ARBA MINCH UNIVERSITY

INSTITUTE OF TECHNOLOGY

FACULTY OF COMPUTING AND SOFTWARE ENGINEERING

Degree Program: *Information Technology*

Module Name: Network design, configuration and administration

Course code: ITec4114

Course Title: Network device and configuration

Prepared By: ***Mr, Amanuel Bahiru(MSc)***

Arba Minch University, Arba Minch, Ethiopia

March, 2023

Table of Contents

Course Title : Network Device and Configuration

Course description

This course is designed on introducing students to different network devices and their characteristics. In addition network device installation and maintenance will be discussed in the course.

Course Objective

After completion of this course student will be able to:

- Discover Foundry network devices
- Advanced knowledge on network device configuration
- Create and configure VLANs
- Monitor changes to Foundry network devices
- Store and retrieve network events
- Configure router
- Configure and manage switch
- Implement and configure network protocols
- Mangling network

CHAPTER ONE

DEVICE CONFIGURATION

1.1. Configuration Wizard

While the configuration wizard is an easy way to display complex configuration options, it does rely on the user having a basic understanding of the software component.

Network Devices

Computer networking devices are units that mediate data in a computer network and are also called network equipment. Units that are the last receiver or generate data are called hosts or data terminal equipment.
Network Models It was developed by the International Organization for Standardization (ISO). It was first introduced in the late 1970s. It is a model for a computer protocol architecture and as a framework for developing protocol standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model.

OSI Model

The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software. It comprises of seven layers.

Advantages:

- Network communication is broken into smaller, more manageable parts.
- Allows different types of network hardware and software to communicate with each other.
- All layers are independent and changes does not affect other layers.
- Easier to understand network communication.

Why layered communication?

- To reduce complexity of communication task by splitting it into several layered small tasks
- assists in protocol design
- changes in one layer do not affect other layers
- provides a common language

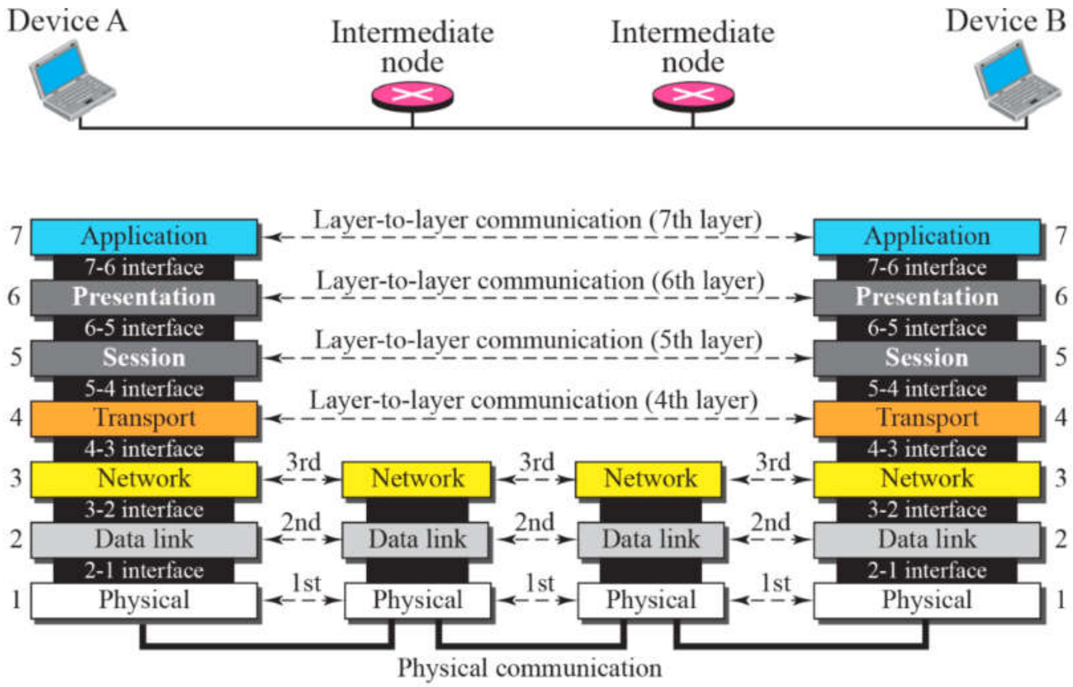


Figure 1. 1 OSI model

LAYER 1: PHYSICAL LAYER

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device. It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.

- Define physical characteristics of network. E.g. wires, connector, voltages, data rates, Asynchronous, Synchronous Transmission.
- Handles bit stream or binary transmission.
- Used to maintain, activate and deactivate physical link.
- For receiver it reassembles bits and send to upper layer for frames.

For Sender it convert frames into bit stream and send on transmission medium.

LAYER 2: DATA LINK

At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer. The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

- Packages raw bits from the physical layer into FRAMES.
- The data link layer provides reliable transit of data across a physical link by using the Media Access Control (MAC) addresses. Source & Destination (address of device that connects one Network to next) address.
- Flow Control: Prevent overwhelming of Receiving Node.
- Error Control: Through Trailer
- Access Control: Which device to have control
- Data Link LAN specifications: Fast Ethernet, Token Ring, FDDI.
- Data Link WAN specifications are: Frame Relay, PPP, X.25.
- Bridges and Switches operate at this layer

Sub layers of Layer 2

- Logical link layer (LLC)
  - Used for communication with upper layers
  - Error correction
  - Flow control
- Media Access Control (MAC)
  - Access to physical medium
  - Header and trailer
  - Trailer: The trailer typically includes a frame check sequence (FCS), which is used to perform error detection.

LAYER 3: NETWORK

The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

- Defines source to destination delivery of packets across NWs.
- Defines logical addressing and best path determination.
- Treat each packet independently
- Defines how routing works and how routes are learned
- Converts frames to packets
- Routed protocols (encapsulate data into packets) and Routing protocols (create routing tables) work on this layer
- Examples of Routed protocols are: IP, IPX, AppleTalk and Routing protocols are OSPF, IGRP/EIGRP, RIP, BGP
- Routers operate at Layer 3.

LAYER 4: TRANSPORT

The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.

- It regulates information flow to ensure process-to- process connectivity between host applications reliably and accurately
- Adds service point address or Port address
- Segmentation & Re-assembly: SEGMENTS data from sending node and reassembles data on receiving node
- Flow control / Error control at Source to destination level
- Connection oriented transport service ensures that data is delivered error free, in sequence with no losses or duplications
- Establishes, maintains and terminates virtual circuits
- Connection oriented / Connectionless:

TCP (Reliable, provides guaranteed delivery),
UDP (Unreliable, less overhead, reliability can be provided by the Application layer)

Provides multiplexing: the support of different flows of data to different applications on the same host

LAYER 5: SESSION

The session layer controls the conversations between different computers. A session or connection between machines is set up and managed at layer 5. Session layer services also include authentication and reconnections.

- The session layer defines how to start, control and end conversations (called sessions) between applications
- Establishes dialog control between the two computers in a session, regulating which side transmits, plus when and how long it transmits (Full duplex)
- Synchronization: Allows processes to add check points. E.g. Insert check point at every 100 page of 2000 page file to ensure that each 100-page unit is received & acknowledged
- Transmits Data

LAYER 6: PRESENTATION

The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it at times also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer.

- Presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
- This layer is primarily responsible for the translation, encryption and compression of data.
- Defines coding and conversion functions
- This layer also manages security issues by providing services such as data encryption and data compression
- Examples of these formats and schemes are: MPEG, QuickTime, ASCII, EBCDIC, GIF, TIFF, JPEG

LAYER 7: APPLICATION

At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication.

- The application layer is responsible for providing services to the user
- Closest to the user and provides user interface
- Establishes the availability of intended communication partners
- Examples of Application layer protocols are: Telnet, SMTP, FTP, SNMP

Layer 1 Vs Layer 2

Layer 1 cannot communicate with upper layers	Layer 2 does this using LLC
Layer 1 cannot identify computer	Layer 2 uses addressing process
Layer 1 can only describe stream of bits	Layer 2 uses framing to organize bits

Data Encapsulation

Data Encapsulation is the process of adding a header to wrap/envelop the data that flows down the OSI model. The 5 Steps of Data Encapsulation are:

1. The Application, Presentation and Session layers create DATA from users' input.
2. The Transport layer converts the DATA to SEGMENTS
3. The NW layer converts the Segments to Packets (datagram)
4. The Data Link layer converts the PACKETS to FRAMES
5. The Physical layer converts the FRAMES to BITS.

Some of application layer protocols and their functions
Simple Mail Transfer Protocol (SMTP)

- Governs the transmission of mail messages and attachments
- SMTP is used in the case of outgoing messages
- More powerful protocols such as POP3 and IMAP4 are needed and available to manage incoming messages
- POP3(Post Office Protocol version 3) is the older protocol
- IMAP4(Internet Mail Access Protocol version 4) is the more advanced protocol

Telnet:

- It allows a user on a remote client machine, called the Telnet client, to access the resources of another machine, the Telnet server, in order to access a command-line interface.

File Transfer Protocol (FTP)

- File Transfer Protocol (FTP) actually lets us transfer files, and it can accomplish this between any two machines using it.
- FTP's functions are limited to listing and manipulating directories, typing file contents, and copying files between hosts.

Simple Network Management Protocol (SNMP)

- Simple Network Management Protocol (SNMP) collects and manipulates valuable network information.

Hypertext Transfer Protocol (HTTP)

- It's used to manage communications between web browsers and web servers and opens the right resource when you click a link, wherever that resource may actually reside.

Hypertext Transfer Protocol Secure (HTTPS)

- Hypertext Transfer Protocol Secure (HTTPS) is also known as Secure Hypertext Transfer Protocol. It uses Secure Sockets Layer (SSL).

Domain Name Service (DNS)

- Domain Name Service (DNS)resolves hostnames—specifically, Internet names, such as www.wcu.edu.et

Dynamic Host Configuration Protocol (DHCP)

- Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to hosts dynamically.
- It allows for easier administration and works well in small to very large network environments.

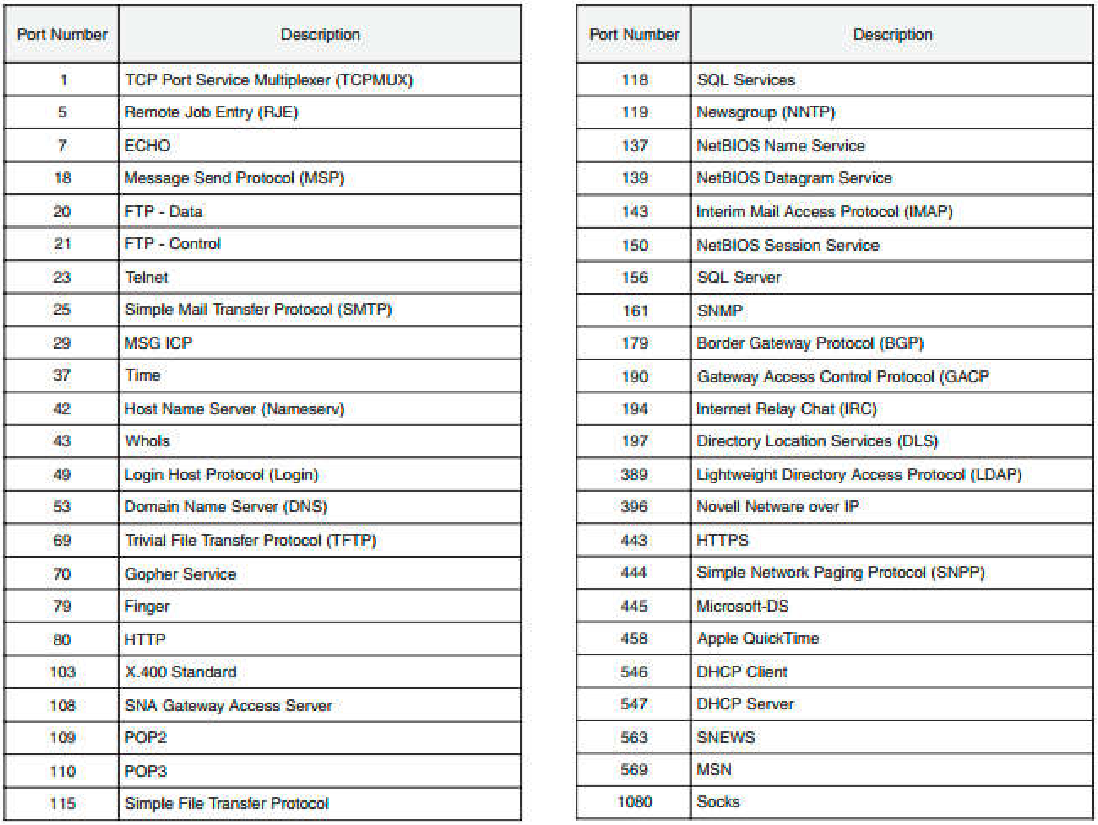
Some of Transport layer protocols and their functions

TCP (Transmission Control Protocol)

- TCP: takes large blocks of information from an application and breaks them into segments.
- It is Connection oriented means that a virtual connection is established before any user data is transferred. (handshake)

User Datagram Protocol (UDP)

- UDP does not sequence the segments and does not care about the order in which the segments arrive at the destination.
- UDP just sends the segments off and forgets about them.



Port Number	Description
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP - Data
21	FTP - Control
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	WhoIs
49	Login Host Protocol (Login)
53	Domain Name Server (DNS)
69	Trivial File Transfer Protocol (TFTP)
70	Gopher Service
79	Finger
80	HTTP
103	X.400 Standard
108	SNA Gateway Access Server
109	POP2
110	POP3
115	Simple File Transfer Protocol
118	SQL Services
119	Newsgroup (NNTP)
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
150	NetBIOS Session Service
156	SQL Server
161	SNMP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP
194	Internet Relay Chat (IRC)
197	Directory Location Services (DLS)
389	Lightweight Directory Access Protocol (LDAP)
396	Novell Netware over IP
443	HTTPS
444	Simple Network Paging Protocol (SNPP)
445	Microsoft-DS
458	Apple QuickTime
546	DHCP Client
547	DHCP Server
563	SNEWS
569	MSN
1080	Socks

Table 1. 1 Well-Known TCP Port Numbers

Network device

Hub

Hubs connect computers together in a star topology network. Due to their design, they increase the chances for collisions. Hubs operate in the physical layer of the OSI model and have no intelligence. Hubs flood incoming packets to all ports all the time. For this reason, if a network is connected using hubs, the chances of a collision increases linearly with the number of computers (assuming equal bandwidth use).

Hubs cannot filter data so data packets are sent to all connected devices/computers and do not have intelligence to find out best path for data packets. This leads to inefficiencies and wastage.

Bridge

In telecommunication networks, a bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol. Having a single incoming and outgoing port and filters traffic on the LAN by looking at the MAC address, bridge is more complex than hub. Bridge looks at the destination of the packet before forwarding unlike a hub. It restricts transmission on other LAN segment if destination is not found. Bridge works at the data-link (physical network) level of a network, copying a data frame from one network to the next network along the communications path. It used to connect two subnetworks that use interchangeable protocols. It combines two LANs to form an extended LAN. The main difference between the bridge and repeater is that the bridge has a penetrating efficiency.

- Transparent Bridges: It is also called learning bridges. Bridge construct its table of terminal addresses on its own as it implements connecting two LANs. It facilitates the source location to create its table. It is self-updating. It is a plug and plays bridge. Transparent Bridges is invisible to the other devices on the network. Transparent Bridge only perform the function of blocking or forwarding data based on MAC address. MAC address may also be referred as hardware address or physical address. These addresses are used to built tables and make decision regarding whether a frame should be forward and where it should be forwarded.
- Source Routing Bridge: Source-route Bridges were designed by IBM for use on Token ring networks. The SR Bridge derives the entire route of the frame embedded within the frame. This allows the Bridge to make specific decision about how the frame should be forwarded through the network. This sending terminal means the bridges that the frames should stay. This type of bridge is used to prevent looping problem.
- Translational Bridge: Translational Bridges are useful to connect segments running at different speeds or using different protocols such as token Ring and Ethernet networks. Depending on the direction of travel, a Translational Bridge can add or remove information and fields from frame as needed.

Repeater

A repeater is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances without degradation. Because repeaters work with the actual physical signal, and do not attempt to interpret the data being transmitted, they operate on the physical layer, the first layer of the OSI model. Repeaters are majorly employed in long distance transmission to reduce the effect of attenuation. It is important to note that repeaters do not amplify the original signal but simply regenerate it.

Modem

Modem (from modulator-demodulator) is a device that turns the digital 1s and 0s of a personal computer into sounds that can be transmitted over the telephone lines

NIC (Network Interface Card)

A network interface card is a computer hardware component designed to allow computers to communicate over a computer network. It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly. Most motherboards today come equipped with a network interface card in the form of a controller, with the hardware built into the board itself, eliminating the need for a standalone card.

Switch

A switch when compared to bridge has multiple ports. Switches can perform error checking before forwarding data, which are very efficient by not forwarding packets that error-end out or forwarding good packets selectively to correct devices only. Switches can support both layer 2 (based on MAC Address) and layer 3 (Based on IP address) depending on the type of switch. Usually large networks use switches instead of hubs to connect computers within the same subnet.

¬ A switch operates in the layer 2, i.e. data link layer of the OSI model.
¬ It is an intelligent network device that can be conceived as a multiport network bridge.
¬ It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
¬ It uses packet switching technique to receive and forward data packets from the source to the destination device.
¬ It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
¬ Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
¬ Switches are active devices, equipped with network software and network management capabilities.
¬ Switches can perform some error checking before forwarding data to the destined port.
¬ The number of ports is higher – 24/48.

Types of Switches

There are variety of switches that can be broadly categorized into 4 types:

- Unmanaged Switch − these are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices needs to be added, more switches are simply added by this plug and play method. They are referred to as unmanaged since they do not require to be configured or monitored. Unmanaged switches are generally made as plug-and-play devices and require little to no special installation beyond an Ethernet cable. The setup of this type of switch relies on auto-negotiation between Ethernet devices to enable communication between them. The switch will automatically determine the best data rate to use, switching between full-duplex mode (where data is received or transmitted in two directions at the same time) or half-duplex mode (where data is received or transmitted two ways but only one direction at a time).
- Managed Switch − these are costly switches that are used in organizations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches. A managed switch is exactly what it sounds like—a switch that requires some oversight by a network administrator. This type of

switch gives you total control over the traffic accessing your network while allowing you to custom-configure each Ethernet port so you get maximum efficiency over data transfers on the network. Managed switches are also typically the best network switches to support the Gigabit standard of Ethernet rather than traditional Fast Ethernet.

- LAN Switch − Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.
- PoE Switch − Power over Ethernet (PoE) switches are used in PoE Gigabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections. A PoE switch distributes power over the network to different devices. This means any device on the network, from PCs to IP cameras and smart lighting systems, can function without the need to be near an AC access point or router, because the PoE switch sends both data and power to the connected devices.

Media Converter

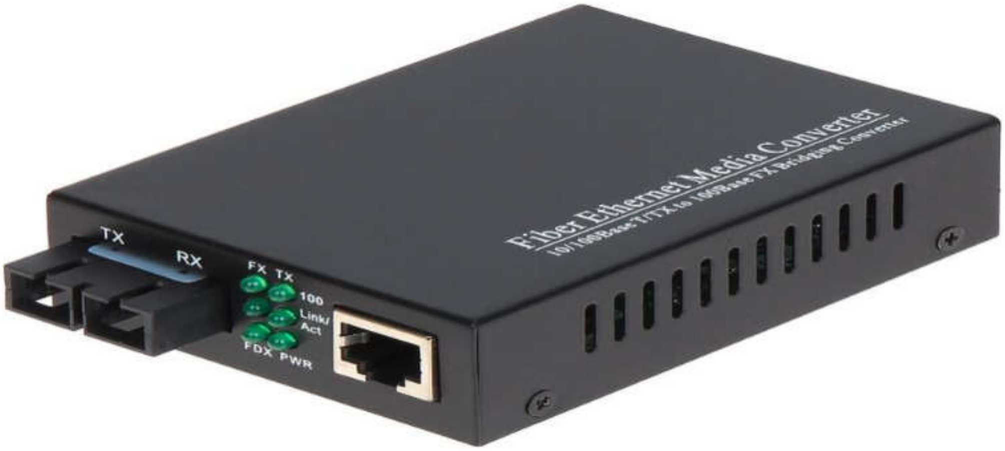
A media converter, in the context of network hardware, is a cost-effective and flexible device intended to implement and optimize fiber links in every kind of network. Among media converters, the most often used type is a device that works as a transceiver, which converts the electrical signal utilized in copper unshielded twisted pair (UTP) network cabling to light waves used for fiber optic cabling. It is essential to have the fiber optic connectivity if the distance between two network devices is greater than the copper cabling is transmission distance.

The copper-to-fiber conversion carried out by a media converter allows two network devices having copper ports to be connected across long distances by means of fiber optic cabling. Media converters are available as Physical Layer or Layer 2 switching devices, and can provide rate-switching and other advanced switching features like VLAN tagging. Media converters are typically protocol specific and are available to support a wide variety of network types and data rates.

Media converters can also convert between wavelengths for Wavelength Division Multiplexing (WDM) applications. Deployed in Enterprise, Government, Data Center, and Telecom Fiber to the x networks, media converters have become the Swiss army knife of networking to enable connectivity and fiber distance extension.

The Benefits of Media Converters

Network complexity, demanding applications, and the growing number of devices on the network are driving network speeds and bandwidth requirements higher and forcing longer distance requirements within the Local Area Network (LAN). Media converters present solutions to these problems, by allowing the use of fiber when it is needed, and integrating new equipment into existing cabling infrastructure. Media converters provide seamless integration of copper and fiber, and different fiber types in Enterprise LAN networks. They support a wide variety of protocols, data rates and media types to create a more reliable and cost-effective network.

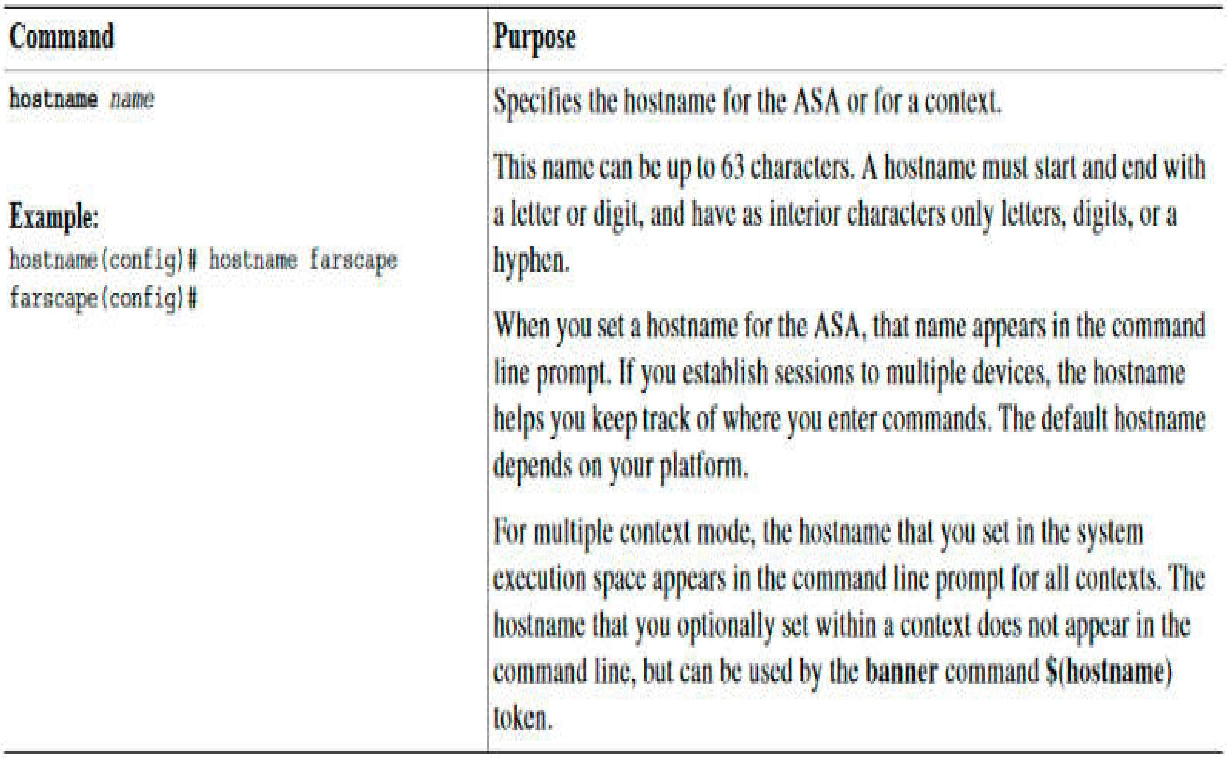


Fiber Ethernet Media Converter
10/100Base T/TX to 100Base FX Bridging Converter
TX
RX
FX
TX
100
Link/Act
FDX
PWR

Figure 1. 2 Multi-mode media converter

Configuring Basic Settings

Setting the Hostname



Command	Purpose

hostname *name*
Example:
`hostname(config)# hostname farscape`
`farscape(config)#`
	Specifies the hostname for the ASA or for a context.
	This name can be up to 63 characters. A hostname must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen.
	When you set a hostname for the ASA, that name appears in the command line prompt. If you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands. The default hostname depends on your platform.
	For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts. The hostname that you optionally set within a context does not appear in the command line, but can be used by the **banner** command **$(hostname)** token.

Cisco switch by default have a host name “switch”. To change this name follow the instructions below:

1. Click on the Switch. A popup window will be opened.
2. Go to CLI tab in the popup window.
3. Click in command box.
4. Press “Enter”.
5. To enable the switch give following command: 1 | enable
6. To enable configuration mode give following command:
   1 | configure terminal
7. To change the host name give following command: 1 | hostname
8. To save the configuration give following command: 1 | do write memory
9. To exit the configuration mode give following command: 1 | exit
10. To exit enable mode give following command:
    1 | exit

Set or change password of cisco switch in cisco packet tracer

Cisco switch by default have no password. To set a password or change previous password follow the instructions below: Click on the Switch. A popup window will be opened. Go to CLI tab in the popup window. Click in command box. Press “Enter” .To enable the switch give following command: enable To enable.

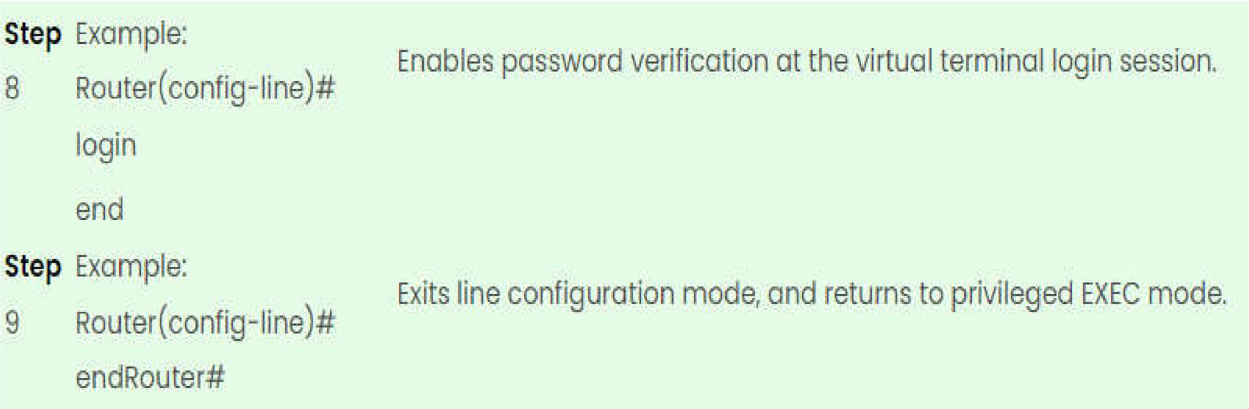
Configuring Command-Line Access

To configure parameters to control access to the router, perform the following steps.

SUMMARY STEPS

1. **configure terminal**
2. **line [aux | console | tty | vty] line-number**
3. **password password**
4. **login**
5. **exec-timeout minutes [seconds]**
6. **line [aux | console | tty | vty] line-number**
7. **password password**
8. **login**
9. **end**

	Command	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	line [aux | console | tty | vty] line-number Example: Router(config)# line console 0	Enters line configuration mode, and specifies the type of line.
Step 3	password password Example: Router(config)# password 5dr4Hepw3	Specifies a unique password for the console terminal line.
Step 4	login Example: Router(config-line)# login	Enables password verification at the terminal login session.
Step 5	exec-timeout minutes [seconds] Example: Router(config-line)# exec-timeout 5 30	Sets the interval that the EXEC command interpreter waits until user input is detected. The default is 10 minutes. You can also optionally add seconds to the interval value.
Step 6	line [aux | console | tty | vty] line-number Example: Router(config-line)# line vty 0 4	Specifies a virtual terminal for remote console access.
Step 7	password password Example: Router(config-line)# password aldf2ad1	Specifies a unique password for the virtual terminal line.



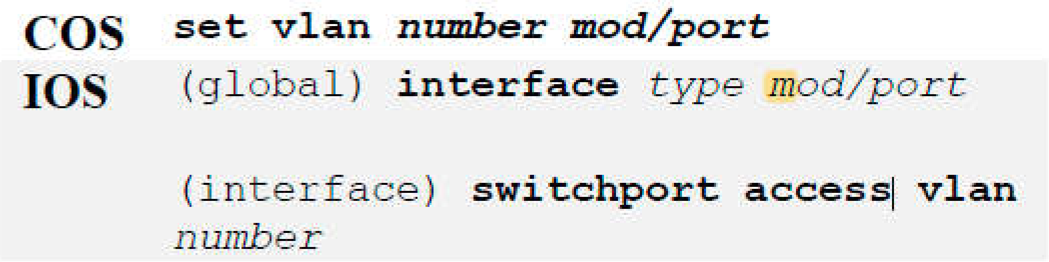
Step 8	Example: Router(config-line)# login end	Enables password verification at the virtual terminal login session.
Step 9	Example: Router(config-line)# endRouter#	Exits line configuration mode, and returns to privileged EXEC mode.

1.2. View VLANs by Device and Port

- VLANs are assigned to individual switch ports.
- Ports can be statically assigned to a single VLAN or dynamically assigned to a single VLAN.
- All ports are assigned to VLAN 1 by default
- Ports are active only if they are assigned to VLANs that exist on the switch.
- Static port assignments are performed by the administrator and do not change unless modified by the administrator, whether the VLAN exists on the switch or not.
- Dynamic VLANs are assigned to a port based on the MAC address of the device plugged into a port.
- Dynamic VLAN configuration requires a VLAN Membership Policy Server (VMPS) client, server, and database to operate properly.

Configuring Static VLANs

On a Cisco switch, ports are assigned to a single VLAN. These ports are referred to as access ports and provide a connection for end users or node devices, such as a router or server. By default, all devices are assigned to VLAN 1, known as the default VLAN. After creating a VLAN, you can manually assign a port to that VLAN and it will be able to communicate only with or through other devices in the VLAN. Configure the switch port for membership in a given VLAN as follows:



```
COS   set vlan number mod/port
IOS   (global) interface type mod/port

      (interface) switchport access vlan
      number
```

To change the VLAN for a COS device, use the set vlan command, followed by the VLAN number, and then the port or ports that should be added to that VLAN. VLAN assignments such as this are considered static because they do not change unless the administrator changes the VLAN configuration.

For the IOS device, you must first select the port (or port range for integrated IOS) and then use the switchport access vlan command followed by the VLAN number.

Configuring Dynamic VLANs

Although static VLANs are the most common form of port VLAN assignments, it is possible to have the switch dynamically choose a VLAN based on the MAC address of the device connected to a port. To achieve this, you must have a VTP database file, a VTP server, a VTP client switch, and a dynamic port. After you have properly configured these components, a dynamic port can choose the VLAN based on whichever device is connected to that port.

Configuring a VLAN based on ports allows PCs in the VLAN to communicate with each other. Application Environment: A company has multiple departments located in different buildings. For service security, it is required that employees in one department be able to communicate with each other, whereas employees in different departments be prohibited from communicating with each other. Devices on the network shown in the following figure. Add ports connecting devices to PCs of the financial department to VLAN 5 and ports connecting devices to PCs of the marketing department to VLAN 9. This configuration prevents employees in financial and marketing departments from communicating with each other.

Configure links between CE and PE as trunk links to allow frames from VLAN 5 and VLAN 9 to pass through, allowing employees of the same department but different buildings to communicate with each other. By configuring port-based VLANs on the PE, CE1, and CE2, employees in the same department can communicate with each other, whereas employees in different departments cannot.

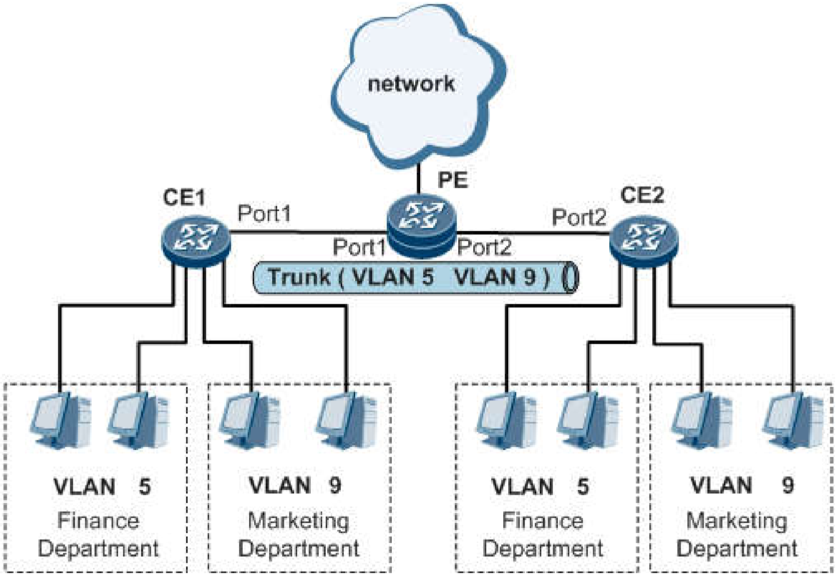


Figure 1. 3 Networking diagram for configuring a VLAN based on ports

Pre-configuration Tasks

Before configuring a VLAN based on ports, complete the following task: Connecting ports and configuring physical parameters of the ports, ensuring that the ports are physically Up.

Configuration Procedures

Figure 8-6 Procedure of configuring a VLAN based on ports

Figure 8-6 Procedure of configuring a VLAN based on ports

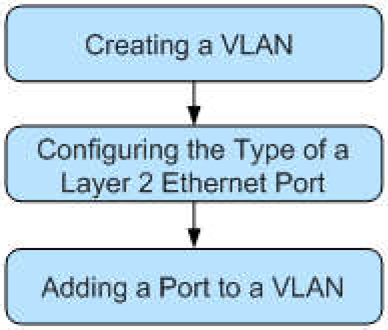


Figure 1. 4 Procedure of configuring a VLAN based on ports

After a VLAN profile is created, assign it to switches, aggregation devices in a Junos Fusion fabric, Virtual Chassis Fabric, members of Layer 3 Fabric, or members of custom groups. You must have one or more existing VLAN profiles, either user-configured or system-created, before you can assign a VLAN profile to a switch, or member of a custom group or port group.

1.3. Automatic Discovery and Configuration Manager

Configuration management is a process closely linked to change management, which is also called configuration control. Any system that needs to be controlled closely and run with good reliability, maintainability and performance benefits greatly from configuration management, i.e., the management of system information and system changes. Configuration management can extend life, reduce cost, reduce risk, and even correct defects. It should be applied over the life cycle of a system in order to provide visibility and control of its performance as well as its functional and physical attributes.

In Configuration Manager 2012, the discovery of users, groups and devices has been improved since Configuration Manager 2007. The discovery feature in Configuration Manager 2012 enables you to identify computer and user resources that can be managed with Configuration Manager. You are able to configure the discovery of resources on different levels in the Configuration Manager 2012 hierarchy.

Active Directory Forest Discovery

The Active Directory Forest Discovery is a new discovery method in Configuration Manager 2012 that allows the discovery of Active Directory Forest where the site servers reside and any trusted forest. With this discovery method, you are able to automatically create the Active Directory or IP subnet boundaries that are within the discovered Active Directory Forests.

Active Directory Forest Discovery can be configured on Central Administration Sites and Primary Sites.

1.4. Wireless Mobility Configuration Menu

A Mobility Domain enables users to roam geographically across the system while maintaining data sessions and VLAN or subnet membership, including IP address, regardless of connectivity to the network backbone. As users move from one area of a building or campus to another, client associations with servers or other resources remains the same.

The clustering functionality ensures mobility across an entire wireless network. With clustering, you can effortlessly create logical groups of controllers and access points, which share network and user information in a proactive manner for continuous and uninterrupted support.

You can create a mobility domain using the Create Mobility Domain window from the Network Director User interface.

A Mobility Group is a group of Wireless LAN Controllers (WLCs) in a network with the same Mobility Group name. These WLCs can dynamically share context and state of client devices, WLC load information, and can forward data traffic among them, which enables inter-controller wireless LAN roam and controller redundancy. Before you add controllers to a mobility group, you must verify that certain requirements are met for all controllers that are to be included in the group.

A Mobility Group is configured manually. The IP and MAC address of the Wireless LAN Controllers (WLCs) that belong to the same Mobility Group are configured on each of the WLCs individually. Mobility Groups can be configured either through the CLI or through the GUI. Mobility Groups can also be configured with the Prime Infrastructure (PI). This alternative method comes in handy when a large number of WLCs is deployed. No Wireless LAN Controllers (WLCs) can be configured only in one Mobility Group.

A Mobility Group can include up to 24 WLCs of any type. The number of access points supported in a Mobility Group is bound by the number of WLCs and WLC types in the group. For example, if a controller supports 6000 access points, a mobility group that consists of 24 such controllers supports up to 144,000 access points (24 * 6000 = 144,000 access points).

You can add different mobility members that are part of a different Mobility Group into the mobility list that is used for mobility anchors that can anchor within a different Mobility Group. There can be up to 72 members in the list with up to 24 in the same Mobility Group.

In a mobility list, the below combinations of mobility groups and members are allowed:

- 3 mobility groups with 24 members in each group
- 12 mobility groups with 6 members in each group
- 24 mobility groups with 3 members in each group
- 72 mobility groups with 1 member in each group

Configuring Mobility Groups (Cisco Wireless LAN Controllers)

To add an entry to a controller mobility configuration using the GUI, go to CONTROLLER > Mobility Management > Mobility Groups, and click on New. Here you enter the MAC address and IP address of the controller management interface you are adding along with the mobility group name of that controller.

Mobility, or roaming, is a wireless LAN client's ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible.

Mobility group is a set of controllers, identified by the same mobility group name that make seamless roaming for wireless clients. By creating a mobility group, we can enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers in the same mobility group can share the context and state of client devices as well as their list of access points so that they do not consider each other's access points as rogue devices.

Wireless access point

A wireless access point (WAP or AP) is a device that allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth or related standards. The WAP usually connects to a wired network, and can relay data between the wireless devices (such as computers or printers) and wired devices on the network.

Basic firewall A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting outward communication. It is also a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria.

Routers

- A router, like a switch forwards packets based on address.
- Usually, routers use the IP address to forward packets, which allows the network to go across different protocols.
- Routers forward packets based on software while a switch (Layer 3 for example) forwards using hardware called ASIC (Application Specific Integrated Circuits).
- Routers support different WAN technologies but switches do not.
- Besides, wireless routers have access point built in.
- The most common home use for routers is to share a broadband internet connection.
- As the router has a public IP address which is shared with the network, when data comes through the router, it is forwarded to the correct computer.

1.5. Device Schedules

Owing to the increasing need for massive data analysis and model training at the network edge, as well as the rising concerns about the data privacy, a new distributed training framework called federated learning (FL) has emerged. In each iteration of FL (called round), the edge devices update local models based on their own data and contribute to the global training by uploading the model updates via wireless channels. Due to the limited spectrum resources, only a portion of the devices can be scheduled in each round.

In order to take a backup of your device configurations, you need to first discover your devices using Network Configuration Manager. The tool also allows you to add devices in bulk. Once the devices are discovered, you can proceed to scheduling network backups. Device configurations need to be backed up often in order to maintain a repository of backups ready to be restored in case of emergencies. In large enterprises with more number of devices, this task of getting the device configuration backup up becomes a huge mundane task taking up most of the time of an admin. Being able to schedule configuration backups is used to free up a network admin's time to do productivity enhancing tasks.

1.6. VPN Policy Manager

A virtual private network (VPN) is a private data network connection that makes use of the public telecommunications infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. Using a virtual private network involves maintaining privacy through the use of authorization, authentication, and encryption controls that encrypt da ta before sending it through the public network and decrypting it at the receiving end. In a site-to-site configuration, a VPN can be contrasted with a system of owned or leased lines that can only be used by one company. In a remote user configuration, a VPN can be contrasted to a privately managed remote access system (e.g. dial-up). The concept of the VPN is to give the agency the same capabilities at much lower costs by using the shared public infrastructure rather than a private one. However, VPN links are considered to be less trusted than dedicated, private connections; therefore, this policy sets forth the security requirements for VPN connections to the State's network.

VPN's enable an organization to use public networks such as the internet, to provide a secure connection among the organization's wide area network. Customers can use VPN's to connect an enterprise Intranet to a wide area network comprised of partners, customers, resellers and suppliers. Traditionally, business have relied on private 56-Kbps or T-1 leased lines to connect remote offices together. Leased lines are expensive to install and maintain. For small companies, the cost is just too high. Using the internet as a backbone, A VPN can securely and cost effectively connect all of companies' offices, telecommuters, mobile workers, customers, partners and suppliers.

Overview of how it Works

- Two connections – one is made to the Internet and the second is made to the VPN.

- Datagrams – contains data, destination and source information.
- Firewalls – VPNs allow authorized users to pass through the firewalls.
- Protocols – protocols create the VPN tunnels.

VPN Gateway and Tunnels

A VPN gateway is a network device that provides encryption and authentication service to a multitude of hosts that connect to it. From the outside (internet), all communications addressed to inside hosts flow through the gateway. There are two types of endpoint VPN tunnels:

- Computer to gateway

For remote access: generally set up for a remote user to connect A corporate LAN

- Gateway to Gateway

This is a typical enterprise-to-enterprise configuration. The two gateways communicate with each other

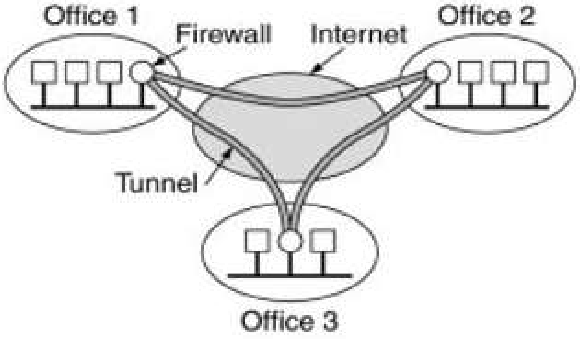


Figure I. 5 Types of endpoint VPN tunnels

1.7. Element Manager

Importance of Managing Network Devices

- Configuration Management
- Performance Management
- Fault Management

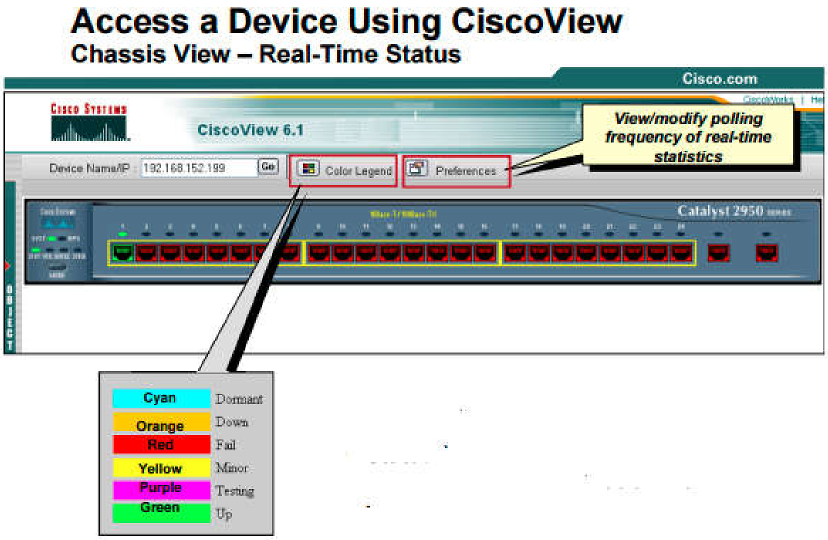
Common ways to analyze the configuration, Performance and Faults on a Cisco Device

- CLI (Command Line Interface)

- SNMP (Simple Network Management Protocol)
- CiscoView

Using SNMP and CiscoView:

- A user can define a VTP domain,
- Configure devices as VTP servers, clients, or transparent devices in the domain,
- Create VLANs within the domain,
- Assign ports to a VLAN, and view the ports assigned to a VLAN.



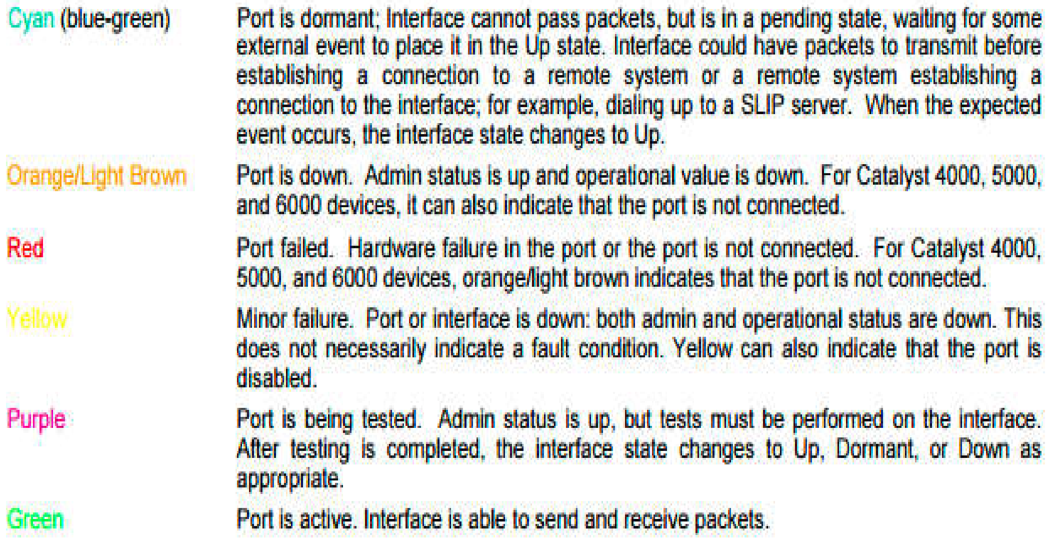
Access a Device Using CiscoView

Chassis View – Real-Time Status

View/modify polling frequency of real-time statistics

Cyan	Dormant
Orange	Down
Red	Fail
Yellow	Minor
Purple	Testing
Green	Up

Figure I. 6 Access a device using CiscoView



Cyan (blue-green)	Port is dormant; Interface cannot pass packets, but is in a pending state, waiting for some external event to place it in the Up state. Interface could have packets to transmit before establishing a connection to a remote system or a remote system establishing a connection to the interface; for example, dialing up to a SLIP server. When the expected event occurs, the interface state changes to Up.
Orange/Light Brown	Port is down. Admin status is up and operational value is down. For Catalyst 4000, 5000, and 6000 devices, it can also indicate that the port is not connected.
Red	Port failed. Hardware failure in the port or the port is not connected. For Catalyst 4000, 5000, and 6000 devices, orange/light brown indicates that the port is not connected.
Yellow	Minor failure. Port or interface is down: both admin and operational status are down. This does not necessarily indicate a fault condition. Yellow can also indicate that the port is disabled.
Purple	Port is being tested. Admin status is up, but tests must be performed on the interface. After testing is completed, the interface state changes to Up, Dormant, or Down as appropriate.
Green	Port is active. Interface is able to send and receive packets.

1.8. CLI Configuration Manager

Configuration Manager can be run from a command line. You want to run the Configuration Manager from the commend line as opposed to using the graphical user interface because of the following reasons:

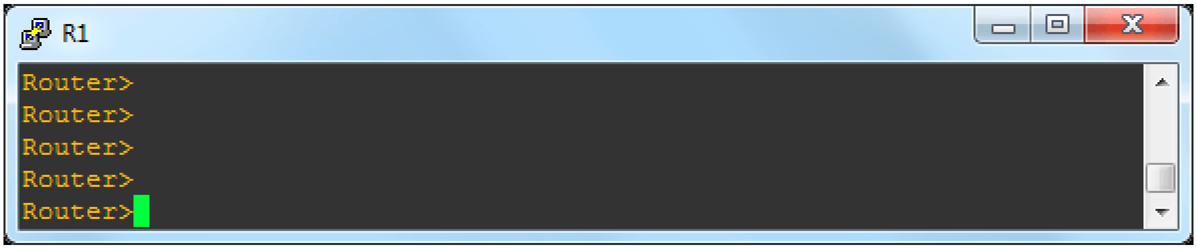
- You want to automate the configuration of the software.
- Your site wants the command-line version run for security reasons.
- You want to create a script to set up your system and then allow a user to run the script.

You begin by generating the configuration XML files that define the application server, the profile type, and the XML file path. You then edit the files to enter values for your environment.

Understanding Cisco IOS Command Line Modes

Cisco Command Line Interface (CLI) is the main interface where we will interact with Cisco IOS devices. CLI is accessible directly via console cable or remotely via methods such as Telnet/SSH. From here, we can do things such as monitoring device status or changing configuration. Cisco has divided its CLI into several different modes. Understanding Cisco IOS Command Line Modes is essential because each mode has its own set of commands. Cisco has at least three main command line modes: user EXEC mode, privileged EXEC mode, and global configuration mode. Of course, there are other more specific modes such as interface configuration mode, extended ACL configuration mode, routing/VLAN configuration mode, etc.

User EXEC mode



```
Router>
Router>
Router>
Router>
Router>
```

By default this is where we begin the session with our Cisco IOS devices (unless a specific privilege level has been granted to our user account).

The characteristics of user EXEC mode are:

- Indicated by a right angle bracket sign (“>”) next to the device hostname.
- Contains commands that we can use to test device/network configuration such as ping and traceroute.
- A limited set of commands that are not changing the device configuration such as the show and clear command are available.
- We can connect to other device from user EXEC mode by using telnet or ssh
- To protect user EXEC mode we can create username and password combination on the device.
- Issuing exit command here will disconnect the session.

This flowchart below will show the position of each node against the other modes.

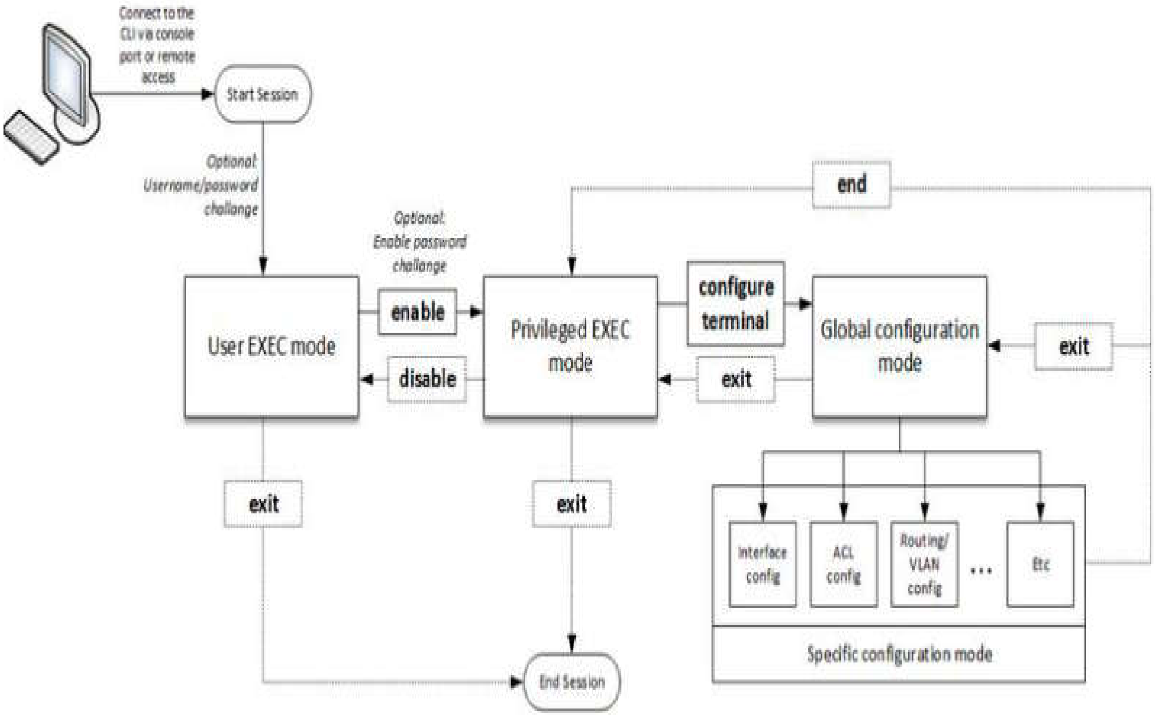
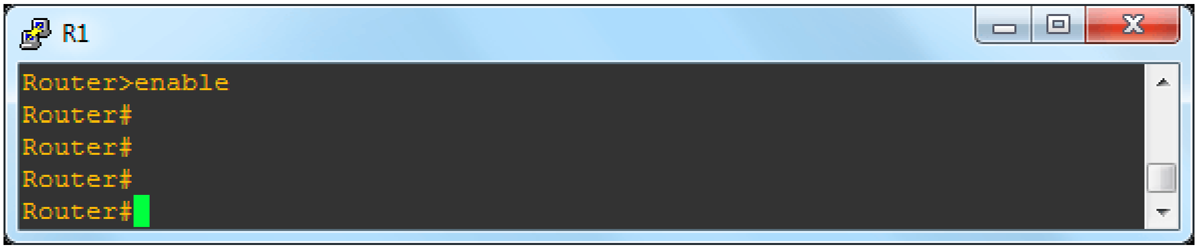

Connect to the CLI via console port or remote access
Start Session
Optional: Username/password challenge
Optional: Enable password challenge
User EXEC mode
enable
disable
Privileged EXEC mode
configure terminal
exit
Global configuration mode
end
exit
exit
exit
Interface config
ACL config
Routing/ VLAN config
...
Etc
Specific configuration mode
End Session

Figure 1. 7 Cisco IOS Command Line Modes

Privileged EXEC mode



```
Router>enable
Router#
Router#
Router#
Router#
```

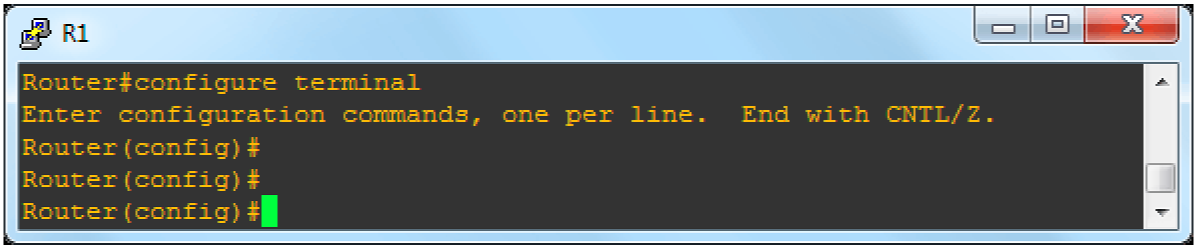
Basically, privileged EXEC mode contains the complete command of what we got in user EXEC mode. In this mode, we still cannot do any configuration changes. However, the configuration mode can only be accessed from privileged EXEC mode. Privileged EXEC mode is activated after we use command enable on user EXEC mode.

Below are the characteristics of privileged EXEC mode:

- Indicated by a hash sign ("#") next to the device hostname
- All commands that are available on user EXEC mode are available in here too

- More complete set of commands under show and clear command are available here. For example, in user EXEC mode there is no show running-config under the show command, but in privileged EXEC mode it is exist.
- Unless the user account that we used has specific privilege level assigned to it, by default it will get the highest privilege level, which is level 15.
- Privileged EXEC mode can be protected using an enable password.
- Issuing disable command here will bring us back to the user EXEC mode.
- Issuing exit command here will disconnect the session.

Global configuration mode



```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#
```

This is where the real configurations are done. We can enter global configuration mode from privileged EXEC mode by using command configure terminal. From here we can do changes on the global device configuration such as hostname, domain-name, creating user accounts, etc; or we can enter more specific configuration within global configuration mode and make changes such as IP address interface, access-list, DHCP, policy, etc.

Some characteristics of global configuration mode are:

- Indicated by device hostname prompt, followed by a word "config" inside a bracket and then hash sign ("#").
- All commands from EXEC mode can be used here by adding a word do before the command that we want to execute, for example if we want to use show running-config in global configuration mode we have to type it as do show running-config.
- Despite that we can change configuration within global configuration mode, if we want to save the configuration we have to do it by exiting back to privileged EXEC mode and issue command write memory or copy running-config startup-startup config from there (however, these two commands can also be used from within global configuration mode by adding a do prefix to the command, as explained in the previous point).
- Global configuration mode can be protected by assigning a custom privilege level to the user account then set allowed commands and block the rest, thus limiting the configuration capability.
- Issuing exit here will bring us back to the privileged EXEC mode.

To change a device configuration, you need to enter the global configuration mode. This mode can be accessed by typing configure terminal (or conf t, the abbreviated version of the command) from the enable mode. The prompt for this mode is hostname(config).

Global configuration mode commands are used to configure a device.

You can set a hostname, configure authentication, set an IP address for an interface, etc.

From this mode, you can also access sub modes, for example the interface mode, from where you can configure interface options. You can get back to a privileged EXEC mode by typing the end /exit command. You can also type CTRL + C to exit the configuration mode.

Sub mode Commands

A global configuration mode contains many sub-modes. For example, if you want to configure an interface you have to enter that interface configuration mode. Each sub mode contains only commands that pertain to the resource that is being configured.

To enter the interface configuration mode you need to specify which interface you would like to configure. This is done by using the interface INTERFACE_TYPE/INTERFACE_NUMBER global configuration command, where INTERFACE_TYPE represents the type of an interface (Ethernet, Fast Ethernet, Serial…) and INTERFACE_NUMBER represents the interface number, since Cisco devices usually have more than one physical interface.

Once inside the interface configuration mode, you can get a list of available commands by typing the "?" character.

Each sub mode has its own prompt.

CHAPTER TWO

ROUTER AND SWITCH

2.1. Basic Configuration

Routers: are small electronic devices that join multiple computer networks together via either wired or wireless connections.

Figure 2. 1 Routers

Both Router and Switch are the connecting devices in networking. The main objective of router is to connect various networks simultaneously and it works in network layer, whereas the main objective of switch is to connect various devices simultaneously and it works in data link layer.

Switch connects multiple devices to create a network; a router connects multiple switches, and their respective networks, to form an even larger network. These networks may be in a single location or across multiple locations. Here is the arrangement of switch and router.

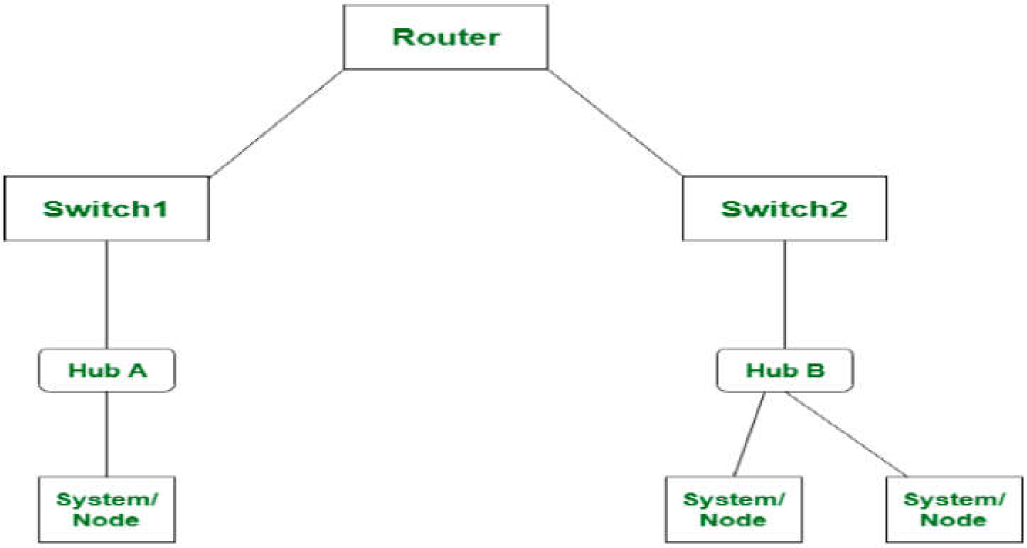


Figure 2. 2 The arrangement of switch and router

The difference between router and switch.

No.	Router	Switch
1	The main objective of router is to connect various networks simultaneously.	While the main objective of switch is to connect various devices simultaneously.
2	It works in network layer.	While it works in data link layer.
3	Router is used by LAN as well as MAN.	While switch is used by only LAN.
4	Through router, data is sent in the form of packet.	While through switch, data is sent in the form of packet and frame.
5	There is less collision take place in router.	While there is no collision, take place in full duplex switch.
6	Router is compatible with NAT.	While it is not compatible with NAT.
7	The types of routing are: Adaptive and Non-adaptive routing.	The types of switching are Circuit, Packet and Message Switching.

A network switch (also called switching hub, bridging hub, officially MAC Bridge) is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device. Unlike less advanced network hubs, a network switch forwards data only to one or multiple devices that need to receive it, rather than broadcasting the same data out of each of its ports.

A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality that most commonly uses IP addresses to perform packet forwarding; such switches are commonly known as layer-3 switches or switches. Beside most commonly used Ethernet switches, they exist for various types of networks, including Fiber Channel, Asynchronous Transfer Mode, and Infini Band.

Figure 2. 3 Switch

How Routers Work

In technical terms, a router is a Layer 3 network gateway device, meaning that it connects two or more networks and that the router operates at the network layer of the OSI model. Routers contain a processor (CPU), several kinds of digital memory, and input- output (I/O) interfaces. They function as special-purpose computers, one that does not require a keyboard or display.

The router's memory stores an embedded operating system (O/S). Compared to general-purpose OS products like Microsoft Windows or Apple Mac OS, router operating systems limit what kind of applications can be run on them and also need much smaller amounts of storage space.

Examples of popular router operating systems include Cisco Internetwork Operating System (IOS) and DD-WRT. These operating systems are manufactured into a binary firmware image and are commonly called router firmware.

By maintaining configuration information in a part of memory called the routing table, routers also can filter both incoming and outgoing traffic based on the addresses of senders and receivers.

Types of Routers and Routing Devices

A class of portable Wi-Fi router is called travel routers are marketed to people and families who want to use the functions of a personal router at other locations besides home. Routing devices called mobile hotspots that share a mobile (cellular) Internet connection with Wi-Fi clients are also available. Many mobile hotspot devices only work with certain brands of cell service.

How to accesses a router

1. Connect the router to the modem: The router sends the modem's internet connection to any computer connected to its network. Ensure that both the modem and the router have their power cables plugged in. Plug one end of a network cable into your modem. Plug the other end into the port on your router labeled Internet, WAN, or WLAN. The labels will vary depending on the type of router you have.
2. Install the software: Depending on the router brand and model, you may or may not receive software to install on the computer. This software is typically an interface to connect to the router and adjust the settings, though it is not required.
3. Connect your computer to the router: You can do this either through an Ethernet cable or over Wi-Fi. If this is your first time setting the router up, then connect your computer via Ethernet so that you can configure the wireless network.

Typically, the Ethernet ports on the Router are labeled 1, 2, 3, 4, etc. but any port not labeled "WAN," "WLAN," or "Internet" will work. Connect the other end of the cable to the Ethernet port on your computer.

Routing Mechanisms mater

How does a router learn about paths (routes) to destinations? There are several routing mechanisms that may be used as input sources to assist a router in building its route table. Typically, routers use a combination of the following routing methods to build a router's route table:

- Directly connected interface
- Static
- Default
- Dynamic

Although there are specific advantages and disadvantages for implementing them, they are not mutually exclusive.

Directly Connected Interface

These routes come from the active router interfaces. Routers add a directly connected route when an interface is configured with an IP address and is activated. Directly connected interfaces are routes that are local to the router. That is, the router has an interface directly connected to one or more networks or subnets. These networks are inherently known through the routers configured interface attached to that network. These networks are immediately recognizable and traffic directed to these networks can be forwarded without any help from routing protocols.

Static Routing

Static routing is a type of network routing technique. Static routing is not a routing protocol; instead, it is the manual configuration and selection of a network route, usually managed by the network administrator. It is employed in scenarios where the network parameters and environment are expected to remain constant. Static routing is only optimal in a few situations. Network degradation, latency and congestion are inevitable consequences of the non-flexible nature of static routing because there is no adjustment when the primary route is unavailable.

Static routes are routes to destination hosts or networks that an administrator has manually entered into the router's route table. Static routes define the IP address of the next hop router and local interface to use when forwarding traffic to a particular destination.

Because this type of route has a static nature, it does not have the capability of adjusting to changes in the network. If the router or interface defined fails or becomes unavailable, the route to the destination fails.

This type of routing method has the advantage of eliminating all traffic related to routing updates. Static routing tends to be ideal where the link is temporary or bandwidth is an issue, so you want to use this method for dial-up networks or point-to-point WAN links. You can implement static routes in conjunction with other routing methods to provide routes to destinations across dial backup links when primary links implementing dynamic routing protocols have failed.

To design an entire network with only this method because you would have to enter a static route on every router for each network they are not directly attached to, thus highly impractical. In addition, if a link or a router within the internetwork fails or is added, you would have to reconfigure each router, removing the failed route or adding a new route. Meanwhile, routers obviously cannot forward traffic to that destination because the original path has become invalid. Static routing can have an extreme amount of overhead in the form of intense administrative hours spent getting the network up and keeping it going.

You want to implement static routes in very small-to-small networks, with perhaps as little as 10 to 15 links total. Even then, dynamic routes offer so much more versatility.

Static routes conserve bandwidth because they do not cause routers to generate route update traffic; however, they tend to be time consuming because a system administrator has to manually update routes when changes occur in the network.

Static routes are also ideal for a stub network providing a single dedicated point-to- point WAN connection outside the network to an upstream ISP (Internet Service Provider) providing Internet access.

Configuring Static Routing

Example: – IP addresses of router interfaces connecting Routers B and C to A. It also shows Router A's interface types, such as S0 and S1 (Serial 0 and Serial 1), which indicates the specific interfaces on Router A connected to these links.

Default

In computer networking, the default route is a configuration of the Internet Protocol (IP) that establishes a forwarding rule for packets when no specific address of a next-hop host is available from the routing table or other routing mechanisms. Or the route that takes effect when no other route is available for an IP destination address. If a packet is received on a routing device, the device first checks to see if the IP destination address is on one of the device's local subnets. If the destination address is not local, the device checks its routing table. If the remote destination subnet is not listed in the routing table, the packet is forwarded to the next hop toward the destination using the default route. The default route generally has a next-hop address of another routing device, which performs the same process. The process repeats until a packet is delivered to the destination.

The default route is generally the address of another router, which treats the packet the same way: if a route matches, the packet is forwarded accordingly; otherwise, the packet is forwarded to the default route of that router. The route evaluation process in each router uses the longest prefix match method to obtain the most specific route. The network with the longest subnet mask or network prefix that matches the destination IP address is the next-hop network gateway. The process repeats until a packet is delivered to the destination host, or earlier along the route, when a router has no default route available and cannot route the packet otherwise. In the latter case, the packet is dropped and an ICMP Destination Unreachable message may be returned. Each router traversal counts as one hop in the distance calculation for the transmission path.

Dynamic Routing

Dynamic routing is a networking technique that provides optimal data routing. Unlike static routing, dynamic routing enables routers to select paths according to real-time logical network layout changes. In dynamic routing, the routing protocol operating on the router is responsible for the creation, maintenance and updating of the dynamic routing table. In static routing, all these jobs are manually done by the system administrator.
Dynamic routing uses multiple algorithms and protocols. The most popular are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

Typically, dynamic routing protocol operations can be explained as follows:

1. The router delivers and receives the routing messages on the router interfaces.
2. The routing messages and information are shared with other routers, which use exactly the same routing protocol.
3. Routers swap the routing information to discover data about remote networks.
4. Whenever a router finds a change in topology, the routing protocol advertises this topology change to other routers.

Dynamic routing is easy to configure on large networks and is more intuitive at selecting the best route, detecting route changes and discovering remote networks. However, because routers share updates, they consume more bandwidth than in static routing; the routers' CPUs and RAM may also face additional loads because of routing protocols. Finally, dynamic routing is less secure than static routing.

Benefits of Router

- Due to the collision feature, network traffic can be reduced.
- Due to broadcasting domains, network traffic can be reduced.
- It provides a MAC address and IP address that will choose the best route across a network.
- Easy to connect to the wired or wireless network.
- Highly secured with a password.
- No loss of information.
- It can connect to different network architecture such as Ethernet cable, Wi-Fi, WLAN.
- The wireless router is easy to connect to the internet for a laptop or pc. No need to worry about a bunch of wires.

2.2. Passwords

The Wi-Fi network password' is the password that you use to join the wireless network. Unless you have set your network to "No security", you are already using a Wi-Fi network password. If you are using the router's default password or a memorable one that you have set yourself, then you should consider replacing this password with a strong password. Remember, that we do not consider the router's default password to be strong.

The router's admin account is the account that you use to log into the router to make configuration changes. Your router shipped with a default "admin" password. To upgrade the "admin" account with a strong password, go to the ADMINISTRATION section. It is usually the first option. On most routers, you can also change the administrator user name from admin. This will make things harder for hackers, but if you've got a 12 character strong password in place, then having people be able to guess what your admin user id is called isn't going to do them much good.

Reason why you should change your router's default password

The first reason is router's default password is printed on the side of the router, and so is on display to anyone within touching distance of the unit. As we already know, sharing passwords or leaving passwords in sight is absolutely not good security practice. Given that our highly important network password is on view to everyone walking past it, we need to change the default as a matter of urgency.

Second, in creating network passwords, router manufacturers often prefer convenience over security. This means that they will prefer shorter passwords over longer ones. Shorter passwords are easier to discover (by a method known as brute-force) than longer ones. Whilst all router manufacturers have different standards for default password generation (and some may be secure), we will always err on the side of caution and assume that the default Wi-Fi network password is going to be easy for attackers to discover, and replace it with something strong and unique.

2.3. Wildcard Masks

A wildcard mask is a mask of bits that indicates which parts of an IP address are available for examination. A wildcard Mask matches everything in the network portion of an IP address with a Zero. Also note the two rules: 0-bit = match and 1-bit = ignore. Wildcard mask can be used to target a specific host/IP address, entire network, subnet, or even a range of IP addresses. For example if we wanted to target, a specific host every bit in the hosts IP address must match. As we mentioned earlier a 0-bit is a match and a 1-bit = ignore. Therefore, to target Wildcard Mask for the host is 0.0.0.0.

Example: To target a specific network every bit in the 'Network' portion of the IP address must be a match. Therefore, if a class C network has the IP 192.168.1.0 the wildcard Mask would be 0.0.0.255. From these examples, you can see the benefit of using Wildcard Masks. They are different from subnet masks in that they can target a specific Host, specific IP address, specific Network, specific Subnet, or a range of IP addresses. They can even target all even or all odd networks. All of these capabilities make the Wildcard Mask much more flexible than the Subnet mask.

A wildcard mask can be thought of as an inverted subnet mask. For example, a subnet mask of 255.255.255.0 (binary equivalent = 11111111.11111111.11111111.00000000) inverts to a wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111).

What is the wild card n access-list in networking?

Wildcard mask is a 32-bit quantity used in conjunction with an IP address to determine which bits in an IP address should be ignored when comparing that address with another IP address. Wildcard masks use the following rules to match binary 1s and 0s:

- Wildcard mask bit 0: Match the corresponding bit value in the address.
- Wildcard mask bit 1: Ignore the corresponding bit value in the address.

Wildcard masking for access lists operates differently from an IP subnet mask. A zero in a bit position of the access list mask indicates that the corresponding bit in the address must be checked; a one in a bit position of the access list mask indicates the corresponding bit in the address is not 'interesting' and can be ignored.

Wildcard subnet mask is used in the following occasion.

- Defining subnet in ACL
- Defining subnet member in OSPF area

Counter Example

Let's say you have the following subnet.

192.168.24.0/24
or 192.168.24.0 with 255.255.255.0 subnet mask

The binary format of the subnet mask is the following
11111111.11111111.11111111.00000000

In binary arithmetic, inverse a number means “flipping” one state to the other (i.e from “on” to “off”, from “0” to “1”).

The inverse of the subnet mask in binary format is then the following
00000000.00000000.00000000.11111111

In decimal format, the inverse subnet mask looks like this 0.0.0.255

When you know, remember, or count the quantity of IP addresses or IP subnet within certain VLSM network; you should be able to quickly deduct how the wildcard or inverse subnet mask in question looks like. This way, you can skip the binary arithmetic and use strict decimal arithmetic to get you a much quicker result with much simpler way.

This FAQ presents two quick ways of finding out how the wildcard or inverse subnet mask looks like using simple decimal-number-based calculation of the quantity of available IP addresses or IP subnet within certain IPv4 VLSM network. Following is the list of ways.

255 Octet Subtraction

This is one way of doing the simple calculation. Note that when we do binary inverse, we do it octet by octet. Each octet has number from 0 to 255. To quickly find the inverse subnet mask, you can use the result of 255 subtracted by the given octet.

Here are illustrations
Example #1: 255.255.255.0
255 – 255 = 0
255 – 0 = 255

1. 255 255 255 255
2. 2.55.255.255.0
3. – ———————-
4. 0. 0. 0. 255

Inverse /24: 0.0.0.255
Example #2: 255.255.255.224
255 – 255 = 0
255 – 224 = 31

1. 255 255 255 255
2. 255.255.255.224

3. – ————————————
4. 0. 0. 0. 31

Inverse is 0.0.0.31
Example #3: 255.255.255.252
255 – 255 = 0
255 – 252 = 3

1. 255 255 255 255
2. 255.255.255.252
3. – ————————————
4. 0. 0. 0. 3

Inverse is 0.0.0.3

Host Number: -this is another way of finding inverse subnet mask. In /24 or smaller subnets, only last octet indicates the number of unique IP addresses exist within the subnet in question. Specifically for /30, the last octet indicates four unique numbers of IP addresses; from 0 to 3. Take the last number and apply that to inverse subnet mask.

As to the 1st three octets, they should "automatically" convert to 0 since only the last octet "matters" from number of IP address perspective in /24 or smaller subnets.

Here are illustrations
Example #1: 252 —> four IP addresses, from 0 to 3
Inverse is 0.0.0.3
Example #2: last octet: 224 —> 32 IP addresses, from 0 to 31
Inverse is 0.0.0.31

Working with Subnet Larger than /24

When you have subnet larger than /24, you need to consider other octets in addition to the last one. Using the 2nd method (the Host Number), you will apply the last number of each octet to the inverse.

Keep in mind that similar to Class C subnet calculation (/24 or smaller subnet), basic concept applies to Class B (/16 or smaller subnet up to /23) and Class A (/8 or smaller subnet up to /15) subnet calculations. When the first 3 octets in Class C subnet calculation are always constant and only last octet changes (as shown above), the first 2 and last octets in Class B subnet calculation are always constant where only the third octet changes. Similarly, the first and last two octets in Class A subnet calculation are always constant where only the second octet changes.

Here are illustrations

Example #1: 255.255.254.0
3rd octet: 254 —> two /24 subnets, from 0 to 1
4th octet: 0 —> 256 IP addresses, from 0 to 255

Inverse is 0.0.1.255

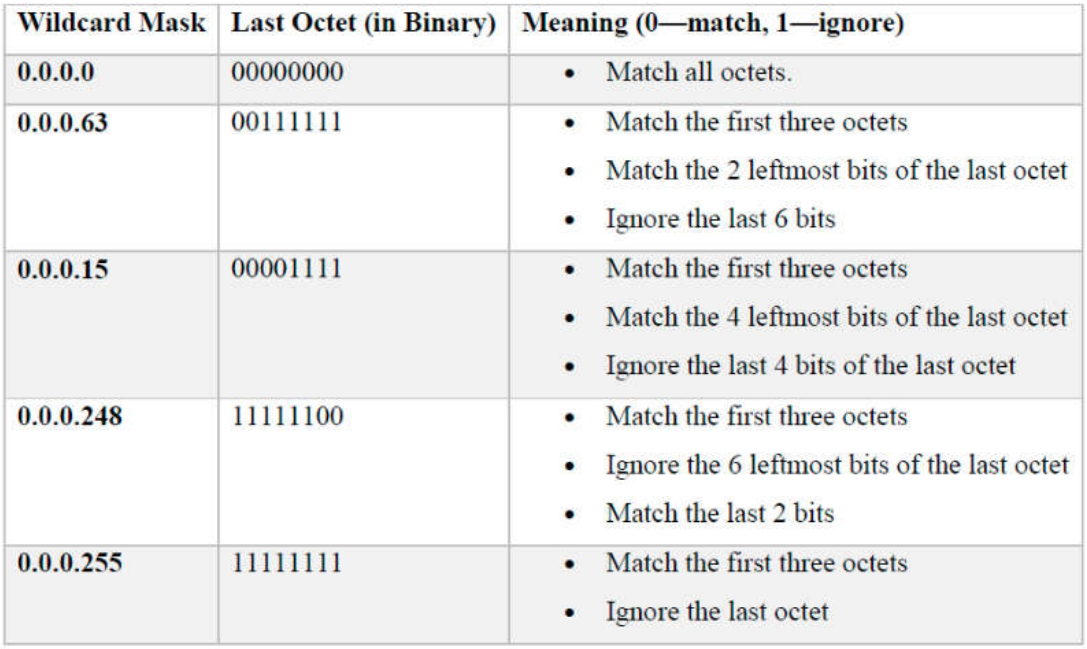
Example #2: 255.255.248.0
3rd octet: 248 —> eight /24 subnets, from 0 to 7
4th octet: 0 —> 256 IP addresses, from 0 to 255

Inverse is 0.0.7.255

Example #3: 192.0.0.0
1st octet: 192 —> sixty four /8 subnets, from 0 to 63
2nd, 3rd, 4th octets: 0 —> 0 to 255

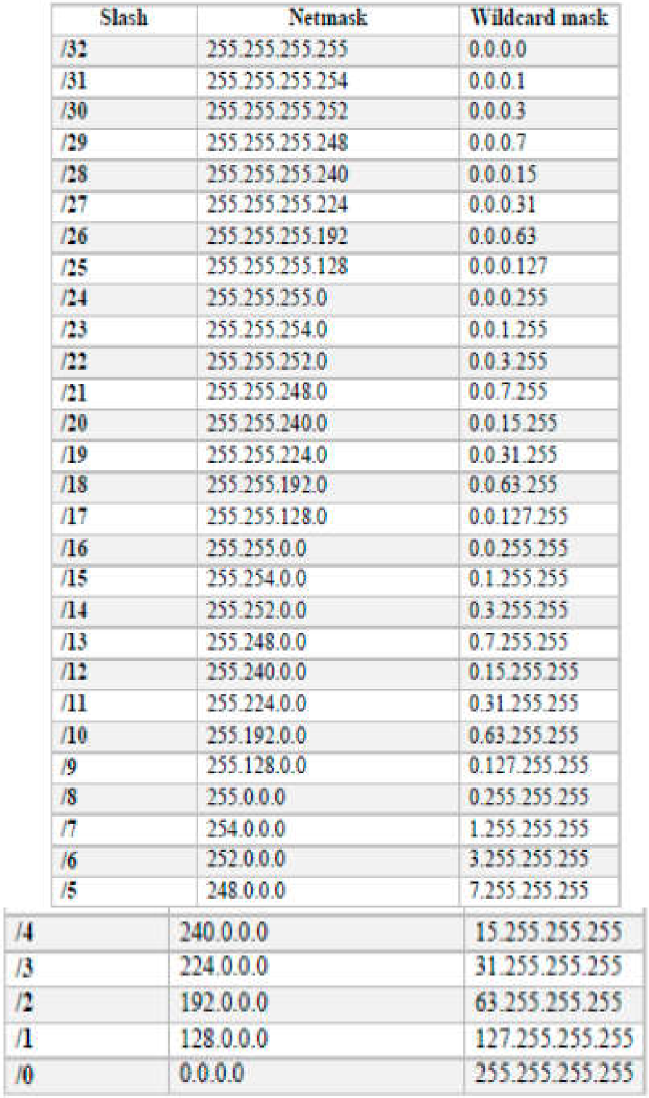
Inverse is 63.255.255.255

Note that the constants in Class A and B subnet calculation is slightly different than in the Class C subnet calculation. The constants in Class C subnet calculation, which are the first three octets, are all 0. In Class B subnet calculation, the constants are 0 for the first two octets while the last octet is constant 255. In Class A subnet calculation, the constant is 0 for the first octet while the last two octet's constant is 255.



Wildcard Mask	Last Octet (in Binary)	Meaning (0—match, 1—ignore)
0.0.0.0	00000000	• Match all octets.
0.0.0.63	00111111	• Match the first three octets • Match the 2 leftmost bits of the last octet • Ignore the last 6 bits
0.0.0.15	00001111	• Match the first three octets • Match the 4 leftmost bits of the last octet • Ignore the last 4 bits of the last octet
0.0.0.248	11111100	• Match the first three octets • Ignore the 6 leftmost bits of the last octet • Match the last 2 bits
0.0.0.255	11111111	• Match the first three octets • Ignore the last octet

Table 2. 2 Examples of Wildcard Masks



Slash	Netmask	Wildcard mask
/32	255.255.255.255	0.0.0.0
/31	255.255.255.254	0.0.0.1
/30	255.255.255.252	0.0.0.3
/29	255.255.255.248	0.0.0.7
/28	255.255.255.240	0.0.0.15
/27	255.255.255.224	0.0.0.31
/26	255.255.255.192	0.0.0.63
/25	255.255.255.128	0.0.0.127
/24	255.255.255.0	0.0.0.255
/23	255.255.254.0	0.0.1.255
/22	255.255.252.0	0.0.3.255
/21	255.255.248.0	0.0.7.255
/20	255.255.240.0	0.0.15.255
/19	255.255.224.0	0.0.31.255
/18	255.255.192.0	0.0.63.255
/17	255.255.128.0	0.0.127.255
/16	255.255.0.0	0.0.255.255
/15	255.254.0.0	0.1.255.255
/14	255.252.0.0	0.3.255.255
/13	255.248.0.0	0.7.255.255
/12	255.240.0.0	0.15.255.255
/11	255.224.0.0	0.31.255.255
/10	255.192.0.0	0.63.255.255
/9	255.128.0.0	0.127.255.255
/8	255.0.0.0	0.255.255.255
/7	254.0.0.0	1.255.255.255
/6	252.0.0.0	3.255.255.255
/5	248.0.0.0	7.255.255.255
/4	240.0.0.0	15.255.255.255
/3	224.0.0.0	31.255.255.255
/2	192.0.0.0	63.255.255.255
/1	128.0.0.0	127.255.255.255
/0	0.0.0.0	255.255.255.255

Table 2. 3 List of wildcard mask

2.4. Access Control Lists

An access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource. Access control lists are also installed in routers or switches, where they act as filters, managing which traffic can access the network.

It is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory).

Access control lists are used throughout many IT security policies, procedures, & technologies. An access control list is a list of objects; each entry describes the subjects that may access that object. Any access attempt by a subject to an object that does not have a matching entry on the ACL will be denied. Technologies like firewalls, routers, and any border technical access device are dependent upon access control lists in order to properly function. One thing to consider when implementing an access control list is to plan for and implement a routine update procedure for those access control lists.

Access Lists perform several functions within a router, including:

- Implement security / access procedures
- Act as a protocol "firewall"

Use Access Lists:

- Deny traffic you do not want based on packet tests (for example, addressing or traffic type)
- Identify packets for priority or custom queuing
- Restrict or reduce the contents of routing updates
- Provide IP traffic dynamic access control with enhanced user authentication using the lock-and-key feature
- Identify packets for encryption
- Identify Telnet access allowed to the router virtual terminals Specify packet traffic for dial-in remote sites using dial-on-demand routing (DDR)

Types of IPv4 ACLs
Standard and Extended ACLs

The previous sections describe the purpose of ACLs as well as guidelines for ACL creation. This section covers standard and extended ACLs and named and numbered ACLs, and it provides examples of placement of these ACLs.
There are two types of IPv4 ACLs:

- Standard ACLs: These ACLs permit or deny packets based only on the source IPv4 address.
- Extended ACLs: These ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports, and more.

The following example shows how to create a standard ACL. In this example, ACL 10 permits hosts on the source network 192.168.10.0/24. Because of the implied "deny any" at the end, all traffic except for traffic coming from the 192.168.10.0/24 network is blocked with this ACL.

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#
```

The following example shows, the extended ACL 100 permits traffic originating from any host on the 192.168.10.0/24 network to any IPv4 network if the destination host port is 80 (HTTP).

```
R1(config)# access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config)#
```

Notice that the standard ACL 10 is only capable of filtering by source address, while the extended ACL 100 is filtering on the source and destination Layer 3 and Layer 4 protocol (for example, TCP) information.

2.5. Remote Access

Remote access allows logging into a system as an authorized user without being physically present at its keyboard. Remote is commonly used on corporate computer networks but can also be utilized on home networks.
Remote working is the practice of completing your normal daily working life away from the office, using some form of technology and an internet connection. Commonly, this means working from home, often with a laptop employed to remotely connect to key systems, which may be in the office or hosted in the cloud.

Remote working is not typically limited by location. Assuming the user has access to technology and an internet connection, they could remotely work from anywhere; a partner's office, for example, or a roadside service station whilst away from the office on another job.

When an organization needs to provide employees or third parties remote access to its network, there are a number of solutions available.

1. **VPNs: Virtual Private Networks**

When employees need to remotely access their company files, a virtual private network (VPN) is often the tool of choice. VPNs are designed to give employees the online privacy and anonymity they (and their company) require, by turning a public internet connection into a private network. VPN software creates a "data tunnel" between the corporate network and an exit node in another location (such as your workplace), which may be anywhere in the world.

In other words, VPNs provide a kind of telepresence: they can make it seem as if you are at the office on your company machine with all of your applications and files at your disposal. To fully achieve its goals, a VPN must accomplish two important tasks:

- Create the connection or tunnel; and
- Protect that connection, so that your files (and your company's network) will not be compromised.

VPNs achieve this second step by encrypting data, these encryption and masking features help protect your online activities and keep them anonymous. Since VPN services establish secure and encrypted connections, an organization's employees can get the remote access they need with greater privacy than the public internet. However, let us face it: using an unsecured Wi-Fi network is simply not an option for company users, because your private information would be totally exposed to anyone snooping on that network.

For all these reasons, VPNs have become a popular option for companies who need to give their employees remote access, but want to provide online security and privacy.

The risks and drawbacks of VPNs

VPNs are certainly an improvement over using unprotected methods to remotely access an organization's network, and in certain business environments, they can provide a useful service. However, VPNs carry a number of drawbacks and inherent risks. Let us examine a few of the major issues.

- Not optimal for remote vendor access: While VPNs may be good for giving remote access to internal employees, it is not the optimal solution for three crucial tasks: identifying, controlling, and auditing third-party vendors. VPNs simply do not have the degree of granular control needed to properly monitor or restrict where a vendor can go and what they can do on a company's network.
- VPNs are exploited in major data breaches: A note of caution for those thinking of using VPNs: their reputation has suffered a major blow due to their implication in a number of serious data breaches. National news stories have reported on how hackers exploited VPNs to cause data breaches at several major companies. For example, in the case of data breaches suffered by Home Depot and Target, malicious actors apparently stole VPN credentials, giving them access to company networks, and the hackers also obtained an administrative credential. This combination let them infiltrate and move through company networks.
- VPNs are leveraged in multi-stage cyberattacks: Hackers have also exploited VPNs in prolonged multi-stage cyberattacks. VPNs are specifically mentioned by name in the alert as a major initial access point for hackers.
- Audit and compliance risks: Another drawback to using VPNs for remote access: they may expose organizations to compliance or regulatory risk. As cyberattacks have become more costly, sophisticated, and frequent, some policy-making groups have imposed tougher standards on their auditing processes and regulators are asking tougher questions about third-party access methods. Many remote access tools such as VPNs may not be able to provide the level of audit detail required and fail to meet these higher standards.

2. Desktop Sharing

Desktop sharing is another way organizations can provide remote access to users. These software tools can provide real-time sharing of files, presentations, or applications with coworkers, vendors, or other clients. There are many applications made possible by desktop sharing including remote support, webinars, and online conferences with audio and visual content (presentation sharing), and real-time global collaboration on projects.
Another application of desktop sharing is remote login for workers who need access to their work computers from any Web-connected device (desktop, laptop, phone, or tablet).

Limitations of desktop sharing

Like VPNs, desktop sharing software tools come with a number of drawbacks. First, there are authentication risks. Anyone, anywhere, can log into a desktop sharing tool if they have the

credentials, meaning they have access to the whole network as if they are in the building. During a remote support session, if an employee surrenders control of their machine to a remote rep whose account has been compromised, your company's internal sensitive files could become visible to bad actors and used for nefarious purposes.
Second, desktop sharing tools are not the best solution for supporting enterprise environments. While these tools can be utilized to provide desktop support and handle helpdesk tasks, they typically do not have the security and functionality required for complex enterprise remote support such as server or application maintenance. They often lack the strict security controls (logging and audit) that enterprises in highly regulated industries need. In addition, while desktop sharing can be useful for end-user support, there are additional tools and protocols needed when supporting servers, databases, and other enterprise applications.

3. PAM: Privileged Access Management

To go beyond VPNs and desktop sharing, you need an alternative that can manage identities closer than mere IAM technologies such as Active Directory. This is especially true of the privileged or admin accounts used for many enterprise-level support tasks. In order to securely manage credentials for privileged accounts, a better solution was developed: Privileged Access Management, or PAM.

PAM is a set of tools and technologies that can be used to secure, control, and monitor access via privileged accounts to an organization's resources. The most effective PAM solutions address several areas of information security defense, such as advanced credential security, systems, and data access control, credential obfuscation and user activity monitoring. Ensuring continuous oversight of these target areas helps lower the threat of unauthorized network access, and makes it easier for IT managers to uncover suspicious activity on the network.

Best practices in PAM indicate that least privilege protocols should be enforced, where users only have access to the specific limited resources they need, rather than free reign to roam the entire network. In addition, network managers should be able to restrict or expand user access as needed, in real-time.

4. VPAM: Vendor Privileged Access Management

Many organizations need to provide privileged accounts to two types of users: internal users (employees) and external users (technology vendors and contractors). However, organizations that use vendors or contractors must protect themselves against potential threats from these sources. External users pose a unique threat because network managers cannot control the security best practices of their vendor partners; they can only protect against risky user behavior.

Vendor privileged access management (VPAM) refers to solutions that address the risks posed from these external vendors and contractors, which are unique to third-party remote access users. As the name implies, VPAM is related to PAM – but there are key differences. Traditional PAM solutions are designed to manage internal privileged accounts, based on the reasonable assumption that admins know the identity and employment status of each person accessing the network. However, this is not the case with third-party users, and so VPAM solutions use multi-factor authentication to provide an extra layer of protection.

In general, network managers and admins must be able to identify and authenticate external users via more advanced VPAM methods that can confirm these users are connected to active vendor employee accounts. A strong, effective VPAM solution will be able to continuously monitor vendor user activity, using detailed tracking to provide optimal protection against unauthorized use.

Both PAM and VPAM have the same overall goal: maintaining network security for all users who have advanced permissions, whether they be internal or external.

Remote Desktop

The most sophisticated form of remote access enables users on one computer to see and interact with the actual desktop user interface of another computer. Setting up remote desktop support involves configuring software on both the host (local computer controlling the connection) and target (remote computer being accessed). When connected, this software opens a window on the host system containing a view of the target's desktop.

Advantages

Remote work is not all bad, of course. If it were, remote working would not be as popular as it is becoming among workers and employers alike. Here are some advantages of remote working to keep in mind:

1. Flexibility
   whilst the lack of routine was listed as a "Disadvantage" because some people struggle to get motivated, others in fact thrive on it. For example, with a flexible work schedule, parents are able take their kids to and from school, which relieves reliance on childcare. In addition to this, there are people who just perform more efficiently when they are in charge of their own schedule.
2. Less costly
   working at home part or full- time means less or no commuting, which means less money spent on transport costs. Many remote workers will also make their lunch and coffee at home. Another way remote workers save money is on their wardrobe! After all, unless you do video conferencing, no one says you cannot wear informal clothes all day – no need for a work wardrobe.
3. Work at your own pace.
   Most people working remotely can choose how and when to work on projects, as long as they deliver them in by the deadline. They can take breaks, or push through and complete a task all in one go. While self-discipline is necessary when it comes to working from home, several studies have shown that at-home workers tend to be more productive than their on-site counterparts.
4. Less sick days
   how many times have you decided not to go to the office because you have a bad cold or a sore throat? When you are at home, you can take care of yourself and still get work done. Researchers have found that remote workers are off ill less frequently than on-site workers.

5. Technological advances make so much possible. Working in an office means that you can hand in reports and communicate with colleagues without any delays. Nowadays though, the huge choice of ways to stay connected by phone and internet ensure that speed is not an issue, even if you are working remotely. 4G networks are available in many countries, and coverage areas are increasing every day. In addition to making it possible to upload and send data four times faster than with 3G, 4G allows for easy transfer of higher definition videos and images. If security is an issue, 4G is also the best option for keeping documents and other information safe. Software can also help like Microsoft Office 365 mean that you can collaborate with colleagues on documents in real time, even if one of you is in the office and the other at home.

Disadvantages

1. Lack of routine
   not all-remote work is the same; some people do have to follow a schedule and check in with their employer at key times. For those in results-based areas like freelancing though, there are no rules about when, for example, you have to get out of bed. There probably are not meetings to go to either, and if there are, these kinds of home workers can often dial in to participate if they want. It may sound like a dream, but some remote workers can struggle with the lack of a schedule, finding it difficult to feel motivated or work efficiently.
2. No workplace social life
   even if you are interacting with clients or co-workers virtually, it is not the same as banter in the office or getting lunch together. Remote workers often report feeling a little isolated. This is why many of them prefer to come into the office at least a few days a week, or possibly do their work in public places like coffee shops.
3. The challenge of the work/life balance.
   You would think that remote working would make it easier to devote time to your personal life. However, when you do not have specific hours or a clear separation of workplace and home space, it can be hard to "switch off" and stop thinking about work you have to do, or stop constantly checking your phone or inbox.
4. Distractions
   Then again, while some struggle with "switching off" from work, others have trouble switching on. Working at home means all the distractions of your personal life, good and bad. If you have small children around, they may demand your attention. On the other hand, the TV may just beg you to watch it for an hour or two. Without the filters that many workplaces put up, remote workers have constant access to time- wasting websites, personal emails and social networks – which can be deadly for productivity.
5. Complete dependence on technology
   Since you are not face-to-face with colleagues or clients when you are a remote worker, you have to make sure you are easily reachable by email, phone and other platforms your office or external contacts may use (Skype for Business, Dropbox, etc.). Luckily, there are many solutions to help you communicate and transfer data quickly. A 4G network, for example, offers incredible speed, security and image definition.

Remote Access to Files

Basic remote network access allows files to be read from and written to the target, even without remote desktop capability in place. Virtual Private Network (VPN) technology provides remote login and file access functionality across wide area networks (WANs). A VPN requires client software be present on host systems and VPN server technology installed on the target network.

2.6. Logging with Syslog Usage

Syslog is a protocol that allows a machine to send event notification messages across IP networks to event message collectors – also known as Syslog Servers or Syslog Daemons. In other words, a machine or a device can be configured in such a way that it generates a Syslog Message and forwards it to a specific Syslog Daemon (Server).

Syslog messages are based on the User Datagram Protocol (UDP) type of Internet Protocol (IP) communications. Syslog messages are received on UDP port 514. Syslog message text is generally no more than 1024 bytes in length. Since the UDP type of communication is connectionless, the sending or receiving host has no knowledge receipt for retransmission. If a UDP packet gets lost due to congestion on the network or due to resource unavailability, it will simply get lost – no one would know about it.

Syslog Daemon
A Syslog Daemon or Server is an entity that would listen to the Syslog messages that are sent to it. You cannot configure a Syslog Daemon to ask a specific device to send it Syslog Messages. If a specific device has no ability to generate Syslog Messages, then a Syslog Daemon cannot do anything about it. To make this thing clear, you can consider a Syslog Server or Syslog Daemon as a TV, which can only display you the program that is currently running on a specific channel. You cannot ask another station to send a new program on that channel.

Format of a Syslog Packet
The full format of a Syslog message seen on the wire has three distinct parts.

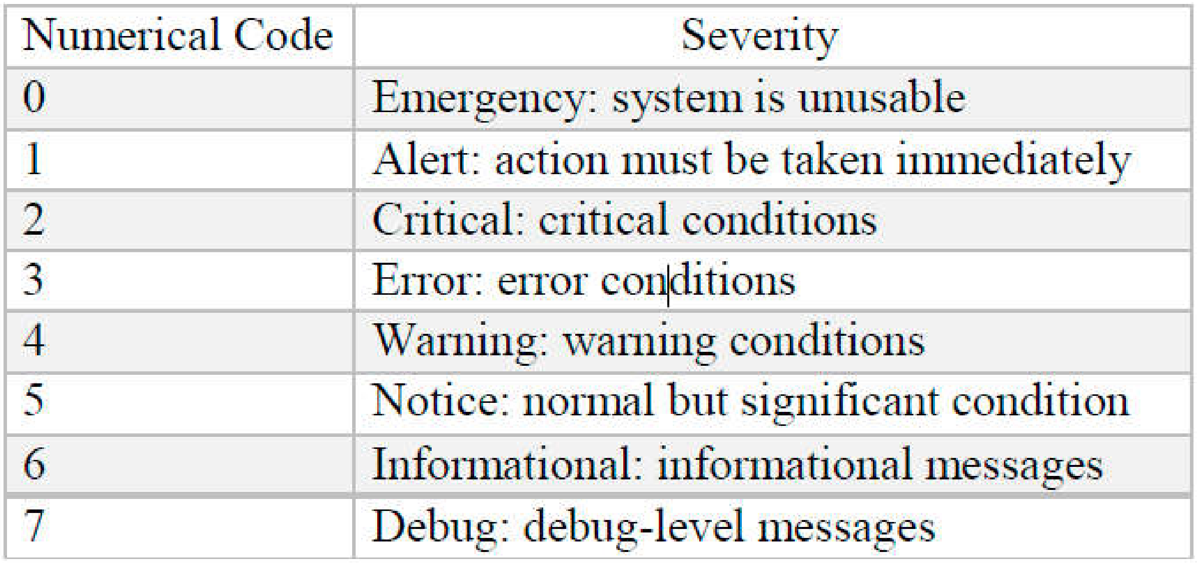
1. PRI
2. HEADER
3. MSG.
   The total length of the packet cannot exceed 1,024 bytes, and there is no minimum length

1. PRI

The Priority part is a number that is enclosed in angle brackets. This represents both the Facility and Severity of the message. This number is an eight-bit number. The first 3 least significant bits represent the Severity of the message (with 3 bits you can represent 8 different Severities) and the other 5 bits represent the Facility of the message. You can use the Facility and the Severity values to apply certain filters on the events in the Syslog Daemon.

Note that Syslog Daemon cannot generate these Priority and Facility values. They are generated by the applications on which the event is generated. Following are the codes for Severity and Facility. Please note that the codes written below are the recommended codes that the applications should generate in the specified situations. You cannot, however, be 100 % sure, if it really is the correct code sent by the application. For example: An application can generate a numerical code for severity as 0 (Emergency) when it should have generated 4 (Warning) instead. Syslog Daemon cannot do anything about it. It will simply receive the message as it is.

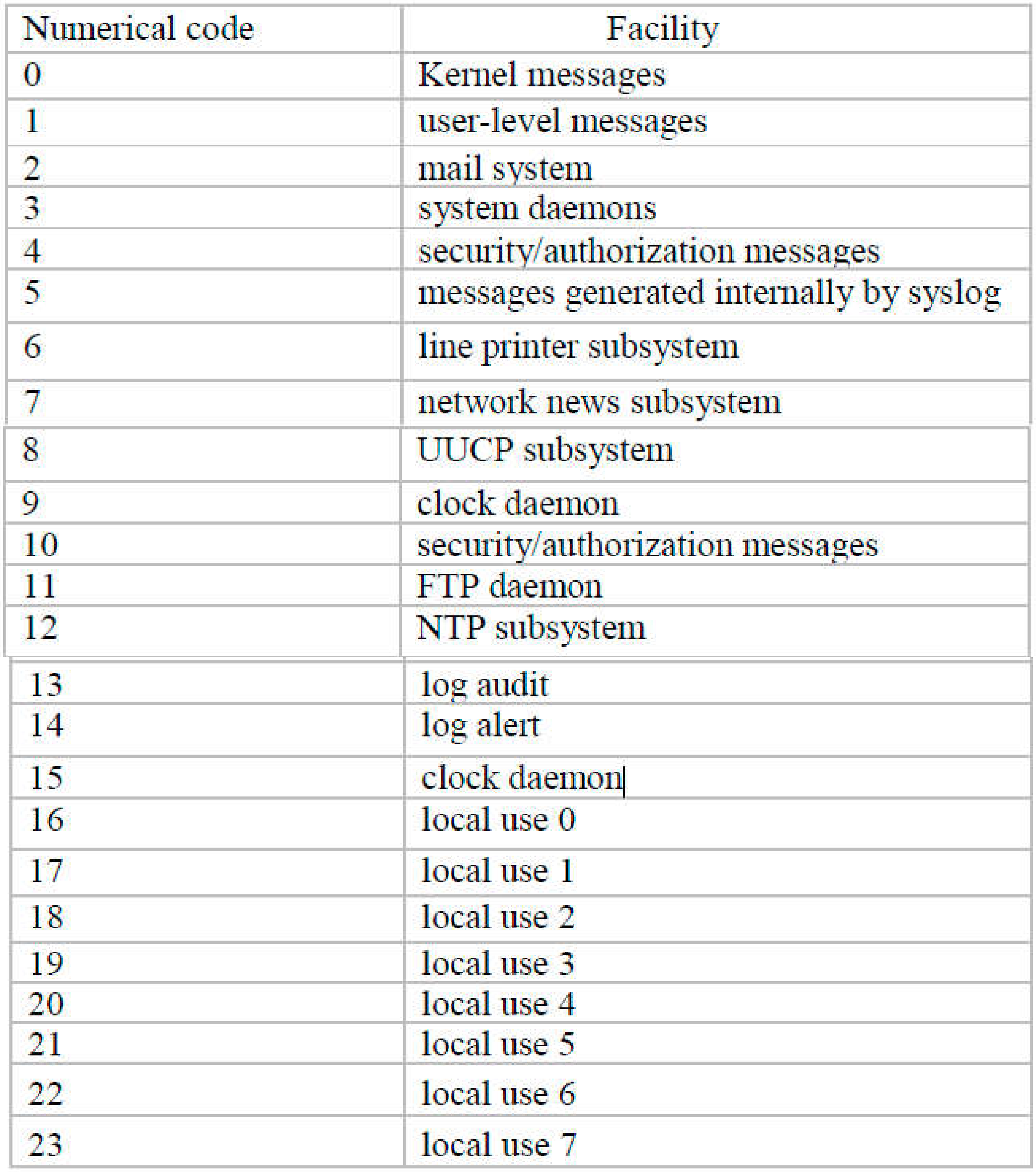
a) Severity Codes: The Severity code is the severity of the message that has been generated.



Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

Table 2. 4 The codes for Severity

b) Facility Codes
The facility is the application or operating system component that generates a log message. Following are the codes for facility:



Numerical code	Facility
0	Kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslog
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	local use 0
17	local use 1
18	local use 2
19	local use 3
20	local use 4
21	local use 5
22	local use 6
23	local use 7

Table 2. 5 Facility Codes

Calculating Priority Value

The Priority value is calculated by first multiplying the Facility number by 8 and then adding the numerical value of the Severity. For example, a kernel message (Facility=0) with a Severity of Emergency (Severity=0) would have a Priority value of 0 (0+8*0). Also, a “local use 4” message (Facility=20) with a Severity of Notice (Severity=5) would have a Priority value of 165 (5+8*20).

In the PRI part of a Syslog message, these values would be placed between the angle brackets as <0> and <165> respectively.

2. Header

   The HEADER part contains the following things:
   a) Timestamp — The Time stamp is the date and time at which the message was generated. Be warned, that this timestamp is picked up from the system time and if the system time is not correct, you might get a packet with totally incorrect time stamp
   b) Hostname or IP address of the device.

3. MSG

   The MSG part will fill the remainder of the Syslog packet. This will usually contain some additional information of the process that generated the message, and then the text of the message. The MSG part has two fields:
   a) TAG field
   b) CONTENT field
   The value in the TAG field will be the name of the program or process that generated the message. The CONTENT contains the details of the message.

   Some Important Points

- As mentioned above, since Syslog protocol is UDP based, it is unreliable. It does not guarantee you the delivery of the messages. They may either be dropped through network congestion, or they may be maliciously intercepted and discarded.
- As mentioned above, since each process, application and operating system was written somewhat independently, there is little uniformity to the content of syslog messages. For this reason, no assumption is made upon the formatting or contents of the messages. The protocol is simply designed to transport these event messages.
- The receiver of a Syslog packet will not be able to ascertain that the message was indeed sent from the reported sender.
- One possible problem associated with the above-mentioned point is of Authentication. A misconfigured machine may send syslog messages to a Syslog Daemon representing itself as another machine. The administrative staff may become confused because the status of the supposed sender of the messages may not be accurately reflected in the received messages.
- Another problem associated with point 2 is that an attacker may start sending fake messages indicating a problem on some machine. This may get the attention of the system administrators who will spend their time investigating the alleged problem. During this time, the attacker may be able to compromise a different machine, or a different process on the same machine.
- The Syslog protocol does not ensure ordered delivery of packets.
- An attacker may record a set of messages that indicate normal activity of a machine. Later, that attacker may remove that machine from the network and replay the syslog messages to the Daemon.

2.7. Miscellaneous

Intrusion Notification

In some situations, you might want to configure the switch to send a notification to an SNMP NMS when MAC addresses are learned by the system or deleted from the CAM table. An example of where this might be used could be a switch that is deployed in a particularly restrictive security zone in the network, like an R&D lab or a DMZ, and where you want to determine if there is anomalous MAC address learning behavior in that part of the network. The following command enables this feature:

Catalyst1(config)#mac-address-table notification Only dynamic and secure MAC addresses generate a MAC address notification. Traps are not sent for self, multicast, or other static addresses.

Switch Security Best Practices
Cisco makes the following recommendations for switch security best practices:

- Secure management: Think security for switch management. Use SSH, a dedicated management VLAN, OOB, and so on as much as possible.
- Native VLAN: Always use a dedicated VLAN ID for trunk ports and avoid using VLAN 1 at all.
- User ports: Non-trunking. (Cisco VoIP phones being the exception. See Chapter 9, “Introduction to Endpoint, SAN, and Voice Security.”)
- Port security: Use for access ports whenever possible.
- SNMP: Limit to the management VLAN if possible and treat community strings like superuser passwords. (See Chapter 4, “Implementing Secure Management and Hardening the Router,” for more information.)
- STP attacks: Use BPDU guard and root guard.
- CDP: Only use if necessary. CDP should be left on for switch ports connected to VoIP phones. An attacker can learn much from CDP advertisements.
- Unused ports: Disable and put them in an unused VLAN for extra security.

CHAPTER THREE

ROUTERS

3.1. Router Basic Configuration

A Router is a computer, just like any other computer including a PC. Routers have many of the same hardware and software components that are found in other computers including:

- CPU
- RAM
- ROM
- Operating System

Figure 3. 1 1841 Integrated Services Router

Router is the basic backbone for the Internet. The main function of the router is to connect two or more than two network and forwards the packet from one network to another. A router connects multiple networks. This means that it has multiple interfaces that each belong to a different IP network. When a router receives an IP packet on one interface, it determines which interface to use to forward the packet onto its destination. The interface that the router uses to forward the packet may be the network of the final destination of the packet (the network with the destination IP address of this packet), or it may be a network connected to another router that is used to reach the destination network. A router uses IP to forward packets from the source network to the destination network. The packets must include an identifier for both the source and destination networks. A router uses the IP address of the destination network to deliver a packet to the correct network. When the packet arrives at a router connected to the destination network, the router uses the IP address to locate the specific computer on the network.

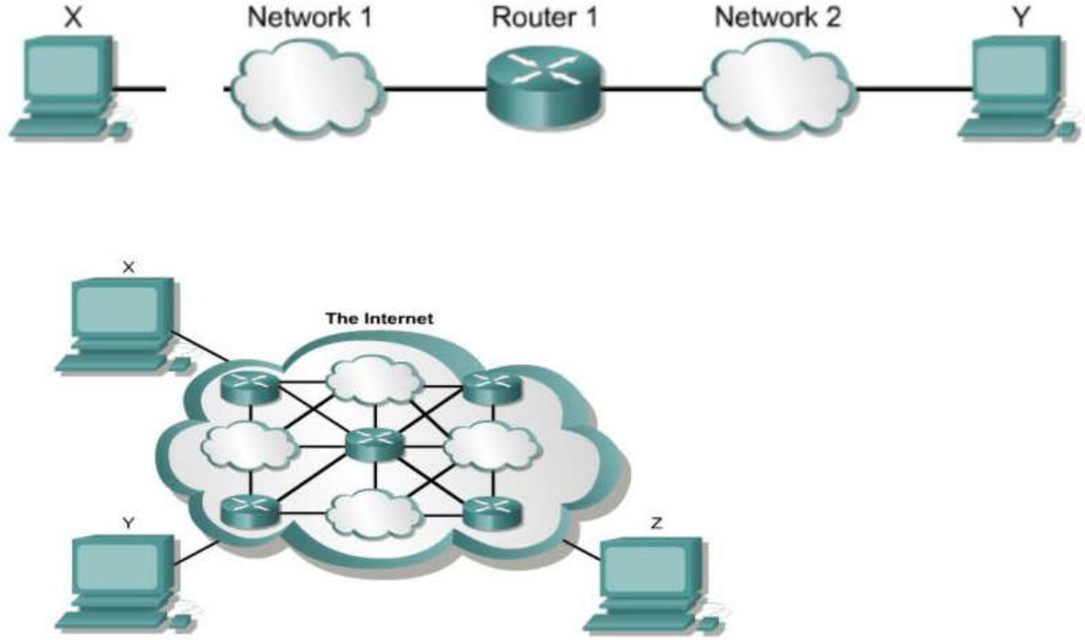


Figure 3. 2 Router connects two network

A router uses IP to forward packets from the source network to the destination network. The packets must include an identifier for both the source and destination networks. A router uses the IP address of the destination network to deliver a packet to the correct network. When the packet arrives at a router connected to the destination network, the router uses the IP address to locate the specific computer on the network.

Routing and Routing Protocols

The primary responsibility of a router is to direct packets destined for local and remote networks by:

- Determining the best path to send packets
- Forwarding packets toward their destination

The router uses its routing table to determine the best path to forward the packet. When the router receives a packet, it examines its destination IP address and searches for the best match with a network address in the router’s routing table. The routing table also includes the interface to be used to forward the packet. Once a match is found, the router encapsulates the IP packet into the data link frame

3.2. Static Routing

Static routes are configured manually, network administrators must add and delete static routes to reflect any network topology changes. In a large network, the manual maintenance of routing tables could require a lot of administrative time. On small networks with few possible changes, static routes require very little maintenance. Static routing is not as scalable as dynamic routing because of the extra administrative requirements. Even in large networks, static routes that are intended to accomplish a specific purpose are often configured in conjunction with a dynamic routing protocol.

When to use static Routing

A network consists of only a few routers. Using a dynamic routing protocol in such a case does not present any substantial benefit. On the contrary, dynamic routing may add more administrative overhead.

A network is connected to the Internet only through a single ISP. There is no need to use a dynamic routing protocol across this link because the ISP represents the only exit point to the Internet.

A large network is configured in a hub-and-spoke topology. A hub-and-spoke topology consists of a central location (the hub) and multiple branch locations (spokes), with each spoke having only one connection to the hub. Using dynamic routing would be unnecessary because each branch has only one path to a given destination through the central location.

Connected Routes

Those network that are directly connected to the Router are called connected routes and are not needed to configure on the router for routing. They are automatically routed by the Router.

Dynamic Routes: Dynamic routing protocol uses a route that a routing protocol adjusts automatically for topology or traffic changes. Non-adaptive routing algorithm When a ROUTER uses a non-adaptive routing algorithm it consults a static table in order to determine to which computer it should send a PACKET of data. This is in contrast to an ADAPTIVE ROUTING ALGORITHM, which bases its decisions on data which reflects current traffic conditions (Also called static route) adaptive routing algorithm When a ROUTER uses an adaptive routing algorithm to decide the next computer to which to transfer a PACKET of data, it examines the traffic conditions in order to determine a route which is as near optimal as possible. For example, it tries to pick a route, which involves communication lines which have light traffic. This strategy is in contrast to a NON-ADAPTIVE ROUTING ALGORITHM. (Also called Dynamic route)

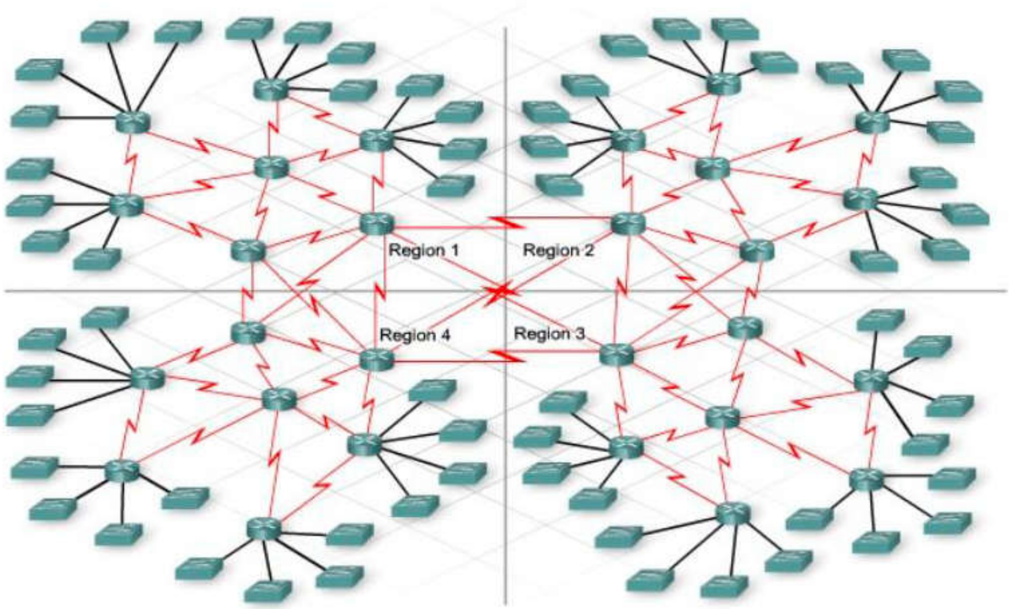


Figure 3. 3 Imagine maintaining static routing configurations

3.3. Dynamic Routing

Dynamic routing is a technique in which a router learns about routing information without an administrator's help and adds the best route to its routing table. A router running a dynamic routing protocol adds the best route to its routing table and can also determine another path if the primary route goes down. Also a networking technique provides optimal data routing. Unlike static routing, dynamic routing enables routers to select paths according to real-time logical network layout changes

At the dynamic routing section, we will discuss the implementation of RIPv1, RIPv2, EIGRP, and Single-Area OSPF.

3.4. Routing Protocols Matrix

Routing Protocol:

A routing protocol is the communication used between routers. A routing protocol allows routers to share information about networks and their proximity to each other. Routers use this information to build and maintain routing tables. Autonomous System: An AS is a collection of networks under a common administration that share a common routing strategy. To the outside world, an AS is viewed as a single entity. The AS may be run by one or more operators while it presents a consistent view of routing to the external world.

The American Registry of Internet Numbers (ARIN), a service provider, or an administrator assigns a 16- bit identification number to each AS.

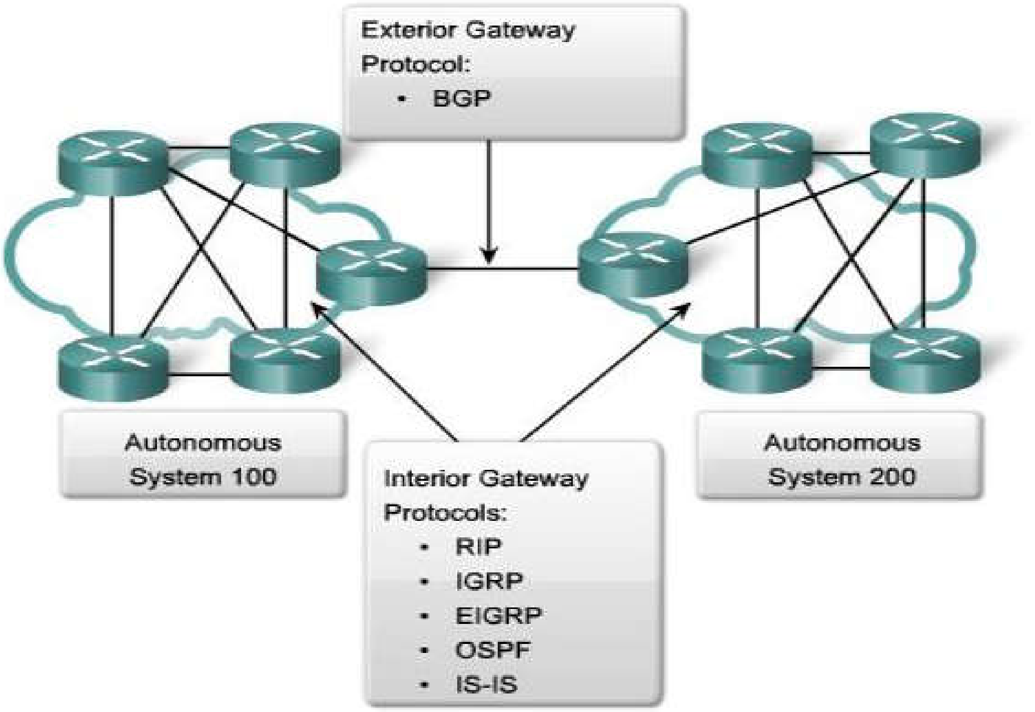


Figure 3. 4 IGP vs Routing Protocols

Dynamic Routing Protocol:

1. Interior Gateway protocol (IGP)
   I. Distance Vector Protocol
   II. Link State Protocol
2. Exterior Gateway Protocol (EGP)

Interior gateway protocol (IGP): Within one Autonomous System.
Exterior Routing Protocol (EGP): Between the Autonomous System. Example BGP (Boarder gateway protocol).

Metric:

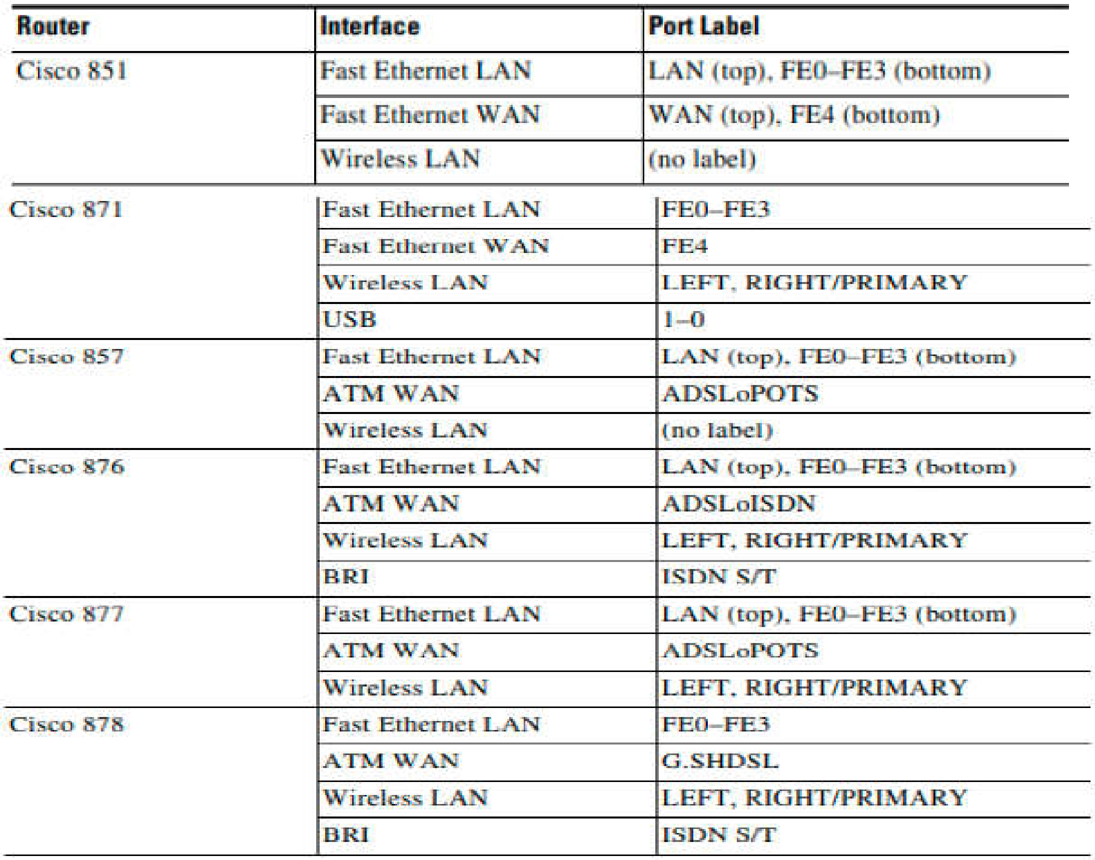
There are cases when a routing protocol learns of more than one route to the same destination. To select the best path, the routing protocol must be able to evaluate and differentiate between the available paths. For this purpose a metric is used. A metric is a value used by routing protocols to assign costs to reach remote networks. The metric is used to determine which path is most preferable when there are multiple paths to the same remote network.

Each routing protocol uses its own metric. For example, RIP uses hop count, EIGRP uses a combination of bandwidth and delay, and Cisco's implementation of OSPF uses bandwidth.

Basic Router Configuration

Interface Port Labels

Table 3.1 lists the interfaces supported for each router and their associated port labels on the equipment.



Router	Interface	Port Label
Cisco 851	Fast Ethernet LAN	LAN (top), FE0–FE3 (bottom)
	Fast Ethernet WAN	WAN (top), FE4 (bottom)
	Wireless LAN	(no label)
Cisco 871	Fast Ethernet LAN	FE0–FE3
	Fast Ethernet WAN	FE4
	Wireless LAN	LEFT, RIGHT/PRIMARY
	USB	1–0
Cisco 857	Fast Ethernet LAN	LAN (top), FE0–FE3 (bottom)
	ATM WAN	ADSLoPOTS
	Wireless LAN	(no label)
Cisco 876	Fast Ethernet LAN	LAN (top), FE0–FE3 (bottom)
	ATM WAN	ADSLoISDN
	Wireless LAN	LEFT, RIGHT/PRIMARY
	BRI	ISDN S/T
Cisco 877	Fast Ethernet LAN	LAN (top), FE0–FE3 (bottom)
	ATM WAN	ADSLoPOTS
	Wireless LAN	LEFT, RIGHT/PRIMARY
Cisco 878	Fast Ethernet LAN	FE0–FE3
	ATM WAN	G.SHDSL
	Wireless LAN	LEFT, RIGHT/PRIMARY
	BRI	ISDN S/T

Table 3.1 Supported Interfaces and Associated Port Labels by Cisco Router

Viewing the Default Configuration

When you first boot up your Cisco router, some basic configuration has already been performed. All of the LAN and WAN interfaces have been created, console and VTY ports are configured, and the inside interface for Network Address Translation has been assigned.

Use the show running-config command to view the initial configuration, as shown in Example 1-1.

```
Router# show running-config
Building configuration…
```

```
Current configuration : 1090 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip subnet-zero
!
ip cef
ip ips po max-events 100
no ftp-server write-enable
!
interface FastEthernet 0
no ip address
shutdown
!
interface FastEthernet 1
no ip address
shutdown
!
interface FastEthernet 2
no ip address
shutdown
!
interface FastEthernet 3
no ip address
shutdown
!
interface FastEthernet 4
no ip address
duplex auto
speed auto
!
interface Dot 11Radio0
no ip address
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
```

```
station-role root
!
interface Vlan1
no ip address
!
ip classless
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
no modem enable
transport preferred all
transport output all
line aux 0
transport preferred all
transport output all
line vty 0 4
login
transport preferred all
transport input all
transport output all
!
End
```

Information Needed for Configuration

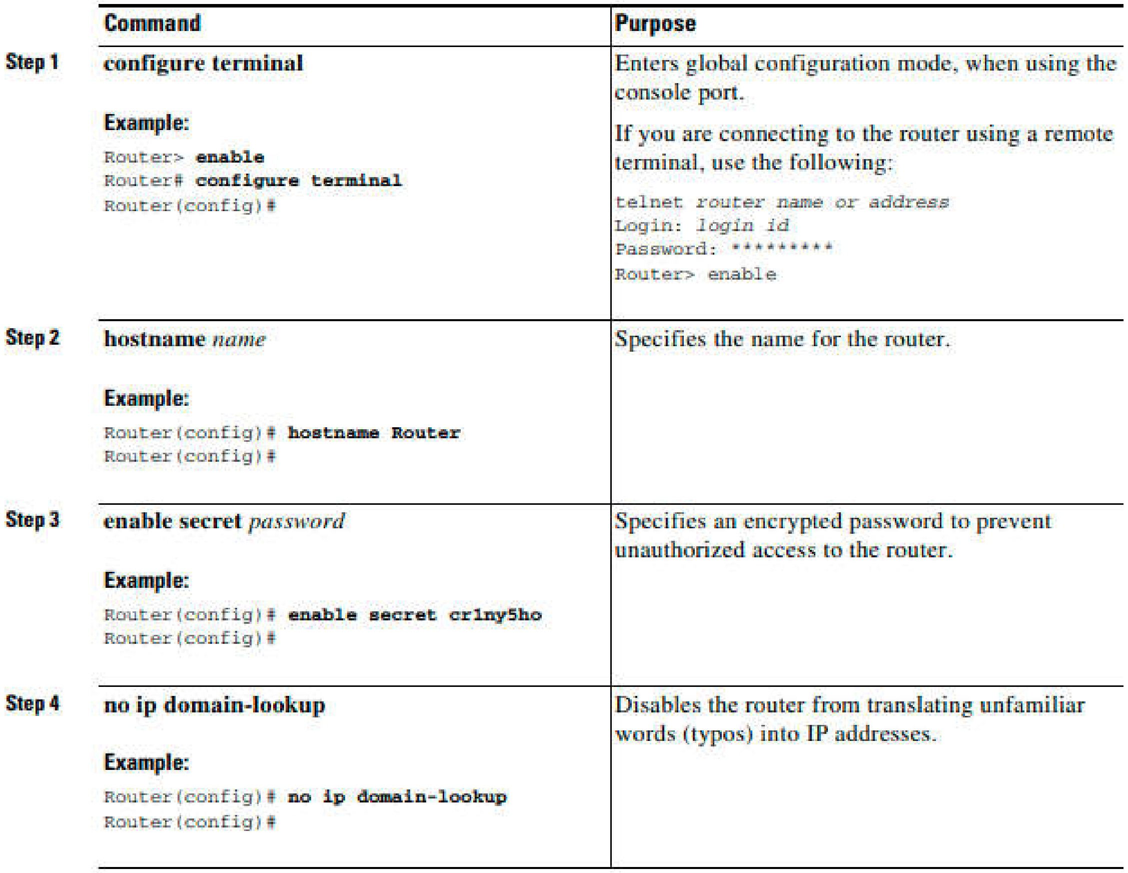
You need to gather some or all of the following information, depending on your planned network scenario, prior to configuring your network

- If you are setting up an Internet connection, gather the following information:
  - Point-to-Point Protocol (PPP) client name that is assigned as your login name
  - PPP authentication type: Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP)
  - PPP password to access your Internet service provider (ISP) account
  - DNS server IP address and default gateways
- If you are setting up a connection to a corporate network, you and the network administrator must generate and share the following information for the WAN interfaces of the routers:
  - PPP authentication type: CHAP or PAP
  - PPP client name to access the router
  - PPP password to access the router
- If you are setting up IP routing:
  - Generate the addressing scheme for your IP network.

- Determine the IP routing parameter information, including IP address, and ATM permanent virtual circuits (PVCs). These PVC parameters are typically virtual path identifier (VPI), virtual circuit identifier (VCI), and traffic shaping parameters.
- Determine the number of PVCs that your service provider has given you, along with their VPIs and VCIs. – For each PVC determine the type of AAL5 encapsulation supported. It can be one of the following: AAL5SNAP
- This can be either routed RFC 1483 or bridged RFC 1483. For routed RFC 1483, the service provider must provide you with a static IP address. For bridged RFC 1483, you may use DHCP to obtain your IP address, or you may obtain a static IP address from your service provider. AAL5MUX PPP
- With this type of encapsulation, you need to determine the PPP-related configuration items.
- If you plan to connect over an ADSL or G.SHDSL line: – Order the appropriate line from your public telephone service provider. For ADSL lines—ensure that the ADSL signaling type is DMT (also called ANSI T1.413) or DMT Issue 2. For G.SHDSL lines—Verify that the G.SHDSL line conforms to the ITU G.991.2 standard and supports Annex A (North America) or Annex B (Europe). Once you have collected the appropriate information, you can perform a full configuration on your router, beginning with the tasks in the “Configuring Basic Parameters” section.

Configure Global Parameters

Perform these steps to configure selected global parameters for your router:



	Command	Purpose

Step 1	**configure terminal**
	Example:
	`Router> `**`enable`**
	`Router# `**`configure terminal`**
	`Router(config)#`
		Enters global configuration mode, when using the console port.
		If you are connecting to the router using a remote terminal, use the following:
		`telnet` *`router name or address`*
		`Login:` *`login id`*
		`Password: *********`
		`Router> enable`

Step 2	**hostname** *name*
	Example:
	`Router(config)# `**`hostname Router`**
	`Router(config)#`
		Specifies the name for the router.

Step 3	**enable secret** *password*
	Example:
	`Router(config)# `**`enable secret cr1ny5ho`**
	`Router(config)#`
		Specifies an encrypted password to prevent unauthorized access to the router.

Step 4	**no ip domain-lookup**
	Example:
	`Router(config)# `**`no ip domain-lookup`**
	`Router(config)#`
		Disables the router from translating unfamiliar words (typos) into IP addresses.

Table 3. 2 For complete information on the global parameter commands

Configure Fast Ethernet LAN Interfaces

The Fast Ethernet LAN interfaces on your router are automatically configured as part of the default VLAN and as such, they are not configured with individual addresses. Access is afforded through the VLAN. You may assign the interfaces to other VLANs if desired.

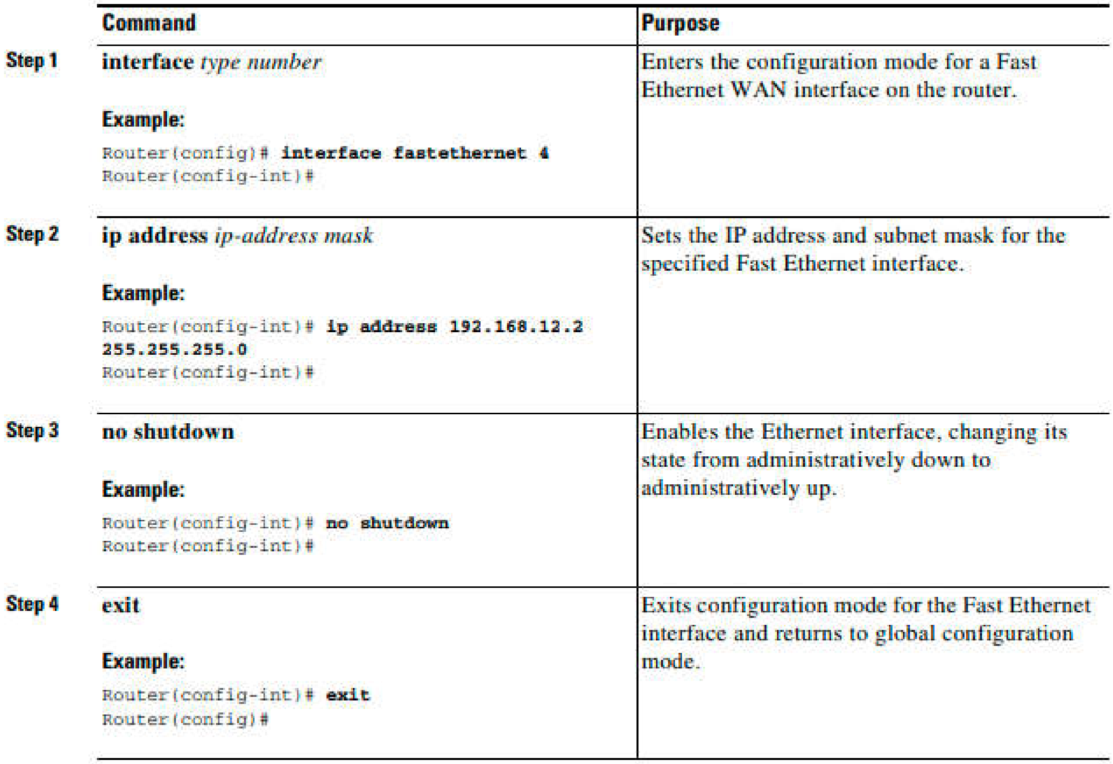
Configure WAN Interfaces

The Cisco 851 and Cisco 871 routers each have one Fast Ethernet interface for WAN connection. The Cisco 857, Cisco 877, and Cisco 878 routers each have one ATM interface for WAN connection.
Based on the router model you have, configure the WAN interface(s) using one of the following procedures:

- Configure the Fast Ethernet WAN Interface
- Configure the ATM WAN Interface

Configure the Fast Ethernet WAN Interface

This procedure applies only to the Cisco 851 and Cisco 871 router models. Perform these steps to configure the Fast Ethernet interface, beginning in global configuration mode:



	Command	Purpose

Step 1	**interface** *type number*
	Example:
	`Router(config)# interface fastethernet 4`
	`Router(config-int)#`
		Enters the configuration mode for a Fast Ethernet WAN interface on the router.

Step 2	**ip address** *ip-address mask*
	Example:
	`Router(config-int)# ip address 192.168.12.2 255.255.255.0`
	`Router(config-int)#`
		Sets the IP address and subnet mask for the specified Fast Ethernet interface.

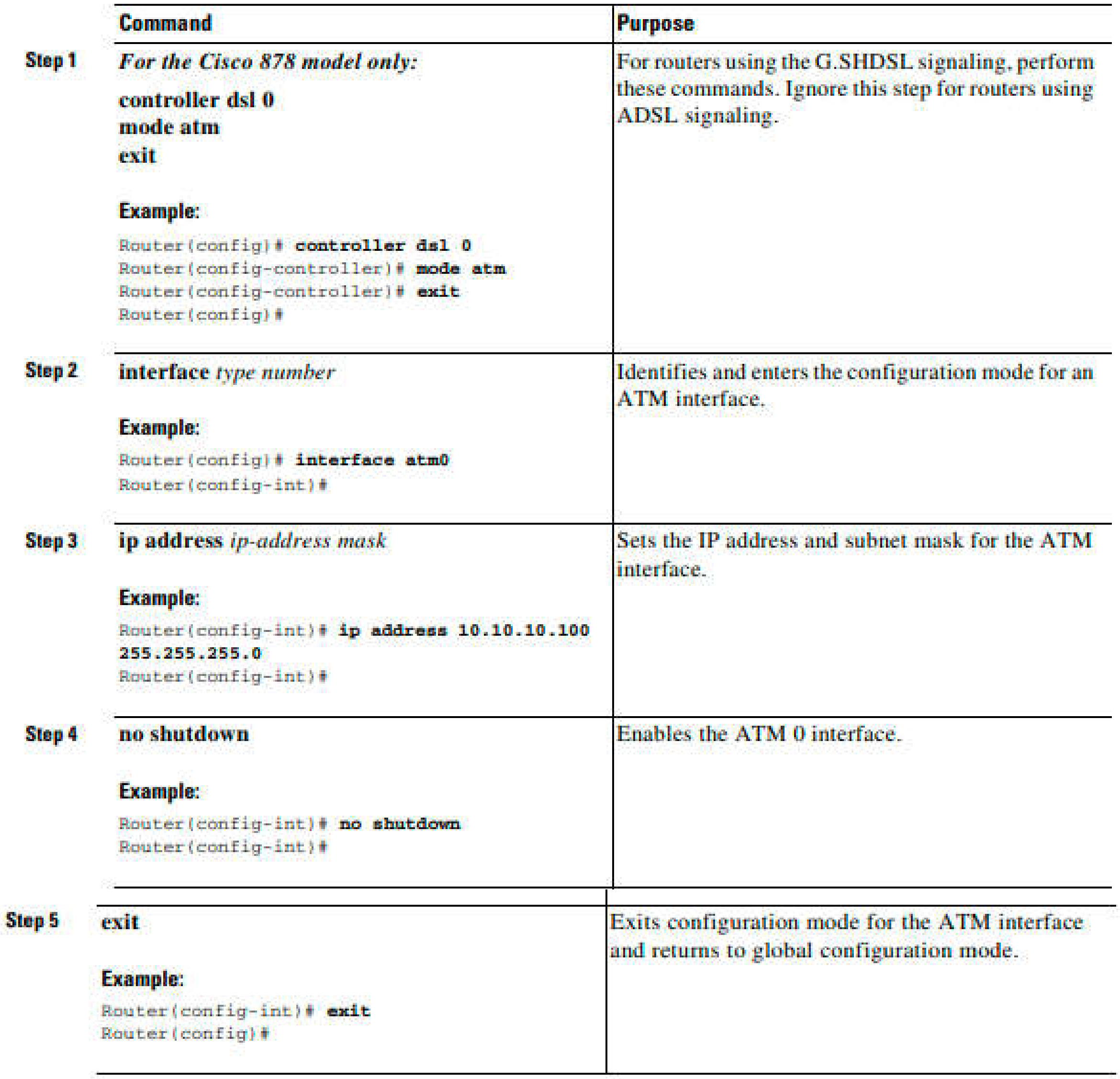
Step 3	**no shutdown**
	Example:
	`Router(config-int)# no shutdown`
	`Router(config-int)#`
		Enables the Ethernet interface, changing its state from administratively down to administratively up.

Step 4	**exit**
	Example:
	`Router(config-int)# exit`
	`Router(config)#`
		Exits configuration mode for the Fast Ethernet interface and returns to global configuration mode.

Table 3. 3 Configure the Fast Ethernet WAN Interface

Configure the ATM WAN Interface

This procedure applies only to the Cisco 857, Cisco 876, Cisco 877 and Cisco 878 models. Perform these steps to configure the ATM interface, beginning in global configuration mode:



	Command	Purpose

Step 1	***For the Cisco 878 model only:***
	controller dsl 0
	mode atm
	exit
	Example:
	`Router(config)# controller dsl 0`
	`Router(config-controller)# mode atm`
	`Router(config-controller)# exit`
	`Router(config)#`
		For routers using the G.SHDSL signaling, perform these commands. Ignore this step for routers using ADSL signaling.

Step 2	**interface** *type number*
	Example:
	`Router(config)# interface atm0`
	`Router(config-int)#`
		Identifies and enters the configuration mode for an ATM interface.

Step 3	**ip address** *ip-address mask*
	Example:
	`Router(config-int)# ip address 10.10.10.100`
	`255.255.255.0`
	`Router(config-int)#`
		Sets the IP address and subnet mask for the ATM interface.

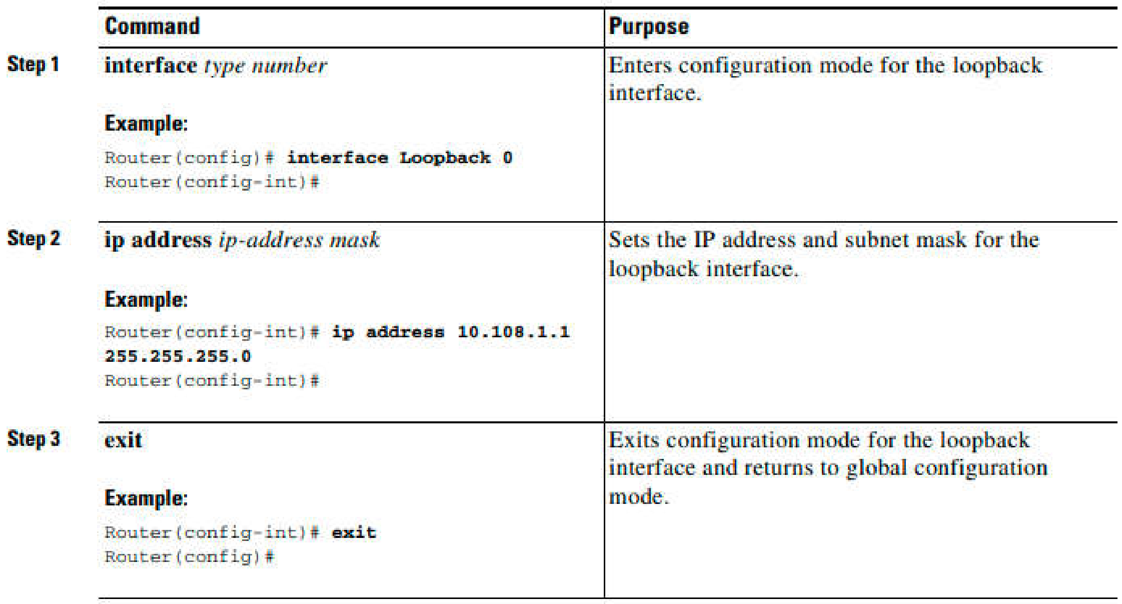
Step 4	**no shutdown**
	Example:
	`Router(config-int)# no shutdown`
	`Router(config-int)#`
		Enables the ATM 0 interface.

Step 5	**exit**
	Example:
	`Router(config-int)# exit`
	`Router(config)#`
		Exits configuration mode for the ATM interface and returns to global configuration mode.

Table 3. 4 Configure the ATM WAN Interface

Configuring a Loopback Interface

The loopback interface acts as a placeholder for the static IP address and provides default routing information



	Command	Purpose

Step 1	**interface** *type number*
	Example:
	`Router(config)# interface Loopback 0`
	`Router(config-int)#`
		Enters configuration mode for the loopback interface.

Step 2	**ip address** *ip-address mask*
	Example:
	`Router(config-int)# ip address 10.108.1.1 255.255.255.0`
	`Router(config-int)#`
		Sets the IP address and subnet mask for the loopback interface.

Step 3	**exit**
	Example:
	`Router(config-int)# exit`
	`Router(config)#`
		Exits configuration mode for the loopback interface and returns to global configuration mode.

Table 3. 5 Configuring a Loopback Interface

Configuration Example

The loopback interface in this sample configuration is used to support Network Address Translation (NAT) on the virtual-template interface. This configuration example shows the loopback interface configured on the Fast Ethernet interface with an IP address of 10.10.10.100/24, which acts as a static IP address.

The loopback interface points back to virtual-template1, which has a negotiated IP address.

```
!
interface loopback 0
ip address 10.10.10.100 255.255.255.0 (static IP address)
ip nat outside
!
interface Virtual-Template1
ip unnumbered loopback0
no ip directed-broadcast
ip nat outside
!
```

Verifying Your Configuration

To verify that you have properly configured the loopback interface, enter the show interface loopback command. You should see verification output similar to the following example:

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
```

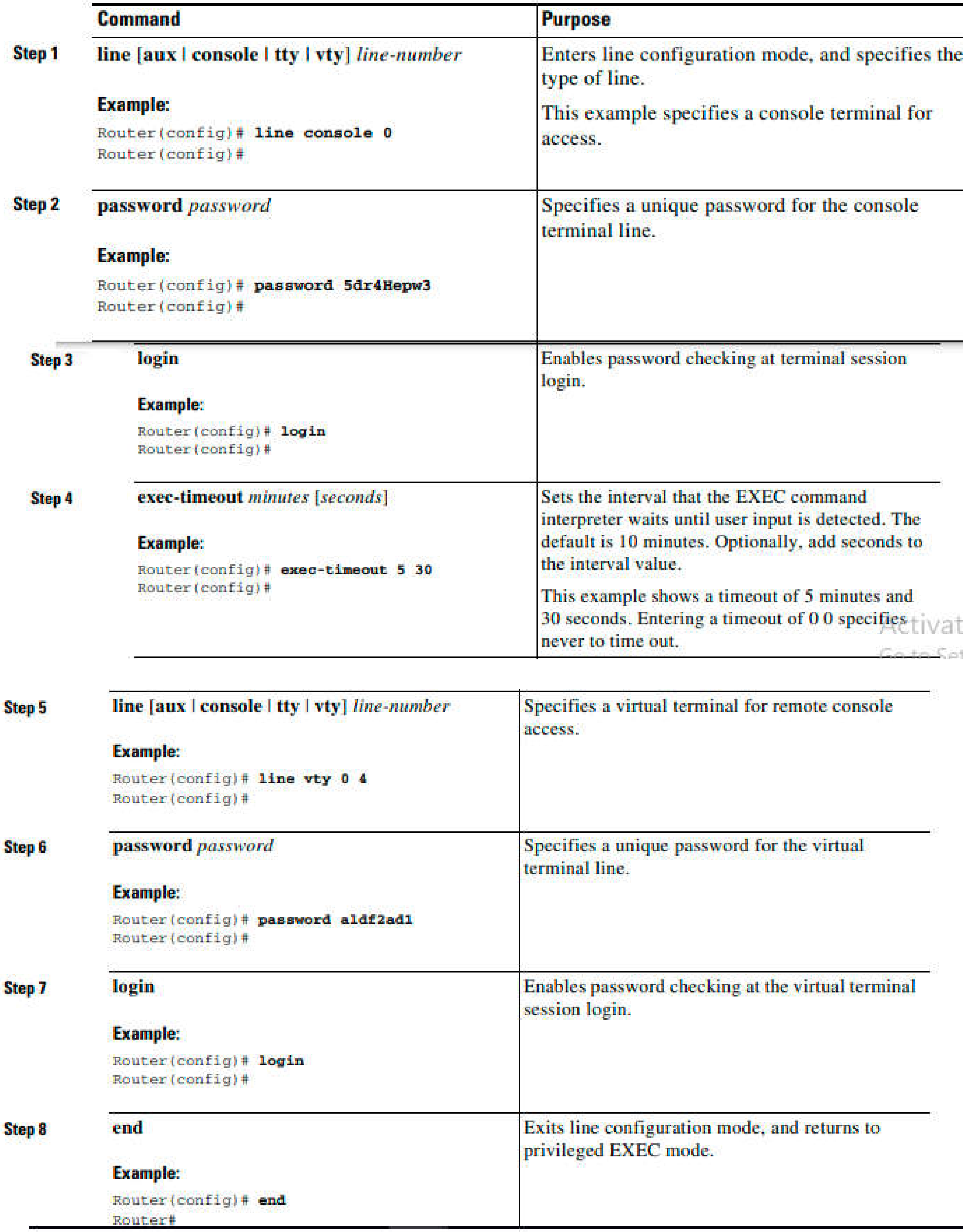
```
Hardware is Loopback
Internet address is 10.10.10.100/24
MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation LOOPBACK, loopback not set
Last input never, output never, output hang never
Last clearing of “show interface” counters never
Queueing strategy: fifo
Output queue 0/0, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec,
0 packets/sec 0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

Another way to verify the loopback interface is to ping it:

```
Router# ping 10.10.10.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Configuring Command-Line Access to the Router

Perform these steps to configure parameters to control access to the router, beginning in global configuration mode.



	Command	Purpose

Step 1	**line** [**aux** | **console** | **tty** | **vty**] *line-number*
	Example:
	`Router(config)# line console 0`
	`Router(config)#`
		Enters line configuration mode, and specifies the type of line.
		This example specifies a console terminal for access.

Step 2	**password** *password*
	Example:
	`Router(config)# password 5dr4Hepw3`
	`Router(config)#`
		Specifies a unique password for the console terminal line.

Step 3	**login**
	Example:
	`Router(config)# login`
	`Router(config)#`
		Enables password checking at terminal session login.

Step 4	**exec-timeout** *minutes* [*seconds*]
	Example:
	`Router(config)# exec-timeout 5 30`
	`Router(config)#`
		Sets the interval that the EXEC command interpreter waits until user input is detected. The default is 10 minutes. Optionally, add seconds to the interval value.
		This example shows a timeout of 5 minutes and 30 seconds. Entering a timeout of 0 0 specifies never to time out.

Step 5	**line** [**aux** | **console** | **tty** | **vty**] *line-number*
	Example:
	`Router(config)# line vty 0 4`
	`Router(config)#`
		Specifies a virtual terminal for remote console access.

Step 6	**password** *password*
	Example:
	`Router(config)# password aldf2ad1`
	`Router(config)#`
		Specifies a unique password for the virtual terminal line.

Step 7	**login**
	Example:
	`Router(config)# login`
	`Router(config)#`
		Enables password checking at the virtual terminal session login.

Step 8	**end**
	Example:
	`Router(config)# end`
	`Router#`
		Exits line configuration mode, and returns to privileged EXEC mode.

Table 3. 6 Configuring Command-Line Access to the Router

Configuration Example

The following configuration shows the command-line access commands. You do not need to input the commands marked “default.” These commands appear automatically in the configuration file generated when you use the **show running-config** command.

```
!
line con 0
exec-timeout 10 0
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line vty 0 4
password secret
login
!
```

3.5. RIP

How to Configure RIPv1 and RIPv2 in Cisco Routers

When would you need this: When you need to implement a routing protocol for a small network and you need the configuration to be simple. Routing Information Protocol is the simplest that it can get.
Special Requirements: None.

1. The first thing to do is to enable the RIP protocol on the router:

   ```
   Router(config)#router rip
   ```

2. Identify the networks to be advertised using the ‘network’ command. Using this command, you need to identify only the networks that are directly connected to the router:

   ```
   Router(config-router)#network network-id
   ```

   If the network is sub netted, you will need to write the main network address without the need to write the subnets. For example, if you have the following subnets connected to the router (172.16.0.0/24, 172.16.1.0/24, and 172.16.2.0/24), you can put them all in single ‘network’ command like this:

   Router(config router) #network 172.16.0.0. The router is intelligent enough to figure out which subnets are connected to the router.

3. If you need to adjust the timers (update, invalid, hold down, and flush timers), use the 'timers basic' command. All the four parameters of this command, update, invalid, hold down, and flush timer consecutively, are in seconds:

   Router (config-router)#timers basic 30 180 180 240 The example above is set with the default values of the RIP timers. Remember to keep the relativity of the timer values. Always keep it as (n 6n 6n 8n). If, for example, you set the update timer to 40, you need to make the other timers 240 240 320 consecutively. It is highly recommended that you keep the timers on their default values.

4. You will need to stop the updates from being broadcasted to the Internet, if one of the router interfaces is connected to the Internet. For this purpose, use the 'passive interface' command. This command prevents the interface from forwarding any RIP broadcasts, but keeps the interface listening to what others are saying in RIP.

   Router (config router)#passive-interface interface-type interface-number where interface-type is the type of the interface, such as Serial, Fast Ethernet, or Ethernet. Interface-number is the number of the interface such as 0/0 or 0/1/0

5. RIP, by nature, sends updates as broadcast. If the router is connected through non-broadcast networks (like Frame Relay), you will need to tell RIP to send the updates on this network as unicast. This is achieved by the 'neighbor' command:

   Router (config-router)#neighbor neighbor-address where neighbor-address is the IP address of the neighbor.

6. Cisco's implementation of RIP Version 2 supports authentication, key management, route summarization, classless inter-domain routing (CIDR), and variable-length subnet masks (VLSMs). By default, the router receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets. You can configure the router to receive and send only Version 2 packets. To do so, use the 'version' command:

   Router (config-router)#version 2 If you like to stick to version one, just replace the 2 in the command above with 1. Furthermore, you can control the versions of the updates sent and received on each interface to have more flexibility in support of both versions.

   This is achieved by the 'ip rip send version' and 'ip rip receive version' commands:

   ```
   Router (config-if)#ip rip send version 2
   Router (config-if)#ip rip receive version 1
   ```

7. Check the RIP configuration using these commands:

   ```
   Router#show ip route
   Router#show ip protocols
   Router#debug ip rip
   ```

How to Configure RIPng for IPv6

When would you need this: When you want to implement a simple routing protocol for a small-to-medium sized IPv6 network.
Special Requirements: None.

1. Enable IPv6 routing:

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

2. Enable RIPng process:

   Router (config) #ipv6 router rip process-name where the process-name can be any unique process name you select. The process name is of local significance, i.e., you do not need to use the same process name on all the routers participating in the RIPng process.

3. On the interface you want to participate in the RIPng process, assign an IP address:

   Router (config-if) #ipv6 address ipv6-address/prefix length where ipv6-address is the IPv6 address you want to assign to this interface. Prefix-length is the IPv6 prefix length of the network this interface is connected to. If you do not wish to assign an IPv6 address to the interface, you can enable the IPv6 operation on the interface and let it create its own link-local address using the following command:

```
Router (config-if)#ipv6 enable
```

4. Enable the RIPng process on the interface:

   Router (config-if) #ipv6 rip process-name where the process-name should be the process name that you have selected in step 2. Repeat this step on all interface you want to take part in the RIPng routing process.

5. For troubleshooting, use the following commands:

```
Router#show ipv6 route
Router#show ipv6 route rip
Router#show ipv6 protocols
83
Router#show ipv6 rip
Router#show ipv6 rip next-hops
Router#debug ipv6 rip
```

3.6. IGRP

How to Configure IGRP (Interior Gateway Routing Protocol)

Interior Gateway Routing Protocol (IGRP) is a distance vector interior routing protocol (IGP) invented by Cisco. It is used by routers to exchange routing data within an autonomous system. GRP is a proprietary protocol. IGRP was created in part to overcome the limitations of RIP (maximum hop count of only 15, and a single routing metric) when used within large networks.

IGRP supports multiple metrics for each route, including bandwidth, delay, load, MTU, and reliability; to compare two routes these metrics are combined together into a single metric, using a formula which can be adjusted through the use of pre-set constants. The maximum hop count of IGRP-routed packets is 255 (default 100), and routing updates are broadcast every 90 seconds (by default).

IGRP is considered a classful routing protocol. Because the protocol has no field for a subnet mask, the router assumes that all sub network addresses within the same Class A, Class B, or Class C network have the same subnet mask as the subnet mask configured for the interfaces in question. This contrasts with classless routing protocols that can use variable length subnet masks. Classful protocols have become less popular as they are wasteful of IP address space.

In order to address the issues of address space and other factors, Cisco created EIGRP (Enhanced Interior Gateway Routing Protocol). EIGRP adds support for VLSM (variable length subnet mask) and adds the Diffusing Update Algorithm (DUAL) in order to improve routing and provide a loopless environment. EIGRP has completely replaced IGRP, making IGRP an obsolete routing protocol. In Cisco IOS versions 12.3 and greater, IGRP is completely unsupported. In the new Cisco CCNA curriculum (version 4), IGRP is mentioned only briefly, as an “obsolete protocol”.

The IGRP protocol allows a number of gateways to coordinate their routing. Its goals are the following:

- Stable routing even in very large or complex networks. No routing loops should occur, even as transients.
- Fast response to changes in network topology.
- Low overhead. That is, IGRP itself should not use more bandwidth than what is actually needed for its task.
- Splitting traffic among several parallel routes when they are of roughly equal desirability
- Taking into account error rates and level of traffic on different paths.

A very simple configuration of IGRP can be:

Router A

```
RouterA# conf t
RouterA(config)# interface eth0
RouterA(config-if)# ip address 70.0.0.1 255.0.0.0
RouterA(config-if)# exit
RouterA(config)# interface serial0
RouterA(config-if)# ip address 20.30.40.2 255.255.255.252
RouterA(config-if)# exit
RouterA(config)# router igrp 1
RouterA(config-router)# redistribute connected
RouterA(config-router)# network 20.0.0.0
RouterA(config-router)# network 70.0.0.0
RouterA(config-router)# network 71.0.0.0
```

Router B

```
RouterB# conf t
RouterB(config)# interface eth0
RouterB(config-if)# ip address 71.0.0.1 255.0.0.0
RouterB(config-if)# exit
RouterB(config)# interface serial0
RouterA(config-if)# ip address 20.30.40.1 255.255.255.252
RouterA(config-if)# exit (config)# router igrp 1
RouterA(config-router)# redistribute connected
RouterA(config-router)# network 20.0.0.0
RouterA(config-router)# network 70.0.0.0
RouterA(config-router)# network 71.0.0.0
```

A few other commands might come in useful. Variance 2 can be used to configure IGRP to load balance between equal cost paths. The command passive-interface eth0 disables IGRP from sending updates out of eth0.

Testing

```
router# debug ip igrp events
```

Only shows the sending or receiving of IGRP packets and the number of routes in each update. It does show the routes that are advertised!

```
router# debug ip igrp transactions
```

Seems as debug ip igrp events but also shows the routes that are advertised.

```
router# show ip route
```

As with debugging any routing problem, look at the routing table. Is there a static route that takes precendece?

```
router# show ip interface brief
```

This command is always useful to quickly verify which links are and which aren't.

3.7. EIGRP

How to Configure EIGRP on a Cisco Router

When would you need this: When you are implementing a routing protocol on a large Internetwork and all the networking devices involved are Cisco devices or devices supporting EIGRP.

Special Requirements: EIGRP is a Cisco proprietary protocol. So, either all the routers in the Internetwork must be Cisco routers, or the routers should be EIGRP capable.

Before we start, if you have not set the bandwidth of the interfaces, set them now. For correct routing decisions, you need to set the bandwidth for the serial interfaces depending on the WAN technologies that you are using. This is done using the following command on each serial interface:

Router (config-if) #bandwidth bandwidth

Where bandwidth is the bandwidth of the WAN connection in kilobits per second.
Next, you can start configuring EIGRP as in the following steps:

1. Enable EIGRP on the router with the command,

   Router (config)#router eigrp autonomous-system where autonomous-system is the autonomous system number. The same autonomous-system number must be used for all the routers that you want to exchange routing information.

2. Instruct the router to advertise the networks that are directly connected to it.

   Router (config-router) #network network-address where network-address is the network address of a network that is directly connected to the router. Repeat this step for each network that is directly connected to the specific router that you are configuring. For sub netted networks, remember that you need only to write the original network address of a group of subnets and the router will automatically identify the subnets. For example, if the router is connected to the networks, 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24, you will need to do one 'network' command with the address 172.16.0.0.

3. By default, EIGRP packets consume a maximum of 50% of the link bandwidth, as configured with the 'bandwidth' interface configuration command. You might want to change that value if a different level of link utilization is required or if the configured bandwidth does not match the actual link bandwidth (it may have been configured to influence route metric calculations). Use the following command to set the percentage of bandwidth to be used on each interface separately:
   Router (config-if) #ip bandwidth-percent eigrp bandwidth percentage
   Where bandwidth-percentage is the percentage of bandwidth to be used
4. You can change the intervals of the hello packets and the hold down timer on each interface using command:
   Router (config-if) #ip hello-interval eigrp autonomous system timer where autonomous-system is the autonomous system number and time is the new hello packet interval time in seconds. Router (config-if) #ip hold-time eigrp autonomous-system time
   Where autonomous-system is the autonomous system number and time is the new hold down time in seconds.
5. Check your configuration on the routers after configuring all the routers in the internetwork using the following commands: To display information about interfaces configured for EIGRP.

Router #show ip eigrp interfaces interface-type autonomous-system Display the EIGRP discovered neighbors.
Router #show ip eigrp neighbors to display the EIGRP topology table for a given process.
Router #show ip eigrp topology autonomous-system
Or
Router #show ip eigrp topology network-address subnet mask To display the number of packets sent and received for all or a specified EIGRP process.

Router #show ip eigrp traffic autonomous-system where interface-type is the interface type. Autonomous-system autonomous system number. Network-address and subnet mask are the network address and subnet mask.

How to Configure EIGRP Metrics on a Cisco Router

Although it is not recommended, if you need to change the way the metrics of the routes are calculated, you can set them using the command: Router (config-router) #metric weights type-of-service K1 K2 K3 K4 K5
Where type-of-service is the type of service index and the values of k1–k5 are used to calculate the metric using the following equation:

$$\text{metric} = \left(k1 \times \text{bandwidth} + \frac{k2 \times \text{bandwidth}}{256 - \text{load}} + k3 \times \text{delay}\right) \times \frac{k5}{\text{reliability} + k4}$$

the default values are k1 = k3 = 1 and k2 = k4 = k5 = 0 and if k5 = 0, the formula is reduces to

$$\text{metric} = \left(k1 \times \text{bandwidth} + \frac{k2 \times \text{bandwidth}}{256 - \text{load}} + k3 \times \text{delay}\right)$$

It is highly recommended that you leave the metric in the default values unless you are a highly experienced network designer.

How to Configure EIGRP for IPv6 on a Cisco Router

When would you need this: When you are implementing a routing protocol on a large IPv6 Internetwork and all the networking devices involved are Cisco devices or devices supporting EIGRP.

Special Requirements: EIGRP is a Cisco proprietary protocol. So, either all the routers in the Internetwork must be Cisco routers, or the routers should be EIGRP capable.

1. Enable IPv6 routing on the router:
   Router (config)#ipv6 unicast-routing
2. Enable EIGRP on the router:
   Router (config) #ipv6 router eigrp autonomous-system number
   Where autonomous-system-number is the number of the autonomous system in which this EIGRP process will run. Remember to use the same autonomous system number in all the routers that you want to exchange routing information.
3. Enable IPv6 on the interface you want to participate in the EIGRP process:
   Router (config-if) #ipv6 enable Using the ‘ipv6 enable’ command will inform the router to create a link-local IPv6 address for this interface. If you want to use a different IPv6 address, you can use the following command instead of ‘ipv6 enable’:
   Router (config-if) #ipv6 address ipv6-address/prefix length
   Where ipv6-address is the IPv6 address you want to assign to this interface. Prefix-length is the prefix length for the IPv6 address.
4. Enable EIGRP on the interface connected to other EIGRP-enabled routers by identifying the autonomous system number this interface will be part of:
   Router (config-if) #ipv6 eigrp autonomous-system-number where autonomous-system-number is the number of the autonomous system in which this EIGRP process will run. Remember to use the same autonomous system number used in steps 2 and 4.
5. If you want to manually set up the RouterID to control the internal process of EIGRP, you can use the following optional steps:
   Router (config-if) #ipv6 router eigrp autonomous system numberRemember to use the same autonomous system number used in steps 2 and 4.
   Router (config-router) #eigrp router-id router-id where router-id is the RouterID used in the EIGRP process. The RouterID is formatted as an IPv4 address even if you are using EIGRP for IPv6 networks. Router (config-router)#exit
6. By default, EIGRP packets consume a maximum of 50% of the link bandwidth, as configured with the ‘bandwidth’ interface configuration command. You might want to change that value if a different level of link utilization is required or if the configured bandwidth does not match the actual link bandwidth (it may have been configured to
   influence route metric calculations). Use the following command to set the percentage of bandwidth to be used on each interface separately:
   Router (config-if) #ipv6 bandwidth-percent eigrp autonomous-system-number bandwidth percentage
   Where autonomous-system-number is the number of the autonomous system in which this EIGRP process will run. Bandwidth-percentage is the percentage of bandwidth to be used.
7. To troubleshoot, use the following commands:
   Router#show ipv6 eigrp autonomous-system-number
   Router#show ipv6 eigrp interface interface-type interface-number
   Router#show ipv6 eigrp interface interface-type interface-number autonomous-system-number

EIGRP Implementation Notes

1. If you are using discontinuous networks, which is mostly the case, you should turn off auto-summarization using the following command: Router (config)#no ip auto-summary.

2. You can set manual summary addresses using the following command: Router (config-if)#ip eigrp summary address autonomous system summarized-network summary-subnet mask where autonomous-system is the autonomous system number and summarized summarized-network is the network address expressing the summary of multiple networks. Summary-subnet mask is the subnet mask for the summarized address.
3. When you are using non-broadcast networking technologies such as Frame Relay and SMDS, you will need to turn off split-horizon to let EIGRP perform efficiently and effectively. Router (config-if)#no ip split-horizon autonomous-system where autonomous-system is the autonomous system number.
4. To clear the neighbour table, use the command:
   Router#clear ip eigrp neighbors

3.8. OSPF

When would you need this: When you need to set up dynamic routing with Cisco and non-Cisco routers.

Special Requirements: None.

OSPF is one of the most widely used dynamic routing protocols. Cisco's version of OSPF is compatible with non-Cisco routers. Single-area OSPF is suitable for small-to-medium internetworks. An area is a logical grouping of routers running OSPF. All routers in the same area share the same topology database. Multiple-Area OSPF is used for large networks to prevent their topology databases from becoming out of the capability of the router. Single-area OSPF configuration is as follows:

1. Since OSPF best route calculations rely solely on bandwidth, you need to set up the bandwidth of the serial interface involved in the routing process using the following command on the interface:
   Router(config-if)#bandwidth bandwidth
   Where: bandwidth is the bandwidth of the connection in kilobits per second. Remember that this command does not change the actual bandwidth. It only changes the bandwidth value being used by the routing protocol for the purpose of best path calculation.
2. Instruct the router to activate the OSPF routing process:
   Router (config)#router ospf process-number Where: process-number is the process number of OSPF. This process number is of local significance. It does not have to be the same on all routers.
3. Instruct the router to advertise the directly connected networks:
   Router(config-router)#network network-address wildcard mask area 0 Where: network-address is the network address of a directly connected network. Wildcard-mask is the wildcard mask of the network address. Since we are setting a single-area OSPF, we will always use 'area 0'.
4. Repeat step 3 for every network that is directly connected to the router. If you finished the first four steps on all the routers involved in the process, everything should work just fine.

If you want to do more configurations, there are a few optional advanced steps to go through:

1. To change the selection process of the DR (Designated Router) and BDR (Backup Designated Router), use the following command to change the router's OSPF priority on a certain interface:
   Router(config)#ip ospf priority priority
   Where: priority is the priority (0–255). The router with the highest priority becomes the DR. A priority of 0 means that this router will never be elected as DR.
2. To restart the whole process of DR and BDR elections, use the command:

   Router#clear ip ospf process *

3. To change the cost of a certain link in the OSPF process, use the following command:
   Router(config-if)#ip ospf cost suggested-cost
   Where: CC is the suggested cost (0–65, 535).

   For troubleshooting, you can use the following commands:

1. To show the OSPF processes information:
   Router#show ip ospf
2. To show the OSPF database of the topology:
   Router#show ip ospf database
3. To show the OSPF operation on the interfaces:
   Router#show ip ospf interface
4. To show the OSPF neighbors table
   Router#show ip ospf neighbor
5. To debug all the OSPF process events:
   Router#debug ip ospf events

How to Configure Single-Area OSPFv3 for IPv6 on a Cisco Router
When would you need this: When you need to set up dynamic routing with Cisco and non-Cisco routers Special Requirements: None.

1. Enable IPv6 routing on the router: Router (config)#ipv6 unicast-routing
2. Since OSPF best route calculations rely solely on bandwidth, you need to set up the bandwidth of the serial interface involved in the routing process using the following command on the interface: Router(config-if)#bandwidth bandwidth
   Where: bandwidth is the bandwidth of the connection in kilobits per second. Remember that this command does not change the actual bandwidth. It only changes the bandwidth value being used by the routing protocol for the purpose of best path calculation.
3. Instruct the router to activate the OSPF routing process: Router(config)#ipv6 router ospf process-number
   Where process-number is the process number of OSPF. This process number is of local significance. It does not have to be the same on all routers.
4. Enable OSFP process on each interface you want to participate in the OSPF process:
   Router(config)#interface interface-type interface number
   Router(config-if)#ipv6 enable
   Router(config-if)#ipv6 ospf process-number Area 0
   Where interface-type and interface-number are the type and number of the interface. Process-

number is the process number of OSPF identified in step 3. Since we are setting a single-area OSPF, we will always use ‘area 0’. Using the ‘ipv6 enable’ command will inform the router to create a link-local IPv6 address for this interface.

If you want to use a different IPv6 address, you can use the following command instead of ‘ipv6 enable’:

```
Router(config-if)#ipv6 address ipv6-address/prefix length
```

Where ipv6-address is the IPv6 address you want to assign to this interface. Prefix-length is the prefix length for the IPv6 address.

5. Repeat step 4 for every network that is directly connected to the router. If you finished the first four steps on all the routers involved in the process, everything should work just fine.

   If you want to do more configurations, there are a few optional advanced steps to go through:

1. To change the selection process of the DR (Designated Router) and BDR (Backup Designated Router), use the following command to change the router’s OSPF priority on a certain interface: Router(config)#ipv6 ospf priority priority where priority is the priority (0–255). The router with the highest priority becomes the DR. A priority of 0 means that this router will never be elected as DR.
2. To restart the whole process of DR and BDR elections, use the command:

   ```
   Router#clear ipv6 ospf process *
   ```

3. To change the cost of a certain link in the OSPF process, use the following command:

   ```
   Router(config-if)#ipv6 ospf cost suggested-cost
   ```

   Where CC is the suggested cost (0–65,535) For troubleshooting, you can use the following commands:

1. To show the OSPF processes information: Router#show ipv6 ospf
2. To show the OSPF database of the topology: Router#show ipv6 ospf database
3. To show the OSPF operation on the interfaces: Router#show ipv6 ospf interface
4. To show the OSPF neighbors table: Router#show ipv6 ospf neighbor
5. To debug all the OSPF process events: Router#debug ipv6 ospf events

How to Configure HSRP on a Cisco Router

When would you need this: When your network design requires redundancy and high availability?

Special Requirements: None.

To understand why and how HSRP protocol works, you need to look into an example. For each local network, there is a default-gateway. This default-gateway is usually the LAN interface of the router. If your network design requires high availability and redundancy, you can use HSRP to set up a different interface in a different router to operate as a standby interface such that whenever the main default-gateway fails, the standby becomes active and the network operation is not interrupted.

HSRP operates by setting a main IP address and a standby IP address for the routers' interfaces that are taking part in the HSRP operation. Most of the time, the IP address used as the default-gateway is called the virtual IP. Let us jump into the configuration:

1. On the first router, configure the main IP address:
   ```
   Router1(config-if)#ip address ip-address subnetmask
   ```
2. On the first router, configure the virtual IP address:
   ```
   Router1(config-if)#standby hsrp-group-number ip virtualip-address
   ```
3. On the first router, set up the priority of the virtual IP
   ```
   Router1(config-if)#standby hsrp-group-number priority standby-priority
   ```
   Where ip-address and subnetmask are the IP main address and subnet mask of the interface. hsrp-group-number is the HSRP group number. You have to use the same number in all the routers that you want to participate in the same HSRP process. Virtual-ip-address is the virtual IP address to be used when the standby router becomes active. Standby-priority is the priority of the standby IP address. The number can be between 0 and 255. The router with the highest priority will be the active one.
4. On the second router, configure the main IP address (which is different from the one used in Router1):
   ```
   Router2(config-if)#ip address ip-address subnetmask
   ```
5. On the second router, configure the virtual IP address:
   ```
   Router2(config-if)#standby hsrp-group-number ip virtualip-address
   ```
6. On the first router, set up the priority of the virtual IP
   ```
   Router2(config-if)#standby hsrp-group-number priority Standby-priority
   ```
   Where ip-address and subnetmask are the IP main address and subnetmask of the interface. hsrp-group-number is the HSRP group number. You have to use the same number in all the routers that you want to participate in the same HSRP process. virtual-ip-address is the virtual IP address to be used when the standby router becomes active. Standby-priority is the priority of the standby IP address. The number can be between 0 and 255. The router with the highest priority will be the active one.
7. You can troubleshoot using the commands:
   ```
   Router#show standby
   Router#show standby brief
   Router#show standby all
   ```

How to Configure VRRP on a Cisco Router

When would you need this: When your network design requires redundancy and high availability.

Special Requirements: None.

VRRP operates by setting a main IP address and a standby IP address for the routers' interfaces that are taking part in the VRRP operation. Most of the time, the IP address used as the default-gateway is called the virtual IP. Let us jump into the configuration:

1. On the first router, configure the main IP address:
   ```
   Router1(config-if)#ip address ip-address subnetmask
   ```
2. On the first router, configure the virtual IP address:
   ```
   Router1(config-if)#vrrp group-number ip virtualip-address
   ```
3. On the first router, set up the priority of the virtual IP
   ```
   Router1(config-if)#vrrp group-number priority standbypriority
   ```
   Where ip-address and subnetmask are the IP main address and subnetmask of the interface. group-number is the VRRP group number. You have to use the same number in all the routers that you want to participate in the same VRRP process. Virtual-ip-address is the virtual IP address to be used when the standby router becomes active. Standby-priority is the priority of the standby IP address. The number can be between 0 and 255. The router with the highest priority will be the active one.
4. On the second router, configure the main IP address (which is different from the one used in Router1 and from the virtual IP):
   ```
   Router2(config-if)#ip address ip-address subnetmask
   ```
5. On the second router, configure the virtual IP address:
   ```
   Router2(config-if)#vrrp group-number ip virtualip-address
   ```
6. On the first router, set up the priority of the virtual IP
   ```
   Router2(config-if)#vrrp group-number priority standbypriority
   ```
   Where ip-address and subnetmask are the IP main address and subnetmask of the interface. group-number is the GLBP group number. You have to use the same number in all the routers that you want to participate in the same GLBP process. virtual-ip-address is the virtual IP address to be used when the standby router becomes active. standby-priority is the priority of the standby IP address. The number can be between 0 and 255. The router with the highest priority will be the active one.
7. You can troubleshoot using the commands:
   ```
   Router#show vrrp
   Router#show vrrp brief
   ```

3.9. DHCP

How to Configure a Cisco Router as a DHCP Client

When would you need this: When your ISP gives you a dynamic IP address upon each connection or you need to configure the router to obtain its interface IP address automatically? Special Requirements: None.

This is done using a single command:

Router(config-if)#ip address dhcp Some service providers might ask you to use a client-id and/or a hostname of their own choice. This can be done by adding the following parameters to the command above:

```
Router(config-if)#ip address dhcp client-id interfacename hostname hostname
```

Where interface-name is the interface name that will be used for the client-id and hostname is the hostname that will be used for the DHCP binding. This hostname can be different from the one that was set for the router in the global configuration. You can use both of these parameters, one of them, or none of them.

How to Configure a Cisco Router as a DHCP Server

When would you need this: When using the router as a DHCP server to provide IP addresses and related information to DHCP clients?

Special Requirements: DHCP server software is supported for these series: 800, 1000, 1400, 1600, 1700 series (support for the Cisco 1700 series was added in Cisco IOS Release 12.0[2]T), 2500, 2600, 3600, 3800, MC3810, 4000, AS5100, AS5200, AS5300, 7000, 7100, 7200, MGX 8800 with an installed Route Processor Module, 12000, uBR900, uBR7200, Catalyst 5000 family switches with an installed Route Switch Module, Catalyst 6000 family switches with an installed Multi-Layer Switch Feature Card, and Catalyst 8500.
The configuration steps are as follows:

1. Define the DHCP address pool:
   ```
   Router(config)#ip dhcp pool dhcp-pool-name
   Router(dhcp-config)#network network-address subnetmask
   ```
   Where dhcp-pool-name is the DHCP pool name, network-address is the network address to be used by the DHCP pool, and subnetmask is the subnet mask for the network. You can replace the subnet mask by (/prefix) to provide the subnet mask.
2. Configure the parameters to be sent to the client:
   ```
   Router(dhcp-config)#dns-server dns-server-address
   ```
   To provide the DNS server IP address:
   ```
   Router(dhcp-config)#default-router default-gateway address
   ```
   To provide the IP address of the default-gateway, which is usually the IP address of the router interface connected to the network.
   ```
   Router(dhcp-config)#domain-name domain
   ```
   To provide the name of the domain of the network (if in a domain environment):
   ```
   Router(dhcp-config)#netbios-name-server netbios-server address
   ```
   To provide the IP address of the NetBIOS name server:
   ```
   Router(dhcp-config)#lease days hours minutes
   ```
   To define the lease time of the addresses given to the client. You can make it infinite, which is not advised, by using this command instead
   ```
   Router(dhcp-config)#lease infinite
   ```
   There is a large group of settings that you can configure to be sent to the clients and I have only mentioned the most frequently used.
3. Configure the IP addresses to be excluded from the pool. This is usually done to avoid the conflicts caused by the DHCP with servers and printers. Remember to give all servers and network printers' static IP addresses in the same range of the DHCP pool. Afterward, exclude these addresses from the pool to avoid conflicts.

Router(config)#ip dhcp excluded-address excluded-ipaddress Use the command in the previous form to exclude a single address. You can repeat it as many times as you see fit for the IP addresses you want to exclude. You can also use the same command to exclude a range of IP addresses all in a single command:

```
Router(config)#ip dhcp excluded-address start-ip-address end-ip-address
```

Where start-ip-address is the first address in the range to be excluded from the pool and end-ip-address is the last excluded address in the range.

4. Enable the DHCP service in the router:

   ```
   Router(config)#service dhcp
   ```

   To disable it, use Router(config)#no service dhcp
   Usually, the DHCP service is enabled by default on your router
5. Use the following commands to check the DHCP operation on the router:

   ```
   Router#show ip dhcp binding
   ```

   This command shows the current bindings of addresses given to clients.

   ```
   Router#show ip dhcp server statistics
   ```

   This command shows the DHCP server statistics.

   ```
   Router#debug ip dhcp server
   ```

   This debug command is used to troubleshoot DHCP issues.

Implementation notes:

1. You can create a DHCP database agent that stores the DHCP binding database. A DHCP database agent is any host; for example, an FTP, TFTP, or RCP server that stores the DHCP bindings' database. You can configure multiple DHCP database agents, and you can configure the interval between database updates and transfers for each agent. To configure a database agent and database agent parameters, use the following command in global configuration mode:

   ```
   Router(config)#ip dhcp database URL [timeout seconds | write-delay seconds]
   ```

   An example URL is this ftp://user:password@192.168.0.3/router-dhcp
   If you choose not to configure a DHCP database agent, disable the recording of DHCP address conflicts on the DHCP server. To disable DHCP address conflict logging, use the following command in global configuration mode:

   ```
   Router(config)#no ip dhcp conflict logging
   ```

2. DHCP service uses port 67 and 68. So, if you are using a firewall, remember to open these ports. To clear DHCP server variables, use the following commands as needed:

   ```
   Router#clear ip dhcp server statistics
   Router#clear ip dhcp binding *
   ```

   If you want to clear a certain binding not all of them, replace the * in the previous command with the IP address to be cleared.

How to Configure a Cisco Router as a DHCP Server for IPv6

When would you need this: When using the router as a DHCP server to provide IPv6 in stateless and stateful configuration of DHCPv6.
Special Requirements: DHCPv6 support in IOS.

1. Create the DHCP pool:
   ```
   Router(config)#ipv6 dhcp pool pool-name
   ```
2. Configure the parameters you want to pass to the clients:
   ```
   Router(config-dhcp)#dns-server server-ipv6-address
   Router(config-dhcp)#domain-name domain
   ```
3. If you are working on a stateless address auto-configuration scenario, skip the next two steps and jump to 6.
4. Configure the IPv6 address prefix:
   ```
   Router(config-dhcp)#address prefix ipv6-address-prefix
   ```
   Where the ipv6-address-prefix is the 64-bit hexadecimal network address prefix.
5. An optional step is to set up a link address prefix: Router(config-dhcp)#link-address ipv6-link-prefix
6. Enable DHCPv6 on the interface you want to be part of the DHCP process and assign a specific pool to the interface:
   ```
   Router(config-if)#ipv6 dhcp server pool-name
   ```
7. Check the address leases (in stateful addressing only):
   ```
   Router#show ipv6 dhcp lease
   ```

How to Configure DHCP Relay in Cisco Router IPv4

If you have a DHCP server other than the router and you would like the router to pass the DHCP requests to this DHCP server laying outside the LAN, go to the LAN interface that does not have the DHCP server and type the following command:

```
Router(config-if)#ip helper-address dhcp-server-address
```

where dhcp-server-address is the IP address of the DHCP server located outside this LAN.

IPv6

If you have a DHCPv6 server other than the router and you would like the router to pass the DHCPv6 requests to this DHCPv6 server laying outside the LAN, go to the LAN interface that does not have the DHCPv6 server and type the following command:

```
Router(config-if)#ipv6 dhcp relay destination dhcp-serveripv6-address
```

Where dhcp-server-ipv6-address is the IPv6 address of the DHCP server located outside this LAN.

3.10. NAT and PAT

When would you need this: When you want to connect a local network to the Internet and the available global IP addresses are less than the local IP addresses. This can also be used as an additional security feature.

Special Requirements: None.

There are two types of NAT that can be configured on a Cisco router: static and dynamic.

Static NAT Configuration

This type is used when you want to do one-to-one assignment of global (namely public) IP addresses to local IP addresses.

1. Establish static translation between an inside local address and an inside global address: Router(config)#ip nat inside source static local-ip-address global-ip-address where local-ip address is the (inside) local address and global-ip-address is the (inside) global address.
2. Specify the local interface (the interface connected to the internal network). This is done by going to the interface configuration mode and issuing:
   Router(config-if)#ip nat inside
3. Specify the global interface (the interface connected to the external network).
   This is done by going to the interface configuration mode and issuing:
   Router(config-if)#ip nat outside

Dynamic NAT Configuration

This type is used when you want the router to do the mapping dynamically. This method is useful when you have too many global and local addresses and you do not want to do the mapping manually, or when the number of global addresses available is less than the local addresses.

This would lead us to two different scenarios:

A. The number of global IP addresses is more than one and it is equal or less than the local addresses.

1. Define a pool of global addresses that would be employed in the translation:

   Router(config)#ip nat pool pool-name first-public-address last-public-address netmask public-subnetmask.
   Where pool-name is the name of the pool, first-public-address is the starting IP address of the pool, last-public-address is the end IP address of the pool, and public-subnetmask is the subnet mask of the network that the pool is part of (i.e., the global network).

2. Define the range of local addresses permitted to participate in the translation using an access-list:
   Router(config)#access-list access-list-number permit local-network-address wildcard-mask
   Where access-list-number is the number of the access-list, which is usually a standard access list; thus, the number can be any number from 1 to 99; local-network-address is the network address of the local network or the starting IP address of the range; and wildcard-mask is the wildcard mask used to define the range. You can issue more than one access-list sentence in the same access-list to define the specific IP address range(s). If you are not familiar with wildcard masks, refer to the note in section.

3. Associate the pool and the local range in a dynamic NAT translation command:
   Router(config)#ip nat inside source list access-list number pool nat-pool-name [overload]
   Where : access-list-number is the number of the access-list, nat-pool-name is the name of the global pool, and overload : This parameter must be used when you have global IP addresses less than local IP addresses (this type of NAT is also known as Port Address Translation, PAT).
4. Specify the local interface. This is done by going to the interface configuration mode and issuing:
   Router(config-if)#ip nat inside
5. Specify the global interface. This is done by going to the interface configuration mode and issuing:
   Router(config-if)#ip nat outside

B. The other scenario is when there is only one global IP address and a group of local IP addresses.

In this case, the only global IP address is assigned to the interface connected to the global network.

1. Define the range of local addresses permitted to participate in the translation using an access-list:
   Router(config)#access-list access-list-number permit local-network-address wildcard mask
   Where: access-list-number is the number of the access-list, which is usually a standard accesslist; thus, the number can be any number from 1 to 99, local-network-address is the network address of the local network or the starting IP address of the range, and wildcard-mask is the wildcard mask used to define the range. You can issue more than one access-list sentence in the same access-list to define the specific IP address range(s). If you are not familiar with wildcard masks, refer to the note in Section.
2. Associate the pool and the local range in a dynamic NAT translation command:
   Router(config)#ip nat inside source list access-listnumber interface interface-type interface-number overload .
   Where: access-list-number is the number of the access-list, interface-type is the type of the interface that has the global IP address (e.g., serial or Ethernet), and interface-number is the number of the interfaces. An example of the interface type and number is serial 0 or Ethernet 0/0.
3. Specify the local interface. This is done by going to the interface configuration mode and issuing:

   Router(config-if)#ip nat inside

4. Specify the global interface. This is done by going to the interface configuration mode and issuing:
   Router(config-if)#ip nat outside

Troubleshooting Commands

1. To show the current translations performed by NAT
   Router#show ip nat translation
   Note that these translations have a certain lifetime. They do not remain in the list forever. If you

need to test your NAT configuration, ping to an outside host from an inside host and look for the translations immediately.

2. To show the static translations of NAT:
   Router#show ip nat static
3. To watch the instantaneous interactions of NAT:
   Router#debug ip nat

Disabling NAT

To disable NAT, you need to do the following steps:

1. Disable NAT on the local and global interfaces:
   Router(config-if)#no ip nat inside on the local, and
   Router(config-if)#no ip nat outside on the global interface.
2. Clear the contents of the translation table:
   Router#clear ip nat translations
3. Remove the NAT assignment command by preceding it with a 'no'. For example,
   Router(config)#no ip nat inside source list access-listnumber interface interface-type interface-number overload
4. Remove the access-list, if any, by putting 'no' ahead of the command: Router(config)#no access-list access-list-number

NAT-PT Configuration for IPv6

When would you need this:

When you have IPv6-only devices that need to communicate with IPv4-only devices.
Special Requirements: None.
NAT-PT, where PT stands for Protocol Translation, is a tunneling protocol that is used to translate IPv6 into IPv4 and vice versa. NAT-PT can operate in one of the three modes: static, dynamic, and Port Address. Translation.

Before configuring NAT-PT, you need to enable IPv6 routing on the translation router using this command:
Router(config)#ipv6 unicast-routing

1. In static configuration, an IPv6 address is statically mapped into an IPv4 address using the following command:
   Router(config)#ipv6 nat v6v4 source ipv6-address ipv4- address
   Where ipv6-address is the IPv6 address assigned to the IPv6-only host and ipv4-address is the

IPv4 address assigned to the IPv4-only host. The previous command needs to be configured once for every address. In a similar fashion, we need to identify the reversed mapping from IPv4 to IPv6 using the following command:

```
Router(config)#ipv6 nat v6v4 source ipv4-address ipv6- address
```

where: ipv6-address is the IPv6 address assigned to the IPv6-only host and ipv4-address is the IPv4 address assigned to the IPv4-only host. The next step is to enable IPv6 NAT on the IPv4 interface:

```
Router(config-if)#ipv6 nat
```

2. In dynamic configuration, you will need to configure translation in both ways: IPv6-to-IPv4 and IPv4-to-IPv6. For the first option, IPv6-to-IPv4, you will need to identify the IPv6 addresses using an access-list and map it to an IPv4 address pool to be used in the translation.
   First, we identify the pool of IPv4 addresses using the command:

   ```
   Router(config)#ipv6 nat v6v4 pool pool-name start-address end-address prefix-length prefix-length
   ```

   Where pool-name is the name of the NAT pool, start-address and end-address are the first and last addresses in the pool, and prefix-length is the prefix length of the IPv4 network. Next, we create a named access-list to identify the range of IPv6 addresses that are allowed to participate in the translation. This is done using the following commands:

   ```
   Router(config)#ipv6 access-list acl-name
   Router(config-ipv6-acl)#permit ip ipv6-source-prefix/ prefix-length any
   ```

   Where: acl-name is the name of the access-list, ipv6-source-prefix is the IPv6 prefix address of the hosts that are allowed to use this NAT translation, and prefix-length is the IPv6 network prefix length.
   Repeat the last command as many times as you need to include all the addresses you want to participate in the translation.
   The last step is to configure the mapping using the following command:

   ```
   Router(config)#ipv6 nat v6v4 source list acl-name pool pool-name
   ```

   Where acl-name is the name of the access-list identified in the previous step and pool-name is the name of the NAT pool we identified earlier. In the second part, we will need to identify the IPv4-to-IPv6 mapping using similar commands to the ones used before but exchanging IPv4 and IPv6 addresses.
   First, we identify the pool of IPv6 addresses using the command:

   ```
   Router(config)#ipv6 nat v6v4 pool pool-name start-address end-address prefix-length prefix-length
   ```

   Where pool-name is the name of the NAT pool, start-address and end-address are the first and last addresses in the pool, and prefix-length is the prefix length of the IPv6 network. Next, we create a numbered (or named) access-list to identify the range of IPv4 addresses that are allowed to participate in the translation.
   This is done using the following commands:

   ```
   Router(config)#access-list acl-number permit ip ipv4- network-address wildcard-mask
   ```

   Where acl-number is the number of the access-list. The number should be within the range 1-99 because it is a standard ACL; ipv4-network-address is the IPv4 network that includes the hosts that are allowed to use this NAT translation; and wildcard-mask is the wildcard mask that identifies the range.
   Repeat the last command as many times as you need to include all the addresses you want to participate in the translation using the same access-list number.

The last step is to configure the mapping using the following command:

```
Router(config)#ipv6 nat v6v4 source list acl-number pool pool-name
```

Where acl-name is the name of the access-list identified in the previous step and pool-name is the name of the NAT pool we identified earlier.

3. Port Address Translation is configured in an identical manner to the previous case of dynamic mapping with the exception of one small difference. In the mapping command, add the word overload at the end after the pool name.
4. For verification purposes, use the following commands:

```
Router#show ipv6 nat translations
Router#clear ipv6 nat translation *
Router#debug ipv6 nat detail
```

3.11. PPP

How to Configure PPP on a Cisco Router

When would you need this: When you are creating a WAN link? This procedure might also be required when the other end of a WAN link is not a Cisco router. Point-to-Point Protocol can be used in synchronous, asynchronous, HSSI, and ISDN links.

Special Requirements: None.

Special Requirements: None.

1. Get to the interface configuration mode of the router's serial interface and issue the following command,

```
Router(config-if)#encapsulation ppp
```

2. If you want to configure authentication (which is almost always the case), go through the following steps:

- Choose the authentication type: Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP)

```
Router(config-if)#ppp authentication authentication type
```

Where authentication type is the authentication type, which can be: PAP, CHAP, PAP CHAP, or CHAP PAP. The last two choices are to use the second authentication type when the first one fails. CHAP is strongly recommended over PAP for two reasons. First, PAP sends the username and password in plaintext, while CHAP sends hashed challenges only.
Second is that CHAP does an operation similar to periodic re-authentication in the middle of the communication session, such that it provides more security than PAP.

- Set a username and a password that the remote router would use to connect to your local router. You can define many username/password pairs for many PPP connections to the same router.

```
Router(config)#username remote-username password remote-password
```

Where remote-username is username sent from the remote router, and remote-password is its password. If the remote router was not configured with a username to send, it will send its hostname instead. Issue this command once for each PPP connection. For example, if you are connecting RouterA to RouterB and RouterC, on RouterA issue this command once for each remote router.

- Now, you can set the username and password that your local router would send to access the remote router. For PAP authentication, you can specify the username and password that the local router will send to the remote router for authentication using the following command, Router(config-if)#ppp pap sent-username sent-username password sent-password For CHAP, two commands are used,

  ```
  Router(config-if)#ppp chap hostname sent-usernam
  Router(config-if)#ppp chap password sent-password
  ```

  The usernames and passwords are case sensitive, so be careful when writing them. This way, you will have to write the username and password of the remote router in your local router and write the username and password of your local router into your remote using the ‘username’ command. If you do not set the username and password that will be sent from the local router to the remote router for authentication, the router will use its hostname and secret password instead.

3. You can monitor the quality of the serial link that is using PPP with the following command,

   ```
   Router(config-if)#ppp quality percentage
   ```

   Where percentage is the minimum accepted link quality. If the link quality drops below the percentage, the link will be shutdown and considered bad.
4. If the available bandwidth is small, you might consider compressing the data being transmitted using the following command,

   ```
   Router(config-if)#ppp compress compression-type
   ```

   Where compression type is the compression type which can be predictor or stacker.
5. To troubleshoot PPP, you can use the following commands,

   ```
   Router#debug ppp negotiations
   Router#debug ppp packets
   Router#debug ppp errors
   Router#debug ppp authentication
   ```

3.12. Frame Relay

How to Configure Frame-Relay in a Cisco Router

When would you need this?

When you are setting up a Frame-relay WAN connection rented from a service provider.

Special Requirements: None.

Frame-relay configuration mainly depends on the topology you are using.

Point-to-Point Connection of Two Sites Using Physical Interfaces

1. On the serial interface, change the encapsulation type to Frame-relay:

   ```
   Router(config)#interface serial interface-number
   Router(config-if)#encapsulation Frame-relay
   ```

where interface number is the number of the serial interface connected to the frame-relay equipment.

2. Configure the LMI type:
   ```
   Router(config-if)#Frame-relay lmi-type lmi-type
   ```
   where lmi-type is the type of LMI standard used. The supported types are Cisco, ansi and q933a. This information should be given to you by the Frame-relay service provider.
3. Assign an IP address to the interface
   ```
   Router(config-if)#ip address ip-address1 subnetmask1
   ```
   where the ip address1 and subnetmask1 are the IP address and subnetmask assigned to the Frame-relay interface on the first side of the link.
4. Map the Frame-relay DLCI number to a destination IP address:
   ```
   Router(config-if)#Frame-relay map ip-address2 dlci-number encapsulation-type
   ```
   where
   ip-address2 is the IP address of the other side of the link. dlci-number is the virtual circuit number given to you by the Frame-relay service provider. encapsulation-type is the type of encapsulation standard used. The value is usually either Cisco or ietf. This information should also be given to you by the Frame-relay service provider.
5. On the other end, the serial interface encapsulation type is changed to Frame-relay:
   ```
   Router(config)#interface serial interface-number
   Router(config-if)#encapsulation Frame-relay
   ```
   where interface number is the number of the serial interface connected to the Frame-relay equipment.
6. Configure the LMI type:
   ```
   Router(config-if)#Frame-relay lmi-type lmi-type
   ```
   where lmi-type is the type of LMI standard used. The supported types are Cisco, ansi and q933a. This information should be given to you by the Frame-relay service provider. Usually, it is the same type used in step 2.
7. Assign an IP address to the interface
   ```
   Router(config-if)#ip address ip-address2 subnetmask2
   ```
   where the ip address2 and subnetmask2 are the IP address and subnetmask assigned to the Frame-relay interface on the second side of the link.
8. Map the Frame-relay DLCI number to a destination IP address:
   ```
   Router(config-if)#Frame-relay map ip-address1 dlci-number encapsulation-type
   ```
   where
   ip address1 is the IP address of the first side of the link. dlci-number is the virtual circuit number given to you by the Frame-relay service provider. encapsulation-type is the type of encapsulation standard used. The value is usually either Cisco or ietf. This information should also be given to you by the Frame-relay service provider.
9. Use the following commands for troubleshooting:
   ```
   Router#show Frame-relay lmi
   Router#show Frame-relay pvc
   ```

Point-to-Multipoint Using Physical Interfaces

In a point-to-multipoint Frame-relay connection, a central node is connected to a group of nodes using a single physical line. The Frame-relay network will recognize the different destinations through the use of different DLCI numbers on the same link. The configuration is similar to the previous subsection except that at the central node multiple mappings are configured on the Frame-relay interface while a single mapping is configured on each terminal interface.

1. At the central node, on the serial interface, change the encapsulation type to Frame-relay:
   ```
   Router(config)#interface serial interface-number
   Router(config-if)#encapsulation Frame-relay
   ```
   where interface number is the number of the serial interface connected to the Frame-relay equipment.
2. Configure the LMI type:
   ```
   Router(config-if)#Frame-relay lmi-type lmi-type
   ```
   where lmi-type is the type of LMI standard used. The supported types are Cisco, ansi and q933a. This information should be given to you by the Frame-relay service provider.
3. Assign an IP address to the interface
   ```
   Router(config-if)#ip address central-ip-address subnetmask1
   ```
   where the central ip address and subnetmask1 are the IP address and subnetmask assigned to the Frame-relay interface on the central side of the link.
4. Map the Frame-relay DLCI number to a destination IP address:
   ```
   Router(config-if)#Frame-relay map ip-address2 dlci-number encapsulation-type
   ```
   where
   ip address2 is the IP address of the other side of the link. dlci-number is the virtual circuit number given to you by the Frame-relay service provider. encapsulation-type is the type of encapsulation standard used. The value is usually either Cisco or ietf. This information should also be given to you by the Frame-relay service provider.
   This command is repeated once for every terminal node. Each terminal node would have a different DLCI number.
5. On the terminal end, the serial interface encapsulation type is changed to Frame-relay:
   ```
   Router(config)#interface serial interface-number
   Router(config-if)#encapsulation Frame-relay
   ```
   where interface number is the number of the serial interface connected to the Frame-relay equipment.
6. Configure the LMI type:
   ```
   Router(config-if)#Frame-relay lmi-type lmi-type
   ```
   where lmi-type is the type of LMI standard used. The supported types are Cisco, ansi and q933a. This information should be given to you by the Frame-relay service provider. Usually, it is the same type used in step 2.
7. Assign an IP address to the interface
   ```
   Router(config-if)#ip address ip-address2 subnetmask2
   ```
   where the ip address2 and subnetmask2 are the IP address and subnetmask assigned to the Frame-relay interface on the second side of the link.
8. Map the Frame-relay DLCI number to a destination IP address:
   ```
   Router(config-if)#Frame-relay map central-ip-address dlci-number encapsulation-type
   ```
   where central-ip-address is the IP address of the central side of the link. dlci-number is the virtual circuit number given to you by the Frame-relay service provider. encapsulation-type is the type of encapsulation standard used. The value is usually either Cisco or ietf. This information should also be given to you by the Frame-relay service provider.

Point-to-Multipoint Using Logical Interfaces

In what we call multiple-point-to-point scenario, a single central station is connected through a single physical link the Frame-relay network. Through that Frame-relay network, the central node is also connected to multiple terminal nodes. However, these connections are done by creating a single logical point-to-multipoint link carried over the single physical link.

1. At the central node, on the serial interface, change the encapsulation type to Frame-relay:
   ```
   Router(config)#interface serial interface-number
   Router(config-if)#encapsulation Frame-relay
   ```
   where interface number is the number of the serial interface connected to the Frame-relay equipment.
2. Configure the LMI type:
   ```
   Router(config-if)#Frame-relay lmi-type lmi-type
   ```
   where lmi-type is the type of LMI standard used. The supported types are Cisco, ansi and q933a. This information should be given to you by the Frame-relay service provider.
3. Assure that there is no IP address assigned to the interface
   ```
   Router(config-if)#no ip address
   ```
4. Create logical interface:
   ```
   Router(config-if)#interface serial interface-number.- logical-interface-number point-to-multipoint
   ```
5. On the logical interface, assign an IP address:
   ```
   Router(config-if)#ip address ip-address1 subnetmask1
   ```
   where the ip-address1 and subnetmask1 are the IP address and subnetmask assigned to the Frame-relay logical interface on the central side of the link.
6. Map the interface to a specific DLCI number:
   ```
   Router(config-subif)#Frame-relay interface-dlci dlcinumber
   ```
   where dlci-number is the virtual circuit number given to you by the Frame-relay service provider. This DLCI number resembles the virtual circuit leading to a specific remote node.
7. Repeat steps 6 for as many remote nodes as you need.
8. On the remote node, the serial interface encapsulation type is changed to Frame-relay:
   ```
   Router(config)#interface serial interface-number
   Router(config-if)#encapsulation Frame-relay
   ```
   where interface number is the number of the serial interface connected to the Frame-relay equipment.
9. Configure the LMI type:
   ```
   Router(config-if)#Frame-relay lmi-type lmi-type
   ```
   where lmi-type is the type of LMI standard used. The supported types are Cisco, ansi and q933a. This information should be given to you by the Frame-relay service provider. Usually, it is the same type used in step 2.
10. Assign an IP address to the interface
    ```
    Router(config-if)#ip address ip-address2 subnetmask2
    ```
    where the ip-address2 and subnetmask2 are the IP address and subnetmask assigned to the Frame-relay interface on the remote side of the link.
11. Map the Frame-relay DLCI number to a destination IP address:
    ```
    Router(config-if)#Frame-relay map ip-address1 dlci-number encapsulation-type
    ```

where ip-address1 is the IP address of the first side of the link. dlci-number is the virtual circuit number given to you by the Frame-relay service provider. encapsulation-type is the type of encapsulation standard used. The value is usually either Cisco or ietf. This information should also be given to you by the Frame-relay service provider.

12. Repeat steps 8, 9, 10, and 11 on each remote node using different IP addresses and DLCI numbers.

Multiple Point-to-Point Using Logical Interfaces

In what we call multiple-point-to-point scenario, a single central station is connected through a single physical link the Frame-relay network. Through that Frame-relay network, the central node is also connected to multiple terminal nodes. However, these connections are done by creating multiple logical point-to-point links carried over the single physical link. This way, the separation of traffic handled from one node to the other is clearer and the remote nodes cannot communicate unless the traffic passes through the central node.

1. At the central node, on the serial interface change the encapsulation type to Frame-relay:
   ```
   Router(config)#interface serial interface-number
   Router(config-if)#encapsulation Frame-relay
   ```
   where interface number is the number of the serial interface connected to the Frame-relay equipment.
2. Configure the LMI type:
   ```
   Router(config-if)#Frame-relay lmi-type lmi-type
   ```
   where lmi-type is the type of LMI standard used. The supported types are Cisco, ansi and q933a. This information should be given to you by the Frame-relay service provider.
3. Assure that there is no IP address assigned to the interface
   ```
   Router(config-if)#no ip address
   ```
4. Create logical interface:
   ```
   Router(config-if)#interface serial interface-number.- logical-interface-number point-to-point
   ```
5. On the logical interface, assign an IP address:
   ```
   Router(config-if)#ip address ip-address1 subnetmask1
   ```
   where the ip-address1 and subnetmask1 are the IP address and subnetmask assigned to the Frame-relay logical interface on the central side of the link.
6. Map the interface to a specific DLCI number:
   ```
   Router(config-subif)#Frame-relay interface-dlci dlcinumber
   ```
   Where dlci-number is the virtual circuit number given to you by the Frame-relay service provider. This DLCI number resembles the virtual circuit leading to a specific remote node.
7. Repeat steps 4, 5 and 6 for as many remote nodes as you need.
8. On the remote node, the serial interface encapsulation type is changed to Frame-relay:
   ```
   Router(config)#interface serial interface-number
   Router(config-if)#encapsulation Frame-relay
   ```
   where interface number is the number of the serial interface connected to the Frame-relay equipment.
9. Configure the LMI type:
   ```
   Router(config-if)#Frame-relay lmi-type lmi-type
   ```
   where lmi-type is the type of LMI standard used. The supported types are Cisco, ansi and q933a.

This information should be given to you by the Frame-relay service provider. Usually, it is the same type used in step 2.

10. Assign an IP address to the interface
    ```
    Router(config-if)#ip address ip-address2 subnetmask2
    ```
    where the ip-address2 and subnetmask2 are the IP address and subnetmask assigned to the Frame-relay interface on the remote side of the link.
11. Map the Frame-relay DLCI number to a destination IP address:
    ```
    Router(config-if)#Frame-relay map ip-address1 dlci-number encapsulation-type
    ```
    where ip-address1 is the IP address of the first side of the link. dlci-number is the virtual circuit number given to you by the Frame-relay service provider. encapsulation-type is the type of encapsulation standard used. The value is usually either Cisco or ietf. This information should also be given to you by the Frame-relay service provider.
12. Repeat steps 8, 9, 10, and 11 on each remote node using different IP addresses and DLCI numbers.

Frame-Relay and Routing Issues

Cisco routers employ a technique called split-horizon. This technique is used to eliminate routing loops by which a routing update cannot be forwarded to the same interface it came from. Building on that logic, split-horizon can cause issues when using Frame-relay point-to-multipoint topologies. Now think of a scenario where a routing update is coming from one of the remote points connected on the other end of a point-to-multipoint link. The routing update, due to split-horizon, will not be forwarded on the same physical link over to the other points connected to the point-to-multipoint topology, because it will be considered coming from one interface and cannot be forwarded over to the same interface. This way, the other points will not be able to exchange routing updates.

Split-horizon can be disabled using the following command on the interface level:

```
Router(config-if)#no ip split-horizon
```

On OSPF, you can use the following command:

```
Router(config-if)#ip ospf network point-to-multipoint
```

3.13. Router on the stick

Configuration of Router on a stick

Switches divide broadcast domain through VLAN (Virtual LAN). VLAN is a partitioned broadcast domain from a single broadcast domain. Switch doesn’t forward packets across different VLANs by itself. If we want to make these virtual LANs communicate with each other, a concept of Inter VLAN Routing is used.

Inter VLAN Routing:

Inter VLAN routing is a process in which we make different virtual LANs communicate with each other irrespective of where the VLANs are present (on same switch or different switch).

Inter VLAN Routing can be achieved through a layer-3 device i.e. Router or layer-3 Switch. When the Inter VLAN Routing is done through Router it is known as Router on a stick.

Router on a Stick:

The Router's interface is divided into sub-interfaces, which acts as a default gateway to their respective VLANs.

Configuration:

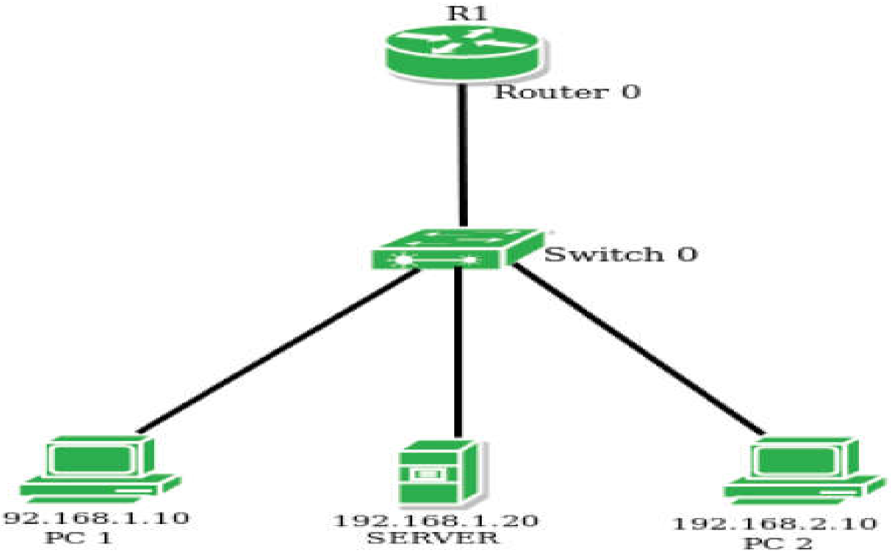


Figure 3. 5 Configuration

Here is a topology in which there is a router and a switch and some end hosts. 2 different VLANs have been created on the switch. The router's interface is divided into 2 sub-interfaces (as there are 2 different VLANs) which will acts as a default gateway to their respective VLANs. Then router will perform Inter VLAN Routing and the VLANs will communicate with each other.

First we will assign IP address to the host PC1 as 192.168.1.10/24, Server 192.168.1.20/24, and the other host PC2 will have IP address 192.168.2.10/24 manually.

Now, we will make sub-interface of fa0/0 as fa0/0.1 and fa0/0.2 and assign IP addresses as 192.168.1.1/24 and 192.168.2.1/24 respectively on the router's ports.

```
r1# int fa0/0.1
r1# encapsulation dot1q 2
r1# ip address 192.168.1.1 255.255.255.0
r1# int fa0/0.2
r1# encapsulation dot1q 3
r1# ip address 192.168.2.1 255.255.255.0
```

NOTE : Here encapsulation type dot1q is used for frame tagging between the 2 different VLAN. When the switch forwards packet of one VLAN to another, it inserts a VLAN into the Ethernet header.

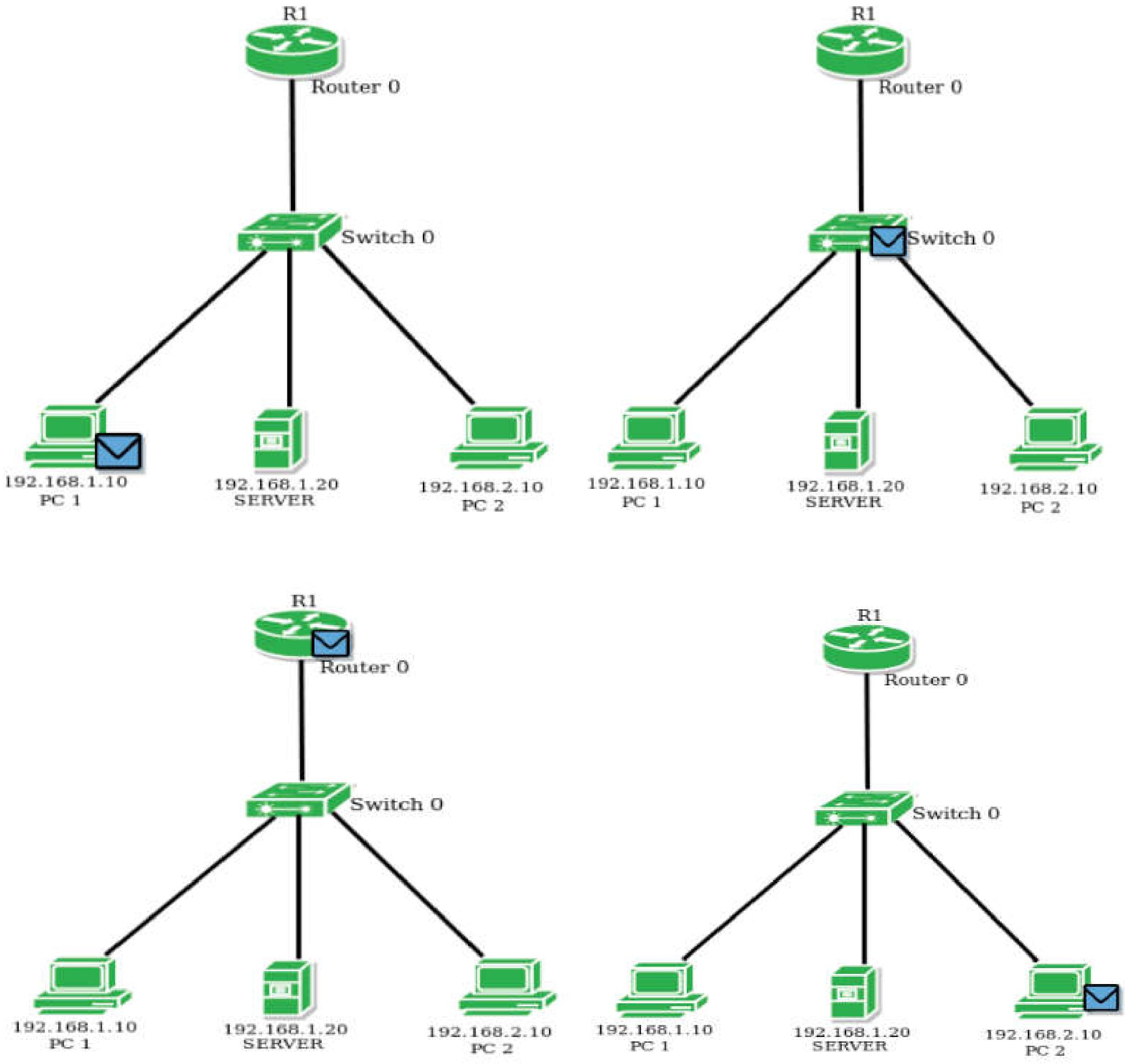
Now, we will make 2 different VLANs on switch namely VLAN 2 and VLAN 3 giving names HR_dept and sales_dept.

```
Switch# vlan 2
Switch# name HR_dept
Switch# vlan 3
Switch# name sales_dept
Switch# int range fa0/1-2
Switch# switchport mode access
Switch# switchport access vlan 2
Switch# int fa0/3
Switch# switchport mode access
Switch# switchport access vlan 3
```

Here, we have assigned VLAN 2 to the specific switch ports fa0/1, fa0/2 and vlan 3 to fa0/3 respectively.

NOTE: int range fa0/1-2 command is used as there are more than one host present in a single VLAN.

Now to check reachability of PC2 from PC1, we will try to PING PC2 from PC1.


R1
Router 0
Switch 0
192.168.1.10
PC 1
192.168.1.20
SERVER
192.168.2.10
PC 2
R1
Router 0
Switch 0
192.168.1.10
PC 1
192.168.1.20
SERVER
192.168.2.10
PC 2
R1
Router 0
Switch 0
192.168.1.10
PC 1
192.168.1.20
SERVER
192.168.2.10
PC 2
R1
Router 0
Switch 0
192.168.1.10
PC 1
192.168.1.20
SERVER
192.168.2.10
PC 2

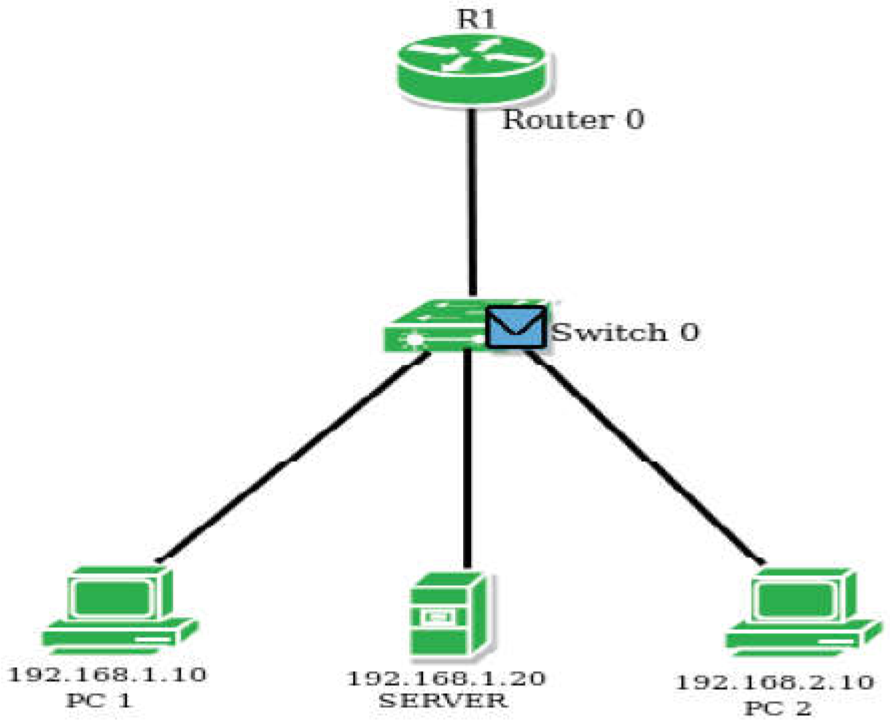


Figure 3. 6 PING PC2 from PC1

From the above figures, we see that the packet is delivered to the router by the switch, because now the broadcast domain have been divided by the different VLANs present on the switch therefore, the packet will be delivered to the default gateway (as PC2 is present on different network) and then to the destination.

CHAPTER FOUR

SWITCHES

4.1. Switch basic configuration

Scenario In this lab, you will examine and configure a standalone LAN switch. Although a switch performs basic functions in its default out-of-the-box condition, there are a number of parameters that a network administrator should modify to ensure a secure and optimized LAN. This lab introduces you to the basics of switch configuration.

Task 1: Cable, Erase, and Reload the Switch

Step 1: Cable a network. Cable a network that is similar to the one in the topology diagram. Create a console connection to the switch. You can use any current switch in your lab as long as it has the required interfaces shown in the topology. The output shown in this lab is from a 2960 switch. If you use other switches, the switch outputs and interface descriptions may appear different.
Note: PC2 is not initially connected to the switch. It is only used in Task 5.
Step 2: Clear the configuration on the switch. Clear the configuration on the switch using the procedure in Appendix 1.

Task 2: Verify the Default Switch Configuration

Step 1: Enter privileged mode.
You can access all the switch commands in privileged mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use. You will set passwords in Task 3. The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the configure command through which access to the remaining command modes are gained. Enter privileged EXEC mode by entering the enable command.

```
Switch>enable
Switch#
```

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Step 2: Examine the current switch configuration.
Examine the current running configuration file.

```
Switch#show running-config
```

Step 3: Display Cisco IOS information.
Examine the following version information that the switch reports.

```
Switch#show version
```

Step 4: Examine the Fast Ethernet interfaces.
Examine the default properties of the Fast Ethernet interface used by PC1.

```
Switch#show interface fastethernet 0/18
```

Step 5: Examine VLAN information.
Examine the default VLAN settings of the switch.

```
Switch#show vlan
```

Step 6: Examine flash memory.
Issue one of the following commands to examine the contents of the flash directory.

```
Switch#dir flash: or Switch#show flash
```

Files have a file extension, such as .bin, at the end of the filename. Directories do not have a file extension. To examine the files in a directory, issue the following command using the filename displayed in the output of the previous command:

```
Switch#dir flash:c2960-lanbase-mz.122-25.SEE3
```

The output should look similar to this:

```
Directory of flash:/c2960-lanbase-mz.122-25.SEE3/
6 drwx 4480 Mar 1 1993 00:04:42 +00:00 html
618 -rwx 4671175 Mar 1 1993 00:06:06 +00:00 c2960-lanbase-mz.122-25.SEE3.bin
619 -rwx 457 Mar 1 1993 00:06:06 +00:00 info
32514048 bytes total (24804864 bytes free)
```

Step 7: Examine the startup configuration file. To view the contents of the startup configuration file, issue the show startup-config command in privileged EXEC mode.

```
Switch#show startup-config
startup-config is not present
```

Let's make one configuration change to the switch and then save it. Type the following commands:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
```

To save the contents of the running configuration file to non-volatile RAM (NVRAM), issue the the command copy running-config startup-config.

```
Switch#copy running-config startup-config
Destination filename [startup-config]? (enter)
Building configuration…
[OK]
```

Note: This command is easier to enter by using the copy run start abbreviation.
Now display the contents of NVRAM using the show startup-config command.

```
S1#show startup-config
Using 1170 out of 65536 bytes
```

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname S1
!
<output omitted>
```

4.2. CAM Table

We dig in deeper into the operations of a switch in the CCNP SWITCH Official Certification Guide. The CAM table is one of the fundamental operations of a switch. It is not only important for the 642-813 SWITCH exam but it is important to know for working on the job. The CAM table, or content addressable memory table, is present in all Cisco Catalysts for layer 2 switching. It is used to record a stations mac address and its corresponding switch port location. In addition, a timestamp for the entry is recorded and it is VLAN assignment.

The CAM table is used in multilayer switching for the purpose of quickly switching frames to their destination. The switch looks at the incoming frame's source MAC address and enters it into the CAM table and keeps it there for 300 seconds before aging out. This is the default value. If the device connected to that switchport is moved to another port, the switch records the incoming source MAC address, updates the CAM table and removes it's previous entry for the same MAC address.

Host A is connected to switch port 1 and Host B is connected to switch port 2.

1. Host A sends traffic to the switch.
2. The switch looks into the frame and records the source MAC address (of Host A) and places an entry into the CAM table. Host A is on switchport 1, has the MAC address of AAAA, VLAND ID of 1, and the timestamp.
3. Host B has not communicated with the switch yet.
4. Host A decides to communicate with Host B.
5. When Host A sends a frame to the switch destined to Host B, the switch notices the destination MAC address (for Host B) in the frame, queries the CAM table for that MAC address but doesn't find it.
6. Because the destination MAC is unknown, the switch marks the frame for flooding and sends the unicast frame to all ports with the same VLAN association.
7. Host B responds to the unicast frame.
8. The switch records the incoming frame from Host B and records Host B's MAC, switchport location, VLAN ID, and applies a timestamp.
9. The next time Host A sends a frame destined for Host B, the switch queries it's CAM table, finds Host B in the table and sends the frame directly to Host B.

CAM Table Before Host B Communicates on the Network [table id=1 /]

CAM Table After Host B Communicates on the Network [table id=2 /]

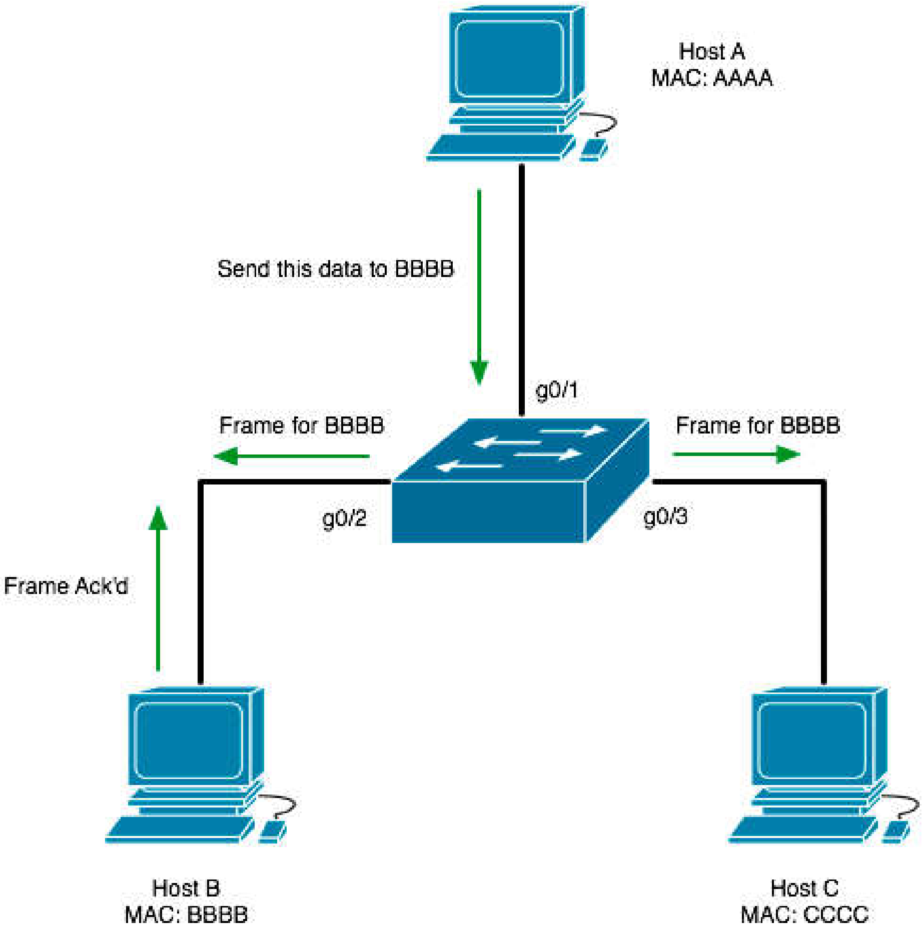


Figure 4. 1 Host A sending data to Host B

4.3. Port Security

Attackers' task is comparatively very easy when they can enter the network they want to attack. Ethernet LANs are very much vulnerable to attack as the switch ports are open to use by default. Various attacks such as Dos attack at layer 2, address spoofing can take place. If the administrator has control over the network then obviously the network is safe. To take total control over the switch ports, the user can use a feature called port-security. If somehow prevent an unauthorized user to use these ports, then the security will increase up to a great extent at layer 2.

Users can secure a port in two steps:

1. Limiting the number of MAC addresses to a single switch port, i.e if more than the limit, Mac addresses are learned from a single port then appropriate action will be taken.

2. If unauthorized access is observed, the traffic should be discarded by using any of the options, or more appropriately, the user should generate a log message so that unauthorized access can be easily observed.

Port security –

Switches learn MAC addresses when the frame is forwarded through a switch port. By using port security, users can limit the number of MAC addresses that can be learned to a port, set static MAC addresses, and set penalties for that port if it is used by an unauthorized user. Users can either use restrict, shut down or protect port-security commands.

Let's discuss these violation modes:

- **Protect** – This mode drops the packets with unknown source mac addresses until you remove enough secure mac addresses to drop below the maximum value.
- **Restrict** – This mode performs the same function as protecting, i.e drops packets until enough secure mac addresses are removed to drop below the maximum value. In addition to this, it will generate a log message, increment the counter value, and will also send an SNMP trap.
- **Shut down** – This mode is mostly preferred as compared to other modes as it shut down the port immediately if unauthorized access is done. It will also generate a log, increment counter value, and send an SNMP trap. This port will remain in a shutdown state until the administrator will perform the "no shutdown" command.
- **Sticky** – This is not a violation mode. By using the sticky command, the user provides static Mac address security without typing the absolute Mac address. For example, if user provides a maximum limit of 2 then the first 2 Mac addresses learned on that port will be placed in the running configuration. After the 2nd learned Mac address, if the 3rd user wants to access then the appropriate action will be taken according to the violation mode applied.
- **Note –** The port security will work on access port only i.e to enable port security, the user first has to make it an access port.

Configuration

Applying port-security on fa0/1 interface of switch .first, convert the port to an access port and will enable port-security.

```
S1(config)#int fa0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
```

Use sticky command so that it will learn the Mac address dynamically and will provide the limit and the appropriate action that should be taken.

```
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security violation shutdown
```

If the user wants to provide a static entry, then configure that by starting its Mac address.

```
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#switchport port-security mac-address aa.bb.cc.dd.ee.ff
```

4.4. VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a switch supporting fallback bridging. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree.

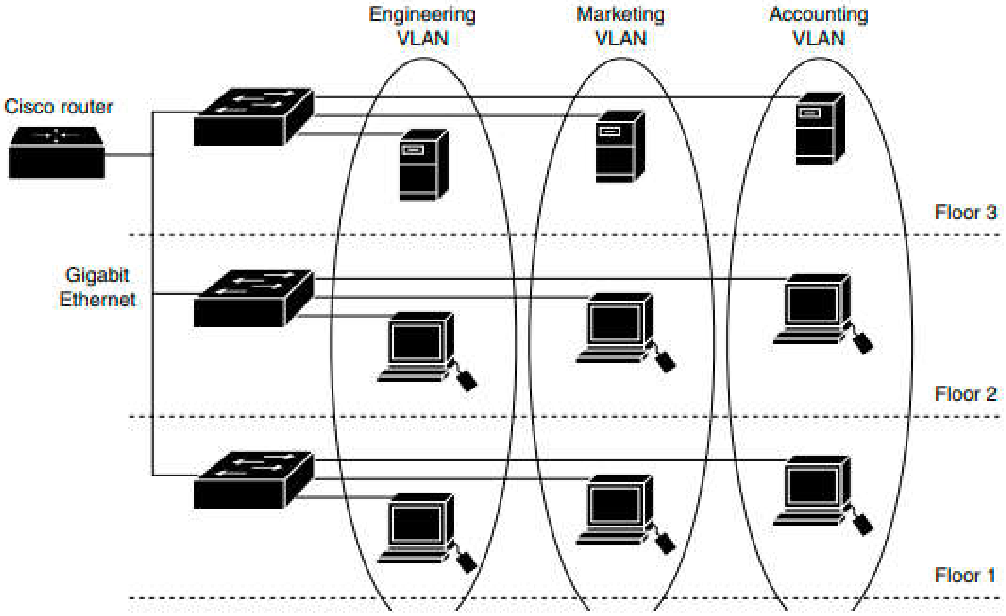


Figure 4. 2 VLANs as Logically Defined Networks

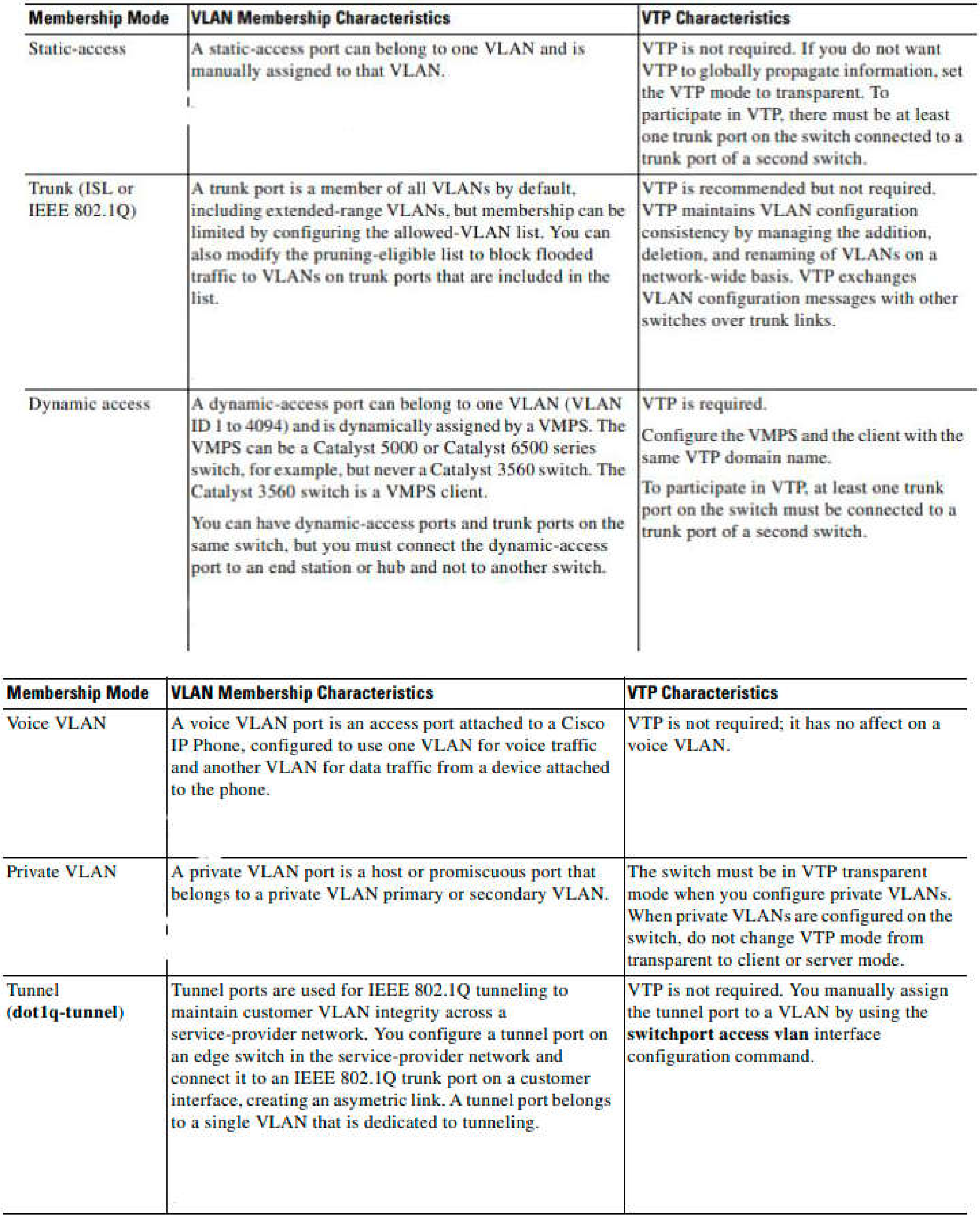
VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch is assigned manually on an interface-by-interface basis. When you assign switch interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership. Traffic between VLANs must be routed or fallback bridged. The switch can route traffic between

VLANs by using switch virtual interfaces (SVIs). An SVI must be explicitly configured and assigned an IP address to route traffic between VLANs.

Note

If you plan to configure many VLANs on the switch and to not enable routing, you can use the sdm prefer vlan global configuration command to set the Switch Database Management (sdm) feature to the VLAN template, which configures system resources to support the maximum number of unicast MAC addresses.

VLAN Port Membership Modes You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic the port carries and the number of VLANs to which it can belong. Table 12-1 lists the membership modes and membership and VTP characteristics.



Membership Mode	VLAN Membership Characteristics	VTP Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned to that VLAN.	VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent. To participate in VTP, there must be at least one trunk port on the switch connected to a trunk port of a second switch.
Trunk (ISL or IEEE 802.1Q)	A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the list.	VTP is recommended but not required. VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other switches over trunk links.
Dynamic access	A dynamic-access port can belong to one VLAN (VLAN ID 1 to 4094) and is dynamically assigned by a VMPS. The VMPS can be a Catalyst 5000 or Catalyst 6500 series switch, for example, but never a Catalyst 3560 switch. The Catalyst 3560 switch is a VMPS client. You can have dynamic-access ports and trunk ports on the same switch, but you must connect the dynamic-access port to an end station or hub and not to another switch.	VTP is required. Configure the VMPS and the client with the same VTP domain name. To participate in VTP, at least one trunk port on the switch must be connected to a trunk port of a second switch.
Voice VLAN	A voice VLAN port is an access port attached to a Cisco IP Phone, configured to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone.	VTP is not required; it has no affect on a voice VLAN.
Private VLAN	A private VLAN port is a host or promiscuous port that belongs to a private VLAN primary or secondary VLAN.	The switch must be in VTP transparent mode when you configure private VLANs. When private VLANs are configured on the switch, do not change VTP mode from transparent to client or server mode.
Tunnel **(dot1q-tunnel)**	Tunnel ports are used for IEEE 802.1Q tunneling to maintain customer VLAN integrity across a service-provider network. You configure a tunnel port on an edge switch in the service-provider network and connect it to an IEEE 802.1Q trunk port on a customer interface, creating an asymetric link. A tunnel port belongs to a single VLAN that is dedicated to tunneling.	VTP is not required. You manually assign the tunnel port to a VLAN by using the **switchport access vlan** interface configuration command.

Table 4. 1 Port Membership Modes and Characteristics

Configuring Normal-Range VLANs

Normal-range VLANs are VLANs with VLAN IDs 1 to 1005. If the switch is in VTP server or VTP transparent mode, you can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)

You can cause inconsistency in the VLAN database if you attempt to manually delete the vlan.dat file. If you want to modify the VLAN configuration, use the commands described in these sections and in the command reference for this release. To change the VTP configuration.

You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the show running-config privileged EXEC command. You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type (Ethernet, Fiber Distributed Data Interface [FDDI], FDDI network entity title [NET], TrBRF, or TrCRF, Token Ring, Token Ring-Net)
- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs
- VLAN number to use when translating from one VLAN type to another

Token Ring VLANs

Although the switch does not support Token Ring connections, a remote device such as a Catalyst 5000 series switch with Token Ring connections could be managed from one of the supported switches. Switches running VTP Version 2 advertise information about these Token Ring VLANs:

¬ Token Ring TrBRF VLANs
¬ Token Ring TrCRF VLANs For more information on configuring Token Ring VLANs, see the Catalyst 5000 Series Software Configuration Guide.

Normal-Range VLAN Configuration Guidelines

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- The switch supports 1005 VLANs in VTP client, server, and transparent modes.
- Normal-range VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.

- VLAN configuration for VLANs 1 to 1005 are always saved in the VLAN database. If the VTP mode is transparent, VTP and VLAN configuration are also saved in the switch running configuration file.
- The switch also supports VLAN IDs 1006 through 4094 in VTP transparent mode (VTP disabled). These are extended-range VLANs and configuration options are limited. Extended-range VLANs are not saved in the VLAN database.
- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. If the switch is a VTP server, you must define a VTP domain or VTP will not function.
- The switch does not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.
- The switch supports 128 spanning-tree instances. If a switch has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 128 VLANs and is disabled on the remaining VLANs. If you have already used all available spanning-tree instances on a switch, adding another VLAN anywhere in the VTP domain creates a VLAN on that switch that is not running spanning-tree. If you have the default allowed list on the trunk ports of that switch (which is to allow all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent switches that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances.

  If the number of VLANs on the switch exceeds the number of supported spanning-tree instances, we recommend that you configure the IEEE 802.1s Multiple STP (MSTP) on your switch to map multiple VLANs to a single spanning-tree instance.

VLAN Configuration in config-vlan Mode

To access config-vlan mode, enter the vlan global configuration command with a VLAN ID. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. You can use the default VLAN configuration or enter multiple commands to configure the VLAN. For more information about commands available in this mode, see the vlan global configuration command description in the command reference for this release. When you have finished the configuration, you must exit config-vlan mode for the configuration to take effect. To display the VLAN configuration, enter the show vlan privileged EXEC command.

VLAN Configuration in VLAN Database Configuration Mode

To access VLAN database configuration mode, enter the vlan database privileged EXEC command. Then enter the vlan command with a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify the VLAN. You can use the default VLAN configuration or enter multiple commands to configure the VLAN. For more information about keywords available in this mode, see the vlan VLAN database configuration command description in the command reference for this release. When you have finished the configuration, you must enter apply or exit for the configuration to take effect. When you enter the exit command, it applies all commands and updates the VLAN database. VTP messages are sent to other switches in the VTP domain, and the privileged EXEC mode prompt appears.

Saving VLAN Configuration

The configurations of VLAN IDs 1 to 1005 are always saved in the VLAN database (vlan.dat file). If the VTP mode is transparent, they are also saved in the switch running configuration file. You can enter the copy running-config startup-config privileged EXEC command to save the configuration in the startup configuration file. To display the VLAN configuration, enter the show vlan privileged EXEC command.

When you save VLAN and VTP information (including extended-range VLAN configuration information) in the startup configuration file and reboot the switch, the switch configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration, and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration does not match the VLAN database, the domain name and VTP mode and configuration for the first 1005 VLANs use the VLAN database information.
- If VTP mode is server, the domain name and VLAN configuration for the first 1005 VLANs use the VLAN database information

4.5. STP

Configuring STP

This part describes how to configure the Spanning Tree Protocol (STP) on port-based VLANs on the Catalyst 3560 switch. The switch can use either the per-VLAN spanning-tree plus (PVST+) protocol based on the IEEE 802.1D standard and Cisco proprietary extensions, or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol based on the IEEE 802.1w standard.

STP Overview

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments. The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree
- Backup—a blocked port in a loopback configuration. The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch.

Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

Spanning-Tree Topology and BPDUs

The stable, active spanning-tree topology of a switched network is controlled by these elements:

- The unique bridge ID (switch priority and MAC address) associated with each VLAN on each switch.
- The spanning-tree path cost to the root switch.
- The port identifier (port priority and MAC address) associated with each Layer 2 interface.

When the switches in a network are powered up, each functions as the root switch. Each switch sends a configuration BPDU through all of its ports. The BPDUs communicate and compute the spanning-tree topology. Each configuration BPDU contains this information:

- The unique bridge ID of the switch that the sending switch identifies as the root switch
- The spanning-tree path cost to the root
- The bridge ID of the sending switch
- Message age
- The identifier of the sending interface
- Values for the hello, forward delay, and max-age protocol timers

When a switch receives a configuration BPDU that contains superior information (lower bridge ID, lower path cost, and so forth), it stores the information for that port. If this BPDU is received on the root port of the switch, the switch also forwards it with an updated message to all attached LANs for which it is the designated switch. If a switch receives a configuration BPDU that contains inferior information to that currently stored for that port, it discards the BPDU. If the switch is a designated switch for the LAN from which the inferior BPDU was received, it sends that LAN a BPDU containing the up-to-date information stored for that port. In this way, inferior information is discarded, and superior information is propagated on the network.

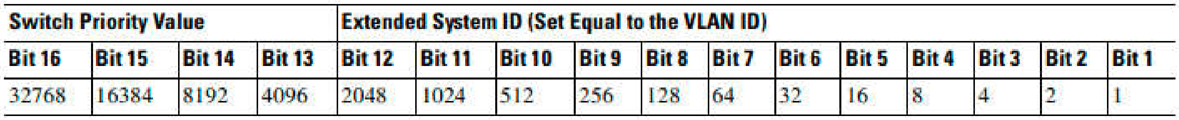
- A BPDU exchange results in these actions:
- One switch in the network is elected as the root switch (the logical center of the spanning-tree topology in a switched network).

  For each VLAN, the switch with the highest switch priority (the lowest numerical priority value) is elected as the root switch. If all switches are configured with the default priority (32768), the switch with the lowest MAC address in the VLAN becomes the root switch. The switch priority value occupies the most significant bits of the bridge ID.

  A root port is selected for each switch (except the root switch). This port provides the best path (lowest cost) when the switch forwards packets to the root switch. The shortest distance to the root switch is calculated for each switch based on the path cost. A designated switch for each LAN segment is selected. The designated switch incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port. All paths that are not needed to reach the root switch from anywhere in the switched network are placed in the spanning-tree blocking mode.

Bridge ID, Switch Priority, and Extended System ID

The IEEE 802.1D standard requires that each switch has a unique bridge identifier (bridge ID), which controls the selection of the root switch. Because each VLAN is considered as a different logical bridge with PVST+ and rapid PVST+, the same switch must have a different bridge IDs for each configured VLAN. Each VLAN on the switch has a unique 8-byte bridge ID. The 2 most-significant bytes are used for the switch priority, and the remaining 6 bytes are derived from the switch MAC address. The switch supports the IEEE 802.1t spanning-tree extensions, and some of the bits previously used for the switch priority are now used as the VLAN identifier. The result is that fewer MAC addresses are reserved for the switch, and a larger range of VLAN IDs can be supported, all while maintaining the uniqueness of the bridge ID. As shown in Table 4-2, the 2 bytes previously used for the switch priority are reallocated into a 4-bit priority value and a 12-bit extended system ID value equal to the VLAN ID.



Switch Priority Value				Extended System ID (Set Equal to the VLAN ID)											
Bit 16	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Table 4. 2 Switch Priority Value and Extended System ID

Spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN. Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For example, when you change the switch priority value, you change the probability that the switch will be elected as the root switch. Configuring a higher value decreases the probability; a lower value increases the probability.

Spanning-Tree Interface States

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can take place at different times and at different places in a switched network. When an interface transitions directly from nonparticipation in the spanning-tree topology to the forwarding state, it can create temporary data loops. Interfaces must wait for new topology information to propagate through the switched LAN before starting to forward frames. They must allow the frame lifetime to expire for forwarded frames that have used the old topology. Each Layer 2 interface on a switch using spanning tree exists in one of these states:

- Blocking—the interface does not participate in frame forwarding.
- Listening—the first transitional state after the blocking state when the spanning tree decides that the interface should participate in frame forwarding.
- Learning—the interface prepares to participate in frame forwarding.
- Forwarding—the interface forwards frames.
- Disabled—the interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.
- An interface moves through these states:
- From initialization to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

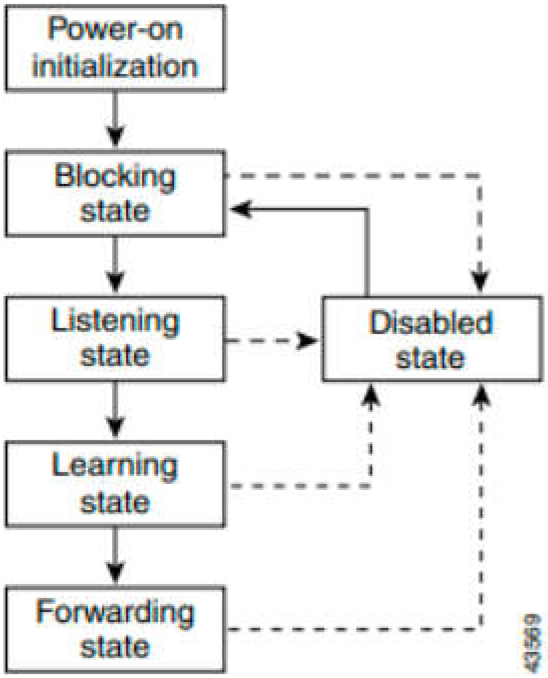


Figure 4. 3 Spanning-Tree Interface States

When you power up the switch, spanning tree is enabled by default, and every interface in the switch, VLAN, or network goes through the blocking state and the transitory states of listening and learning. Spanning tree stabilizes each interface at the forwarding or blocking state.

When the spanning-tree algorithm places a Layer 2 interface in the forwarding state, this process occurs:

1. The interface is in the listening state while spanning tree waits for protocol information to move the interface to the blocking state.
   While spanning tree waits the forward-delay timer to expire, it moves the interface to the learning state and resets the forward-delay timer.
2. In the learning state, the interface continues to block frame forwarding as the switch learns end-station location information for the forwarding database.
3. When the forward-delay timer expires, spanning tree moves the interface to the forwarding state, where both learning and frame forwarding are enabled.

Blocking State

A Layer 2 interface in the blocking state does not participate in frame forwarding. After initialization, a BPDU is sent to each switch interface. A switch initially functions as the root until it exchanges BPDUs with other switches. This exchange establishes which switch in the network is the root or root switch. If there is only one switch in the network, no exchange occurs, the forward-delay timer expires, and the interface moves to the listening state. An interface always enters the blocking state after switch initialization. An interface in the blocking state performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Receives BPDUs

Listening State

The listening state is the first state a Layer 2 interface enters after the blocking state. The interface enters this state when the spanning tree decides that the interface should participate in frame forwarding. An interface in the listening state performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Receives BPDUs

Learning State

A Layer 2 interface in the learning state prepares to participate in frame forwarding. The interface enters the learning state from the listening state. An interface in the learning state performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Learns addresses
- Receives BPDUs

Forwarding State

A Layer 2 interface in the forwarding state forwards frames. The interface enters the forwarding state from the learning state. An interface in the forwarding state performs these functions:

- Receives and forwards frames received on the interface
- Forwards frames switched from another interface
- Learns addresses
- Receives BPDUs

Disabled State

A Layer 2 interface in the disabled state does not participate in frame forwarding or in the spanning tree. An interface in the disabled state is nonoperational. A disabled interface performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Does not receive BPDUs

4.6. VTP

This portion describes how to use the VLAN Trunking Protocol (VTP) and the VLAN database for managing VLANs with the Catalyst 3560 switch.

Understanding VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations. Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches. VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database. The switch supports 1005 VLANs, but the number of routed ports, SVIs, and other configured features affects the usage of the switch hardware. If the switch is notified by VTP of a new VLAN and the switch is already using the maximum available hardware resources, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the show vlan user EXEC command shows the VLAN in a suspended state. VTP only learns about normal-range VLANs (VLAN IDs 1 to 1005). Extended-range VLANs (VLAN IDs greater than 1005) are not supported by VTP or stored in the VTP VLAN database.

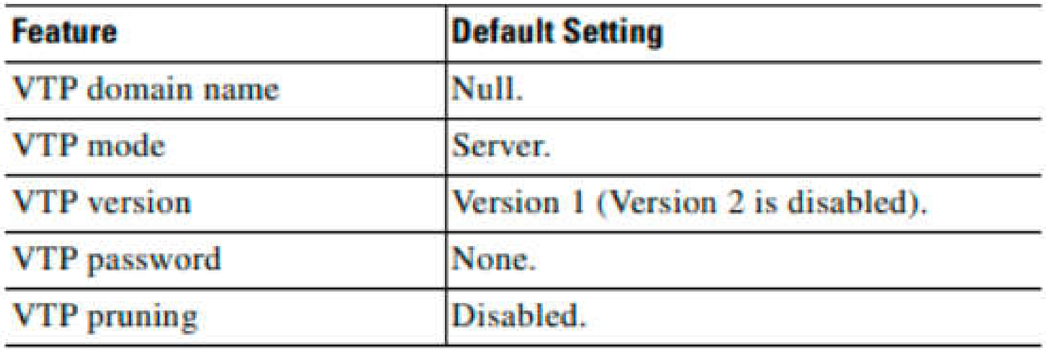
The VTP Domain

A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches under the same administrative responsibility sharing the same VTP domain name. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain. By default, the switch is in the VTP no-management-domain state until it receives an advertisement for a domain over a trunk link (a link that carries the traffic of multiple VLANs) or until you configure a domain name. Until the management domain name is specified or learned, you cannot create or modify VLANs on a VTP server, and VLAN information is not propagated over the network. If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch then ignores advertisements with a different domain name or an earlier configuration revision number.

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP advertisements are sent over all IEEE trunk connections, including Inter-Switch Link (ISL) and IEEE 802.1Q. VTP dynamically maps VLANs with unique names and internal index associates across multiple LAN types. Mapping eliminates excessive device administration required from network administrators. If you configure a switch for VTP transparent mode, you can create and modify VLANs, but the changes are not sent to other switches in the domain, and they affect only the individual switch. However, configuration changes made when the switch is in this mode are saved in the switch running configuration and can be saved to the switch startup configuration file.

Configuring VTP

Default VTP Configuration



Feature	Default Setting
VTP domain name	Null.
VTP mode	Server.
VTP version	Version 1 (Version 2 is disabled).
VTP password	None.
VTP pruning	Disabled.

Table 4. 3 Default VTP Configuration

Configuration Mode

VTP Configuration in Global Configuration Mode

You can use the vtp global configuration command to set the VTP password, the version, the VTP file name, the interface providing updated VTP information, the domain name, and the mode, and to disable or enable pruning. For more information about available keywords, see the command descriptions in the command reference for this release. The VTP information is saved in the VTP VLAN database. When VTP mode is transparent, the VTP domain name and mode are also saved in the switch running configuration file, and you can save it in the switch startup configuration file by entering the copy running-config startup-config privileged EXEC command. You must use this command if you want to save VTP mode as transparent, even if the switch resets. When you save VTP information in the switch startup configuration file and reboot the switch, the switch configuration is selected as follows:

¬ If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the

VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
¬ If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for the first 1005 VLANs use the VLAN database information.

VTP Configuration in VLAN Database Configuration Mode

You can configure all VTP parameters in VLAN database configuration mode, which you access by entering the vlan database privileged EXEC command. For more information about available keywords, see the vtp VLAN database configuration command description in the command reference for this release. When you enter the exit command in VLAN database configuration mode, it applies all the commands that you entered and updates the VLAN database. VTP messages are sent to other switches in the VTP domain, and the privileged EXEC mode prompt appears. If VTP mode is transparent, the domain name and the mode (transparent) are saved in the switch running configuration, and you can save this information in the switch startup configuration file by entering the copy running-config startup-config privileged EXEC command.

VTP Configuration Guidelines

These sections describe guidelines you should follow when implementing VTP in your network.

Domain Names

When configuring VTP for the first time, you must always assign a domain name. You must configure all switches in the VTP domain with the same domain name. Switches in VTP transparent mode do not exchange VTP messages with other switches, and you do not need to configure a VTP domain name for them.

Passwords

You can configure a password for the VTP domain, but it is not required. If you do configure a domain password, all domain switches must share the same password and you must configure the password on each switch in the management domain. Switches without a password or with the wrong password reject VTP advertisements. If you configure a VTP password for a domain, a switch that is booted without a VTP configuration does not accept VTP advertisements until you configure it with the correct password. After the configuration, the switch accepts the next VTP advertisement that uses the same password and domain name in the advertisement. If you are adding a new switch to an existing network with VTP capability, the new switch learns the domain name only after the applicable password has been configured on it.

VTP Version

Follow these guidelines when deciding which VTP version to implement:

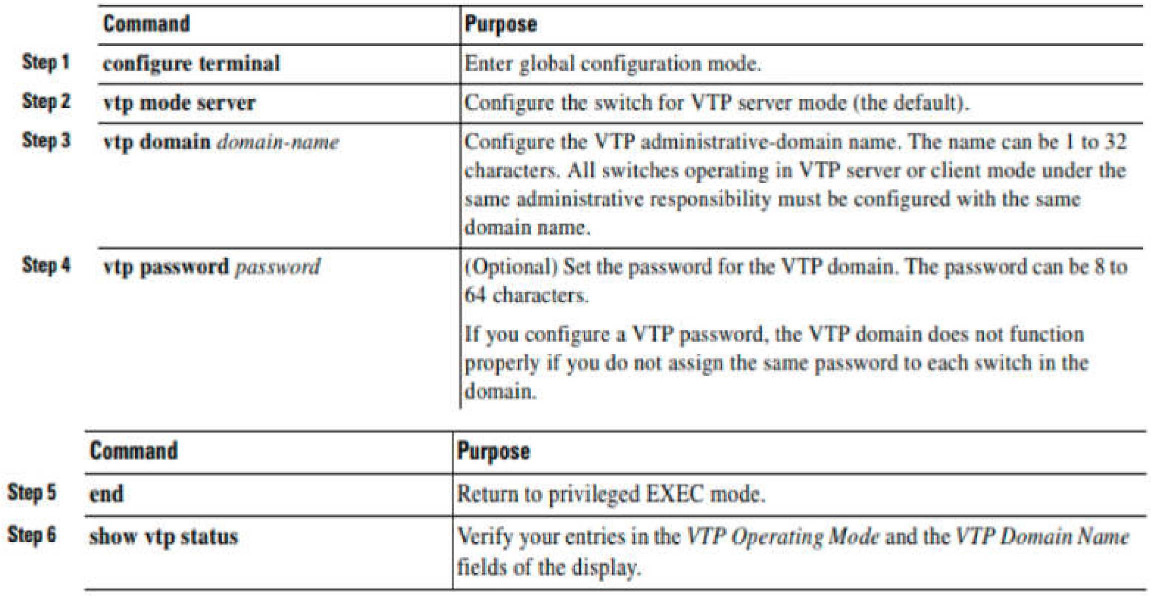
- All switches in a VTP domain must run the same VTP version.
- A VTP Version 2-capable switch can operate in the same VTP domain as a switch running VTP Version 1 if Version 2 is disabled on the Version 2-capable switch (Version 2 is disabled by default).
- Do not enable VTP Version 2 on a switch unless all of the switches in the same VTP domain are Version-2-capable. When you enable Version 2 on a switch, all of the Version-2-capable switches in the domain enable Version 2. If there is a Version 1-only switch, it does not exchange VTP information with switches that have Version 2 enabled.
- If there are TrBRF and TrCRF Token Ring networks in your environment, you must enable VTP Version 2 for Token Ring VLAN switching to function properly. To run Token Ring and Token Ring-Net, disable VTP Version 2.

Configuration Requirements

When you configure VTP, you must configure a trunk port so that the switch can send and receive VTP advertisements to and from other switches in the domain. If you are configuring VTP on a cluster member switch to a VLAN, use the rcommand privileged EXEC command to log in to the member switch. For more information about the command, see the command reference for this release. If you are configuring extended-range VLANs on the switch, the switch must be in VTP transparent mode. VTP does not support private VLANs. If you configure private VLANs, the switch must be in VTP transparent mode. When private VLANs are configured on the switch, do not change the VTP mode from transparent to client or server mode.

Configuring a VTP Server

When a switch is in VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.



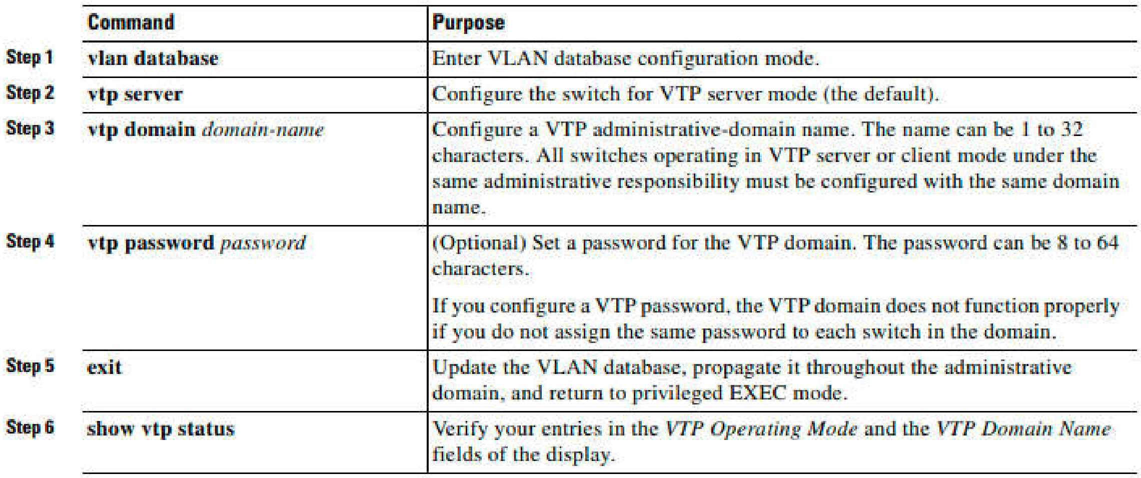
	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp mode server**	Configure the switch for VTP server mode (the default).
Step 3	**vtp domain** *domain-name*	Configure the VTP administrative-domain name. The name can be 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name.
Step 4	**vtp password** *password*	(Optional) Set the password for the VTP domain. The password can be 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show vtp status**	Verify your entries in the *VTP Operating Mode* and the *VTP Domain Name* fields of the display.

Table 4. 4 Configuring a VTP Server

When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain. To return the switch to a no-password state, use the no vtp password global configuration command. This example shows how to use global configuration mode to configure the switch as a VTP server with the domain name eng_group and the password mypassword:
Switch# config terminal

```
Switch(config)# vtp mode server
Switch(config)# vtp domain eng_group
Switch(config)# vtp password mypassword
Switch(config)# end
```

You can also use VLAN database configuration mode to configure VTP parameters. Beginning in privileged EXEC mode, follow these steps to use VLAN database configuration mode to configure the switch as a VTP server:



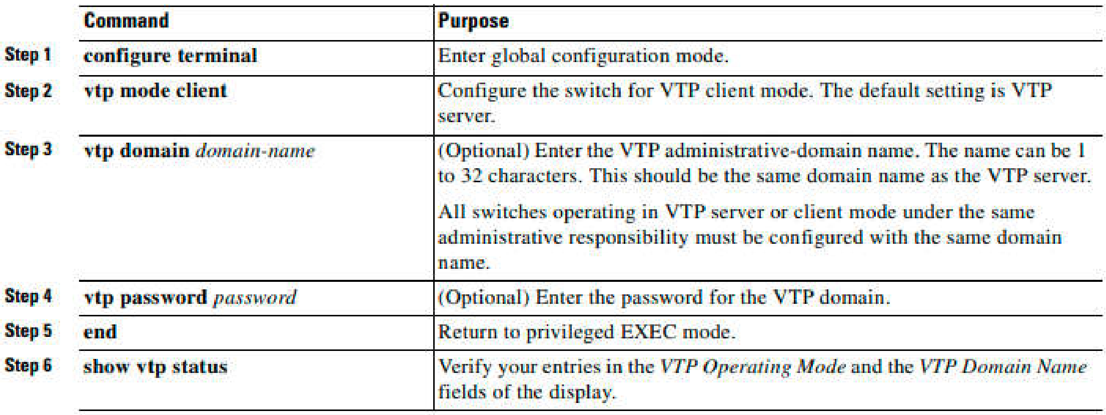
	Command	Purpose
Step 1	**vlan database**	Enter VLAN database configuration mode.
Step 2	**vtp server**	Configure the switch for VTP server mode (the default).
Step 3	**vtp domain** *domain-name*	Configure a VTP administrative-domain name. The name can be 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name.
Step 4	**vtp password** *password*	(Optional) Set a password for the VTP domain. The password can be 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain.
Step 5	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 6	**show vtp status**	Verify your entries in the *VTP Operating Mode* and the *VTP Domain Name* fields of the display.

When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain. To return the switch to a no-password state, use the no vtp password VLAN database configuration command. This example shows how to use VLAN database configuration mode to configure the switch as a VTP server with the domain name eng_group and the password mypassword:

```
Switch# vlan database
Switch(vlan)# vtp server
Switch(vlan)# vtp domain eng_group
Switch(vlan)# vtp password mypassword
Switch(vlan)# exit
APPLY completed.
Exiting….
Switch#
```

Configuring a VTP Client

When a switch is in VTP client mode, you cannot change its VLAN configuration. The client switch receives VTP updates from a VTP server in the VTP domain and then modifies its configuration accordingly.



	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp mode client**	Configure the switch for VTP client mode. The default setting is VTP server.
Step 3	**vtp domain** *domain-name*	(Optional) Enter the VTP administrative-domain name. The name can be 1 to 32 characters. This should be the same domain name as the VTP server. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name.
Step 4	**vtp password** *password*	(Optional) Enter the password for the VTP domain.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show vtp status**	Verify your entries in the *VTP Operating Mode* and the *VTP Domain Name* fields of the display.

Use the no vtp mode global configuration command to return the switch to VTP server mode. To return the switch to a no-password state, use the no vtp password privileged EXEC command. When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain.

4.7. Inter VLAN Communication

After VLANs are assigned, broadcast packets are only forwarded in the same VLAN. This means that hosts in different VLANs cannot communicate at Layer 2. In real-world scenarios, hosts in different VLANs often need to communicate, so inter-VLAN communication needs to be implemented to resolve this.

Similar to intra-VLAN communication described in Intra-VLAN Communication, inter-VLAN communication goes through three phases: packet transmission from the source host, Ethernet switching in a switch, and adding and removing VLAN tags during the exchange between devices. According to the Ethernet switching principle, broadcast packets are only forwarded in the same VLAN and hosts in different VLANs cannot directly communicate at Layer 2. Layer 3 routing or VLAN translation technology is required to implement inter-VLAN communication.

Inter-VLAN Communication Technologies

Huawei provides a variety of technologies to implement inter-VLAN communication. The following two technologies are commonly used:

- VLANIF interface A VLANIF interface is a Layer 3 logical interface that can be used to implement inter-VLAN Layer 3 connectivity. It is simple to configure a VLANIF interface, so VLANIF interfaces are the most commonly used for inter-VLAN communication. However, a VLANIF interface needs to be configured for each VLAN and each VLANIF interface requires an IP address. As a result, this technology wastes IP addresses.
- Dot1q termination sub-interface A sub-interface is also a Layer 3 logical interface that can be used to implement inter-VLAN Layer 3 connectivity. A Dot1q termination sub-interface applies to scenarios where a Layer 3 Ethernet interface connects to multiple VLANs. In such a scenario,

data flows from different VLANs preempt bandwidth of the primary Ethernet interface; therefore, the primary Ethernet interface may become a bottleneck when the network is busy.

- VLAN aggregation VLAN aggregation associates a super-VLAN with a super-VLAN. The sub-VLANs share the IP address of the super-VLAN, which acts as the gateway IP address, to implement Layer 3 connectivity with an external network. Proxy ARP can be enabled between sub VLANs to implement Layer 3 connectivity between sub-VLANs. VLAN aggregation conserves IP addresses. VLAN aggregation applies to scenarios where multiple VLANs share a gateway. For details about VLAN aggregation, see VLAN Aggregation Configuration.
- VLAN Switch switch-vlan VLAN Switch switch-vlan requires a pre-configured static forwarding path along switching nodes on a network. When a switching node receives VLAN-tagged frames matching VLAN Switch entries, it directly forwards the frames to corresponding interfaces according to the static forwarding path, thus implementing Layer 2 communication. Switch-VLAN does not require lookup of the MAC address table, so the forwarding efficiency and security are enhanced. If a switching node connects to many user devices, the network administrator needs to configure each user device in advance to establish a static forwarding path. This increases the manual configuration workload and makes network management inconvenient. Switch-VLAN applies to small-scale networks.

Inter-VLAN Communication through the Same Switch

Host_1 (source host) and Host_2 (destination host) connect to the same Layer 3 switch, are located on different network segments, and belong to VLAN 2 and VLAN 3, respectively. After VLANIF 2 and VLANIF 3 are created on the switch and allocated IP addresses, the default gateway addresses of the hosts are set to IP addresses of the VLANIF interfaces.

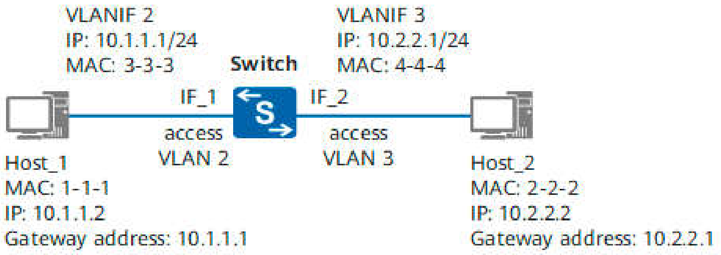


Figure 4. 4 Using VLANIF interfaces to implement inter-VLAN communication through the same switch

When Host_1 sends a packet to Host_2, the packet is transmitted as follows (assuming that no forwarding entry exists on the switch):

1. Host_1 determines that the destination IP address is on a different network segment from its own IP address, and therefore sends an ARP Request packet to request the gateway MAC address. The ARP Request packet carries the destination IP address of 10.1.1.1 (gateway's IP address) and all-F destination MAC address.

2. When the ARP Request packet reaches IF_1 on the Switch, the Switch tags the packet with VLAN 2 (PVID of IF_1). The Switch then adds the mapping between the source MAC address, VLAN ID, and interface (1-1-1, 2, IF_1) in its MAC address table.
3. The Switch detects that the packet is an ARP Request packet and the destination IP address is the IP address of VLANIF 2. The Switch then encapsulates VLANIF 2's MAC address of 3-3-3 into the ARP Reply packet before sending it from IF_1. In addition, the Switch adds the binding of the IP address and MAC address of Host_1 in its ARP table.
4. After receiving the ARP Reply packet from the Switch, Host_1 adds the binding of the IP address and MAC address of VLANIF 2 on the Switch in its ARP table and sends a packet to the Switch. The packet carries the destination MAC address of 3-3-3 and destination IP address of 10.2.2.2 (Host_2's IP address).
5. After the packet reaches IF_1 on the Switch, the Switch tags the packet with VLAN 2.
6. The Switch updates its MAC address table based on the source MAC address, VLAN ID, and inbound interface of the packet, and compares the destination MAC address of the packet with the MAC address of VLANIF 2. If they are the same, the Switch determines that the packet should be forwarded at Layer 3 and searches for a Layer 3 forwarding entry based on the destination IP address. If no entry is found, the Switch sends the packet to the CPU. The CPU then searches for a routing entry to forward the packet.
7. The CPU looks up the routing table based on the destination IP address of the packet and detects that the destination IP address matches a directly connected network segment (network segment of VLANIF 3). The CPU continues to look up its ARP table but finds no matching ARP entry. Therefore, the Switch broadcasts an ARP Request packet with the destination address of 10.2.2.2 to all interfaces in VLAN 3. The ARP Request packet will be send from IF_2.
8. After receiving the ARP Request packet, Host_2 detects that the IP address is its own IP address and sends an ARP Reply packet with its own. Additionally, Host_2 adds the mapping between the MAC address and IP address of VLANIF 3 to its ARP table.
9. After IF_2 on the Switch receives the ARP Reply packet, IF_2 tags the packet with VLAN 3 to the packet and adds the binding of the MAC address and IP address of Host_2 in its ARP table. Before forwarding the packet from Host_1 to Host_2, the Switch removes the tag with VLAN 3 from the packet. The Switch also adds the binding of Host_2's IP address, MAC address, VLAN ID, and outbound interface in its Layer 3 forwarding table.

The packet sent from Host_1 then reaches Host_2. The packet transmission process from Host_2 to Host_1 is similar. Subsequent packets between Host_1 and Host_2 are first sent to the gateway (Switch), and the Switch forwards the packets at Layer 3 based on its Layer 3 forwarding table.

Inter-VLAN Communication through Multiple Switches

When hosts in different VLANs connect to multiple Layer 3 switches, you need to configure static routes or a dynamic routing protocol in addition to VLANIF interface addresses. This is because IP addresses of VLANIF interfaces can only be used to generate direct routes.

In Figure 4-14, Host_1 (source host) and Host_2 (destination host) are located on different network segments, connect to Layer 3 switches Switch_1 and Switch_2, and belong to VLAN 2 and VLAN 3, respectively. On Switch_1, VLANIF 2 and VLANIF 4 are created and allocated IP addresses of 10.1.1.1 and 10.1.4.1. On Switch_2, VLANIF 3 and VLANIF 4 are created and allocated IP addresses of 10.1.2.1 and 10.1.4.2. Static routes are configured on Switch_1 and Switch_2. On Switch_1, the destination network segment in the static route is 10.1.2.0/24 and the next hop address is 10.1.4.2. On Switch_2, the destination network segment in the static route is 10.1.1.0/24 and the next hop address is 10.1.4.1.

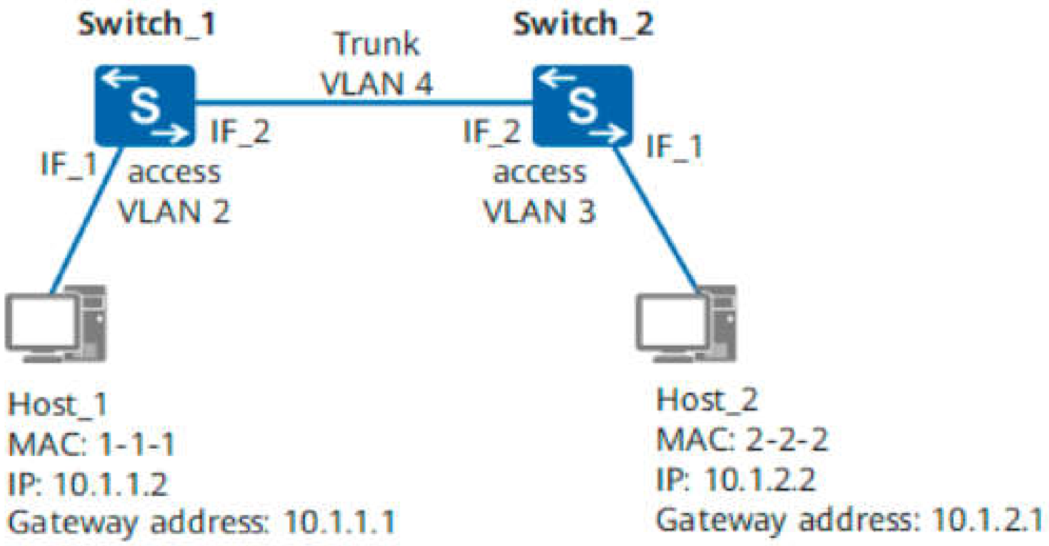


Figure 4. 5 Using VLANIF interfaces to implement inter-VLAN communication through multiple switches

When Host_1 sends a packet to Host_2, the packet is transmitted as follows (assuming that no forwarding entry exists on Switch_1 and Switch_2):

1. The first six steps are similar to steps 1 to 6 in inter-VLAN communication when hosts connect to the same switch. After the steps are complete, Switch_1 sends the packet to its CPU and the CPU looks up the routing table.
2. The CPU of Switch_1 searches for the routing table based on the destination IP address of 10.1.2.2 and finds a static route. In the static route, the destination network segment is 10.1.2.0/24 and the next hop address is 10.1.4.2. The CPU continues to look up its ARP table but finds no matching ARP entry. Therefore, Switch_1 broadcasts an ARP Request packet with the destination address of 10.1.4.2 to all interfaces in VLAN 4. IF_2 on Switch_1 transparently transmits the ARP Request packet to IF_2 on Switch_2 without removing the tag from the packet.
3. After the ARP Request packet reaches Switch_2, Switch_2 finds that the destination IP address of the ARP Request packet is the IP address of VLANIF Switch_2 then sends an ARP Reply packet with the MAC address of VLANIF 4 to Switch_1.
4. IF_2 on Switch_2 transparently transmits the ARP Reply packet to Switch_1. After Switch_1 receives the ARP Reply packet, it adds the binding of the MAC address and IP address of VLANIF4 in its ARP table.

5. Before forwarding the packet of Host_1 to Switch_2, Switch_1 changes the destination MAC address of the packet to the MAC address of VLANIF 4 on Switch_2 and the source MAC address to the MAC address of VLANIF 4 on itself. In addition, Switch_1 records the forwarding entry (10.1.2.0/24, next hop IP address, VLAN, and outbound interface) in its Layer 3 forwarding table. Similarly, the packet is transparently transmitted to IF_2 on Switch_2.
6. After Switch_2 receives packets of Host_1 forwarded by Switch_1, the steps similar to steps 6 to 9 in inter-VLAN communication when hosts connect to the same switch are performed. In addition, Switch_2 records the forwarding entry (Host_2's IP address, MAC address, VLAN, and outbound interface) in its Layer 3 forwarding table.

4.8. Miscellaneous

This part contains miscellaneous configurations that are specific to certain access points.

Using the LAN ports on 700W APs

The Cisco Aironet 700W series access points have one 10/100/1000BASE-T PoE Uplink/WAN port and four 10/100/1000BASE-T RJ-45 local Ethernet ports for wired device connectivity. The fourth port functions as a PoE-Out port when the AP is powered by 802.3at Ethernet switch, Cisco power injector AIR-PWRJ4=, or Cisco Power Supply. By default, all four local Ethernet ports are disabled. You can be enable them when required. You can also configure the local Ethernet ports to a VLAN ID using the interface configuration command, vlan vlan-id.

Enable LAN ports on 702W

Step 1 Enter global configuration mode.

```
ap#conf t

Enter configuration commands, one per line. End with CNTL/Z.
```

Step 2 Enable the LAN port.

```
ap(config)#lan-Port
port-id 1
ap(config-lan-port)#no shutdown
ap(config-lan-port)#end
```

Assign a VLAN to the LAN ports

Use the commands given in the example below.

```
ap#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#lan-Port port-id 1
ap(config-lan-port)#vlan 25
ap(config-lan-port)#end
```

Verifying the LAN Port Configurations

Use the command given in the example below

```
voip#sh lan config LAN table entries:
Port Status Vlan valid Vlan Id
—- ——— ———- ——-
LAN1 DISABLED 25 NA
LAN2 ENABLED NO NA
LAN3 DISABLED NO NA
LAN4 ENABLED NO NA
LAN POE out state = ENABLED
```

700W AP as Workgroup Bridge

Like other Cisco Access points 702W AP series also can be configured as a Workgroup Bridge (WGB). A WGB can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter in order to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB supports up to 20 Ethernet-enabled devices to a Wireless LAN (WLAN). The WGB associates to the root AP through the wireless interface. In this way, wired clients obtain access to the wireless network. A WGB can associate to:

- An AP
- A root bridge (in AP mode)
- A controller through a lightweight AP

When a Cisco 702W access point acts as a WGB, the wired Ethernet clients behind the WGB can be either connected to the LAN or WAN ports present on the 702W AP.