprise network and a service provider network.

Trust boundaries are also common in governmental and educational networks between different departments, ministries, institutes, schools, or organizations. In an enterprise campus network, the trust boundary is almost always at the edge switch.

QoS markings in traffic coming from an untrusted domain are usually ignored. Traffic at the trust boundary is classified and marked, before being forwarded to the trusted domain. Ignoring markings that come from untrusted networks prevents end-user-controlled markings from taking unfair or disastrous advantage of the network QoS treatments.

QoS Mechanisms—Classification and Marking

A classifier is a tool that inspects packets within a field to identify the type of traffic that the packet is carrying. Traffic is then directed to a policy-enforcement mechanism for that type of traffic. Policy enforcement mechanisms include marking, queuing, policing, shaping, or any combination of those mechanisms. A marker is a tool that writes a value in the header of the packet, frame, cell, tag, or label. The aim of marking is to preserve the classification decision that the classifier tool reached. Devices that follow the device where marking was performed do not have to do classification and analysis (which are resource-consuming tasks) to determine how to treat the packet.



CoS, ToS, DSCP, Class Selector, and TID are different terms to describe designated fields in a frame or packet header. How devices treat packets in your network depends on the field values.

- **CoS** is usually used with Ethernet frames and contains 3 bits.
- **ToS** is generally used to indicate the Layer 3 IPv4 packet field and comprises 8 bits, 3 of which are designated as the IP precedence field. IPv6 changes the terminology for the same field in the packet header to "Traffic Class."
- **DSCP** is a set of 6-bit values that are used to describe the meaning of the Layer 3 IPv4 ToS field. While IP precedence is the old way to mark ToS, DSCP is the new way. Transition from IP precedence to DSCP was made because IP precedence only offers 3 bits, or eight different values, to describe different classes of traffic. DSCP is backwards-compatible with IP precedence.
- **Class Selector** is a term that is used to indicate a 3-bit subset of DSCP values. Class Selector designates the same 3 bits of the field as IP precedence.
- **TID** is a term that is used to describe a 3-bit field in the QoS control field of wireless frames (802.11 MAC frame). Values correspond approximately, but not exactly, to Ethernet CoS values and meanings. TID is used for wireless Ethernet connections, CoS is used for wired Ethernet connections.

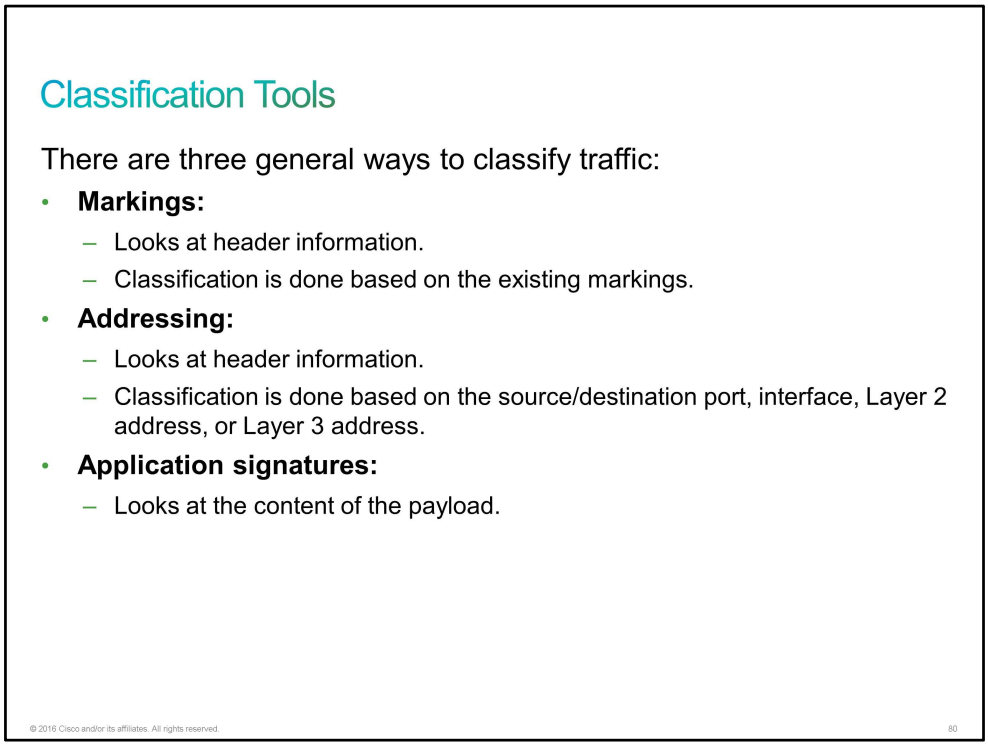
Ultimately, there are various Layer 2 and Layer 3 mechanisms that are used in the network for marking traffic. In addition to the mentioned marking fields, there are also numerous other technologies that allow marking. Such examples are GRE, MPLS, and IPsec.

Layer 3 packet marking with IP precedence and DSCP is the most widely deployed marking option because Layer 3 packet markings have end-to-end significance. Layer 3 markings can also be easily translated to and from Layer 2 markings.

Classification Tools

Classification of traffic determines which type of traffic the packets or frames belong to. Only after you identify the traffic can you apply policies to it (marking, shaping, policing, and so on).

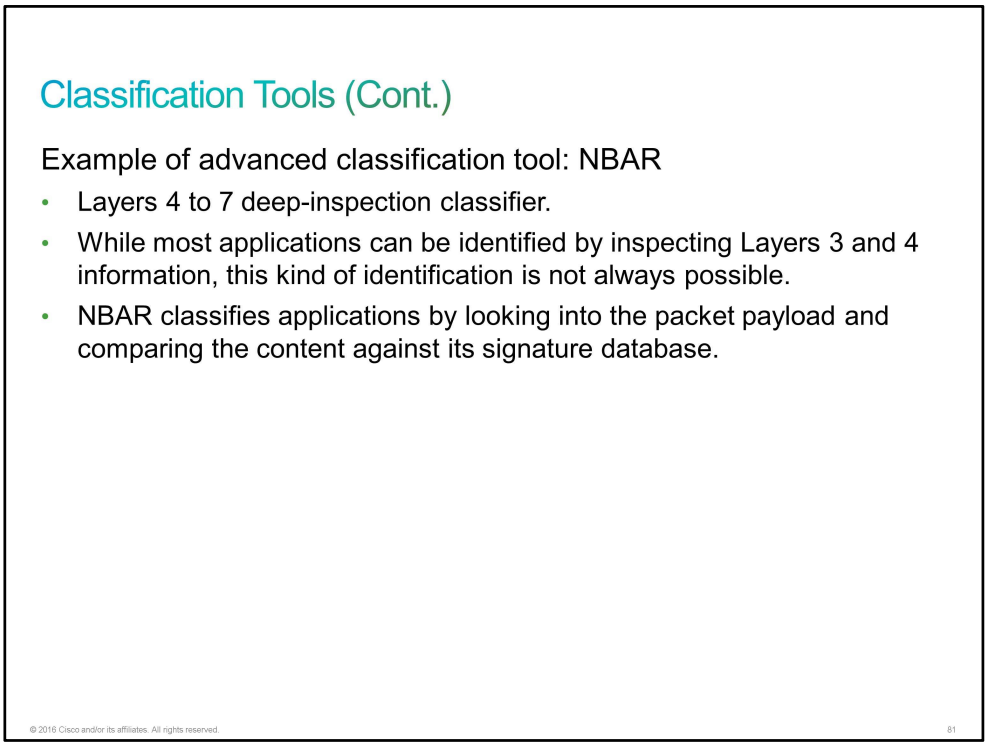
The best practice when it comes to classification is to identify and mark traffic as close to the trust boundary as possible. One example is within trusted devices such as IP phones. If marking is applied correctly, all devices that follow do not need to repeat the same in-depth classification. These devices can apply policies, such as scheduling, that is based on marking made previously.



Three most common ways to classify traffic are:

- **Markings:** Classification is done on existing Layer 2 or Layer 3 settings.
- **Addressing:** Classification is done based on source/destination interface, or Layer 2 destination address, or Layer 3 source/destination address, or source/destination Layer 4 port. Using an IP address classifies traffic by a group of devices. Using a port number classifies traffic by traffic type.
- **Application signatures:** Classification is done based on application content inside the packet payload. This classification is also called deep packet inspection.

Note	Different devices have QoS mechanisms implemented in different ways. MQC is a platform-independent and flexible configuration interface to simplify configuration of QoS features on Cisco IOS-based platforms. MQC abstracts the QoS behavioral model to the extent that the network administrator does not have to know the details of the platforms where the syntax is executed.



NBAR is a Layer 4 to Layer 7 deep-packet inspection classifier. NBAR is more CPU-intensive than marking that is done by the existing markings, addresses, or ACLs.

Mostly, data applications can be identified using Layer 3 or Layer 4 criteria (like IP addresses and well-known TCP/UDP port numbers). However, classifiers cannot identify all applications by these criteria alone. For example, some peer-to-peer applications negotiate ports dynamically.

NBAR recognizes packets by examining the data payload and identifying the application layer protocols by matching them against a PDLM. PDLM is an application signature database.

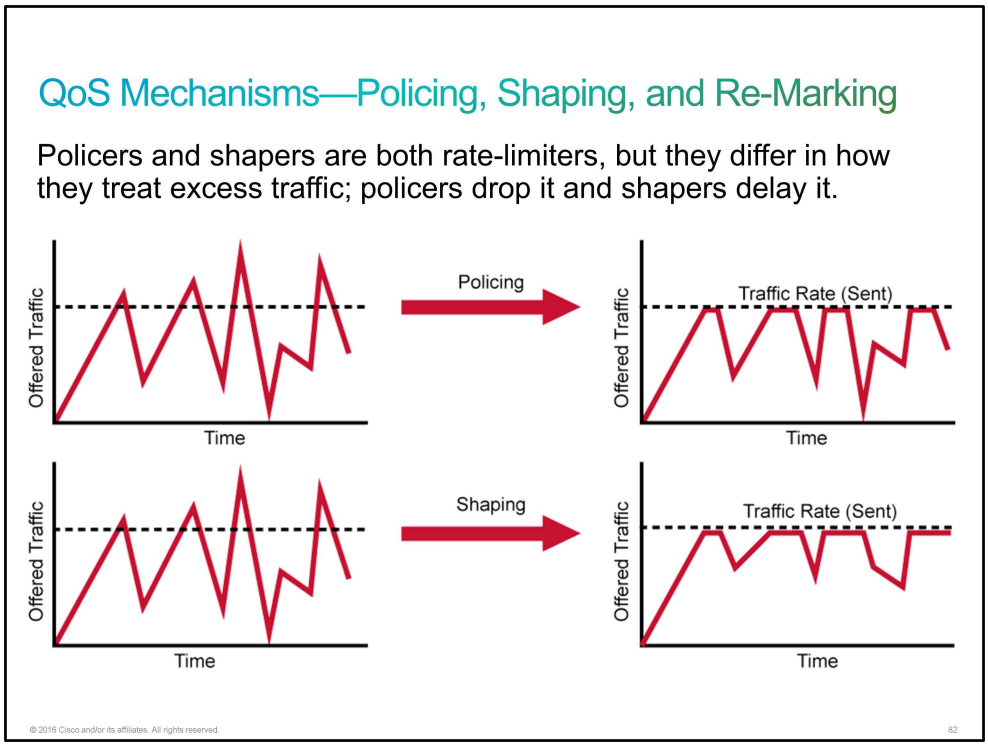
NBAR has two different modes of operation:

- **Passive mode:** Provides real-time statistics on applications per protocol or per interface and gives bidirectional statistics such as bit rate, packet, and byte counts.
- **Active mode:** Classifies applications for traffic marking, so that QoS policies can be applied.

Note	NBAR2 is the most recent version of the NBAR tool and is also commonly referred to as the Next Generation NBAR. NBAR2 can classify very large set protocols, including non-TCP and non-UDP protocols, protocols using statically or dynamically assigned TCP and UDP port numbers, protocols using dynamically assigned TCP, and UDP port numbers. NBAR2 is backwards-compatible with NBAR. NBAR2 is not available on all Cisco platforms.

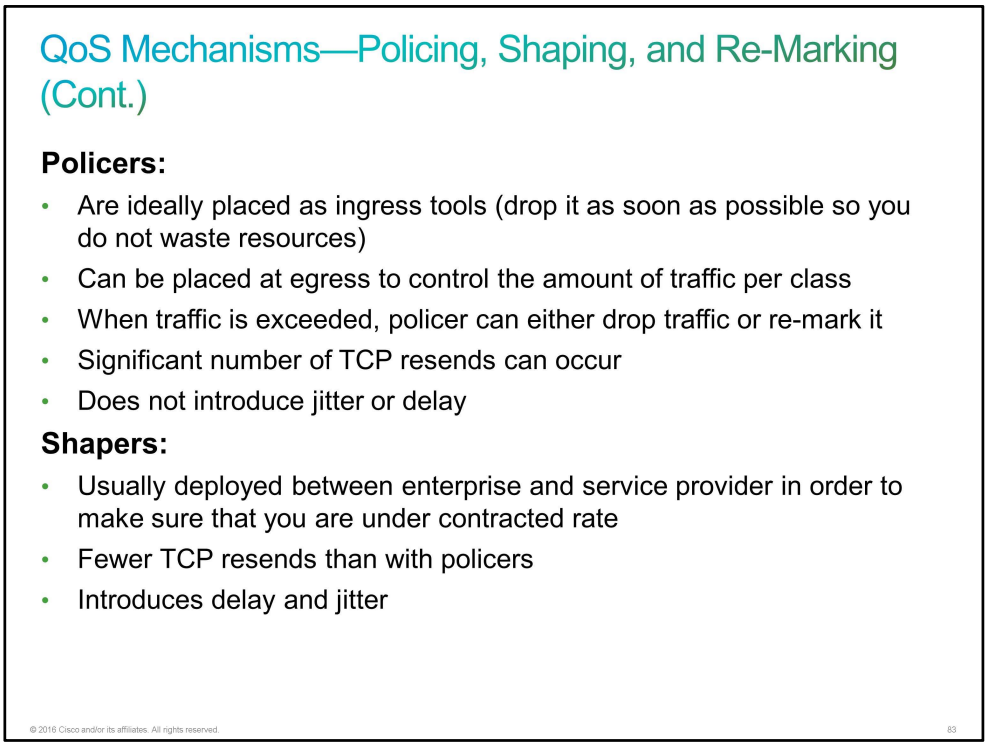
QoS Mechanisms—Policing, Shaping, and Re-Marking

After you have identified and marked traffic, you can treat it by a set of actions. These actions include bandwidth assignment, policing, shaping, queuing, and dropping decisions.



Policers and shapers are tools that identify and respond to traffic violations. They usually identify traffic violations in a similar manner, but they differ in their response:

- **Policers** perform checks for traffic violations against a configured rate. The action that they take in response is either dropping or re-marking the excess traffic. Policers do not delay traffic; they only check traffic and take action if needed.
- **Shapers** are traffic-smoothing tools that work in cooperation with buffering mechanisms. Shaper does not drop traffic, but it smooths it out so it never exceeds the configured rate. Shapers are usually used to meet SLAs. Whenever the traffic spikes above the contracted rate, the excess traffic is buffered and thus delayed until the offered traffic goes below the contracted rate.



Policers make instantaneous decisions and are thus optimally deployed as ingress tools. The logic is that if you are going to drop the packet, you might as well drop it before spending valuable bandwidth and CPU-cycles on it. However, policers can also be deployed at egress in order to control the bandwidth that a particular class of traffic uses. Such decisions sometimes cannot be made until the packet reaches the egress interface.

When traffic exceeds the allocated rate, the policer can take one of two actions. It can either drop traffic or re-mark it to another class of service. The new class usually has a higher drop probability.

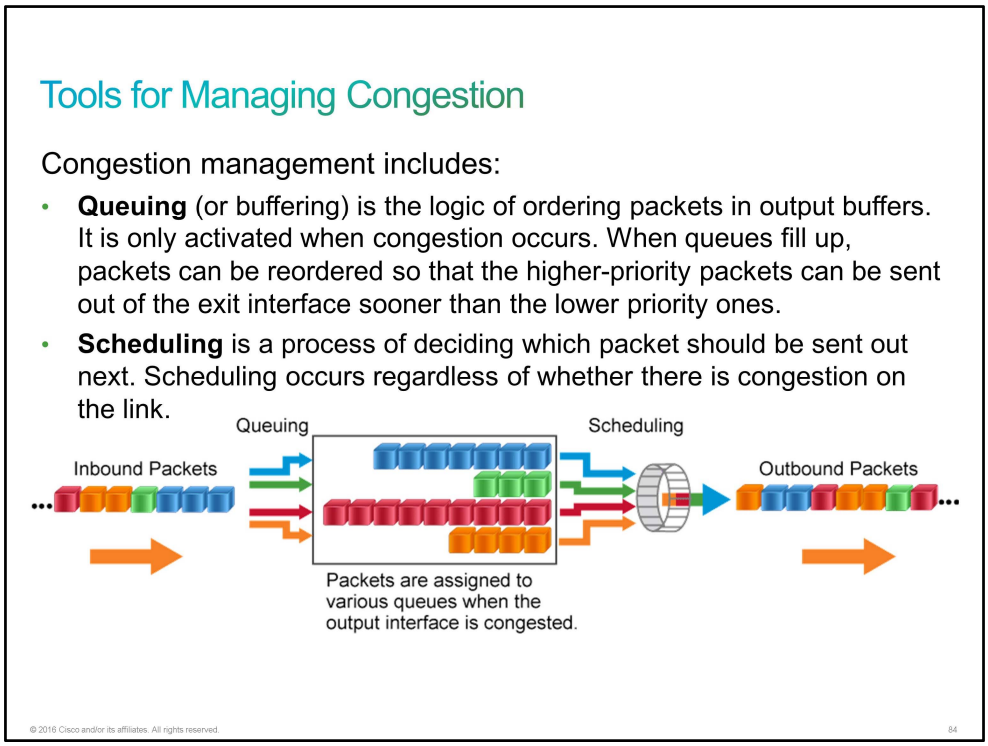
Shapers are commonly deployed on enterprise-to-service provider links on the enterprise egress side. Shapers ensure that traffic going to the service provider does not exceed the contracted rate. If the traffic exceeds the contracted rate, it would get policed by the service provider and likely dropped.

While policers can cause a significant number of TCP resends, when traffic is dropped, shaping involves fewer TCP resends. Policing does not cause delay or jitter in a traffic stream, but shaping does.

Note	Regulating real-time traffic such as voice and video with policing and shaping is generally counterproductive. You should use CAC strategies to prevent real-time traffic from exceeding the capacity of the network. Policing and shaping tools are best employed to regulate TCP-based data traffic.

Tools for Managing Congestion

Whenever a packet enters a device faster than it can exit, the potential for congestion occurs. If there is no congestion, packets are sent as soon as they arrive. If congestion occurs, congestion management tools are activated. Queuing is temporary storage of backed-up packets. You perform queuing in order to avoid dropping packets.



Different scheduling mechanisms exist. The following are three basic examples:

- **Strict priority:** The queues with lower priority are only served when the higher-priority queues are empty. There is a risk with this kind of scheduler that the lower-priority traffic will never be processed. This situation is commonly referred to as traffic starvation.
- **Round-robin:** Packets in queues are served in a set sequence. There is no starvation with this scheduler, but delays can badly affect the real-time traffic.
- **Weighted fair:** Queues are weighted, so that some are served more frequently than others. This method thus solves starvation and also gives priority to real-time traffic. One drawback is that this method does not provide bandwidth guarantees. The resulting bandwidth per flow instantaneously varies based on the number of flows present and the weights of each of the other flows.

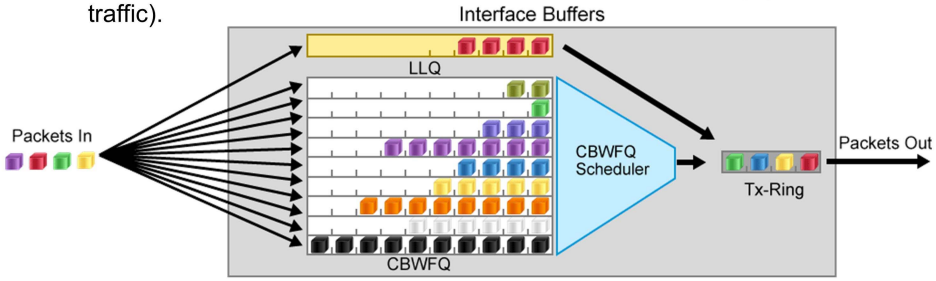
The scheduling tools that you use for QoS deployments therefore offer a combination of these algorithms and various ways to mitigate their downsides. This combination allows you to best tune your network for the actual traffic flows present.

Queuing can happen at different levels. Most complex queuing can be done at Layer 3. There is also queuing at Layer 2, for certain interface types. When Layer 2 queues fill up, they, in turn, push back packets into the Layer 3 queues. A final queue, also called the transmit ring, or Tx-ring, is a Layer 1 queue. When the Tx-ring fills up, the higher-level queues are pressed into service and this situation is essentially when QoS becomes active on the device.

Tools for Managing Congestion (Cont.)

There are many queuing mechanisms. Two modern examples from Cisco are as follows:

- **Class-based weighted fair queuing:**
  - Traffic classes get fair bandwidth guarantees.
  - No latency guarantees—only suitable for data networks.
- **Low-latency queuing:**
  - Takes the previous model and adds a queue with strict priority (for real-time traffic).



There are many different queuing mechanisms. Older methods are insufficient for modern rich-media networks. However, you need to understand these older methods in order to comprehend the newer methods:

- FIFO: A single queue with packets that are sent in the exact order that they arrived.
- PQ**:** A set of four queues that are served in strict-priority order. By enforcing strict priority, the lower-priority queues are served only when the higher-priority queues are empty. This method can starve traffic in the lower priority queues.
- CQ**:** A set of 16 queues with a round-robin scheduler. In order to prevent traffic starvation, it provides traffic guarantees. The drawback of this method is that it does not provide strict priority for real-time traffic.
- WFQ**:** An algorithm that divides the interface bandwidth by the number of flows, thus ensuring proper distribution of the bandwidth for all applications. This method provides a good service for the real-time traffic, but there are no guarantees for a particular flow.

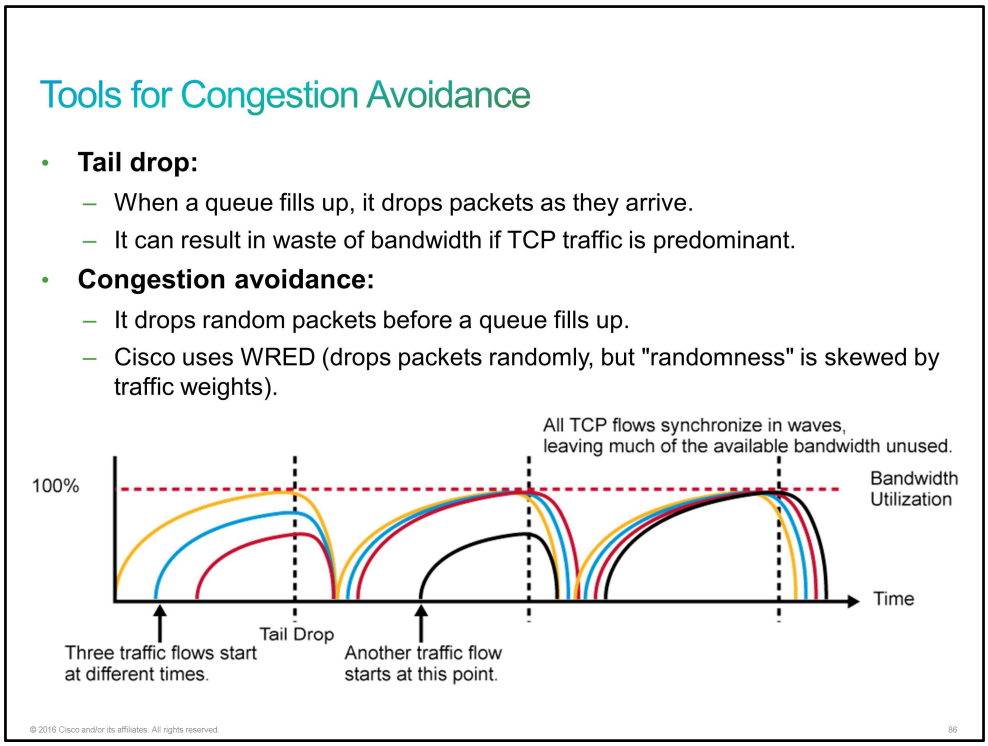
Two examples of newer queuing mechanisms that are recommended for rich-media networks:

- **CBWFQ:** A combination of bandwidth guarantee with dynamic fairness of other flows. It does not provide latency guarantee and is only suitable for data traffic management.
- **LLQ:** This method is essentially CBWFQ with strict priority. This method is suitable for mixes of data and real-time traffic. LLQ provides both latency and bandwidth guarantees.

Note	In the figure, you can see the LLQ queuing mechanism, which is suitable for networks with real-time traffic. If you remove the low-latency queue (at the top, in yellow), what you are left with is CBWFQ, which is only suitable for data-traffic networks.

Tools for Congestion Avoidance

Queues are finite on any interface. Devices can either wait for queues to fill up and then start dropping packets, or drop packets before the queues fill up. Dropping packets as they arrive is called *tail drop*. Selective dropping of packets during the time queues are filling up is called *congestion avoidance*. Queuing algorithms manage the front of the queue and congestion mechanisms manage the back of the queue.



Note	TCP has built-in flow-control mechanisms that operate by increasing the transmission rates of traffic flows until packet loss occurs. When packet loss occurs, TCP drastically slows down the transmission rate and then again begins to increase the transmission rate. Because of TCP behavior, tail drop of traffic can result in suboptimal bandwidth utilization. TCP global synchronization is a phenomena that can happen to TCP flows during periods of congestion because each sender will reduce their transmission rate at the same time when packet loss occurs.

Randomly dropping packets instead of dropping them all at once, as it is done in a tail drop, avoids global synchronization of TCP streams. One such mechanism that randomly drops packets is random early detection or RED. RED monitors the buffer depth and performs early discards (drops) on random packets when the minimum defined queue threshold is exceeded.

Cisco IOS Software does not support pure RED, but WRED. The principle is the same as with RED, except that the traffic weights skew the randomness of packet drop. In other words, traffic that is more important will be less likely dropped than less important traffic.

Challenge

1. Which three features are properties and one-way requirements for voice traffic? (Choose three.)

   A. Voice traffic is bursty.
   B. Voice traffic is smooth.
   C. Latency should be below 400 ms.
   D. Latency should be below 150 ms.
   E. The required bandwidth is roughly between 30 and 128 kbps.
   F. The required bandwidth is roughly between 0.5 and 20 Mbps.

2. Which statement about QoS trust boundaries or domains is true?

   A. The trust boundary is always a router.
   B. PCs, printers, and tablets are usually part of a trusted domain.
   C. The service provider and the enterprise network need to be one single trust domain; otherwise, routing will not work.
   D. The IP phone is a common trust boundary.

3. Which advanced classification tool can be used to classify data applications?

   A. NBAR
   B. PDLM
   C. ToS
   D. DSCP

4. How many bits constitute the DSCP field of the IP header?

   A. 3 bits
   B. 4 bits
   C. 6 bits
   D. 8 bits

5. Which option is a Layer 2 QoS marking?

   A. CoS
   B. DSCP
   C. EXP
   D. QoS group

6. Which QoS mechanism will drop traffic if a session uses more than the allotted bandwidth?

   A. marking
   B. policing
   C. shaping
   D. congestion management

7. Which option is a congestion-avoidance mechanism?

   A. LFI
   B. QPM
   C. MRF
   D. WRED

Answer Key

Challenge

1. B, D, E
2. D
3. A
4. C
5. A
6. B
7. D

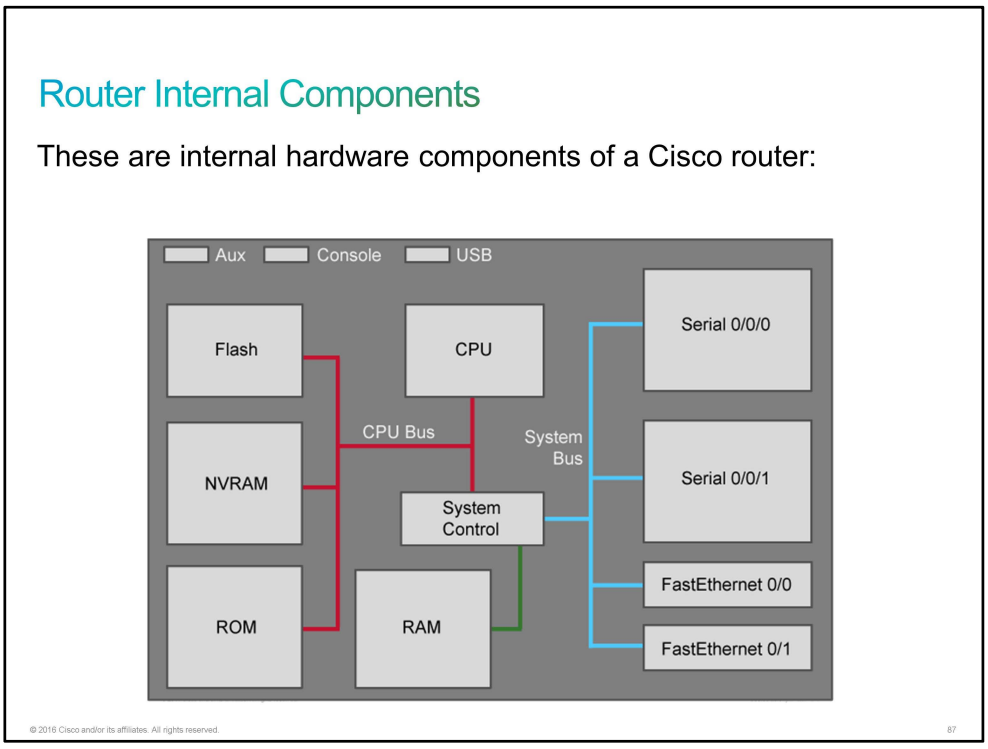
Lesson 4: Managing Cisco Devices

Introduction

This lesson describes the internal components of Cisco devices, including the CPU, interfaces, RAM, ROM, flash memory, and NVRAM, and how to manage them.

Router Internal Components

The major internal components of a Cisco router include the CPU, interfaces, RAM, ROM, flash memory, and NVRAM.



A router is a computer, similar to a PC. Routers have several hardware and software components that you can find in other computers, including the following:

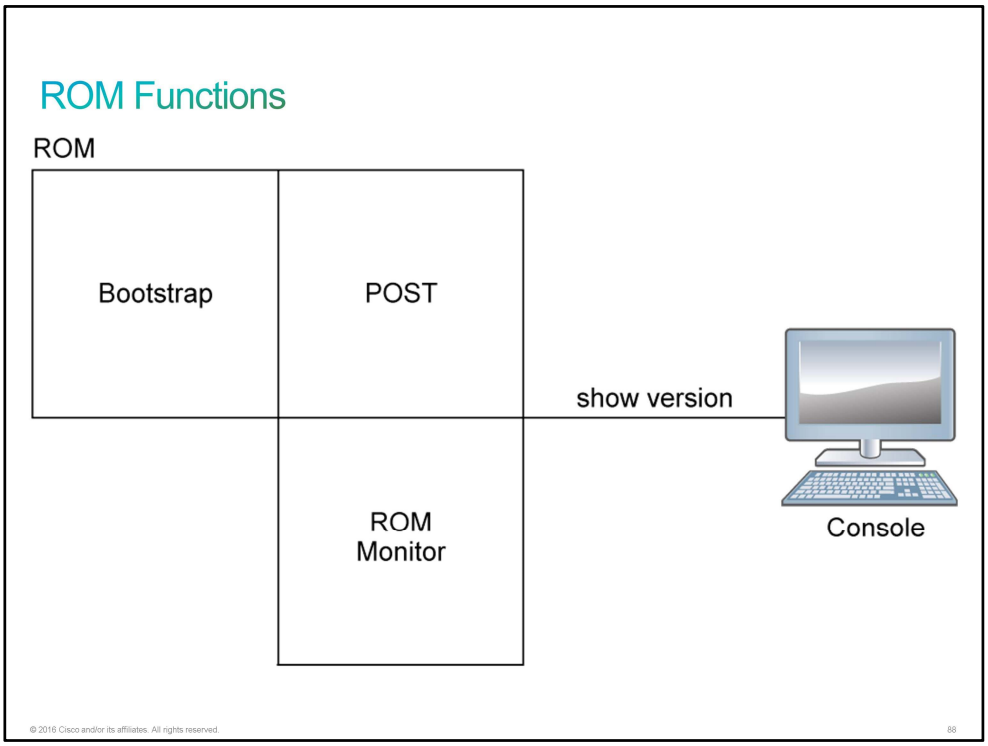
- **CPU:** The CPU executes operating system instructions such as system initialization, routing functions, and switching functions.
- **RAM:** RAM stores the instructions and data that the CPU needs to execute. This read/write memory contains the software and data structures that allow the router to function. RAM is volatile memory and loses its content when the router is powered down or restarted. However, the router also contains permanent storage areas such as ROM, Flash, and NVRAM. RAM is used to store the following components:
  - **Operating system:** Cisco IOS Software is copied into RAM during the boot process.
  - **Running configuration file:** This file stores the configuration commands that Cisco IOS Software is currently using on the router. With few exceptions, all commands that are configured on the router are stored in the running configuration file, which is also known as "running-config."
  - **IP routing table:** This file stores information about directly connected and remote networks. It is used to determine the best path to forward the packet.
  - **ARP cache:** ARP cache contains the IPv4 address to MAC address mappings, such as the ARP cache on a PC. The ARP cache is used on routers that have LAN interfaces such as Ethernet interfaces.
  - **Packet buffer:** Packets are temporarily stored in a buffer when they are received on an interface or before they exit an interface.

- **ROM:** ROM is a form of permanent storage. This type of memory contains microcode for basic functions to start and maintain the router. ROM contains the ROM monitor, which is used for router disaster recovery functions such as password recovery. ROM is nonvolatile, so it maintains the memory contents even when the power is turned off.
- **Flash memory:** Flash memory is nonvolatile computer memory that can be electrically stored and erased. Flash is used as permanent storage for the operating system. In most models of Cisco routers, Cisco IOS Software is permanently stored in the flash memory and copied into RAM during the boot process, where the CPU then executes it. Some older models of Cisco routers run Cisco IOS Software directly from flash. Flash consists of SIMMs or PCMCIA cards that can be upgraded to increase the amount of flash memory. The flash memory does not lose its contents when the router loses power or is restarted.
- **NVRAM:** NVRAM does not lose its information when the power is turned off. Cisco IOS Software uses NVRAM as permanent storage for the startup configuration file, which is also known as "startup-config." All configuration changes are stored in the running configuration file in RAM, and with few exceptions, Cisco IOS Software implements them immediately. To save these changes in case the router is restarted or loses power, the running configuration must be copied to NVRAM, where it is stored as the startup configuration file.
- **Configuration register:** The configuration register is used to control how the router boots. The configuration register value is stored in NVRAM.
- **Interfaces:** Interfaces are the physical connections to the external world for the router and include the following types, among others:
  - Ethernet, Fast Ethernet, and Gigabit Ethernet.
  - Asynchronous and synchronous serial.
  - USB interface, which can be used to add a USB flash drive to a router
  - Console and auxiliary ports. A console can have an RJ-45 or mini-USB connector.

Although there are several different types and models of routers, every router has the same general hardware components. Depending on the model, these components are located in different places inside the router.

ROM Functions

The ROM in a Cisco router contains microcode for basic router functions.



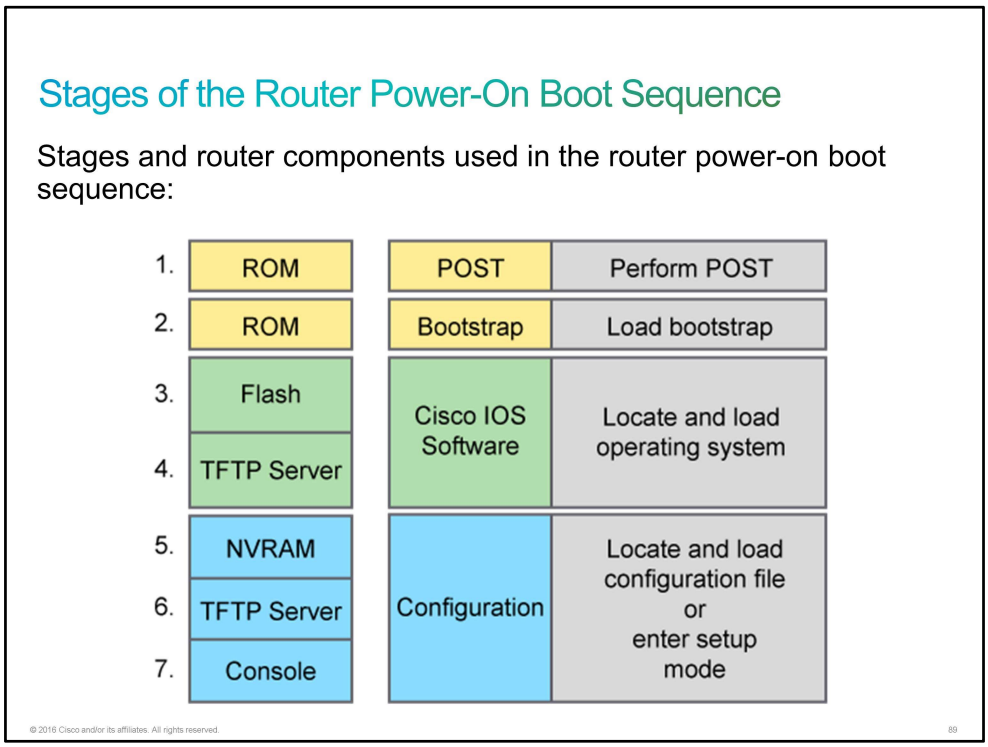
The figure shows three areas of the microcode that is generally contained in ROM:

- **Bootstrap code:** The bootstrap code is used to bring up the router during initialization. It reads the configuration register to determine how to boot and then, if instructed to do so, loads the Cisco IOS Software.
- **POST:** POST is the microcode that is used to test the basic functionality of the router hardware and determine which components are present.
- **ROM monitor:** The ROM monitor area includes a low-level operating system that is normally used for manufacturing, testing, troubleshooting, and password recovery. In ROM monitor mode, the router has no routing or IP capabilities.

Note	Depending on the specific Cisco router platform, the components that are listed may be stored in the flash memory or in the bootstrap memory to enable field upgrade to later versions.

Stages of the Router Power-On Boot Sequence

When a router boots, it performs a series of steps that include loading the Cisco IOS Software and the router configuration.



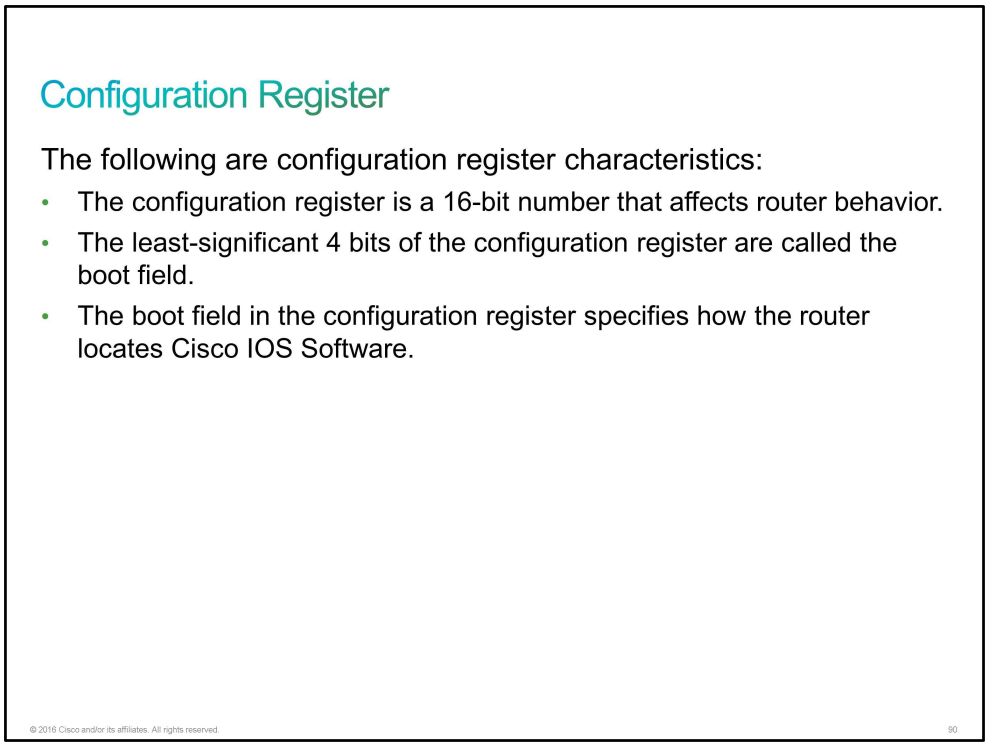
The sequence of events that occurs during the power-up (boot) of a router is explained in detail here. Understanding these events will help you accomplish operational tasks and troubleshoot router problems.

1. **Perform POST:** This event is a series of hardware tests that verifies if all components of a Cisco router are functional. During this test, the router also determines which hardware is present. POST executes from microcode that is resident in the system ROM.
2. **Load and run bootstrap code:** Bootstrap code is used to perform subsequent events such as locating the Cisco IOS Software, loading it into RAM, and running it. After the Cisco IOS Software is loaded and running, the bootstrap code is not used until the next time the router is reloaded or power-cycled.
3. **Find the Cisco IOS Software:** The bootstrap code determines the location of the Cisco IOS Software that will be run. Normally, the Cisco IOS Software image is located in the flash memory, but it can also be stored in other places such as a TFTP server. The configuration register and configuration file determine where the Cisco IOS Software images are located and which image file to use. If a complete Cisco IOS image cannot be located, a scaled-down version of the Cisco IOS Software is copied from ROM into RAM. This version of the Cisco IOS Software is used to help diagnose any problems and can be used to load a complete version of the Cisco IOS Software into RAM.
4. **Load the Cisco IOS Software:** After the bootstrap code has found the correct image, it loads this image into RAM and starts the Cisco IOS Software. Some older routers do not load the Cisco IOS Software image into RAM but execute it directly from flash memory instead.
5. **Find the configuration:** After the Cisco IOS Software is loaded, the bootstrap program searches for the startup configuration file in NVRAM.

6. **Load the configuration:** If a startup configuration file is found in NVRAM, the Cisco IOS Software loads it into RAM as the running configuration and executes the commands in the file, one line at a time. The running configuration file contains interface addresses, starts routing processes, configures router passwords, and defines other characteristics of the router. If no configuration exists, the router enters the setup utility or attempts an autoinstall to look for a configuration file from a TFTP server.
7. **Run the configured Cisco IOS Software:** When the prompt is displayed, the router is running the Cisco IOS Software with the current running configuration file. You can then begin using Cisco IOS commands on the router.

Configuration Register

The configuration register is a 16-bit number that resides in the NVRAM of a router.



Each bit has value 1 (on or set) or value 0 (off or clear), and each bit setting affects the router behavior upon the next reload power cycle.

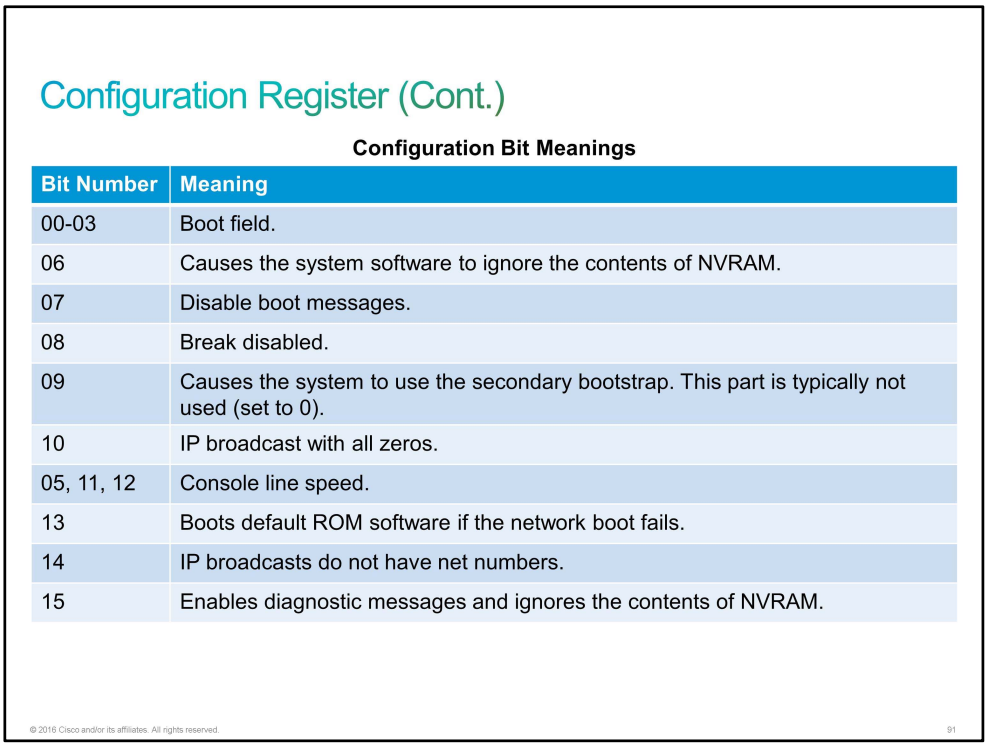
You can use the 16-bit configuration register to do the following:

- Force the router to boot into the ROM monitor.
- Select a boot source and default boot filename.
- Control broadcast addresses.
- Recover a lost password.
- Change the console line speed.

The lowest 4 bits (the rightmost number when displayed in hexadecimal) are called the boot field. The boot field specifies how the router locates Cisco IOS Software.

While the configuration register is a 16-bit number, it is displayed in hexadecimal. For example, when you issue the **show version** command, the value of the configuration register will appear something like 0x2102. The leading 0x simply indicates that the following value is displayed in hexadecimal format. As you know, each hexadecimal digit is 4 bits, which is why a 16-bit value can be displayed as a 4-digit hexadecimal number.

Here you can see the description of configuration register bit meanings, however they may differ between different platforms.

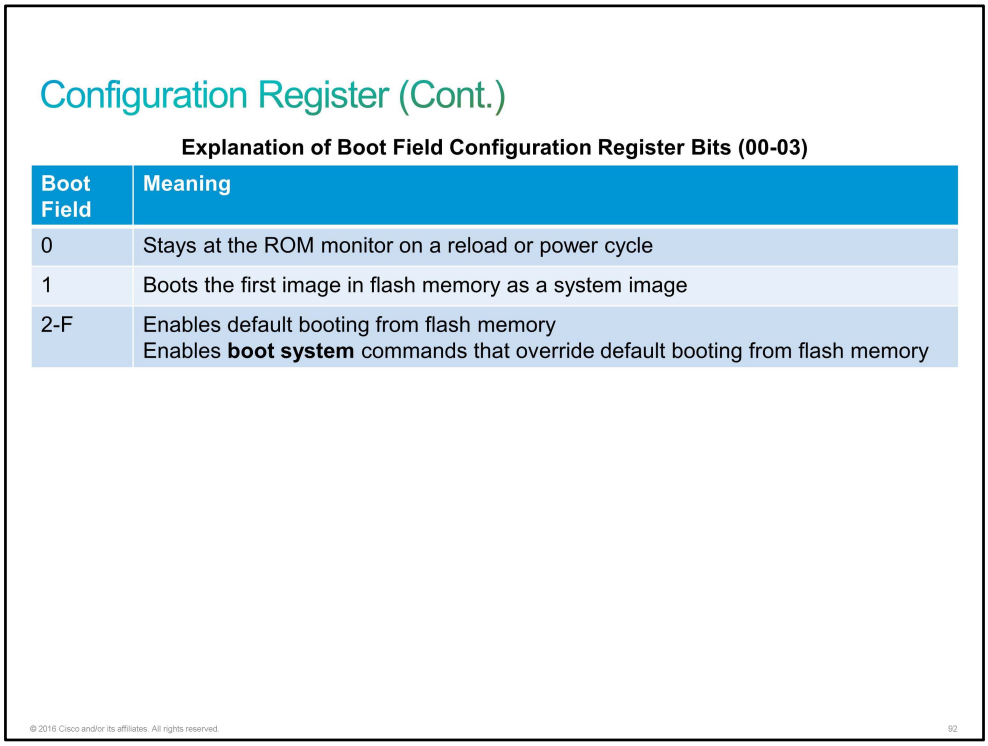


- Bit 8 controls the console Break key. Setting bit 8 (the factory default) causes the processor to ignore the console Break key. Clearing bit 8 causes the processor to interpret Break as a command to force the router into the bootstrap monitor, halting normal operation. Break can always be sent in the first 60 seconds while the router is rebooting, regardless of the configuration settings.
- Bit 9 controls the system boot. Clearing bit 9 (the factory default) causes the system to boot from flash memory. Clearing bit 9 causes the system to use the secondary bootstrap (netbooting), which is typically not used.
- Bit 10 controls the host portion of the IP broadcast address. Setting bit 10 causes the processor to use all zeros; clearing bit 10 (the factory default) causes the processor to use all ones. Bit 10 interacts with bit 14, which controls the network and subnet portions of the broadcast address. Table shows the combined effect of bit 10 and bit 14.

Configuration Register Settings for Broadcast Address Destination

Bit 10	Bit 14	Address (<net> <host>)
Off	Off	<ones> <ones>
On	Off	<zeros> <zeros>
On	On	<net> <zeros>
Off	On	<net> <ones>

- Bit 13 determines the router's response to a bootload failure. Setting bit 13 causes the router to load operating software from ROM after six unsuccessful attempts to load a boot file. Clearing bit 13 causes the router to continue indefinitely to attempt loading a boot file. By factory default, bit 13 is set to 0.



The boot field specifies a number in binary form. If you set the boot field value to 0, you must have console port access to boot the operating system manually. If you set the boot field to a value of 2 to F, and there is a valid **boot system** command that is stored in the configuration file, the router software processes each **boot** command in sequence until the process is successful or the end of the list is reached. If there are no **boot** commands in the configuration file, the router attempts to boot the first file in the flash memory.

Bit 5, bit 11, and bit 12 of the configuration register determine the baud rate of the console terminal. Table shows the bit settings for the eight available rates. The default baud rate is 9600 bps.

Configuration Register (Cont.)

Console Terminal Baud Rate Settings

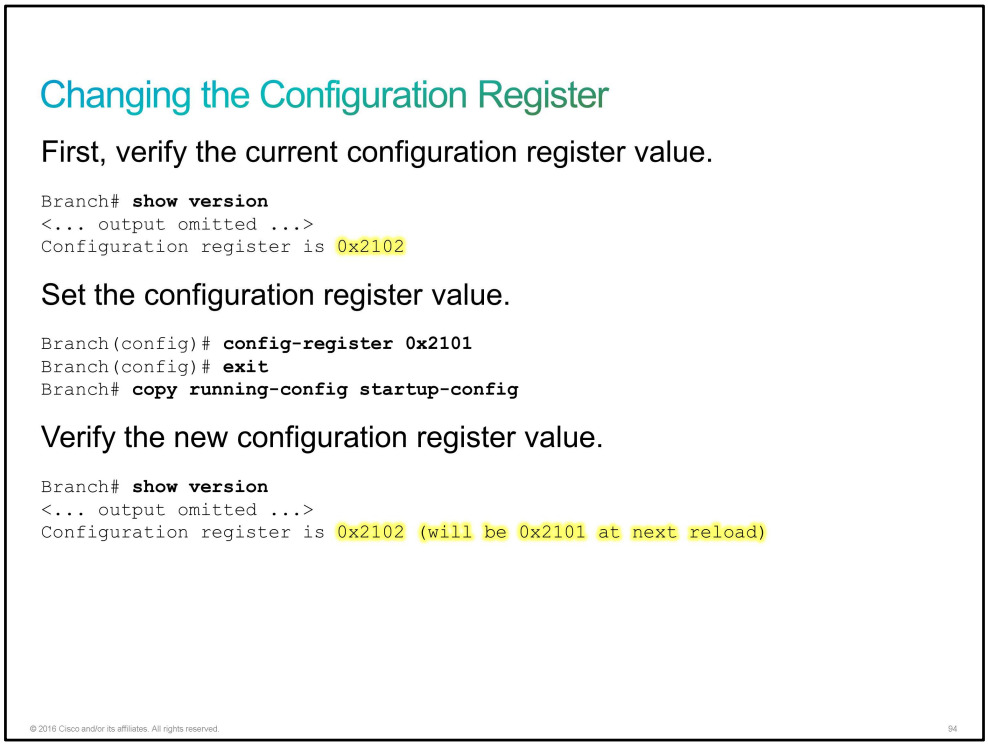
Baud	Bit 5	Bit 12	Bit 11
115200	1	1	1
57600	1	1	0
38400	1	0	1
19200	1	0	0
9600 (Default)	0	0	0
4800	0	0	1
2400	0	1	1
1200	0	1	0

Changing the Configuration Register

Before altering the configuration register, you should use the **show version** command to determine the current configuration register value. The last line of the **show version** command output shows the configuration register value.

Note	Record the configuration register setting, which is typically 0x2102, so you can change it back to the original setting if necessary.

You can use the **config-register** command in the global configuration mode to set the configuration register value. The syntax for this command is **config-register** *value*. The value argument is a hexadecimal number.



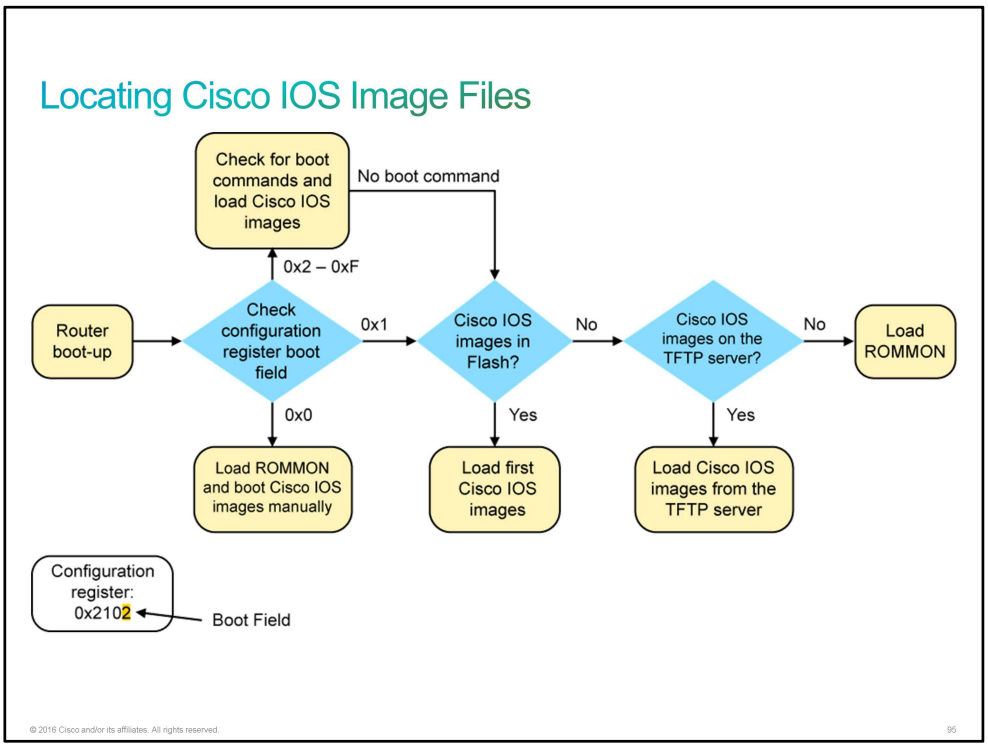
You should be careful when using the **config-register** command because the value argument sets all 16 bits of the configuration register. Only the lowest 4 bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. For example, the default value of 0x2102 not only instructs the router to boot the system image from flash memory but also instructs the router to load the startup configuration with a console speed of 9600 baud (for most platforms), ignore the console Break key, and boot into ROM if the initial boot fails. If you modify the configuration register value, the change takes effect when the router reloads.

In the example, the configuration register value is changed from the default setting to 0x2101, and the configuration is saved to NVRAM. The new configuration register value will cause the router to load the bootstrap code.

If you issue the **show version** command again after changing the configuration register value, the command output shows both the currently configured value of the configuration register and the value that will be used at the next reload.

Locating Cisco IOS Image Files

When a Cisco router boots, it searches for the Cisco IOS image in a specific sequence. It searches for the location that is specified in the configuration register, flash memory, a TFTP server, and ROM.



The bootstrap code is responsible for locating the Cisco IOS Software. It searches for the Cisco IOS image in the following sequence:

1. The bootstrap code checks the boot field of the configuration register. The boot field tells the router how to boot up. The boot field can point to flash memory for the Cisco IOS image, the startup configuration file (if one exists) for commands that tell the router how to boot, or a remote TFTP server. Alternatively, the boot field can specify that no Cisco IOS image will be loaded, and the router should start a Cisco ROM monitor.
2. The bootstrap code executes the specifications of the configuration register boot field value as described in the following bullets. In a configuration register value, the "0x" indicates that the digits that follow are in hexadecimal notation. A configuration register value of 0x2102 has a boot field value of 0x2. The right-most digit in the register value is 2 and represents the lowest 4 bits of the register.
   - If the boot field value is 0x0, the router boots to the ROM monitor at the next power cycle or reload.
   - If the boot field value is 0x1, the router searches flash memory for Cisco IOS images.
   - If the boot field value is 0x2 to 0xF, at the next power cycle or reload, the bootstrap code parses the startup configuration file in NVRAM for **boot system** commands that specify the name and location of the Cisco IOS Software image to load. (Examples of **boot system** commands will follow.) If **boot system** commands are found, the router sequentially processes each **boot system** command in the configuration. If there are no **boot system** commands in the configuration, the router searches the flash memory for a Cisco IOS image.
3. If the router searches for and finds valid Cisco IOS images in flash memory, it loads the first valid image and runs it.

4. If it does not find a valid Cisco IOS image in flash memory, the router attempts to boot from a network TFTP server using the boot field value as part of the Cisco IOS image filename.
5. After six unsuccessful attempts at locating a TFTP server, the router loads the ROM monitor.

Note	The procedure for locating the Cisco IOS image depends on the Cisco router platform and default configuration register values. The procedure that is described here applies to the Cisco Integrated Services Routers.

Entering **boot system** commands in sequence in a router configuration can create a fault-tolerant boot plan. The **boot system** command is a global configuration command that allows you to specify the source for the Cisco IOS Software image to load. For example, the following command boots the system boot image file that is named c2900-universalk9-mz.SPA.152-4.M1.bin from the flash memory device:

```
Branch(config)#  boot system flash:c2900-universalk9-mz.SPA.152-4.M1.bin
```

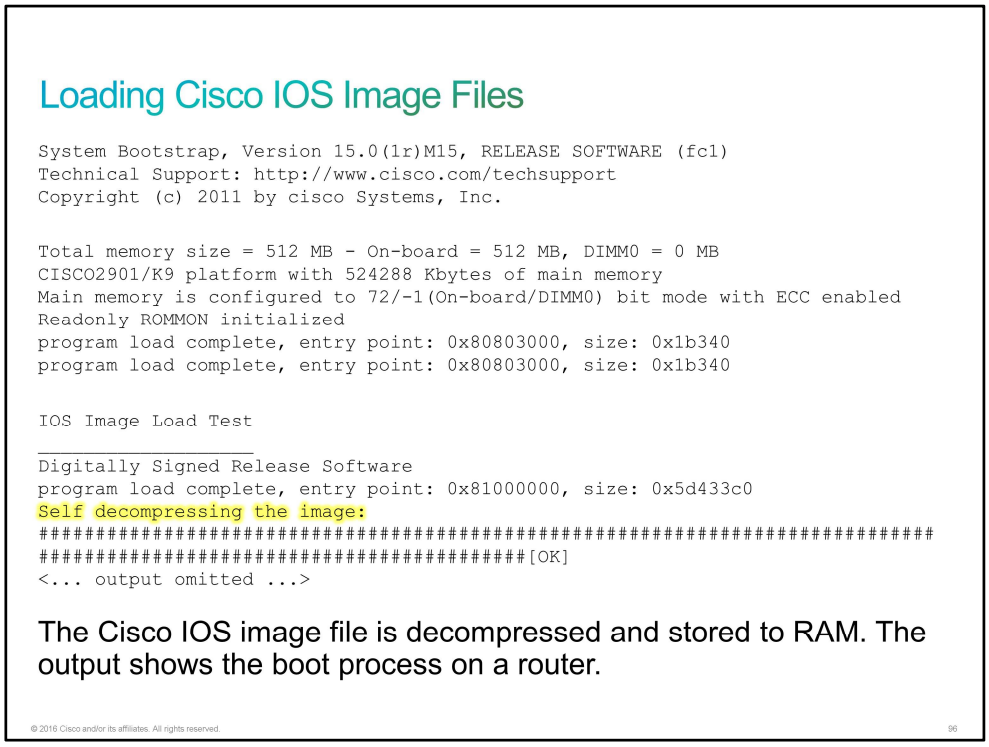
This next example specifies a TFTP server as a source of a Cisco IOS image, with a ROM monitor as the backup:

```
Branch(config)# boot system tftp://c2900-universalk9-mz.SPA.152-4.M1.bin
Branch(config)# boot system rom
```

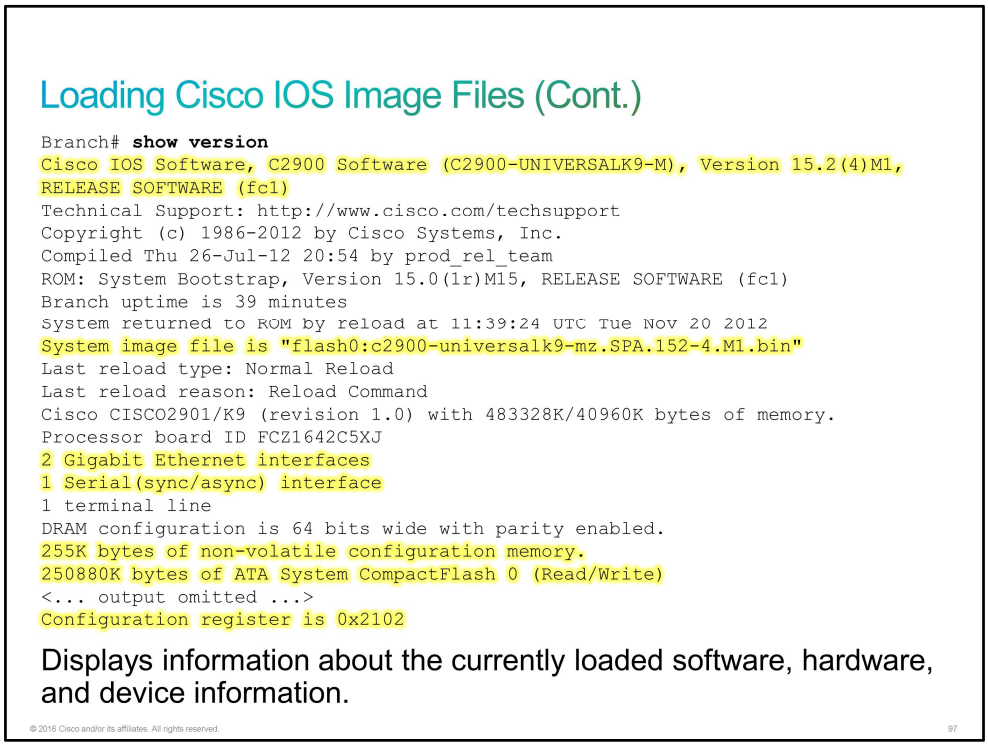
Loading Cisco IOS Image Files

When the router locates a valid Cisco IOS image file in the flash memory, the Cisco IOS image is normally loaded into RAM to run.

When the router locates a valid Cisco IOS image file in the flash memory, the Cisco IOS image is normally loaded into RAM to run. If the image needs to be loaded from the flash memory into RAM, it must first be decompressed. After the file is decompressed into RAM, it is started. When the Cisco IOS Software begins to load, you may see a string of pound signs (#), as shown in the figure, while the image decompresses.



The **show version** command can be used to help verify and troubleshoot some of the basic hardware and software components of the router. The **show version** command displays information about the version of the Cisco IOS Software that is currently running on the router, the version of the bootstrap program, and information about the hardware configuration, including the amount of system memory.



The output from the **show version** command includes the following:

- **Cisco IOS version**

```
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.2(4)M1, RELEASE
SOFTWARE (fc1)
```

This line from the example output shows the version of the Cisco IOS Software in RAM that the router is using.

- **ROM bootstrap program**

```
ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
```

This line from the example output shows the version of the system bootstrap software that is stored in ROM and was initially used to boot up the router.

- **Location of Cisco IOS image**

```
System image file is "flash0:c2900-universalk9-mz.SPA.152-4.M1.bin"
```

This line from the example output shows where the Cisco IOS image is located and loaded as well as its complete filename.

- **Interfaces**

```
2 Gigabit Ethernet interfaces

1 Serial (sync/async) interface
```

This section of the output displays the physical interfaces on the router. In this example, the Cisco 2901 router has two GigabitEthernet interfaces and one serial interface.

- **Amount of NVRAM**

```
255 KB of NVRAM
```

This line from the example output shows the amount of NVRAM on the router.

- **Amount of Flash**

```
250,880 KB of ATA System CompactFlash 0 (Read/Write)
```

This line from the example output shows the amount of flash memory on the router.

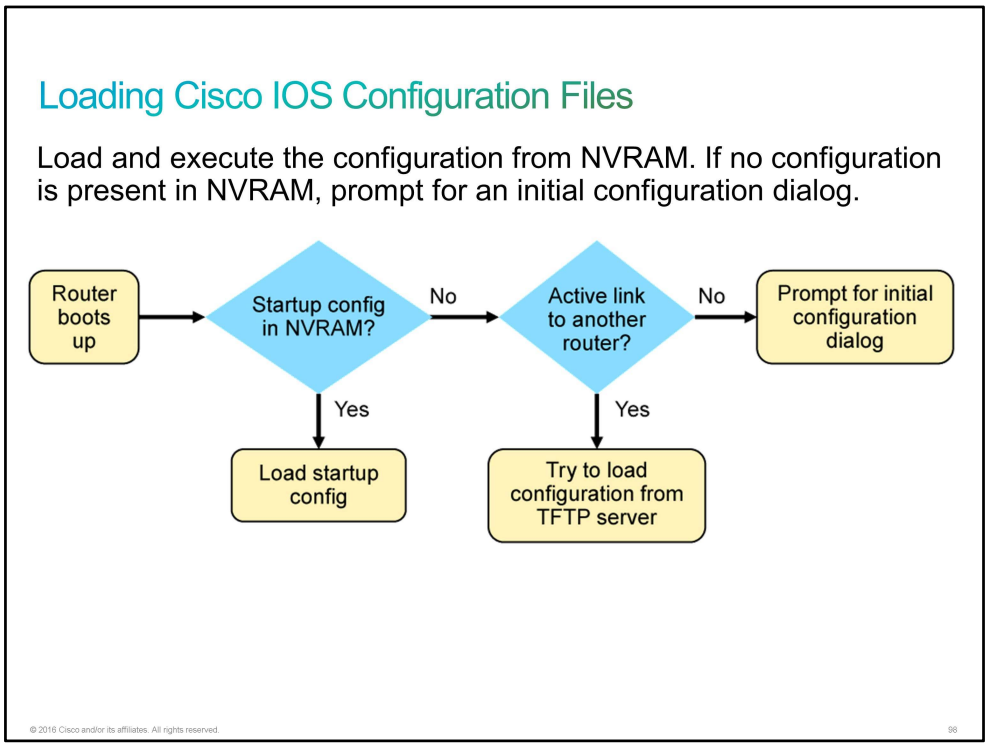
- **Configuration register**

```
Configuration register is 0x2102
```

The last line of the **show version** command displays the current configured value of the software configuration register in hexadecimal format. This value indicates that the router will attempt to load a Cisco IOS Software image from flash memory and load the startup configuration file from NVRAM.

Loading Cisco IOS Configuration Files

After the Cisco IOS Software image is loaded and started, the router must be configured to be useful. If there is an existing saved configuration file (startup-config) in NVRAM, it is executed. If there is no saved configuration file in NVRAM, the router either begins autoinstall or enters the setup utility.



If the startup configuration file does not exist in NVRAM, the router may search for a TFTP server. If the router detects that it has an active link to another configured router, it sends a broadcast searching for a configuration file across the active link. This condition will cause the router to pause, but you will eventually see a console message such as the following:

```
%Error opening tftp://255.255.255.255/network-confg(Timed out)
%Error opening tftp://255.255.255.255/cisconet.cfg (Timed out)
```

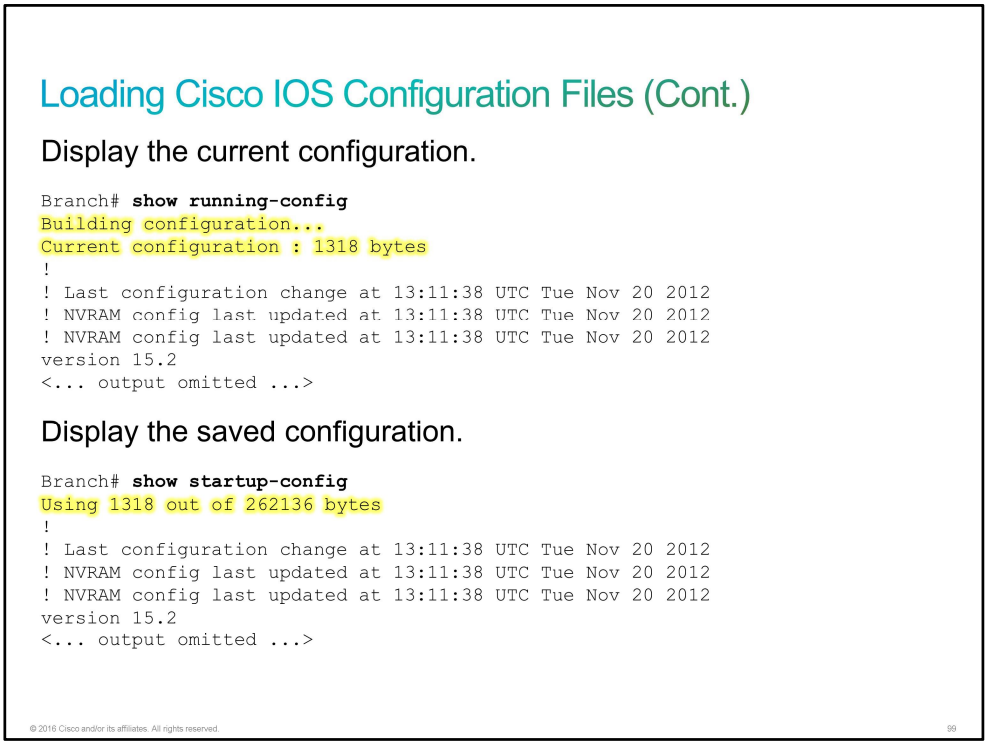
The setup utility prompts the user at the console for specific configuration information to create a basic initial configuration on the router, as shown in this example:

```
<... output omitted ...>
If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO2901/K9 (revision 1.0) with 483328K/40960K bytes of memory.
Processor board ID FCZ1642C5XJ
2 Gigabit Ethernet interfaces
1 Serial(sync/async) interface
1 terminal line
DRAM configuration is 64 bits wide with parity enabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)

         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```



The **show running-config** and **show startup-config** commands are among the most common Cisco IOS Software EXEC commands because they allow you to see the current running configuration in RAM on the router or the startup configuration commands in the startup configuration file in NVRAM that the router will use at the next restart.

If the words "**Current configuration**" are displayed, the active running configuration from RAM is being displayed.

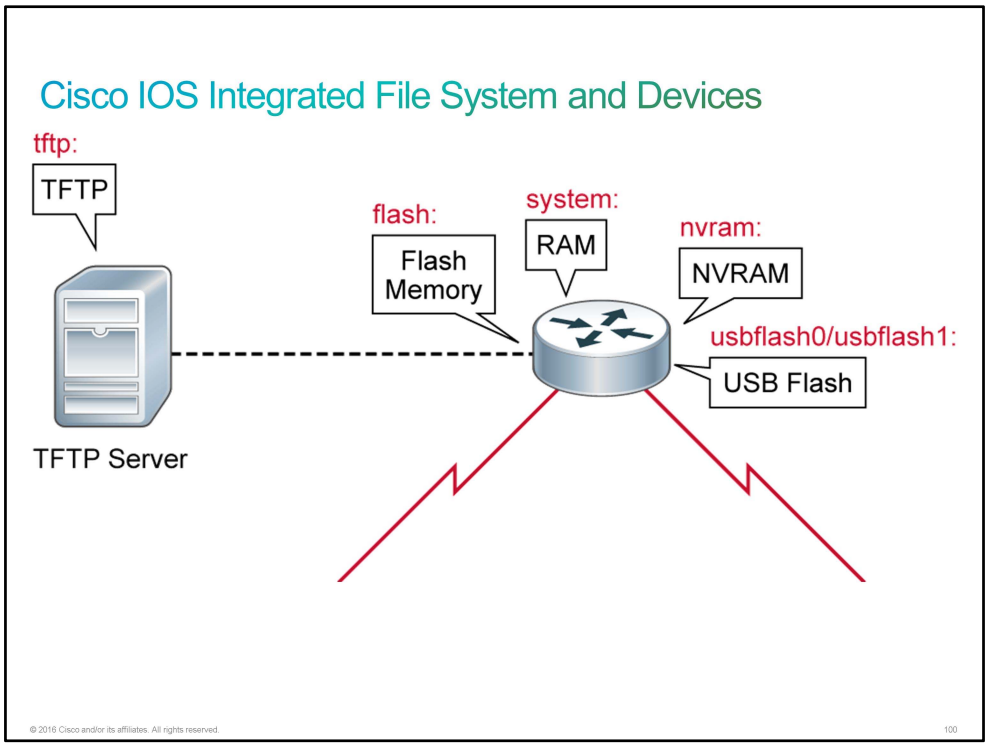
If there is a message at the top indicating how much nonvolatile memory is being used ("Using 1318 out of 262,136 B" in this example), the startup configuration file from NVRAM is being displayed.

Cisco IOS Integrated File System and Devices

The availability of the network can be at risk if the configuration of a router or the operating system is compromised. Attackers who gain access to infrastructure devices can alter or delete configuration files. They can also upload incompatible Cisco IOS images or delete the Cisco IOS image. The changes are invoked automatically or invoked when the device is rebooted. To protect your network from these attacks, you have to be able to save, back up, and restore configurations and Cisco IOS images.

Cisco IOS devices provide a feature that is called the Cisco IOS Integrated File System (Cisco IFS). This system allows you to create, navigate, and manipulate directories on a Cisco device. The directories that are available depend on the platform. The Cisco IFS feature provides a single interface to all the file systems that a Cisco router uses, including the following:

- Flash memory file systems
- Network file systems such as TFTP, rcp, and FTP
- Any other endpoint for reading or writing data (such as NVRAM, the running configuration in RAM, and so on)



The next figure shows the output of the **show file systems** command, which lists all the available file systems on a Cisco 2901 Integrated Services Router. This command provides insightful information such as the amount of available and free memory and the type of file system and its permissions. Permissions include read only (as indicated by the "ro" flag), write only (as indicated by the "wo" flag), and read and write (as indicated by the "rw" flag). The FFS has an asterisk preceding it, which indicates the current default file system. The bootable Cisco IOS Software is located in the flash memory, so the pound symbol (#) that is appended to the Flash listing indicates a bootable disk.

Cisco IOS Integrated File System and Devices (Cont.)

```
Branch# show file systems
File Systems:
       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*    256610304     153710592      disk     rw   flash0: flash:#
             -             -      disk     rw   flash1:
        262136        255626     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -    opaque     rw   xmodem:
             -             -    opaque     rw   ymodem:
             -             -   network     rw   rcp:
             -             -   network     rw   http:
             -             -   network     rw   ftp:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
```

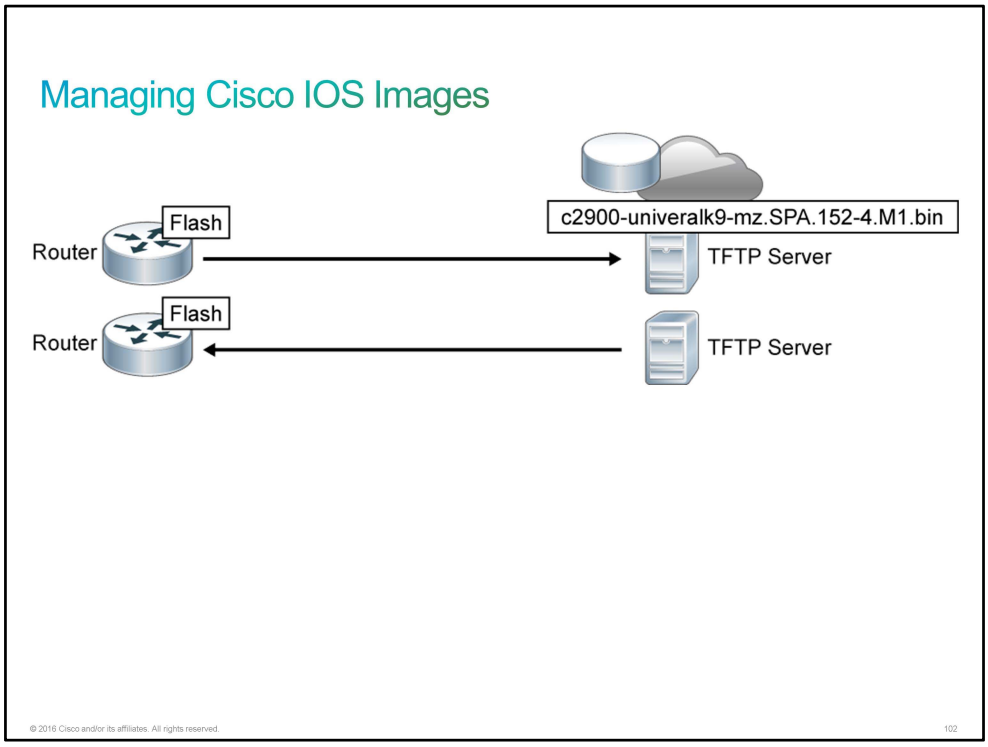

An important feature of the Cisco IFS is the use of the URL convention to specify files on network devices and the network. The URL prefix specifies the file system. The table contains some commonly used URL prefixes for Cisco network devices.

Prefix	Description
flash:	Flash memory. This prefix is available on all platforms. For platforms that do not have a device that is named Flash, the flash: prefix is aliased to slot0. Therefore, the flash: prefix can be used to refer to the main flash memory storage area on all platforms.
ftp:	FTP network server.
http:	HTTP network server.
nvram:	NVRAM.
rcp:	RCP network server.
system:	Contains the system memory, including the current running configuration.
tftp:	TFTP network server.
usbflash0, usbflash1	USB flash.

Managing Cisco IOS Images

As a network grows, storage of Cisco IOS Software images and configuration files on a central TFTP server enables control of the number and revision level of Cisco IOS images and configuration files that must be maintained.

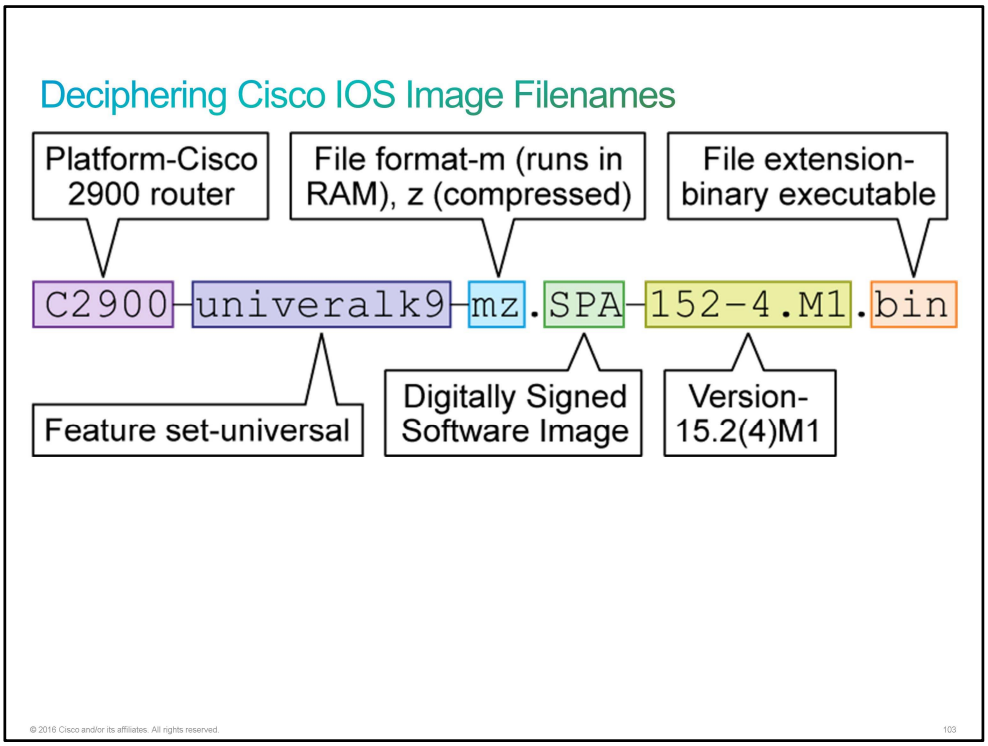
Production internetworks usually span wide areas and contain multiple routers. For any network, it is prudent to retain a backup copy of the Cisco IOS Software image in case the system image in the router becomes corrupted or accidentally erased.



Widely distributed routers need a source or backup location for Cisco IOS Software images. Using a network TFTP server allows image and configuration uploads and downloads over the network. Storage of Cisco IOS Software images and configuration files on a central TFTP server enables you to control the number and revision level of Cisco IOS images and configuration files that must be maintained. The network TFTP server can be another router, a workstation, or a host system.

Deciphering Cisco IOS Image Filenames

Before upgrading a Cisco IOS router, you must select a Cisco IOS image with the correct feature set and version. The Cisco IOS image file is based on a special naming convention. The name for the Cisco IOS image file contains multiple parts, each with a specific meaning. It is important that you understand this naming convention when upgrading and selecting Cisco IOS Software.



This list describes the parts of the example filename that is shown in the figure:

- The first part (c2900) identifies the platform on which the image runs. In this example, the platform is a Cisco 2900 Series Integrated Services Router.
- The second part (universal) specifies the feature set. In this case, "universal" refers to the universal, single image set that includes the IP base, security, unified communications, and data feature sets. Each router is activated for an IP base feature set. However, for other feature sets, software activation is needed.
- The third part (mz) indicates where the image runs and if the file is compressed. In this example, "mz" indicates that the file runs from RAM and is compressed.
- The fourth part (SPA) indicates that it is the file extension that Cisco software build process creates. Digitally signed Cisco IOS software is identified by a three-character extension in the image name.

File extension character	Character meaning
S (first character)	Stands for digitally signed software.
P or S (second character)	P and S stand for a production and special (development) image, respectively. A production (P) image is Cisco software that is approved for general release; a special (S) image is development software that is provided under special conditions for limited use.

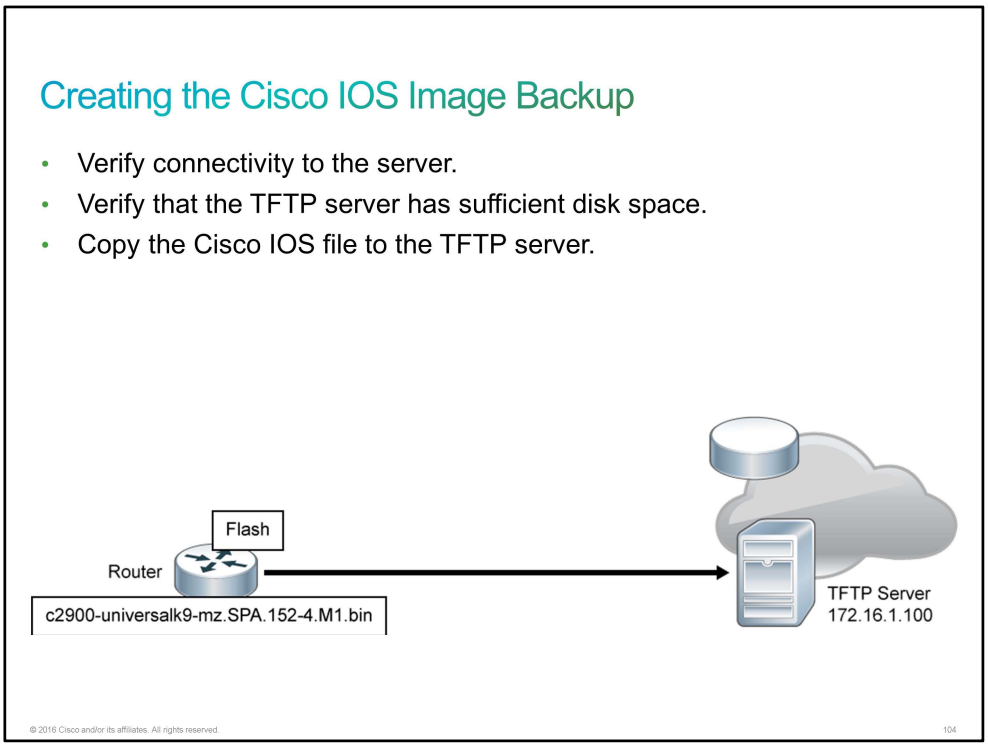
File extension character	Character meaning
A (third character)	Indicates the key version that is used to digitally sign the image. A key version is identified by an alphabetical character—for example, A, B, C, etc.

- The fifth part (15.2(4)M1) is the version number.
- The final part (bin) is the file extension. This extension indicates that this file is a binary executable file.

Note	The Cisco IOS Software naming conventions, field meaning, image content, and other details are subject to change.

Creating the Cisco IOS Image Backup

To maintain network operations with minimum down time, it is necessary to have procedures in place for backing up Cisco IOS images. In this way, you can quickly copy an image back to a router in case of a corrupted or erased image on the router.



Follow these steps to create a backup of Cisco IOS images to the TFTP server:

- Make sure that there is access to the network TFTP server. You can ping the TFTP server to test connectivity.
- Verify that the TFTP server has sufficient disk space to accommodate the Cisco IOS Software image. Use the **show flash0:** command on the router to determine the size of the Cisco IOS image file.
- Copy the image to the TFTP server using the **copy** command.

Creating the Cisco IOS Image Backup (Cont.)

1. Verify connectivity to the server.

```
Branch# ping 172.16.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
```

2. Verify Cisco IOS image size.

```
Branch# show flash0:
-#- --length-- -----date/time------ path
1      97794040 Nov 30 1983 00:00:00 +00:00 c2900-universalk9-mz.SPA.152-4.M1.bin
<... output omitted ...>
```


Before creating an image backup, verify connectivity to the TFTP server. You can verify connectivity by pinging the TFTP server from the router. In the example, the TFTP server is accessible from the router.

You should then make sure that you have sufficient disk space on the TFTP server to accommodate the Cisco IOS Software image. You can use the **show flash** command to verify the Cisco IOS Software image file size. The file in the example is 97,794,040 B (93 MB).

In this example, you will create a backup of the current image file on the router (c2900-universalk9-mz.SPA.152-4.M1.bin) to the TFTP server at 172.16.1.100.

Creating the Cisco IOS Image Backup (Cont.)

3. Copy image to the TFTP server.

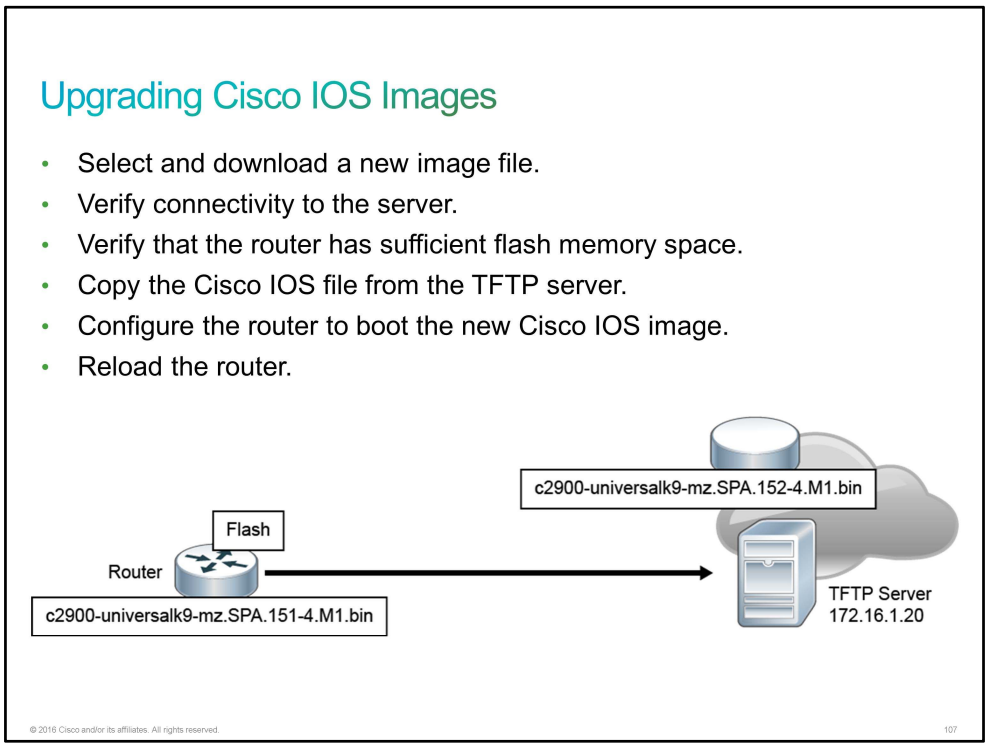
```
Branch# copy flash0: tftp:
Source filename []? c2900-universalk9-mz.SPA.152-4.M1.bin
Address or name of remote host []? 172.16.1.100
Destination filename []? c2900-universalk9-mz.SPA.152-4.M1.bin
!!!!!!!!!!!!!!!!!
<... output omitted ...>
97794040 bytes copied in 363.468 secs (269058 bytes/sec)
```

Finally, copy the Cisco IOS Software image file to the server, using the **copy** command. After you issue the command with specified source and destination URLs, you will be prompted for the source file name, IP address of the remote host, and destination filename. After you enter all this information, transfer of the file will occur. The table describes the command.

Command	Description
copy *source-url destination-url*	Copies any file from a source to a destination. The exact format of the source and destination URLs varies according to the file or directory location.

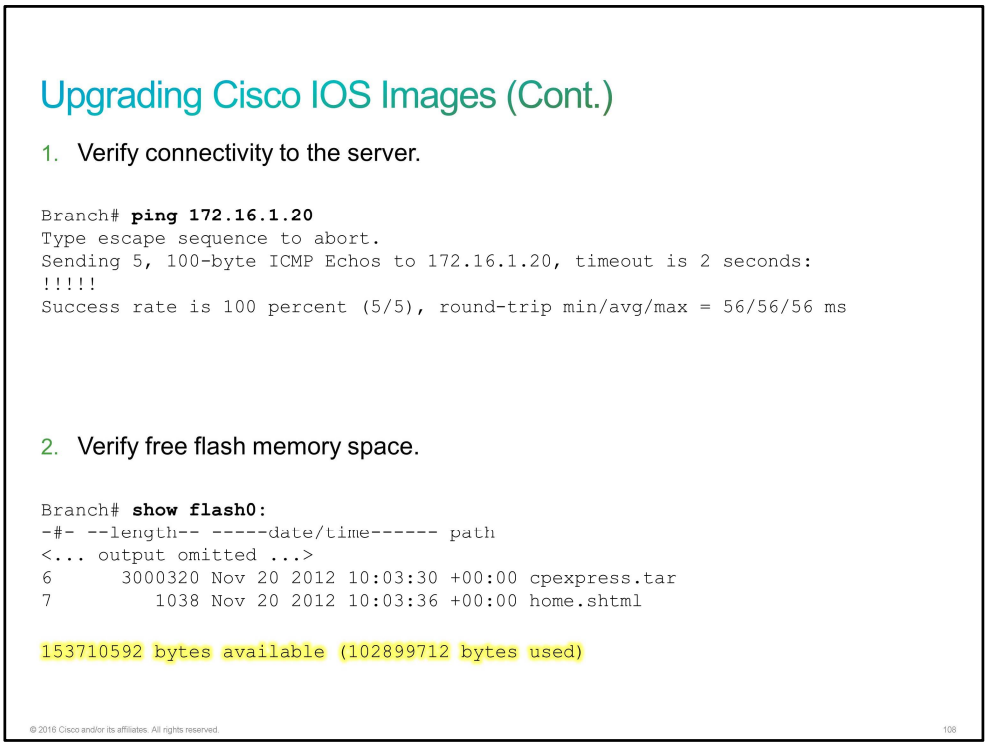
Upgrading Cisco IOS Images

Cisco constantly releases new Cisco IOS Software versions to resolve caveats (software defects) and provide new features.



If you decide to upgrade the software on the Cisco router, follow these steps:

- Select a Cisco IOS image file that meets your requirements in terms of platform, features, and software defects. Download the file from http://www.cisco.com and transfer it to the TFTP server.
- Make sure that there is access to the network TFTP server. Ping the TFTP server to test connectivity.
- Make sure that there is sufficient flash memory space on the router that is being upgraded. You can verify the amount of free flash space by using the **show flash0:** command. Compare the free flash space with the new image file size.
- Copy the Cisco IOS image file from the TFTP server to the router using the **copy** command.
- When the image is saved on the router flash memory, you have to instruct the router to load the new image during the boot. Save the configuration.
- Finally, reload the router in order to boot the new image.



After you download the correct Cisco IOS image file and transfer it to the TFTP server, you should verify connectivity to the TFTP server by pinging the TFTP server from the router. In the example, the TFTP server is accessible from the router.

You should then make sure that you have sufficient disk space in the flash memory to accommodate the Cisco IOS image. You can use the **show flash** command to verify free the flash memory space. Free flash space in the example is 153,710,592 B.

In this example, you will load the new image file (c2900-universalk9-mz.SPA.152-4.M1.bin) from the TFTP server at 172.16.1.20 to the router.

Upgrading Cisco IOS Images (Cont.)

3. Copy the image from the TFTP server.

```
Branch# copy tftp: flash0:
Address or name of remote host []? 172.16.1.20
Source filename []? c2900-universalk9-mz.SPA.152-4.M1.bin
Destination filename []? c2900-universalk9-mz.SPA.152-4.M1.bin
Accessing tftp://172.16.1.20/c2900-universalk9-mz.SPA.152-4.M1.bin...

Loading c2900-universalk9-mz.SPA.152-4.M1.bin from 172.16.1.20 (via
GigabitEthernet0/0): !!!!!!!!!!!!!!!!!!!!
<... output omitted ...>
[OK - 97794040 bytes]
97794040 bytes copied in 368.128 secs (265652 bytes/sec)
```

4. Set the image to boot and reload the router.

```
Branch# configure terminal
Branch(config)# boot system flash0://c2900-universalk9-mz.SPA.152-4.M1.bin
Branch# copy running-config startup-config
Branch# reload
```


Copy the Cisco IOS image file from the server to the router flash memory using the **copy** command. After you issue the command with specified source and destination URLs, you will be prompted for the IP address of the remote host, source file name, and destination file name. After you enter all the required information, the transfer of the file will begin.

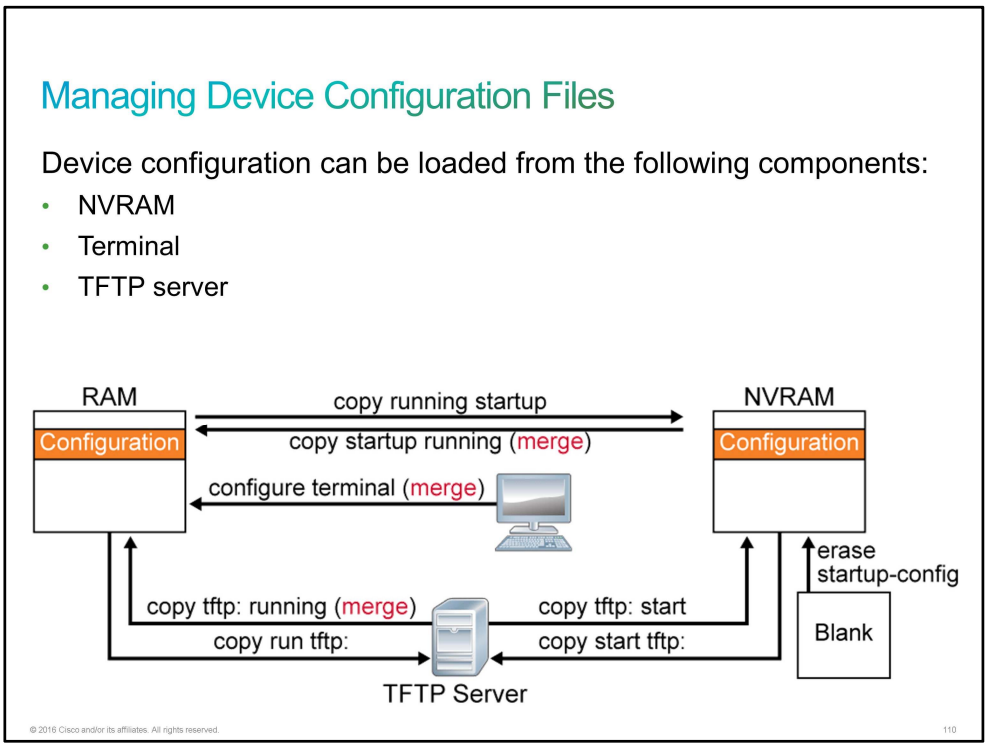
When the image file has been copied to the router, you have to instruct the router to boot the new image file. Use the **boot system** command to instruct the router to boot the specific file. Recall that the boot field in the configuration register has to be set to 0x2 to 0xF in order for the router to check the boot commands. Save the configuration.

Reload the router to boot the router with the new image. When the router has booted, you can verify if the new image has loaded using the **show version** command.

Command	Description
boot system *url*	Specify the system image that the router loads at startup.

Managing Device Configuration Files

Device configuration files contain a set of user-defined configuration commands that customize the functionality of a Cisco device.



Configuration files of a Cisco router are stored in the following locations:

- The running configuration is stored in RAM.
- The startup configuration is stored in NVRAM.

You can copy configuration files from the router to a file server using FTP or TFTP. For example, you can copy configuration files to back up a current configuration file to a server before changing its contents, therefore allowing the original configuration file to be restored from the server. The protocol that is used depends on which type of server is used.

You can copy configuration files from a server to the running configuration in RAM or to the startup configuration file in NVRAM of the router for one of the following reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another router. For example, you may add another router to the network and want it to have a similar configuration as the original router. By copying the file to the network server and making the changes to reflect the configuration requirements of the new router, you can save time by not recreating the entire file.
- To load the same configuration commands onto all the routers in the network so that all the routers have similar configurations.
- To use the configuration file for another router. For example, you may add another router.

For example, in the **copy running-config tftp** command, the running configuration in RAM is copied to a TFTP server.

Use the **copy running-config startup-config** command after a configuration change is made in RAM and must be saved to the startup configuration file in NVRAM. Similarly, copy the startup configuration file in NVRAM back into RAM with the **copy startup running:** command (this is a merge, not a real copy). Notice that you can abbreviate the commands.

Similar commands exist for copying between a TFTP server and either NVRAM or RAM.

The following examples show common **copy** command usage. The examples list two methods to accomplish the same tasks. The first example is simple syntax, and the second example provides more explicit syntax.

- Copy the running configuration from RAM to the startup configuration in NVRAM, overwriting the existing file:

```
R2# copy running-config startup-config
R2# copy system:running-config nvram:startup-config
```

- Copy the running configuration from RAM to a remote location, overwriting the existing file:

```
R2# copy running-config tftp
R2# copy system:running-config tftp
```

- Copy a configuration from a remote source to the running configuration, merging the new content with the existing file:

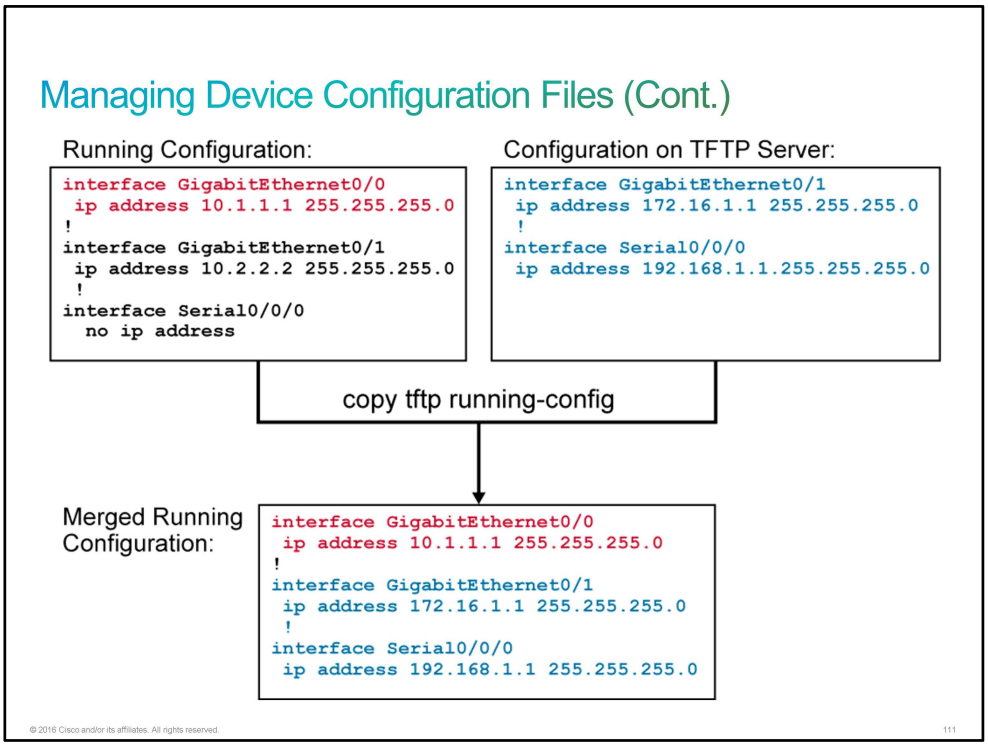
```
R2# copy tftp running-config
R2# copy tftp system:running-config
```

- Copy a configuration from a remote source to the startup configuration, overwriting the existing file:

```
R2# copy tftp startup-config
R2# copy tftp nvram:startup-config
```

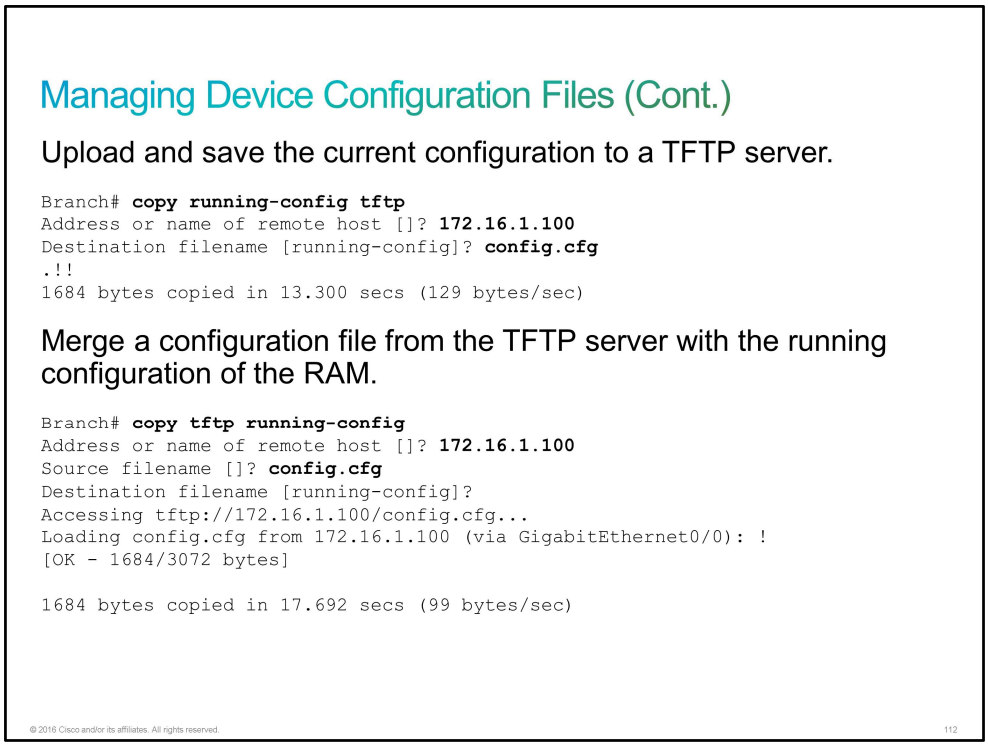
Use the **configure terminal** command to interactively create configurations in RAM from the console or remote terminal.

Use the **erase startup-config** command to delete the saved startup configuration file in NVRAM.



This figure shows an example of how to use the **copy tftp running-config** command to merge the running configuration in RAM with a saved configuration file on a TFTP server.

Note	When a configuration is copied into RAM from any source, the configuration merges with or overlays any existing configuration in RAM, rather than overwriting it. New configuration parameters are added, and changes to existing parameters overwrite the old parameters. Configuration commands that exist in RAM for which there are no corresponding commands in NVRAM remain unaffected. Copying the running configuration from RAM into the startup configuration file in NVRAM will overwrite the startup configuration file in NVRAM.



You can use the TFTP servers to store configurations in a central place, allowing centralized management and updating. Regardless of the size of the network, there should always be a copy of the current running configuration online as a backup.

The **copy running-config tftp** command allows the current configuration to be uploaded and saved to a TFTP server. The IP address or name of the TFTP server and the destination filename must be supplied. A series of exclamation marks in the display shows the progress of the upload.

The **copy tftp running-config** command downloads a configuration file from the TFTP server to the running configuration of the RAM. Again, the address or name of the TFTP server and the source and destination filename must be supplied. In the example, IPv4 is used as a transport protocol. In this case, because you are copying the file to the running configuration, the destination filename should be running-config. This process is a merge process, not an overwrite process.

Password Recovery

If the password is mistyped or forgotten, access to the router privileged EXEC mode is not possible, and you must perform a password recovery procedure.

Different routers and switches may have different password recovery procedure. Refer to the http://www.cisco.com to find password recovery procedure for your router or switch. The following procedure describes password recovery for Cisco ISRs (Cisco Integrated Services Routers).

Password Recovery

The password recovery procedure differs for different router and switch platforms.

1. Switch off the router.
2. Switch on the router. Press **Break** to enter ROM monitor mode.
3. When in the ROM monitor mode, check the configuration register.

```
rommon 1> confreg
```


Password Recovery (Cont.)

4. In the ROM monitor mode, set the configuration register to 0x2142.

```
rommon 1> confreg 0x2142
```

5. Reset the router.

```
rommon 1> reset
```

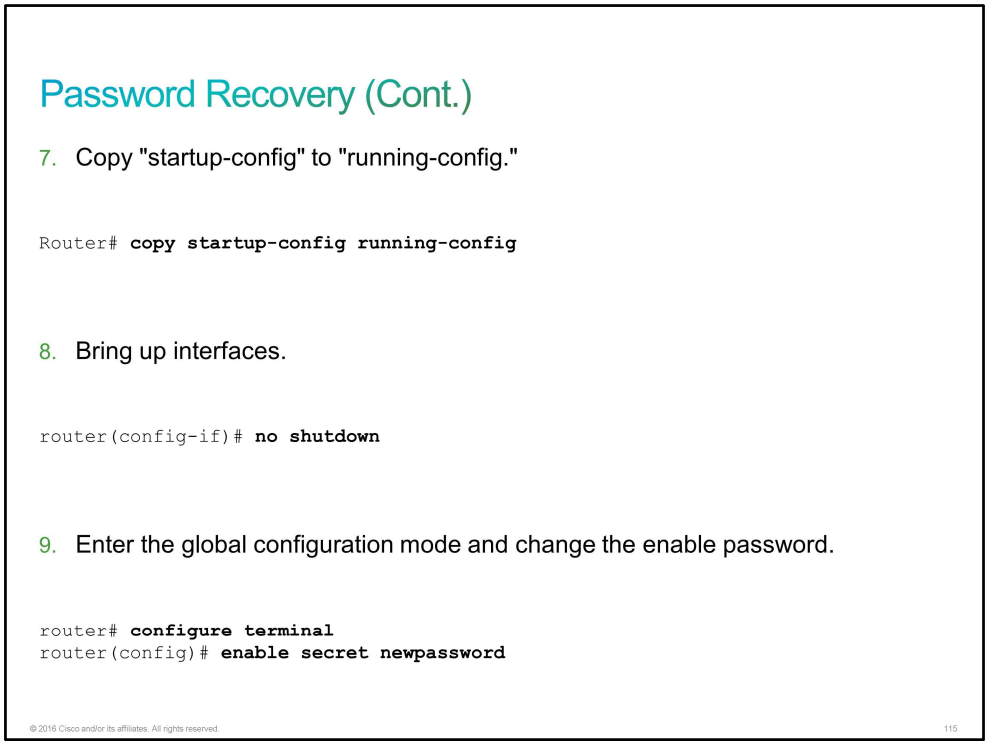
6. Enter the privileged EXEC mode.

```
Router> enable
```

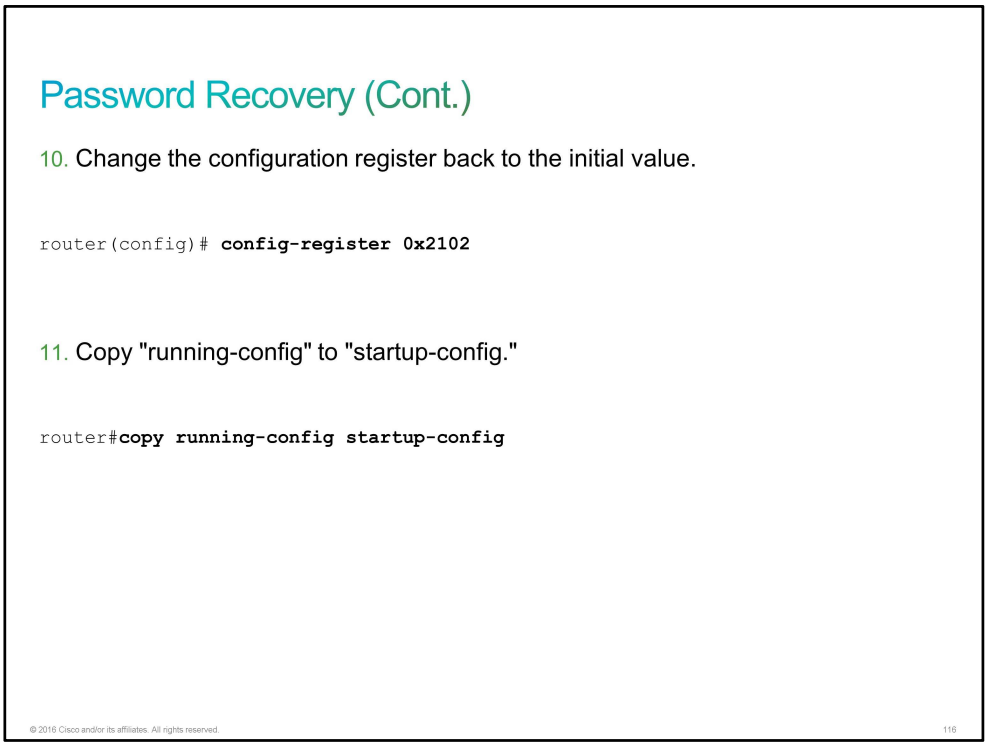

You can use the configuration register to perform the password recovery procedure. You have to set the configuration register value to a value that will instruct the router to ignore the startup configuration, which includes the forgotten enable password. Because a user cannot enter the privileged EXEC mode in order to change the configuration register, the register has to be changed in the ROM monitor. In order to enter the ROM monitor, reboot the router and press **Break** to interrupt the boot process to get into the ROM monitor.

Follow these steps to perform password recovery:

- Either switch off or shut down the router.
- Switch on the router. Press **Break** to interrupt the boot process to get into the ROM monitor.
- When the router is in the ROM monitor mode, check configuration register by using the **confreg** command.
- Set the configuration register to 0x2142. The hexadecimal number of 4 indicates that bit 6 is set and this will instruct the router to ignore the startup configuration at the next reload.
- Reset the router. The router reboots but ignores the saved configuration. Do not enter the interactive setup dialog.
- Enter the privileged EXEC mode. You should be able to do so because the saved configuration is ignored and the empty configuration without the enable password is loaded.



- Copy "startup-config" to "running-config" in order to load the saved configuration. After this step, all interfaces might be disabled. You have to enable the desired interfaces using the **no shutdown** command.
- Because the startup configuration merged into the running configuration, the interfaces will be shut down. Bring up the appropriate interfaces using the **no shutdown** command.
- Enter the global configuration mode and change the enable password to a new value. Do not forget or mistype the password this time.



- Change the configuration register back to the initial value. Change the value to the previously recorded value or to 0x2102. This action will instruct the router to not ignore the startup configuration at the next reload.
- Copy "running-config" to "startup-config" in order to save changes regarding the new enable password and the configuration register value.

Challenge

1. Which router component stores the IP routing table?

   A. NVRAM
   B. RAM
   C. ROM
   D. flash memory

2. Which microcode is used to test the basic functionality of router hardware and to determine which components are present?

   A. POST
   B. bootstrap
   C. ROM monitor
   D. ROM

3. From which two router components could the router obtain its operating system? (Choose two.)

   A. ROM
   B. flash
   C. TFTP server
   D. NVRAM
   E. console

4. From which three router components could the router obtain its configuration? (Choose three.)

   A. ROM
   B. flash
   C. TFTP server
   D. NVRAM
   E. console

5. Which Cisco IOS command can you use to examine the configuration register?

   A. **show running-config**
   B. **show startup-config**
   C. **show version**
   D. **show config-register**

6. Which Cisco IOS command do you use to verify the Cisco IOS image size?

   A. **show flash0:**
   B. **show running-config**
   C. **show startup-config**
   D. **show file systems**

7. When a configuration is copied into the startup configuration file in NVRAM from any source, the configuration merges with or overlays any existing configuration in NVRAM. True or false?

   A. true
   B. false

8. Put the commands in the order in which they should be used when upgrading a Cisco IOS image.

show flash	1
copy	2
ping	3
boot system	4
reload	5

Answer Key

Challenge

1. B
2. A
3. B, C
4. C, D, E
5. C
6. A
7. B
8.

ping	1
show flash	2
copy	3
boot system	4
reload	5

Lesson 5: Licensing

Introduction

Your boss sends you to your customer to explain how to verify the current version of the license and how to back up, install, and uninstall a license.

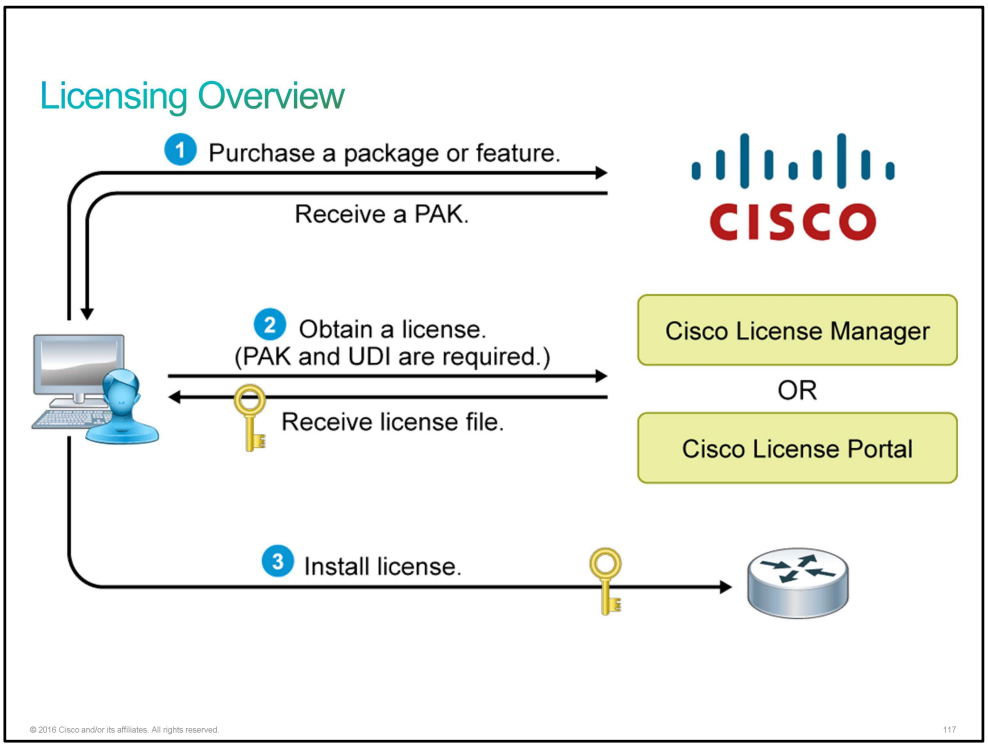
Introducing Licensing

When you order a new router, it is shipped preinstalled with the software images and the corresponding permanent licenses for the packages and features that you specified.

Note	Use the Cisco IOS **show license** command to determine the licenses that are activated on your system.

Your router comes with an evaluation license, also known as a temporary license, for most packages and features that are supported on your router. If you want to try a new software package or feature, activate the evaluation license for this package or feature. If you want to permanently activate a software package or feature on your router, you must get a new software license.

Software Claim Certificates are used for licenses that require software activation. The claim certificate provides the PAK for your license and important information regarding the Cisco End User License Agreement (Cisco EULA). Usually, Cisco or your Cisco partner will already have activated the licenses that were ordered at the time of purchase, and no Software Claim Certificate is provided.

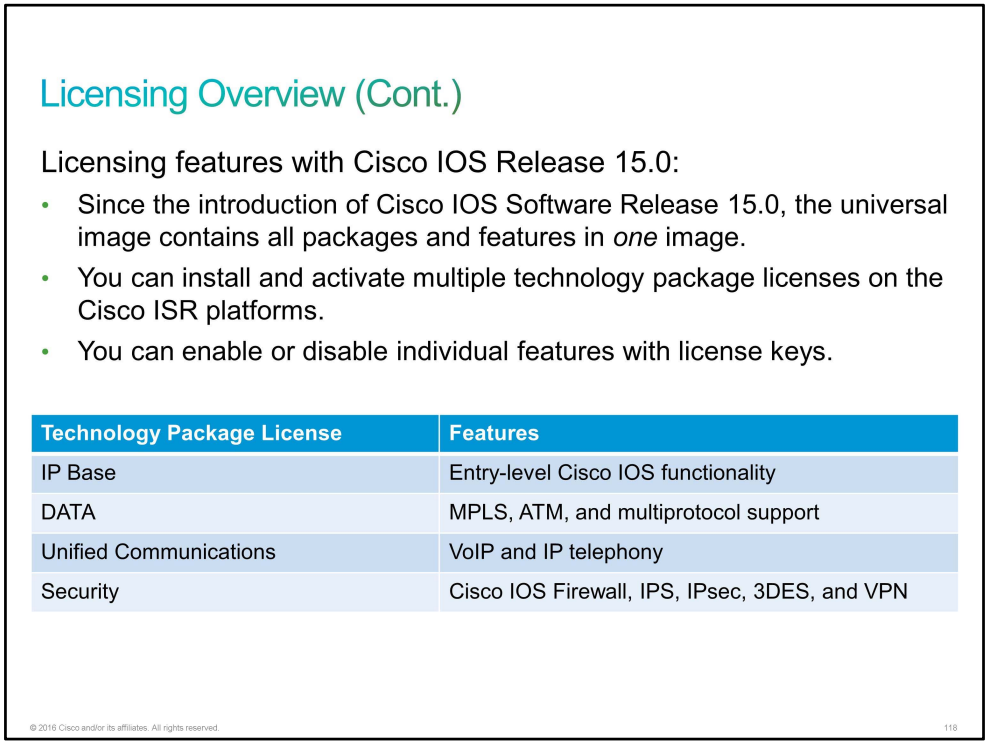


Complete these steps to permanently activate a software package or feature on a router:

1. Purchase the software package or feature that you want to install. You receive a PAK with your purchase.
2. Obtain the license file using one of these options:
   - **Cisco License Manager:** A free software application that is available at http://www.cisco.com/go/clm.
   - **Cisco License Registration Portal:** The web-based portal for obtaining and registering individual software licenses. It is available at http://www.cisco.com/go/license.
3. Use the Cisco IOS Command-Line Interface (Cisco IOS CLI) to install and manage licenses.

To obtain the license, you might also need the UDI, which has two main components: the PID and the serial number. The following example shows the output from the **show license udi** command that reveals the product ID and serial number of the router:

```
Router# show license udi
Device#  PID                    SN              UDI
-------------------------------------------------------------------------------
*0        CISCO2901/K9           FCZ1642C5XD     CISCO2901/K9:FCZ1642C5XD
```



Beginning with the Cisco Integrated Services Routers (Cisco ISRs), Cisco has revised the licensing model of Cisco IOS Software. Routers come with IP Base installed. You can install additional feature pack licenses as bolt-on additions to expand the feature set of the device.

The Cisco IOS universal image contains all packages and features in one image. The universal image on the Cisco ISR routers is a superset of Cisco IOS simplified technology packages. Each package is a grouping of technology-specific features. You can install and activate multiple technology package licenses on the Cisco ISR platforms.

Note	Use the **show license feature** command to view the technology package licenses and feature licenses that are supported on your router.

Premium features beyond what is included in the default IP Base package are generally grouped into three major technology package licenses: Data, Security, and Unified Communications. These three packages represent most features that are available in Cisco IOS Software.

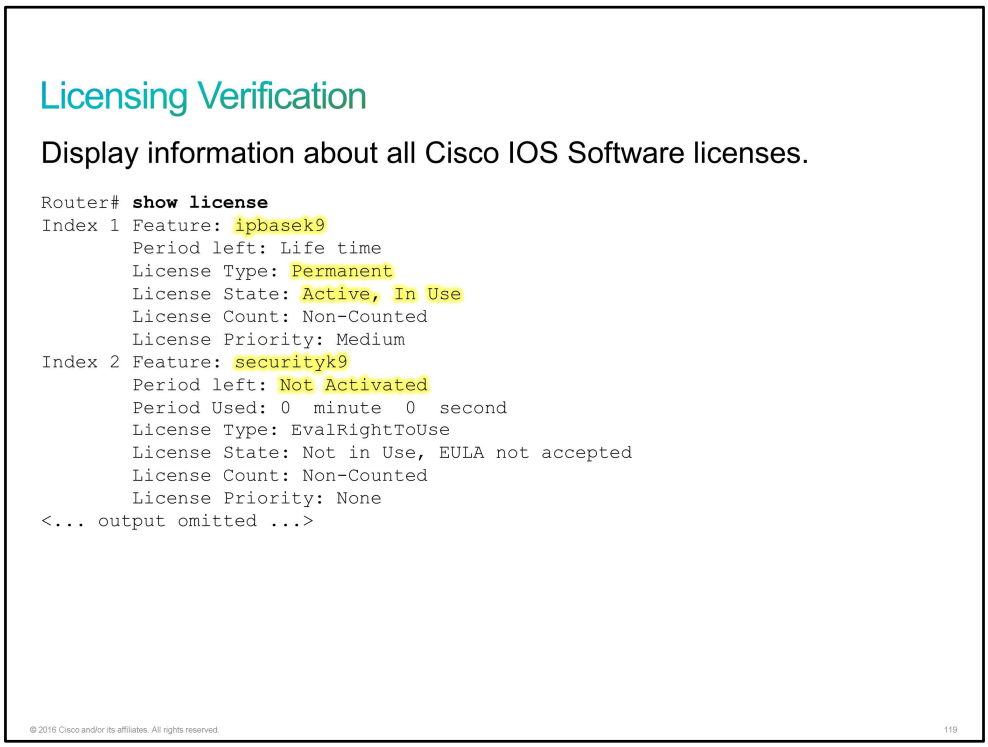
The table lists the technology package licenses that are supported on Cisco Integrated Services Routers Generation 2 (Cisco ISR G2) platforms.

Technology Package License	Features
ipbasek9 (IP Base)	Entry-level Cisco IOS functionality
datak9 (DATA)	MPLS, ATM, and multiprotocol support
uck9 (Unified Communications)	VoIP and IP telephony
securityk9 (Security)	Cisco IOS Firewall, IPS, IPsec, 3DES, and VPN

Note The IP Base license is a prerequisite for installing the Data, Security, and Unified Communications license.

Licensing Verification

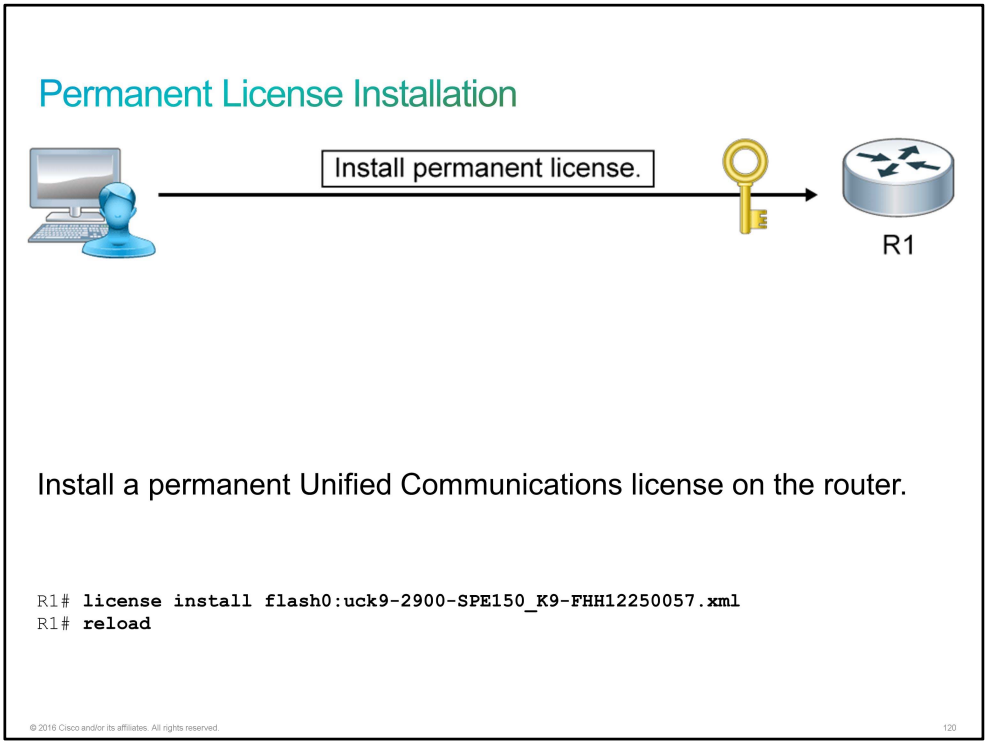
To display information about a Cisco IOS Software license, use the **show license** command in the privileged EXEC mode.



Permanent License Installation

Installing a permanent license is based on the steps that the following table describes.

Command	Description
license install *stored-location-url*	Installs a license file.
reload	Reloads the router. You do not need to reload the router if an evaluation license is active. You have to reload it to activate a technology package license if an evaluation license is not active.



The figure shows the configuration for installing the permanent Unified Communications license on the router. It is assumed that you obtained the license file from Cisco and that you stored it on the flash memory of the router.

Permanent licenses are perpetual (that is, no usage period is associated with them). When permanent licenses are installed, they provide all the permissions that are needed to access features in the software image.

Note	Cisco manufacturing preinstalls the appropriate permanent license on the ordered device for the purchased feature set. No customer interaction with the Cisco IOS Software Activation processes is required to enable a license on new hardware.

Use the **license install** command to install the permanent license.


```
R1# license install flash0:uck9-C2900-SPE150_K9-FHH12250057.xml
Installing licenses from "uck9-C2900-SPE150_K9-FHH12250057.xml"
Installing...Feature:uck9...Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
upt-3945-1#
*Jul  7 17:24:57.391: %LICENSE-6-INSTALL: Feature uck9 1.0 was installed in this
device.
UDI=C3900-SPE150/K9:FHH12250057; StoreIndex=15:Primary License Storage
*Jul  7 17:24:57.615: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name =
c2900
Next reboot level = uck9 and License = uck9
```

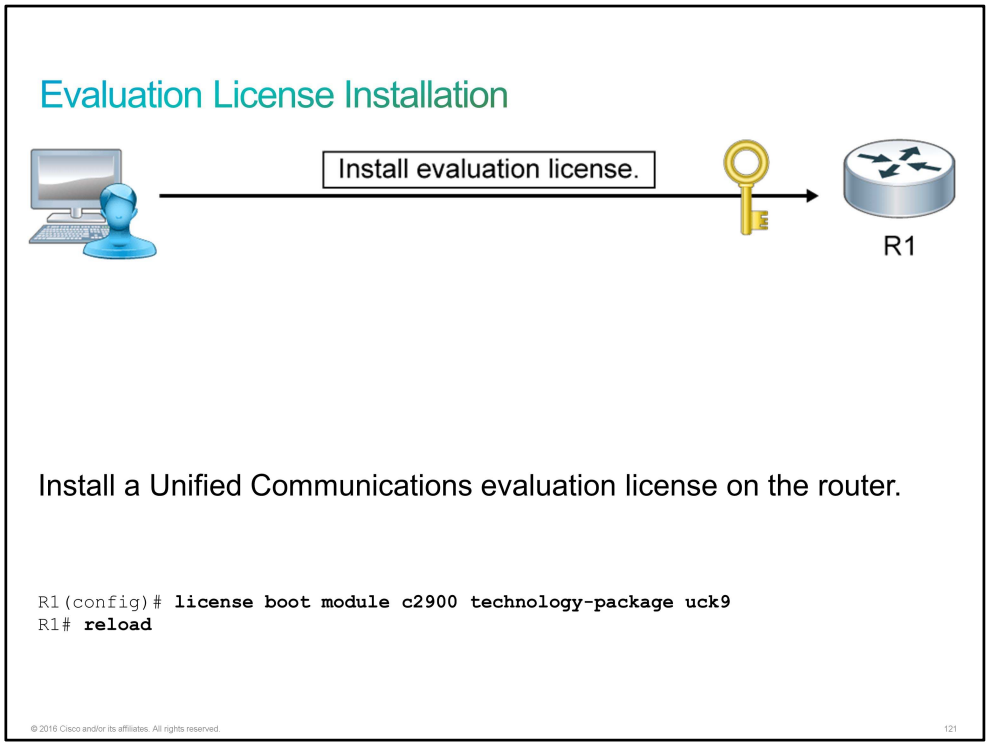
After the license is successfully installed, reload the router using the **reload** command. After the router reloads, use the **show version** command to verify that the license has been installed.

Note	You do not need to reload the router if an evaluation license is active. However, you need to reload it to activate a technology package license if an evaluation license is not active.

```
R1# show version
<... output omitted ...>
License Info:
License UDI:
-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        C3900-SPE150/K9       FHH12250057
Technology Package License Information for Module:'c2900'
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
uc            uck9          Permanent     uck9
data          None          None          None
Configuration register is 0x0
```

Evaluation License Installation

Note	Starting with Cisco IOS Releases 15.0(1)M6, 15.1(1)T4, 15.1(2)T4, 15.1(3)T2, and 15.1(4)M, evaluation licenses are replaced with evaluation right-to-use licenses. Follow the steps that are detailed in the table to activate an evaluation right-to-use license.



The figure shows the configuration for activating a Unified Communications evaluation license on the router. Evaluation licenses are temporary, and you use them to evaluate a feature set on new hardware. Temporary licenses are limited to a specific usage period (for example, 60 days).

Activating the evaluation license is based on the steps that the following table describes.

Command	Description
license boot module *module-name* **technology-package** *package-name*	Enables the evaluation license. Use the **?** command with the **module** command to see the module name for your router and with the **technology-package** command to see the software packages and features that are supported on your router.
reload	Reloads the router. A reload is required to activate the software package.

Use the **license boot module** command to enable the evaluation license.

```
R1(config)# license boot module c2900 technology-package uck9
PLEASE READ THE FOLLOWING TERMS CAREFULLY.  INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH
PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product, including during the 60-day evaluation period, is subject
to the Cisco End User License Agreement at
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html.
If you use the product feature beyond the 60-day evaluation period, you
must submit the appropriate payment to Cisco for the license.  After the
60-day evaluation period, your use of the product features will be
governed solely by the Cisco End User License Agreement (link above),
together with any supplements relating to such product features.  The
above applies even if the evaluation license is not automatically
terminated and you do not receive any notice of the expiration of the
evaluation period.  It is your responsibility to determine when the
evaluation period is complete, and you are required to make payment to
Cisco for your use of the product features beyond the evaluation period.

Your acceptance of this agreement for the software features on one
product shall be deemed your acceptance with respect to all such
software on all Cisco products you purchase, which includes the same
software.  (The foregoing notwithstanding, you must purchase a license
for each software feature you use past the 60-day evaluation period,
so that if you enable a software feature on 1000 devices, you must
purchase 1000 licenses for use past the 60-day evaluation period.)

Activation of the software command line interface will be evidence of
your acceptance of this agreement.

ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot

Nov 27 08:44:14.395: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name=
c2900 Next reboot level = uck9 and License = uck9
Nov 27 08:44:15.023: %LICENSE-6-EULA_ACCEPTED: EULA for feature uck9 1.0 has been
accepted. UDI=CISCO2901/K9:FCZ1642C5XD; StoreIndex=1:Built-In License Storage
```

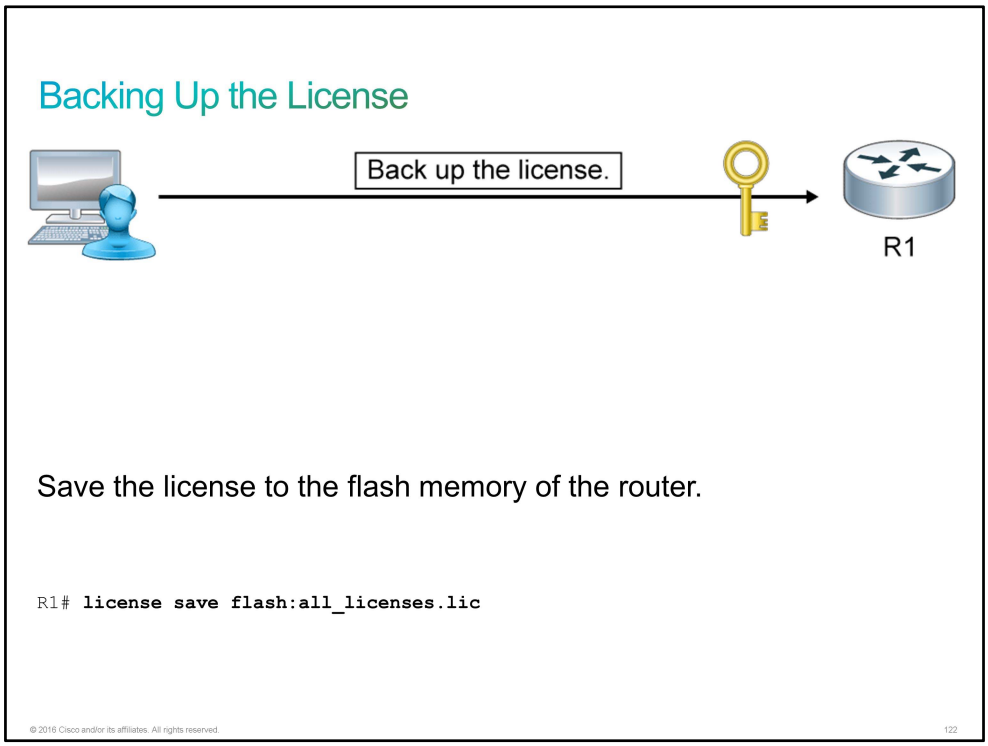
After the license is successfully installed, reload the router using the **reload** command. Use the **show license** command after the router is reloaded to verify that the license has been installed.

```
R1# show license
Index 1 Feature: ipbasek9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: securityk9
        Period left: Not Activated
        Period Used: 0  minute  0  second
        License Type: EvalRightToUse
        License State: Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
Index 3 Feature: uck9
        Period left: 8  weeks 3  days
        Period Used: 9  minutes 30 seconds
        License Type: EvalRightToUse
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Low
<... output omitted ...>
```


Backing Up the License

Saving or backing up the license is based on the step that the following table describes.

Command	Description
license save *file-sys://lic-location*	Saves copies of all licenses on a device. The *lic-location* argument is the license storage location, which can be a directory or a URL that points to a file system. Use the **?** command to see the storage locations that your device supports.



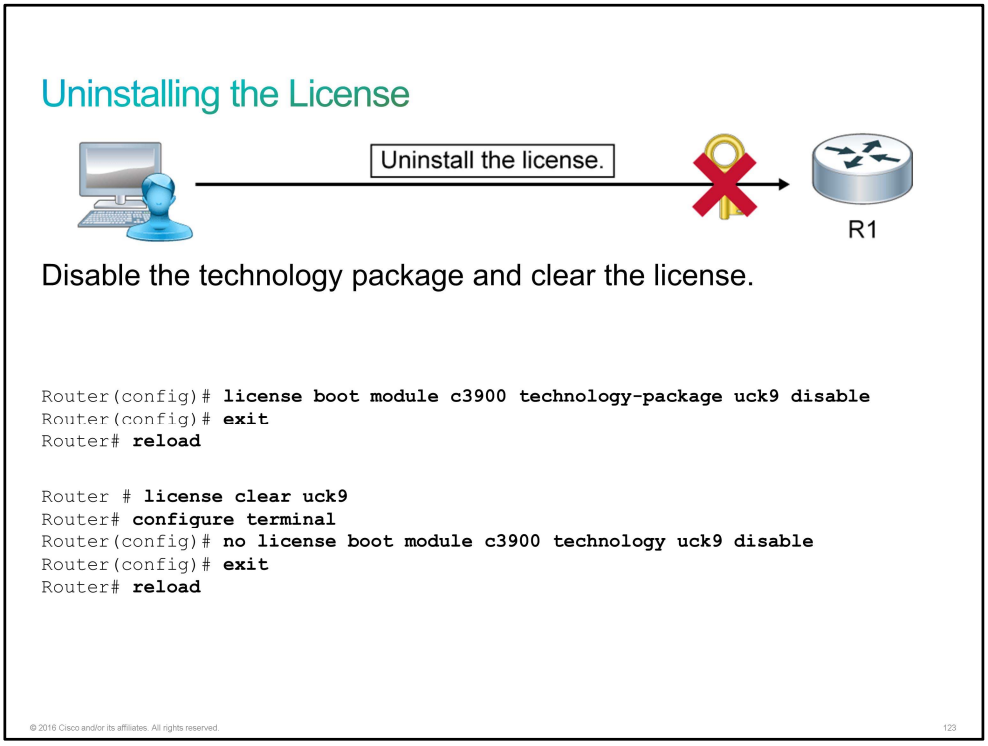
The figure shows the configuration for backing up the license on the router. You can restore saved licenses by using the **license install** command.

```
Router# license save flash:all_licenses.lic
license lines saved ..... to flash:all_licenses.lic
```

Uninstalling the License

To clear an active permanent license from the Cisco Integrated Services Router (Cisco ISR), perform the following tasks:

1. Disable the technology package.
2. Clear the license.



The figure shows the configuration for clearing an active permanent license from the Cisco ISR routers. First, you need to disable the technology package and then clear the license. Each of these two steps requires a reload of the router.

Note	You cannot clear some licenses, such as built-in licenses. You can remove only the licenses that you have added using the **license install** command. Evaluation licenses are not removed.

Clearing the active permanent license is based on the steps that the following table describes.

Command	Description
license boot module *module-name* **technology-package** *package-name* **disable**	Disables the active license.
reload	Reloads the router. A reload is required to make the software package inactive.
license clear *feature-name*	Clears the technology package license from the license storage.

Command	Description
no license boot module *module-name* **technology-package** *package-name* **disable**	Clears the **license boot module** *module-name* **technology-package** *package-name* **disable** command that is used for disabling the active license.
reload	Reloads the router. A reload is required to make the software package inactive.

The following example shows how to clear an active license on a Cisco 3900 router:

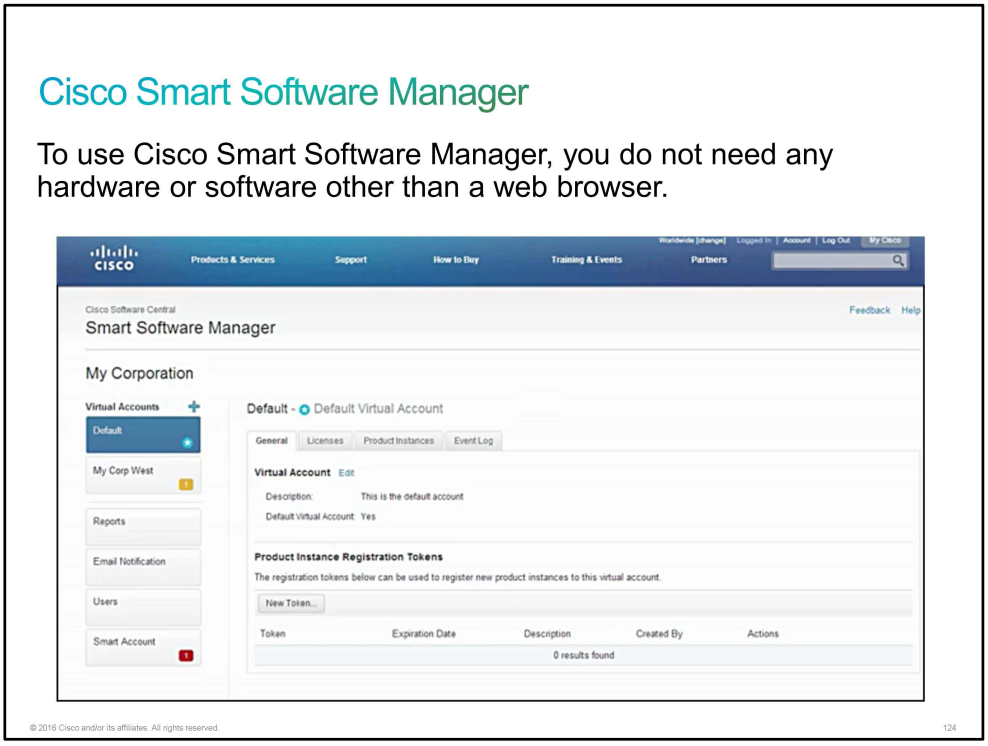
```
Router(config)# license boot module c3900 technology-package uck9 disable
% use 'write' command to make license boot config take effect on next boot
Router(config)# exit
Router# reload

Router# license clear uck9
*Jul  7 00:34:23.691: %SYS-5-CONFIG_I: Configured from console by consoleclear uck9
Feature: uck9
    1   License Type: Permanent
        License State: Active, Not in Use
        License Addition: Exclusive
        License Count: Non-Counted
        Comment:
        Store Index: 15
        Store Name: Primary License Storage
Are you sure you want to clear? (yes/[no]): yes
upt-3945-1#
*Jul  7 00:34:31.223: %LICENSE-6-REMOVE: Feature uck9 1.0 was removed from this
device.
UDI=C3900-SPE150/K9:FHH12250057; StoreIndex=15:Primary License Storage
Router#
Router# configure terminal
Router(config)# no license boot module c3900 technology uck9 disable
Router(config)# exit
Router# reload
```

Cisco Smart Software Manager

Cisco Smart Software Manager enables you to manage all your Cisco Smart software licenses from one centralized website. With Cisco Smart Software Manager, you organize and view your licenses in groups that are called virtual accounts.

Virtual accounts are collections of licenses and product instances. You can create virtual accounts in Cisco Smart Software Manager to organize the licenses for your company into logical entities. You can use them to organize licenses by business unit, product type, IT group, or whatever makes sense for your organization. For example, if you segregate your company into different geographic regions, you can create a virtual account for each region to hold the licenses and product instances for that region. You can use Cisco Smart Software Manager to transfer the licenses between virtual accounts as needed.



The user interface of Cisco Smart Software Manager is divided into two main sections: a *Navigation pane* on the left and the main *Work pane,* as you can see in the figure.

For additional information, see *Cisco Smart Software Manager User Guide*: http://www.cisco.com/web/ordering/smart-software-manager/docs/smart-software-manager-user-guide.pdf.

Challenge

1. Match the step number with the step description to install license to the Cisco router?

Step 3	Install the license on a Cisco router.
Step 4	Receive a PAK.
Step 2	Receive a license file.
Step 1	Obtain a license.
Step 5	Purchase a package or feature.

2. What Cisco IOS command do you use to determine the licenses that are activated on the system?

   A. **show running-config license**
   B. **show running-config**
   C. **show udi license**
   D. **show license**

3. What two options are available for obtaining the license file? (Choose two.)

   A. Cisco License Manager
   B. Cisco License Registration Portal
   C. Cisco Registration Portal
   D. Cisco Manager
   E. Cisco Registration Manager

4. Which Cisco IOS command do you use to view the technology package licenses and feature licenses that are supported on the router?

   A. **show running-config license**
   B. **show running-config**
   C. **show license feature**
   D. **show udi license feature**

5. Which three features are supported in the securityk9 technology package license? (Choose three.)

   A. MPLS
   B. ATM
   C. VoIP
   D. IPS
   E. IPsec
   F. 3DES

6. Which three features are supported in the datak9 technology package license? (Choose three.)

   A. MPLS
   B. ATM
   C. VoIP
   D. IPS
   E. multiprotocol support
   F. 3DES

7. Which Cisco IOS command do you use to save the license to the flash memory of the router?

   A. **write**
   B. **license install**
   C. **license boot**
   D. **license save**
   E. **copy running-config startup-config**

Answer Key

Challenge

1.

Step 5	Install the license on a Cisco router.
Step 2	Receive a PAK.
Step 4	Receive a license file.
Step 3	Obtain a license.
Step 1	Purchase a package or feature.

2. D
3. A, B
4. C
5. D, E, F
6. A, B, E
7. D

Module 13: Summary Challenge

Introduction

This module challenges you to use the knowledge and skill that you have obtained related in the *previous* modules.

Lesson 1: Troubleshooting Scalable Multiarea Network

Introduction

You work for RMZ Networking. Your colleague, Peter did some improvements on the network over the weekend and now you are seeing certain network issues. In this lesson, you will be working on resolving these issues.

Challenge

1. Which of the following is not correct about OSPF?

   A. Allow extensive control of routing updates
   B. Support VLSM
   C. Confine network instability to one area of the network.
   D. Increase routing overhead on the network.

2. Which of the following authentication protocol does not use encryption ?

   A. PAP
   B. CHAP
   C. MD5
   D. None of the above

3. Which of the following are MLP over Serial interface features ?

   A. Load Balancing
   B. Link fragmentation and interleaving (LFI)
   C. Increased redundancy
   D. All the above.

4. What is the default encapsulation protocol on a Serial interface on a Cisco router ?

   A. PPP
   B. HDLC
   C. Frame Relay
   D. None of the above

5. What is the main difference between SNMPv3 and SNMPv2 ?

   A. management
   B. integration
   C. classification
   D. enhanced security

6. GRE tunneling can transport multicast and IPv6 traffic between networks. True or False ?

   A. True
   B. False

7. Which commands will you use to check if BGP session is established ? (Choose two)

   A. **show ip bgp summary**
   B. **show ip bgp**
   C. **show ip bgp neighbor**
   D. **show ip route bgp**

Answer Key

Challenge

1. D
2. A
3. D
4. B
5. D
6. A
7. A, C

Lesson 2: Implementing and Troubleshooting Scalable Multiarea Network

Introduction

You work for TMC Networking. Your colleague, Peter did some improvements on the network over the weekend and now you are seeing certain network issues. In this lesson, you will be working on resolving these issues.

Challenge

1. Can you form IPv6 OSPF neighbors over a GRE tunnel ?

   A. Yes
   B. No

2. What is the OSPF router ID in a DR/BDR election used for?

   A. It is used with the OSPF priority values to determine which interface will be used to form a neighbor relationship with another OSPF router.
   B. It is used with the OSPF priority values to determine which OSPF router will become the DR or BDR in a point-to-point network.
   C. It is used with the OSPF priority values to determine which router will become the DR or BDR in a multiaccess network.
   D. It is used to determine which interfaces will send Hello packets to neighboring OSPF routers.

3. Which of the following are components of an OSPF hello packet ? (Choose two)

   A. Router ID
   B. Bandwidth
   C. Area ID
   D. OSPF cost

4. Which of the following are key security additions to SNMPv3 ?

   A. Uses MD5 or SHA hashes for authentication
   B. Can encrypt the entire packet
   C. Can guarantee message integrity
   D. All the above

5. Which of the following statements are true?

   A. Northbound APIs are used for communication between the controllers and network devices.
   B. Southbound APIs are used for communication between the controllers and network devices.
   C. OnePK is Cisco proprietary.
   D. The control plane is responsible for the forwarding of frames or packets.

6. Which of the following is true about APIC-EM ACL analysis?

   A. Allows fast and easy comparison of ACLs between devices to visualize differences and identify misconfigurations.
   B. Ability to trace application-specific paths between end devices to quickly identify ACLs in use and problem areas.
   C. Enables inspection, interrogation, and analysis of network access control policies.
   D. All the above

7. Which of the following command will you use to get information about the TCP session in BGP ?

   A. **show ip bgp**
   B. **show ip bgp summary**
   C. **show ip bgp neighbor**
   D. **show bgp**

Answer Key

Challenge

1. A
2. C
3. A, C
4. D
5. B, C
6. D
7. C

Glossary

ACL

access control list. A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

API

application programming interface. The means by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. A set of standard software interrupts, calls, and data formats that computer application programs use to initiate contact with other devices (for example, network services, mainframe communications programs, or other program-to-program communications). Typically, APIs make it easier for software developers to create the links that an application needs to communicate with the operating system or with the network.

APIC

Cisco Application Policy Infrastructure Controller.

ARP

Address Resolution Protocol. Internet protocol that is used to map an IP address to a MAC address. Defined in RFC 826.

AS

autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the IANA.

ATM

Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.

BGP

Border Gateway Protocol. Interdomain routing protocol that replaces EGP. BGP exchanges reachability information with other BGP systems. It is defined by RFC 1163.

CAC

Call Admission Control.

CBWFQ

class-based weighted fair queuing. Extends the standard WFQ functionality to provide support for user-defined traffic classes.

CE

customer edge. Identifies the network devices, connected to a provider network, that are under the administrative control of the customer.

CHAP

Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access.

CO

central office. The local telephone company office to which all local loops in a given area connect and in which circuit switching of subscriber lines occurs.

CoS

class of service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages. In SNA subarea routing, CoS definitions are used by subarea nodes to determine the optimal route to establish a given session. A CoS definition comprises a virtual route number and a transmission priority field. Also called ToS.

CPE

customer premises equipment. Terminating equipment such as terminals, telephones, and modems supplied by the telephone company, installed at customer sites, and connected to the telephone company network. Can also refer to any telephone equipment residing on the customer site.

CQ

custom queuing.

CSU

channel service unit. Digital interface device that connects end-user equipment to the local digital telephone loop. Often referred to together with DSU, as *CSU/DSU*.

DCE

data communications equipment (EIA expansion) (*common term*).

DHCP

Dynamic Host Configuration Protocol (*common term*). Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DMVPN

Dynamic Multipoint VPN.

DSL

digital subscriber line (*common term*). Public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel.

DSLAM

DSL access multiplexer.

DSU

data service unit. Device used in digital transmission that adapts the physical interface on a DTE device to a transmission facility, such as T1 or E1. The DSU also is responsible for such functions as signal timing. Often referred to together with CSU, as *CSU/DSU*.

DTE

data terminal equipment (*common term*). Device at the user end of a user-network interface that serves as a data source, destination, or both. DTE connects to a data network through a DCE device (for example, a modem) and typically uses clocking signals that are generated by the DCE. DTE includes devices such as computers, protocol translators, and multiplexers.

E1

Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps. E1 lines can be leased for private use from common carriers.

EBGP

Exterior Border Gateway Protocol

E-carrier

E-carrier is a European digital transmission format. It is the equivalent of the North American T-carrier system format.

EGP

exterior gateway protocol.

EIGRP

Enhanced Interior Gateway Routing Protocol. It's the advanced version of IGRP developed by Cisco. It provides superior convergence properties and operating efficiency, and it combines the advantages of link-state protocols with those of distance vector protocols.

Ethernet

Baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mbps. Ethernet is similar to the IEEE 802.3 series of standards. It is the most commonly used LAN technology because its protocol is easy to understand, implement, manage, and maintain. It allows low-cost network implementations, provides extensive topological flexibility for network installation, and guarantees successful interconnection and operation of standards-compliant products, regardless of manufacturer.

FFS

flash file system.

FIFO queuing

first-in, first-out queuing (*common term*). Involves buffering and forwarding of packets in the order of arrival. FIFO embodies no concept of priority or classes of traffic. There is only one queue, and all packets are treated equally. Packets are sent out an interface in the order in which they arrive.

Frame Relay

Industry-standard, packet-switched data link layer protocol that handles multiple virtual circuits between connected devices.

FTP

File Transfer Protocol. Protocol for exchanging files over the Internet.

GET VPN

GET VPN or Group Encrypted Transport VPN is a tunnel-less VPN technology. GET VPN is the Cisco implementation of GDOI (Group Domain of Interpretation), specified in RFC 6407.

GRE

Generic Routing Encapsulation. It's a tunneling protocol that was developed by Cisco that can encapsulate a variety of protocol packet types inside IP tunnels. This process creates a virtual point-to-point link to Cisco routers at remote points over an IP network.

HDLC

High-Level Data Link Control. Bit-oriented synchronous data link layer protocol developed by ISO. Derived from SDLC, HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

IANA

Internet Assigned Numbers Authority. Organization operated under the auspices of the ISOC as a part of the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the InterNIC and other organizations. IANA also maintains a database of assigned protocol identifiers that is used in the TCP/IP stack, including autonomous system numbers.

IBGP

Internal Border Gateway Protocol.

ICMP

Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information that is relevant to IP packet processing. Documented in RFC 792.

IEEE 802.11

A set of standards for implementing WLAN computer communications in the 2.4-, 3.6-, and 5-GHz frequency bands.

IETF

Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC.

IGP

interior gateway protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP.

IKE

Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPsec) that require keys. Before any IPsec traffic can be passed, each router, firewall, or host must verify the identity of its peer. Verification can be done by manually entering pre-shared keys into both hosts or by a CA service.

ILMI

Integrated Local Management Interface.

IoT

Internet of Things.

IP

Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.

IP address

A 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. CIDR provides a new way of representing IP addresses and subnet masks. Also called an Internet address.

IPCP

IP Control Protocol. This network control protocol establishes IP over PPP.

IPsec

IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

IPv4

IP version 4 *(common term)*. Internet Protocol version 4 is the fourth version in the development of IP and the first version of the protocol to be widely deployed. Along with IPv6, IPv4 is at the core of standards-based internetworking methods of the Internet. IPv4 is still used to route most traffic across the Internet. IPv4 is a connectionless protocol for use on packet-switched link layer networks (for example, Ethernet). It operates on a best-effort delivery model in that it does not guarantee delivery and does not assure proper sequencing or avoidance of duplicate delivery.

IPv6

IP version 6 *(common term)*. Replacement for the current version of IP (version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

IPX

Internetwork Packet Exchange. NetWare network layer (Layer 3) protocol used for transferring data from servers to workstations. IPX is similar to IP and XNS.

ISDN

Integrated Services Digital Network. Communication protocol offered by telephone companies that permits telephone networks to carry data, voice, and other source traffic.

ISP

Internet service provider. Company that provides Internet access to other companies and individuals.

IWAN

Intelligent WAN

IXP

Internet exchange point.

LAN

local-area network. High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.

LCP

link control protocol. a protocol that establishes, configures, and tests data-link connections for use by PPP.

LLQ

low latency queuing. provides a strict priority queue mechanism to CBWFQ.

MAC

Media Access Control. The lower of the two sublayers of the data link layer that is defined by the IEEE. The MAC sublayer handles access to shared media, such as whether token passing or contention will be used.

MAC address

a standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. A MAC address is 6 bytes long and is controlled by the IEEE. It is also known as a hardware address, MAC layer address, and physical address.

MD5

Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPsec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

MIB

Management Information Base. A database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP. The value of an MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MLP

Multilink PPP. A method of splitting, recombining, and sequencing datagrams across multiple logical data links.

MPLS

Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

MQC

modular QoS CLI. A command line structure that allows modular configuration of QoS configuration elements to provide independence between classification and policy.

multicast

single packets that are copied by the network and sent to a specific subset of network addresses. These addresses are specified in the Destination Address field.

NAT

Network Address Translation. A mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating these addresses into globally routable address space. Also known as Network Address Translator.

NBAR

Network-Based Application Recognition. A Cisco protocol discovery and classification mechanism that performs Layers 4 through 7 classification of IP packets.

NBAR2

Next-generation Network-Based Application Recognition.

NCP

Network Control Protocol. A series of protocols for establishing and configuring different network layer protocols, such as for AppleTalk over PPP.

NETCONF

Network Configuration Protocol.

NFV

Network Function Virtualization.

NMS

network management system. A system that is responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

NVRAM

nonvolatile RAM. RAM that retains its contents when a unit is powered off.

ONF

Open Networking Foundation.

OSI

Open Systems Interconnection. International standardization program created by ISO and ITU-T to develop standards for data networking that facilitate multivendor equipment interoperability.

OSPF

Open Shortest Path First.
Link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the IS-IS protocol.

P router

provider router.

PADI

PPPoE Active Discovery Initiation.

PADO

PPPoE Active Discovery Offer.

PADR

PPPoE Active Discovery Request.

PADS

PPPoE Active Discovery Session-confirmation.

PAK

Product Authorization Key.

PAP

Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and the host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access but merely identifies the remote end. The router or access server then determines whether that user is allowed access. PAP is supported only on PPP lines.

PCMCIA

Personal Computer Memory Card International Association. Standard used for credit-card-sized computer peripherals. Type I devices are very thin memory cards, Type 2 devices include most modems and interfaces, and Type 3 devices are used for disk drives and thicker components.

PDLM

Packet Description Language Module. A file that can be installed on an NBAR-capable device to extend the list of protocols that NBAR can recognize.

PE

provider edge. Identifies the network devices, under the administrative control of the provider, that connect to CE devices.

PID

product identifier.

POP

point of presence. In OSS, a physical location where an interexchange carrier installed equipment to interconnect with a local exchange carrier (LEC).

POST

power-on self test. Set of hardware diagnostics that runs on a hardware device when this device is powered on.

PPP

Point-to-Point Protocol. Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

PPPoE

PPP over Ethernet.

PQ

priority queuing. A queuing algorithm in which queues are serviced in a strict order based on priority. A lower priority queue is not serviced until all higher priority queues are empty.

PSK

preshared key. Shared secret key that is used during IKE authentication.

PSTN

public switched telephone network. General term referring to the variety of telephone networks and services in place worldwide. Sometimes called POTS.

QoE

quality of experience.

QoS

quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

rcp

remote copy protocol. Protocol that allows users to copy files to and from a file system residing on a remote host or server on the network. The rcp protocol uses TCP to ensure the reliable delivery of data.

RED

random early detection.

RFC

Request for Comments. Document series that is used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some RFCs are humorous or historical. RFCs are available online from numerous sources.

RIP

Request in Progress.

RJ-45

"Registered Jack-45" is an eight-wire connector that is commonly used to connect computers onto a LAN.

ROM

read-only memory. Nonvolatile memory that can be read, but not written, by the microprocessor.

RPC

remote-procedure call. Technological foundation of client/server computing. RPCs are procedure calls that are built or specified by clients and are executed on servers, with the results returned over the network to the clients.

RSVP

Resource Reservation Protocol. A network-control protocol that allows endpoints to request specific QoS for their data flows.

SDN

software-defined networking.

SHA

Secure Hash Algorithm.

SIMM

single in-line memory module

SLA

service level agreement.

SNMP

Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMPv1

Simple Network Management Protocol Version 1.

SNMPv2

SNMP Version 2. Version 2 of the popular network management protocol. SNMP2 supports centralized as well as distributed network management strategies, and includes improvements in the SMI, protocol operations, management architecture, and security.

SNMPv2c

SNMPv2c is the community string-based administrative framework for SNMPv2. Community string is a type of password, which is transmitted in cleartext. SNMPv2c is an update of the protocol operations and data types of party-based Simple Network Management Protocol Version 2 (SNMPv2p) and uses the community-based security model of SNMPv1.

SNMPv3

Simple Network Management Protocol Version 3.

SSH

Secure Shell Protocol. Protocol that provides a secure remote connection to a route through a TCP application.

SSL

Secure Socket Layer. Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

STP

Spanning Tree Protocol. Bridge protocol that uses the spanning-tree algorithm, enabling a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange BPDU messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning Tree Protocol standard and the earlier Digital Equipment Corporation Spanning Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital version.

syslog

system logging.

T1

digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network, using AMI or B8ZS coding.

T-carrier

TDM transmission method, usually referring to a line or a cable carrying a DS-1 signal.

TCP

Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

TDM

time-division multiplexing. Technique in which information from multiple channels can be allocated bandwidth on a single wire based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.

Telnet

standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log into remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.

TFTP

Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).

TID

Traffic Identifier

ToS

type of service.

Tx

transmit or transmitting.

UDI

unique device identifier.

UDP

User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

VLAN

virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VoIP

Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323. A primary attraction of VoIP is its ability to reduce expenses, because phone calls travel over the data network rather than over the phone company network.

VPLS

Virtual Private LAN Service.

VPN

virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.

VPWS

Virtual Private Wire Service.

WAN

wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.

WFQ

weighted fair queuing. Congestion management algorithm that identifies conversations (in the form of traffic streams), separates packets that belong to each conversation, and ensures that capacity is shared fairly between these individual conversations. WFQ is an automatic way of stabilizing network behavior during congestion and results in increased performance and reduced retransmission.

WRED

weighted random early detection. Queuing method that ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

X.25

ITU-T standard that defines how connections between DTE and DCE are maintained for remote terminal access and computer communications in PDNs. X.25 specifies LAPB, a data link layer protocol, and PLP, a network layer protocol. Frame Relay has to some degree superseded X.25.

