CISCO

Indhold

[Explore the Networking 7](#_Toc523909166)

[CISCO Chapters 7](#_Toc523909167)

[Chapter 1 7](#_Toc523909168)

[Characteristics of network: 8](#_Toc523909169)

[Why routing? 8](#_Toc523909170)

[Routers are computers: 8](#_Toc523909171)

[Routers Interconnect Networks: 9](#_Toc523909172)

[Routers Choose Best Paths: 9](#_Toc523909173)

[Packet Forwarding Mechanisms 9](#_Toc523909174)

[Process switching 9](#_Toc523909175)

[Fast switching 10](#_Toc523909176)

[Cisco Express Forwarding (CEF) 10](#_Toc523909177)

[Connect to a Network 10](#_Toc523909178)

[Default Gateways 11](#_Toc523909179)

[Document Network Addressing 11](#_Toc523909180)

[Enable IP on a Host 12](#_Toc523909181)

[Device LEDs 12](#_Toc523909182)

[Console Access 12](#_Toc523909183)

[Enable IP on a Switch 13](#_Toc523909184)

[Configure Basic Router Settings 13](#_Toc523909185)

[Configure an IPv4 Router Interface 14](#_Toc523909186)

[Configure an IPv6 Router Interface 14](#_Toc523909187)

[Configure an IPv6 Loopback Interface 15](#_Toc523909188)

[Verify Interface Settings: 15](#_Toc523909189)

[Verify IPv6 Interface Settings: 15](#_Toc523909190)

[Filter Show Command Output: 16](#_Toc523909191)

[Command History Feature 16](#_Toc523909192)

[Router Switching Function 16](#_Toc523909193)

[Send a Packet: 17](#_Toc523909194)

[Forward to the Next Hop: 17](#_Toc523909195)

[Packet Routing: 17](#_Toc523909196)

[Reach the Destination: 17](#_Toc523909197)

[Routing Decisions: 17](#_Toc523909198)

[Best Path 18](#_Toc523909199)

[Load Balancing 18](#_Toc523909200)

[Administrative Distance 19](#_Toc523909201)

[The Routing Table 19](#_Toc523909202)

[Routing table sources 19](#_Toc523909203)

[Remote Network Routing Entries 20](#_Toc523909204)

[Directly Connected Interfaces: 21](#_Toc523909205)

[Directly Connected Routing Table Entries 21](#_Toc523909206)

[Static Routes 22](#_Toc523909207)

[Dynamic Routing 23](#_Toc523909208)

[IPv4 Routing protocols 23](#_Toc523909209)

[IPv6 Routing Protocols 23](#_Toc523909210)

[Explore the Networking 28](#_Toc523909211)

[CISCO Chapters 28](#_Toc523909212)

[Chapter 1 28](#_Toc523909213)

[Characteristics of network: 28](#_Toc523909214)

[Why routing? 28](#_Toc523909215)

[Routers are computers: 29](#_Toc523909216)

[Routers Interconnect Networks: 29](#_Toc523909217)

[Routers Choose Best Paths: 29](#_Toc523909218)

[Packet Forwarding Mechanisms 30](#_Toc523909219)

[Process switching 30](#_Toc523909220)

[Fast switching 30](#_Toc523909221)

[Cisco Express Forwarding (CEF) 30](#_Toc523909222)

[Connect to a Network 30](#_Toc523909223)

[Default Gateways 31](#_Toc523909224)

[Document Network Addressing 31](#_Toc523909225)

[Enable IP on a Host 32](#_Toc523909226)

[Device LEDs 32](#_Toc523909227)

[Console Access 32](#_Toc523909228)

[Enable IP on a Switch 33](#_Toc523909229)

[Configure Basic Router Settings 33](#_Toc523909230)

[Configure an IPv4 Router Interface 34](#_Toc523909231)

[Configure an IPv6 Router Interface 34](#_Toc523909232)

[Configure an IPv6 Loopback Interface 35](#_Toc523909233)

[Verify Interface Settings: 35](#_Toc523909234)

[Verify IPv6 Interface Settings: 35](#_Toc523909235)

[Filter Show Command Output: 36](#_Toc523909236)

[Command History Feature 36](#_Toc523909237)

[Router Switching Function 36](#_Toc523909238)

[Send a Packet: 37](#_Toc523909239)

[Forward to the Next Hop: 37](#_Toc523909240)

[Packet Routing: 37](#_Toc523909241)

[Reach the Destination: 37](#_Toc523909242)

[Routing Decisions: 37](#_Toc523909243)

[Best Path 38](#_Toc523909244)

[Load Balancing 38](#_Toc523909245)

[Administrative Distance 39](#_Toc523909246)

[The Routing Table 39](#_Toc523909247)

[Routing table sources 39](#_Toc523909248)

[Remote Network Routing Entries 40](#_Toc523909249)

[Directly Connected Interfaces: 41](#_Toc523909250)

[Directly Connected Routing Table Entries 41](#_Toc523909251)

[Static Routes 42](#_Toc523909252)

[Dynamic Routing 43](#_Toc523909253)

[IPv4 Routing protocols 43](#_Toc523909254)

[IPv6 Routing Protocols 43](#_Toc523909255)

[Chapter 2: Static Routing 44](#_Toc523909256)

[Why Use Static Routing? 44](#_Toc523909257)

[When to Use Static Routes 45](#_Toc523909258)

[Static Route Applications 46](#_Toc523909259)

[Standard Static Route 46](#_Toc523909260)

[Default Static Route 46](#_Toc523909261)

[Summary Static Route 47](#_Toc523909262)

[Floating Static Route 47](#_Toc523909263)

[Configure an IPv4 Floating Static Route 48](#_Toc523909264)

[Test the IPv4 Floating Static Route 48](#_Toc523909265)

[Automatically Installed Host Routes 49](#_Toc523909266)

[Configure IPv4 and IPv6 Static Host Routes 50](#_Toc523909267)

[IP route Command 50](#_Toc523909268)

[Next-Hop Options 51](#_Toc523909269)

[Configure a Next-Hop Static Route 51](#_Toc523909270)

[Configure a Directly Connected Static Route 52](#_Toc523909271)

[Configure a Fully Specified Static Route 52](#_Toc523909272)

[Verify a Static Route 53](#_Toc523909273)

[Default Static Route 53](#_Toc523909274)

[Troubleshoot a Missing Route 53](#_Toc523909275)

[Chapter 3: Dynamic Routing 53](#_Toc523909276)

[Dynamic Routing Protocol Components 54](#_Toc523909277)

[Static Routing Uses 54](#_Toc523909278)

[Static Routing Advantages and Disadvantages 55](#_Toc523909279)

[Dynamic Routing Protocols Uses 55](#_Toc523909280)

[Dynamic Routing Advantages and Disadvantages 56](#_Toc523909281)

[Advertise Networks 56](#_Toc523909282)

[Verify RIP Routing 57](#_Toc523909283)

[Enabling and verify RIPv2 57](#_Toc523909284)

[Disable Auto Summarization 58](#_Toc523909285)

[Configure Passive Interfaces 58](#_Toc523909286)

[Propagate a Default Route 58](#_Toc523909287)

[Routing Table Entries 59](#_Toc523909288)

[Directly Connected Entries 60](#_Toc523909289)

[Remote Network Entries 60](#_Toc523909290)

[Routing Table Terms 61](#_Toc523909291)

[Ultimate Route 62](#_Toc523909292)

[Level 1 Route 63](#_Toc523909293)

[Level 1 Parent Route 64](#_Toc523909294)

[Level 2 Child Route 64](#_Toc523909295)

[Router look up process 65](#_Toc523909296)

[Best routs == longest match 65](#_Toc523909297)

[IPv6 routing table entries 65](#_Toc523909298)

[Chapter 4: switched networks 66](#_Toc523909299)

[Growing complexity of networks 66](#_Toc523909300)

[Elements of a converged Network 66](#_Toc523909301)

[Cisco Borderless Networks 66](#_Toc523909302)

[Hierarchy in the Borderless Switched Network 66](#_Toc523909303)

[Access, Distribution, and Core Layers 67](#_Toc523909304)

[Role of Switched Networks 68](#_Toc523909305)

[Form Factors 68](#_Toc523909306)

[Switching as a General Concept in Networking and Telecommunications 68](#_Toc523909307)

[Dynamically Populating a Switch MAC Address Table 68](#_Toc523909308)

[Switch Forwarding Methods 69](#_Toc523909309)

[Collision Domains 69](#_Toc523909310)

[Broadcast Domains 69](#_Toc523909311)

[Alleviating Network Congestion 70](#_Toc523909312)

[Chapter 5: Switch Configuration 70](#_Toc523909313)

[Recovering From a System Crash 71](#_Toc523909314)

[Switch LED Indicators 71](#_Toc523909315)

[Preparing for Basic Switch Management 72](#_Toc523909316)

[Configuring Basic Switch Management Access with IPv4 72](#_Toc523909317)

[Duplex Communication 72](#_Toc523909318)

[Configure Switch Ports at the Physical Layer 73](#_Toc523909319)

[Auto-MDIX 74](#_Toc523909320)

[Verifying Switch Port Configuration 76](#_Toc523909321)

[Network Access Layer Issues 76](#_Toc523909322)

[Troubleshooting Network Access Layer Issues 78](#_Toc523909323)

[SSH Operation 78](#_Toc523909324)

[Configuring SSH 79](#_Toc523909325)

[Verifying SSH 80](#_Toc523909326)

[Secure Unused Ports 80](#_Toc523909327)

[Port Security: Operation 80](#_Toc523909328)

[Port Security: Violation Modes 82](#_Toc523909329)

[Port Security: Verifying 83](#_Toc523909330)

[Ports in Error Disabled State 85](#_Toc523909331)

[Chapter 6: VLANs 86](#_Toc523909332)

[Benefits of VLANs 88](#_Toc523909333)

[Types of VLANs 88](#_Toc523909334)

[Voice VLANs 89](#_Toc523909335)

[VLAN Trunks 89](#_Toc523909336)

[Controlling Broadcast Domains with VLANs 89](#_Toc523909337)

[Tagging Ethernet Frames for VLAN Identification 89](#_Toc523909338)

[Native VLANs and 802.1Q Tagging 90](#_Toc523909339)

[Voice VLAN Tagging 90](#_Toc523909340)

[VLAN Ranges on Catalyst Switches 91](#_Toc523909341)

[Creating a VLAN 92](#_Toc523909342)

[Assigning Ports to VLANs 92](#_Toc523909343)

[Changing VLAN Port Membership 93](#_Toc523909344)

[Deleting VLANs 93](#_Toc523909345)

[Verifying VLAN Information 94](#_Toc523909346)

[Configuring IEEE 802.1Q Trunk Links 94](#_Toc523909347)

[Resetting the Trunk to Default State 95](#_Toc523909348)

[Verifying Trunk Configuration 95](#_Toc523909349)

[IP Addressing Issues with VLAN 96](#_Toc523909350)

[Missing VLANs 96](#_Toc523909351)

[Missing VLANs (cont.) 96](#_Toc523909352)

[Introduction to Troubleshooting Trunks 96](#_Toc523909353)

[Common Problems with Trunks 97](#_Toc523909354)

[Common Problems with Trunks (cont.) 97](#_Toc523909355)

[Incorrect Port Mode 97](#_Toc523909356)

[Incorrect VLAN List 98](#_Toc523909357)

[Legacy Inter-VLAN Routing 99](#_Toc523909358)

[Router-on-a-Stick Inter-VLAN Routing 99](#_Toc523909359)

[Configure Legacy Inter-VLAN Routing: Preparation 100](#_Toc523909360)

[Configure Legacy Inter-VLAN Routing: Switch Configuration 100](#_Toc523909361)

[Configure Legacy Inter-VLAN Routing: Router Interface Configuration 100](#_Toc523909362)

[Configure Router-on-a-Stick: Preparation 100](#_Toc523909363)

[Configure Router-on-a-Stick: Switch Configuration 101](#_Toc523909364)

[Configure Router-on-a-Stick: Router Subinterface Configuration 101](#_Toc523909365)

[Configure Router-on-a-Stick: Verifying Subinterfaces 101](#_Toc523909366)

[Configure Router-on-a-Stick: Verifying Routing 101](#_Toc523909367)

[The Inside Track 102](#_Toc523909368)

[Chapter 7: Access Control Lists 103](#_Toc523909369)

[FTP Denied 103](#_Toc523909370)

[Chapter 8: DHCP 104](#_Toc523909371)

[Class Activity - IoE and DHCP 104](#_Toc523909372)

[Chapter 9: NAT for IPv4 105](#_Toc523909373)

[NAT Check 105](#_Toc523909374)

[Packet Tracer - Skills Integration Challenge 105](#_Toc523909375)

[Chapter 10: Device Discovery, Management, and Maintenance 106](#_Toc523909376)

# Explore the Networking

Packet Tracer: it is a software that can be used to create an own virtual network. Benefits of using that is, the user can check if the private (own network) network platform is usable by testing it virtually. And it can be good practice for new students who don’t have much experience on networking.

# CISCO Chapters

## Chapter 1

### Characteristics of network:

**Topology** - There are physical and logical topologies. The physical topology is the algorithm of the cables and the end device connections it shows how it is connected to each device.

The logical topology describes how the network devices appear connected to network users. In other words it more detailed way of showing how the network has been build.

**Speed** - Speed is measured by bits per second (b/s) it describe how fast is the network is. For example how long will it take to upload and download something using the network?

**Cost** - Cost indicates the scale of general expense for set up a network

**Security** - Security indicates how protected the network is.

**Availability** - Availability is makes the network available for use when it is required.

**Scalability** - Scalability indicates how easily the network can accommodate more users and data transmission requirements. It makes the network flexible to use

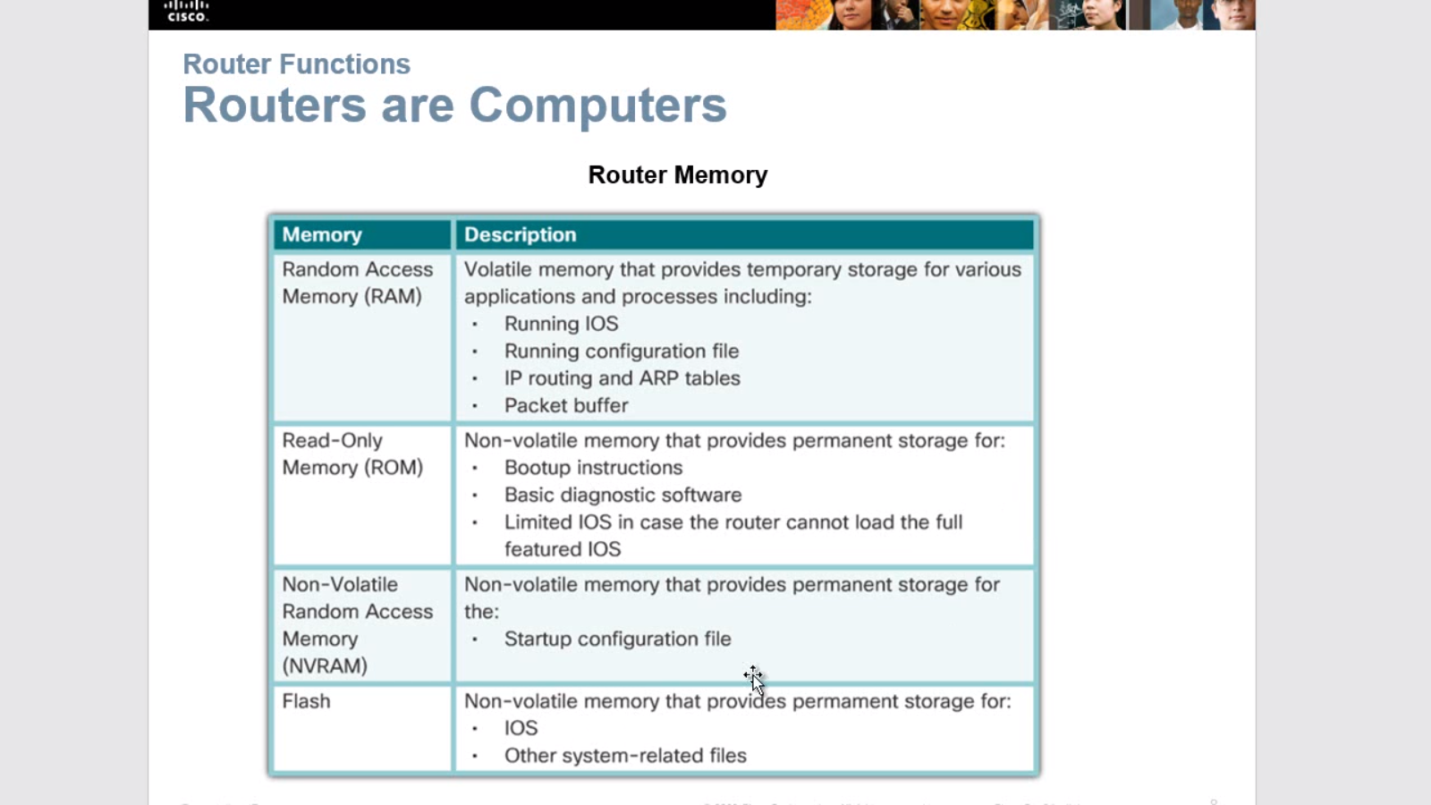
**Reliability** - Reliability indicates the dependability of the network. The network should be available at all time needed.

### Why routing?

Routers are making decisions to ping with other networks to communicate with them, you won't be able communicate with other LAN without routers doing their job.

### Routers are computers:

Routers have the almost the same compounds as a personal computer such as CPU, Memory and storage and an operating system. And routers have specialized ports and a NIC to interconnect to other network



### Routers Interconnect Networks:

Routes on routers between the user and other users those routers allow each other to communicate through network.

### Routers Choose Best Paths:

Router will always find the best path to communicate with other routers which makes the communication is faster and it use static and dynamic IP address. Static IP is manual and dynamic is automatic and faster and the IP connectivity will allow the remote network.

**Routers use static routes and dynamic routing protocols to learn about remote networks and build their routing tables.**

### 

### Packet Forwarding Mechanisms

There are three methods. Basically oldest and slowest and fastest and most efficient

### Process switching

This method was the oldest and the slowest. This method takes every packet and then processes it to see where it should be sent to and then it slowly by packet by packet.

### Fast switching

A common packet forwarding use the method call cash to store to store next hop information so if a packet the arrived in the control plane and match an entry in the fast switching cash it will go ahead and send it out fast to the proper interface and if there not a match it it go through the process swish and try to find a matching interface. This method will not use the CUP if the next hop information is saved.

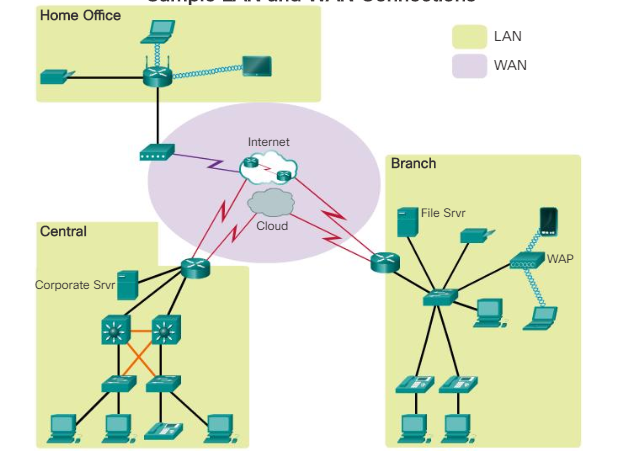
Next hop (network to network/ router to router. **each router is a hop**)

### Cisco Express Forwarding (CEF)

The most recent and the fastest forwarding technique. CEF builds a Forwarding Information Base (FIB), and an adjacency table that is what is responsible for this method. It will lean and contains information of all the available next hop in the network there for all the data will be sent as fast as possible because the processing is not needed. And the CPU will not be use because of that.

### Connect to a Network

Basically use Ethernet setups and wireless setups to connect devices together and connect the devices to the network



### Default Gateways

If want to be able to get off the network then the IP address and subnet mask and default gateway is needed.

default gateway is the router internet that is connected to the IP address of the network and the devices of that network is using that IP address to get off the network

* IP address - Identifies a unique host on a local network.
* Subnet mask - Identifies with which network subnet the host can communicate.
* Default gateway - Identifies the IP address of the router to send a packet to when the destination is not on the same local network subnet.

### Document Network Addressing

When documenting a network have to make sure Device names,Interfaces used in the design, IP addresses and subnet masks,Default gateway addresses are visible to read properly at minimum.

### Enable IP on a Host

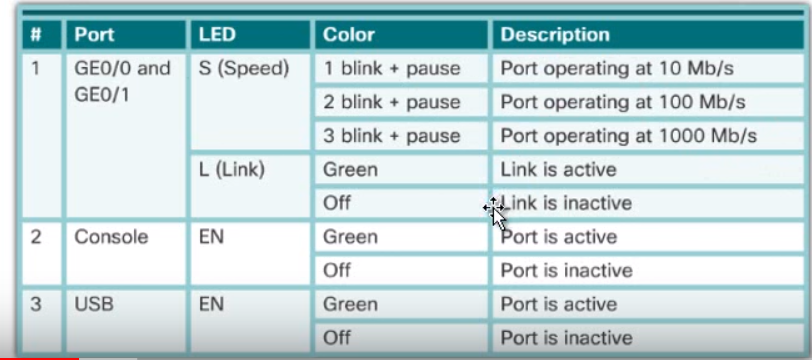
A host can be assigned IP address information either:

**Statically** - The host is manually assigned the correct IP address, subnet mask, and default gateway. The DNS server IP address can also be configured.

**Dynamically** - IP address information is provided automatically  by a server using the Dynamic Host Configuration Protocol (DHCP). The DHCP server provides a valid IP address, subnet mask, and default gateway for end devices.

### Device LEDs

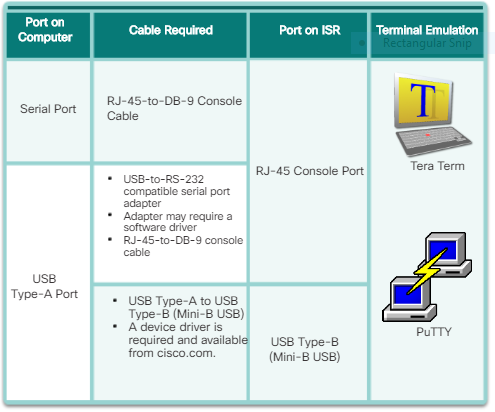
It’s important to know what the lights mean in the cisco device or the router.



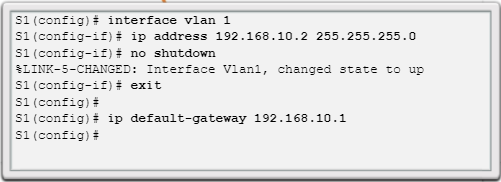
### Console Access

To get access to the console control the router or the cisco device has to be connected by using the USB or serial port and a terminal software is also needed

* **Console cable** - RJ-45-to-DB-9 serial cable or a USB serial cable
* **Terminal emulation software** - Teraterm, PuTTY, HyperTerminal

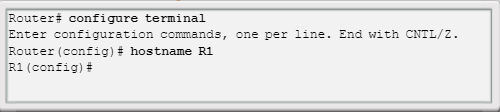


### Enable IP on a Switch

Need to use some specific commands in order to enable Ip on a switch

### Configure Basic Router Settings

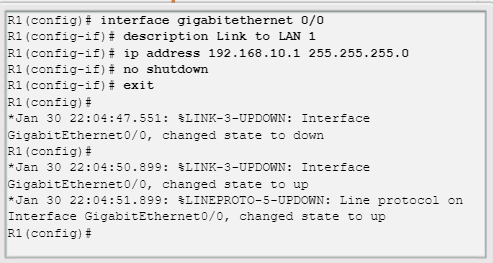
Need to have knowledge about commands that used in a switch



### Configure an IPv4 Router Interface

to be available, an interface must be:

* **Configured with an IP address and a subnet mask** - Use the **ip address** *ip-address subnet-mask* interface configuration command.
* **Activated** - By default, LAN and WAN interfaces are not activated (**shutdown**). To enable an interface, it must be activated using the **“no shutdown”** command. The interface must also be connected to another device (a hub, a switch, or another router) for the physical layer to be active.



### Configure an IPv6 Router Interface

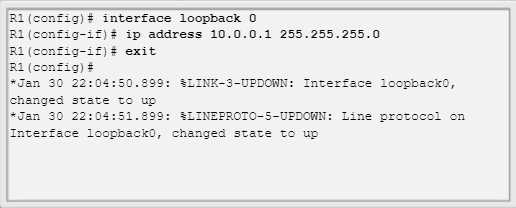
An IPv6 interface must be:

* **Configured with IPv6 address and subnet mask** - Use the **ipv6 address** ipv6-address/prefix-length **[link-local | eui-64]** interface configuration command.
* **Activated** - The interface must be activated using the **“no shutdown”** command.

### Configure an IPv6 Loopback Interface

**A loopback interface is logical interface that is internal to the router**

* It’s considered as a software interface that is automatically an UP state.
* This interface used for testing and management
* It’s important in the OSPF routing process



### Verify Interface Settings:

Show commands are used to verify operation and configuration of an interface:

* **show ip interfaces brief** - display the interface
* **show ip route**
* **show running-config**

Show commands that are used for get more information about the running interface

* **show interfaces**
* **show ip interface**- display the status and all ip addresses for this interface

### Verify IPv6 Interface Settings:

It is the same commands as ipv4 but has to write ipv6 instead of ipv4

* **Show ipv6 interface brief** - displays a summary for each of the interfaces.
* **Show ipv6 interface gigabit Ethernet 0/0** -display the status and all the ipv6 addresses for this interface.
* **Show ipv6 route** - verifies that ipv6 network and specific ipv6 interface addresses have been in the ipv6 routing table.

### Filter Show Command Output:

Show commands output can be managed using the following coma filters

* Use the **terminal length** number command to specify the number of the Niles to be displayed
* To filter specify output of commands use the (I) pipe character after show command. Parameters that can be used after pipe include:
* **Section**
* **include**
* **exclude**
* **begin**

### Command History Feature

It’s like to the undo feature and browser history feature in the computer.

There are some specific commands that can be used to execute these features.

Such as:

* To recall commands in the history buffer, press **Ctrl+P** or the **Up Arrow** key.
* To return to more recent commands in the history buffer, press **Ctrl+N** or the **Down Arrow** key

By default, command history is enable and the system captures the æast 10 commands in the buffer. use the **show history** privileged EXEC command to display the contents of the buffer.

Use the **terminal history size** user ECCE command to increase or decrease the size of the buff

### Router Switching Function

Router is going to receive a packet and use the switching function to move the packet from one interface to another. The router receive the packet through **ingress** port and send it through **egress** port or an exit port.

The router will make a decision based on de-encapsulate everything up to layer 3 and the find the ip address destination the paket is heading for and check that against routing table and make couple of process to make a decisions and then send it to the appropriate interface.

When the packet receive and it will look through the layer 3 information but It will not change the layer 3 information because IP addresses won’t change. But it will change layer 2 information because MAC address will change every hop. Also because you might need to re-encapsulate to send it over ethernet cable,wireless or other method so therefor the **layer 2 information will change but layer 3 information will not change.**

### Send a Packet:

The mac address is always going to have the destination of the next hop in the path so the mac address will change but the destination IP address will never change.

### Forward to the Next Hop:

Routers are using an ARP table and routing table to get information to build a frame for forward packets. Because **the ARP table and routing table have informing for the next hop**.

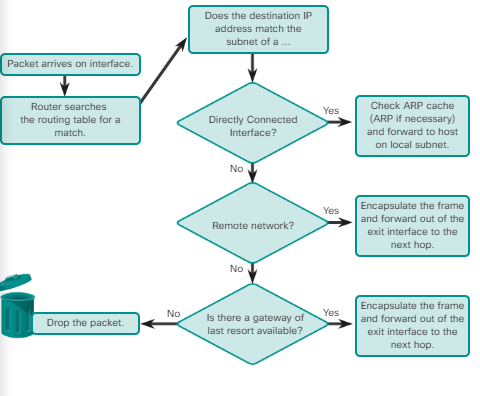
### Packet Routing:

When the paket is at the end point of the LAN and ready to sent it to the destination LAN router does not need a MAC address, it’s just need the destination IP address and when it sent to the destination ip address the router of that network will sent it to the destination MAC address.

### Reach the Destination:

When the paket destination is in the same network the router use the MAC address destination to sent it the correct destination.

### Routing Decisions:



The way of router make the decisions to send a packet to the correct destination.

### Best Path

The best path is doing to be determined by a metric ( a metric is a value used to measure the distance to a given network ) **best path to a network is the path with the lowest metric.**

Metric can be few different thing the other protocols use their own rules build metric.

The most simple one is called **Routing Information Protocol(RIP)** - hop count. It counts how many hops(routers) are there in between you and the destination network.

**Open Shortest Path First (OSPF)** - protocol that has been used between all different kind of devices. Cisco’s cost based on cumulative bandwidth from source to destination this is abit more relatable than RIP.

**Enhanced Interior Gateway Routing Protocol (EIGRP)** -  Bandwidth, delay, load, reliability calculates EIGRP metric.

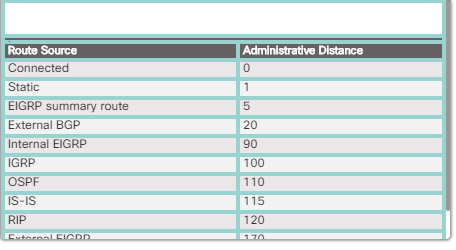
### Load Balancing

Load balancing is when there are more than one path to send data and it has the equal about of metic, the computer will send equal amount of data through both paths (half and half) and it will optimize the speed and time. **Equal cost load balance can improve network performance.**

This method will avoid overloading a network path between routers.

**Only protocol that use unequal cost load balancing is (EIGRP)**

### Administrative Distance

The trustworthy or effectiveness of a route **lower is better.**the default Administrative Distance.

### The Routing Table

There are directly connected and remote routers.

**A routing table is a file that stored in a RAM and it contains information about remote routers and directly connected routers .**

### Routing table sources

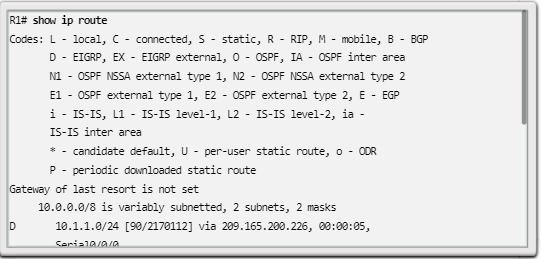
The **show ip route** command is used to display the contents of the routing table.

**Local route interfaces -** when the interface is configured it will be added to the routing table.

**Directly connected interface -**  added to the routing table when the interface is configured and active.

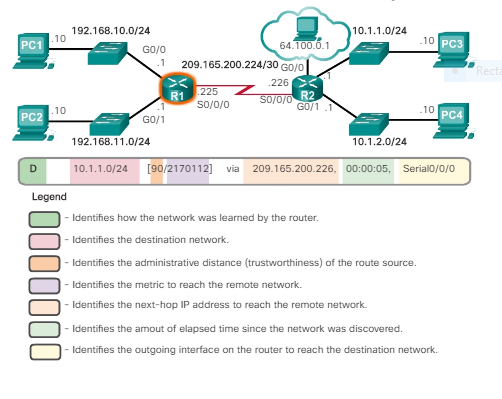
**Static routes -** added when manually configured by the user.

**Dynamic routing protocol -** automatically added based on whichever protocol is been used.



### Remote Network Routing Entries

* **Route source** - Identifies how the route was learned.
* **Destination network** - Identifies the address of the remote network.
* **Administrative distance** - Identifies the trustworthiness of the route source. Lower values indicate preferred route source.
* **Metric** - Identifies the value assigned to reach the remote network. Lower values indicate preferred routes.
* **Next-hop** - Identifies the IPv4 address of the next router to forward the packet to.
* **Route timestamp** - Identifies how much time has passed since the route was learned.
* **Outgoing interface** - Identifies the exit interface to use to forward a packet toward the final destination.

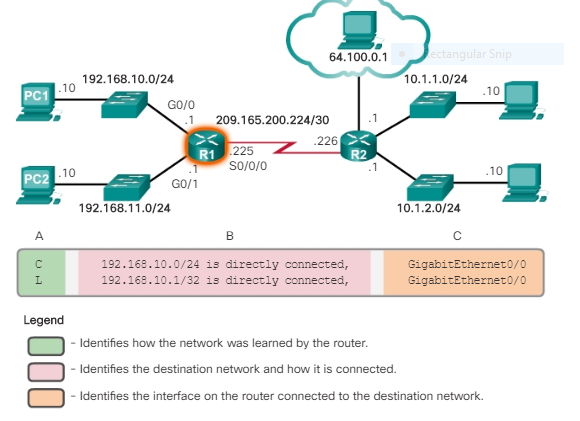


### Directly Connected Interfaces:

A newly deployed router, with no interface configured  has an empty routing table.

### Directly Connected Routing Table Entries

When the network is directly connected, directly connected interfaces have two route source codes. ‘C’ identifies a directly connected network. ’L’ identifies the IPv4 address assigned to the router’s interface.



**Destination network** - The address of the remote network.

**Outgoing interface** - Identifies the exit interface to use when forwarding packets to the destination network.

### Static Routes

Static routes are manually configured therefor the main disadvantage of using a static router is if the network topology changes the static routes should me manually re-configure unlikely dynamic routes although using static routes improved security and resource efficiency.

Static routes use less bandwidth than dynamic routing protocols, and no CPU cycles are used to calculate and communicate routes

There are two common types of static routes in the routing table:

* Static route to a specific network

A static route can be configured to reach a specific remote network. IPv4 static routes are configured using the following command:

Router(config)# **ip route** *network mask* {*next-hop-ip* | *exit-intf* }

A static route is identified in the routing table with the code ‘**S**’

* Default static route

A default static route is similar to a default gateway on a host.

The default static route specifies the exit point to use when the routing table does not contain a path for the destination network. A default static route is useful when a router has only one exit point to another router

To configure an IPv4 default static route, use the following command:

Router(config)# **ip route 0.0.0.0 0.0.0.0** { *exit-intf* | *next-hop-ip* }

### Dynamic Routing

Dynamic routers are automatically learning about the paths to different networks.Dynamic routing protocols are used by routers to share information about the reachability and status of remote networks. It performs network discovery and maintains routing tables.

**Dynamic routers has a good knowledge about all the routers around them**

If there are multiple ways to get to a network and one goes down a dynamic router can finds it way around the network automatically unlikely statistic routers.

### IPv4 Routing protocols

A router running a dynamic routing protocol does not only make a best path determination to a network, it also determines a new best path if the topology changes because the routers that use dynamic routing protocols automatically share informations with other routers

Cisco routers can support a variety of dynamic IPv4 routing protocols including:

* **EIGRP** - Enhanced Interior Gateway Routing Protocol
* **OSPF** - Open Shortest Path First
* **IS-IS** - Intermediate System-to-Intermediate System
* **RIP** - Routing Information Protocol

### IPv6 Routing Protocols

ISR devices support dynamic IPv6 routing protocols including:

* RIPng (RIP next generation)
* OSPFv3
* EIGRP for IPv6

Support for dynamic IPv6 routing protocols is dependent on hardware and IOS version.

To enable IPv6 routers to forward traffic, must configure the **ipv6 unicast-routing** global configuration command.

CISCO

Indhold

[Explore the Networking 5](#_Toc522090096)

[CISCO Chapters 5](#_Toc522090097)

[Chapter 1 5](#_Toc522090098)

[Characteristics of network: 5](#_Toc522090099)

[Why routing? 5](#_Toc522090100)

[Routers are computers: 6](#_Toc522090101)

[Routers Interconnect Networks: 6](#_Toc522090102)

[Routers Choose Best Paths: 6](#_Toc522090103)

[Packet Forwarding Mechanisms 7](#_Toc522090104)

[Process switching 7](#_Toc522090105)

[Fast switching 7](#_Toc522090106)

[Cisco Express Forwarding (CEF) 7](#_Toc522090107)

[Connect to a Network 7](#_Toc522090108)

[Default Gateways 8](#_Toc522090109)

[Document Network Addressing 8](#_Toc522090110)

[Enable IP on a Host 9](#_Toc522090111)

[Device LEDs 9](#_Toc522090112)

[Console Access 9](#_Toc522090113)

[Enable IP on a Switch 10](#_Toc522090114)

[Configure Basic Router Settings 10](#_Toc522090115)

[Configure an IPv4 Router Interface 11](#_Toc522090116)

[Configure an IPv6 Router Interface 11](#_Toc522090117)

[Configure an IPv6 Loopback Interface 12](#_Toc522090118)

[Verify Interface Settings: 12](#_Toc522090119)

[Verify IPv6 Interface Settings: 12](#_Toc522090120)

[Filter Show Command Output: 13](#_Toc522090121)

[Command History Feature 13](#_Toc522090122)

[Router Switching Function 14](#_Toc522090123)

[Send a Packet: 14](#_Toc522090124)

[Forward to the Next Hop: 14](#_Toc522090125)

[Packet Routing: 14](#_Toc522090126)

[Reach the Destination: 14](#_Toc522090127)

[Routing Decisions: 14](#_Toc522090128)

[Best Path 15](#_Toc522090129)

[Load Balancing 15](#_Toc522090130)

[Administrative Distance 16](#_Toc522090131)

[The Routing Table 16](#_Toc522090132)

[Routing table sources 16](#_Toc522090133)

[Remote Network Routing Entries 17](#_Toc522090134)

[Directly Connected Interfaces: 18](#_Toc522090135)

[Directly Connected Routing Table Entries 18](#_Toc522090136)

[Static Routes 19](#_Toc522090137)

[Dynamic Routing 20](#_Toc522090138)

[IPv4 Routing protocols 20](#_Toc522090139)

[IPv6 Routing Protocols 20](#_Toc522090140)

[Chapter 2 21](#_Toc522090141)

[Explore the Networking 25](#_Toc522090142)

[CISCO Chapters 25](#_Toc522090143)

[Chapter 1 25](#_Toc522090144)

[Characteristics of network: 25](#_Toc522090145)

[Why routing? 26](#_Toc522090146)

[Routers are computers: 26](#_Toc522090147)

[Routers Interconnect Networks: 26](#_Toc522090148)

[Routers Choose Best Paths: 26](#_Toc522090149)

[Packet Forwarding Mechanisms 27](#_Toc522090150)

[Process switching 27](#_Toc522090151)

[Fast switching 27](#_Toc522090152)

[Cisco Express Forwarding (CEF) 27](#_Toc522090153)

[Connect to a Network 27](#_Toc522090154)

[Default Gateways 28](#_Toc522090155)

[Document Network Addressing 28](#_Toc522090156)

[Enable IP on a Host 29](#_Toc522090157)

[Device LEDs 29](#_Toc522090158)

[Console Access 29](#_Toc522090159)

[Enable IP on a Switch 30](#_Toc522090160)

[Configure Basic Router Settings 30](#_Toc522090161)

[Configure an IPv4 Router Interface 31](#_Toc522090162)

[Configure an IPv6 Router Interface 31](#_Toc522090163)

[Configure an IPv6 Loopback Interface 32](#_Toc522090164)

[Verify Interface Settings: 32](#_Toc522090165)

[Verify IPv6 Interface Settings: 32](#_Toc522090166)

[Filter Show Command Output: 33](#_Toc522090167)

[Command History Feature 33](#_Toc522090168)

[Router Switching Function 34](#_Toc522090169)

[Send a Packet: 34](#_Toc522090170)

[Forward to the Next Hop: 34](#_Toc522090171)

[Packet Routing: 34](#_Toc522090172)

[Reach the Destination: 34](#_Toc522090173)

[Routing Decisions: 34](#_Toc522090174)

[Best Path 35](#_Toc522090175)

[Load Balancing 35](#_Toc522090176)

[Administrative Distance 36](#_Toc522090177)

[The Routing Table 36](#_Toc522090178)

[Routing table sources 36](#_Toc522090179)

[Remote Network Routing Entries 37](#_Toc522090180)

[Directly Connected Interfaces: 38](#_Toc522090181)

[Directly Connected Routing Table Entries 38](#_Toc522090182)

[Static Routes 39](#_Toc522090183)

[Dynamic Routing 40](#_Toc522090184)

[IPv4 Routing protocols 40](#_Toc522090185)

[IPv6 Routing Protocols 40](#_Toc522090186)

[Chapter 2: Static Routing 41](#_Toc522090187)

[Why Use Static Routing? 41](#_Toc522090188)

[When to Use Static Routes 42](#_Toc522090189)

[Static Route Applications 43](#_Toc522090190)

[Standard Static Route 43](#_Toc522090191)

[Default Static Route 43](#_Toc522090192)

[Summary Static Route 44](#_Toc522090193)

[Floating Static Route 44](#_Toc522090194)

[Configure an IPv4 Floating Static Route 45](#_Toc522090195)

[Test the IPv4 Floating Static Route 45](#_Toc522090196)

[Automatically Installed Host Routes 46](#_Toc522090197)

[Configure IPv4 and IPv6 Static Host Routes 47](#_Toc522090198)

[IP route Command 47](#_Toc522090199)

[Next-Hop Options 48](#_Toc522090200)

[Configure a Next-Hop Static Route 48](#_Toc522090201)

[Configure a Directly Connected Static Route 49](#_Toc522090202)

[Configure a Fully Specified Static Route 49](#_Toc522090203)

[Verify a Static Route 50](#_Toc522090204)

[Default Static Route 50](#_Toc522090205)

[Troubleshoot a Missing Route 50](#_Toc522090206)

[Chapter 3: Dynamic Routing 50](#_Toc522090207)

[Dynamic Routing Protocol Components 51](#_Toc522090208)

[Static Routing Uses 51](#_Toc522090209)

[Static Routing Advantages and Disadvantages 52](#_Toc522090210)

[Dynamic Routing Protocols Uses 53](#_Toc522090211)

[Dynamic Routing Advantages and Disadvantages 53](#_Toc522090212)

[Advertise Networks 53](#_Toc522090213)

[Verify RIP Routing 54](#_Toc522090214)

[Enabling and verify RIPv2 55](#_Toc522090215)

[Disable Auto Summarization 55](#_Toc522090216)

[Configure Passive Interfaces 55](#_Toc522090217)

[Propagate a Default Route 56](#_Toc522090218)

# Explore the Networking

Packet Tracer: it is a software that can be used to create an own virtual network. Benefits of using that is, the user can check if the private (own network) network platform is usable by testing it virtually. And it can be good practice for new students who don’t have much experience on networking.

# CISCO Chapters

# Chapter 1

### Characteristics of network:

**Topology** - There are physical and logical topologies. The physical topology is the algorithm of the cables and the end device connections it shows how it is connected to each device.

The logical topology describes how the network devices appear connected to network users. In other words it more detailed way of showing how the network has been build.

**Speed** - Speed is measured by bits per second (b/s) it describe how fast is the network is. For example how long will it take to upload and download something using the network?

**Cost** - Cost indicates the scale of general expense for set up a network

**Security** - Security indicates how protected the network is.

**Availability** - Availability is makes the network available for use when it is required.

**Scalability** - Scalability indicates how easily the network can accommodate more users and data transmission requirements. It makes the network flexible to use

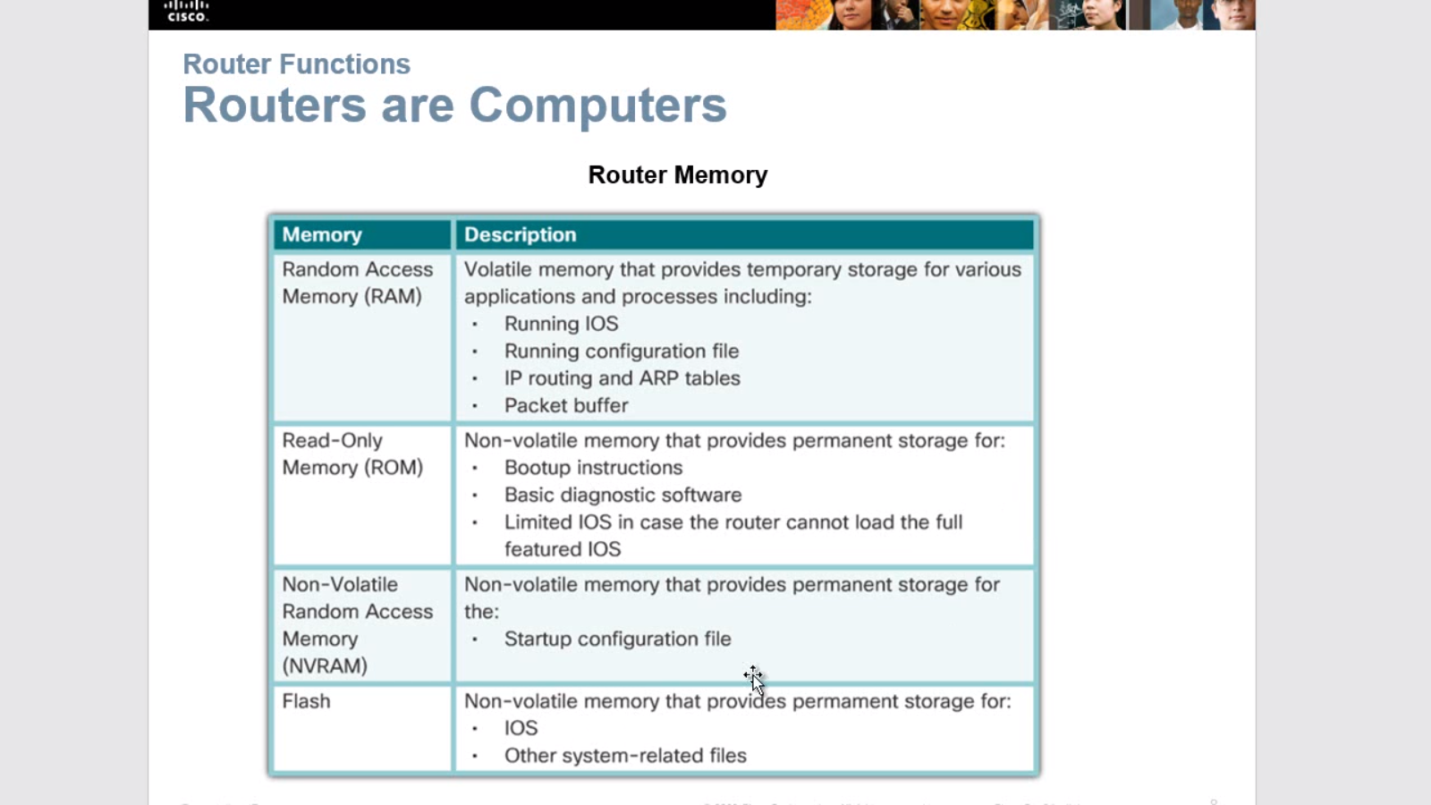
**Reliability** - Reliability indicates the dependability of the network. The network should be available at all time needed.

### Why routing?

Routers are making decisions to ping with other networks to communicate with them, you won't be able communicate with other LAN without routers doing their job.

### Routers are computers:

Routers have the almost the same compounds as a personal computer such as CPU, Memory and storage and an operating system. And routers have specialized ports and a NIC to interconnect to other network



### Routers Interconnect Networks:

Routes on routers between the user and other users those routers allow each other to communicate through network.

### Routers Choose Best Paths:

Router will always find the best path to communicate with other routers which makes the communication is faster and it use static and dynamic IP address. Static IP is manual and dynamic is automatic and faster and the IP connectivity will allow the remote network.

**Routers use static routes and dynamic routing protocols to learn about remote networks and build their routing tables.**

### Packet Forwarding Mechanisms

There are three methods. Basically oldest and slowest and fastest and most efficient

### Process switching

This method was the oldest and the slowest. This method takes every packet and then processes it to see where it should be sent to and then it slowly by packet by packet.

### Fast switching

A common packet forwarding use the method call cash to store to store next hop information so if a packet the arrived in the control plane and match an entry in the fast switching cash it will go ahead and send it out fast to the proper interface and if there not a match it it go through the process swish and try to find a matching interface. This method will not use the CUP if the next hop information is saved.

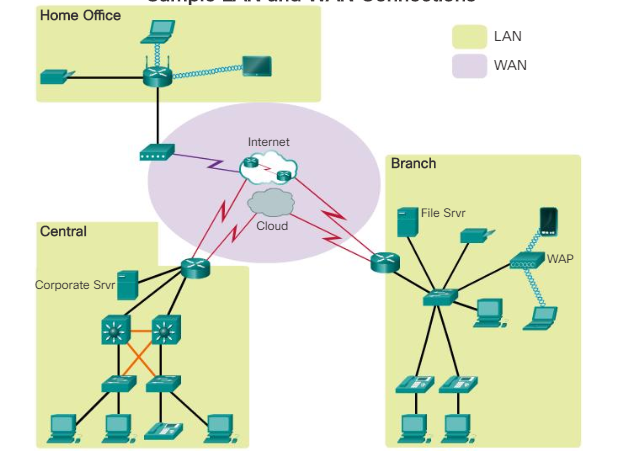
Next hop (network to network/ router to router. **each router is a hop**)

### Cisco Express Forwarding (CEF)

The most recent and the fastest forwarding technique. CEF builds a Forwarding Information Base (FIB), and an adjacency table that is what is responsible for this method. It will lean and contains information of all the available next hop in the network there for all the data will be sent as fast as possible because the processing is not needed. And the CPU will not be use because of that.

### Connect to a Network

Basically use Ethernet setups and wireless setups to connect devices together and connect the devices to the network



### Default Gateways

If want to be able to get off the network then the IP address and subnet mask and default gateway is needed.

default gateway is the router internet that is connected to the IP address of the network and the devices of that network is using that IP address to get off the network

* IP address - Identifies a unique host on a local network.
* Subnet mask - Identifies with which network subnet the host can communicate.
* Default gateway - Identifies the IP address of the router to send a packet to when the destination is not on the same local network subnet.

### Document Network Addressing

When documenting a network have to make sure Device names,Interfaces used in the design, IP addresses and subnet masks,Default gateway addresses are visible to read properly at minimum.

### Enable IP on a Host

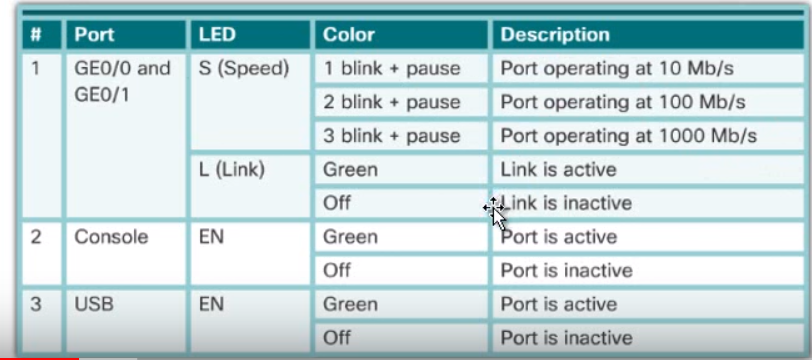
A host can be assigned IP address information either:

**Statically** - The host is manually assigned the correct IP address, subnet mask, and default gateway. The DNS server IP address can also be configured.

**Dynamically** - IP address information is provided automatically  by a server using the Dynamic Host Configuration Protocol (DHCP). The DHCP server provides a valid IP address, subnet mask, and default gateway for end devices.

### Device LEDs

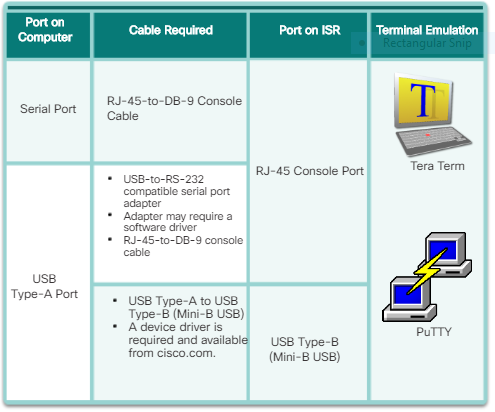
It’s important to know what the lights mean in the cisco device or the router.



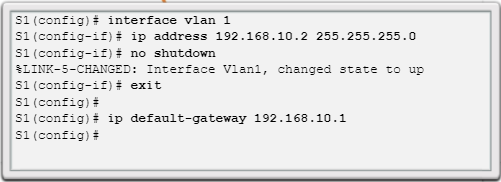
### Console Access

To get access to the console control the router or the cisco device has to be connected by using the USB or serial port and a terminal software is also needed

* **Console cable** - RJ-45-to-DB-9 serial cable or a USB serial cable
* **Terminal emulation software** - Teraterm, PuTTY, HyperTerminal

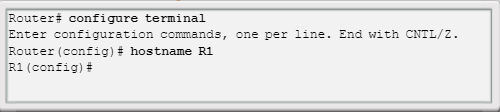


### Enable IP on a Switch

Need to use some specific commands in order to enable Ip on a switch

### Configure Basic Router Settings

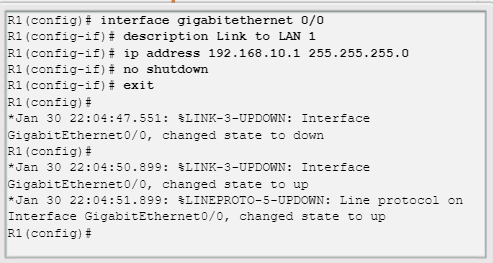
Need to have knowledge about commands that used in a switch



### Configure an IPv4 Router Interface

to be available, an interface must be:

* **Configured with an IP address and a subnet mask** - Use the **ip address** *ip-address subnet-mask* interface configuration command.
* **Activated** - By default, LAN and WAN interfaces are not activated (**shutdown**). To enable an interface, it must be activated using the **“no shutdown”** command. The interface must also be connected to another device (a hub, a switch, or another router) for the physical layer to be active.



### Configure an IPv6 Router Interface

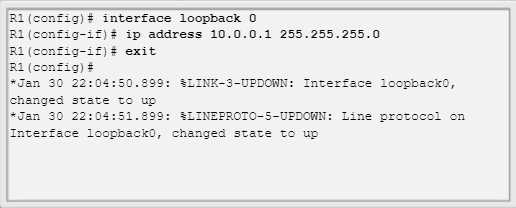
An IPv6 interface must be:

* **Configured with IPv6 address and subnet mask** - Use the **ipv6 address** ipv6-address/prefix-length **[link-local | eui-64]** interface configuration command.
* **Activated** - The interface must be activated using the **“no shutdown”** command.

### Configure an IPv6 Loopback Interface

**A loopback interface is logical interface that is internal to the router**

* It’s considered as a software interface that is automatically an UP state.
* This interface used for testing and management
* It’s important in the OSPF routing process



### Verify Interface Settings:

Show commands are used to verify operation and configuration of an interface:

* **show ip interfaces brief** - display the interface
* **show ip route**
* **show running-config**

Show commands that are used for get more information about the running interface

* **show interfaces**
* **show ip interface**- display the status and all ip addresses for this interface

### Verify IPv6 Interface Settings:

It is the same commands as ipv4 but has to write ipv6 instead of ipv4

* **Show ipv6 interface brief** - displays a summary for each of the interfaces.
* **Show ipv6 interface gigabit Ethernet 0/0** -display the status and all the ipv6 addresses for this interface.
* **Show ipv6 route** - verifies that ipv6 network and specific ipv6 interface addresses have been in the ipv6 routing table.

### Filter Show Command Output:

Show commands output can be managed using the following coma filters

* Use the **terminal length** number command to specify the number of the Niles to be displayed
* To filter specify output of commands use the (I) pipe character after show command. Parameters that can be used after pipe include:
* **Section**
* **include**
* **exclude**
* **begin**

### Command History Feature

It’s like to the undo feature and browser history feature in the computer.

There are some specific commands that can be used to execute these features.

Such as:

* To recall commands in the history buffer, press **Ctrl+P** or the **Up Arrow** key.
* To return to more recent commands in the history buffer, press **Ctrl+N** or the **Down Arrow** key

By default, command history is enable and the system captures the æast 10 commands in the buffer. use the **show history** privileged EXEC command to display the contents of the buffer.

Use the **terminal history size** user ECCE command to increase or decrease the size of the buff

### Router Switching Function

Router is going to receive a packet and use the switching function to move the packet from one interface to another. The router receive the packet through **ingress** port and send it through **egress** port or an exit port.

The router will make a decision based on de-encapsulate everything up to layer 3 and the find the ip address destination the paket is heading for and check that against routing table and make couple of process to make a decisions and then send it to the appropriate interface.

When the packet receive and it will look through the layer 3 information but It will not change the layer 3 information because IP addresses won’t change. But it will change layer 2 information because MAC address will change every hop. Also because you might need to re-encapsulate to send it over ethernet cable,wireless or other method so therefor the **layer 2 information will change but layer 3 information will not change.**

### Send a Packet:

The mac address is always going to have the destination of the next hop in the path so the mac address will change but the destination IP address will never change.

### Forward to the Next Hop:

Routers are using an ARP table and routing table to get information to build a frame for forward packets. Because **the ARP table and routing table have informing for the next hop**.

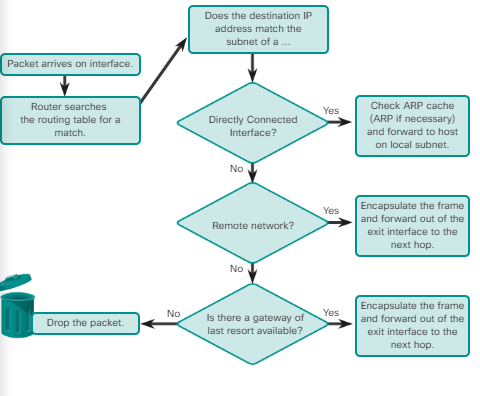
### Packet Routing:

When the paket is at the end point of the LAN and ready to sent it to the destination LAN router does not need a MAC address, it’s just need the destination IP address and when it sent to the destination ip address the router of that network will sent it to the destination MAC address.

### Reach the Destination:

When the paket destination is in the same network the router use the MAC address destination to sent it the correct destination.

### Routing Decisions:



The way of router make the decisions to send a packet to the correct destination.

### Best Path

The best path is doing to be determined by a metric ( a metric is a value used to measure the distance to a given network ) **best path to a network is the path with the lowest metric.**

Metric can be few different thing the other protocols use their own rules build metric.

The most simple one is called **Routing Information Protocol(RIP)** - hop count. It counts how many hops(routers) are there in between you and the destination network.

**Open Shortest Path First (OSPF)** - protocol that has been used between all different kind of devices. Cisco’s cost based on cumulative bandwidth from source to destination this is abit more relatable than RIP.

**Enhanced Interior Gateway Routing Protocol (EIGRP)** -  Bandwidth, delay, load, reliability calculates EIGRP metric.

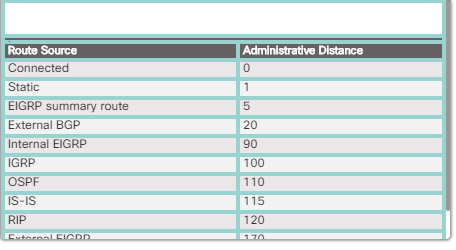
### Load Balancing

Load balancing is when there are more than one path to send data and it has the equal about of metic, the computer will send equal amount of data through both paths (half and half) and it will optimize the speed and time. **Equal cost load balance can improve network performance.**

This method will avoid overloading a network path between routers.

**Only protocol that use unequal cost load balancing is (EIGRP)**

### Administrative Distance

The trustworthy or effectiveness of a route **lower is better.**the default Administrative Distance.

### The Routing Table

There are directly connected and remote routers.

**A routing table is a file that stored in a RAM and it contains information about remote routers and directly connected routers .**

### Routing table sources

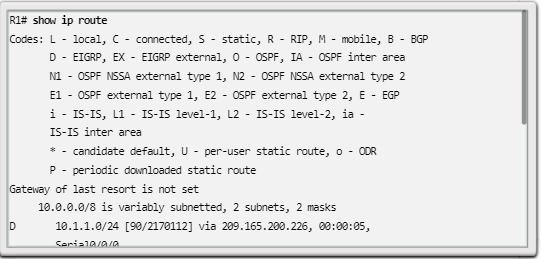
The **show ip route** command is used to display the contents of the routing table.

**Local route interfaces -** when the interface is configured it will be added to the routing table.

**Directly connected interface -**  added to the routing table when the interface is configured and active.

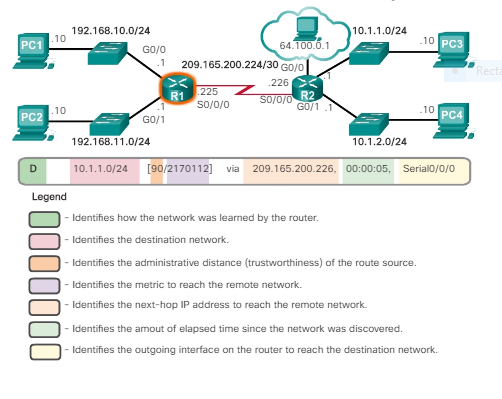
**Static routes -** added when manually configured by the user.

**Dynamic routing protocol -** automatically added based on whichever protocol is been used.



### Remote Network Routing Entries

* **Route source** - Identifies how the route was learned.
* **Destination network** - Identifies the address of the remote network.
* **Administrative distance** - Identifies the trustworthiness of the route source. Lower values indicate preferred route source.
* **Metric** - Identifies the value assigned to reach the remote network. Lower values indicate preferred routes.
* **Next-hop** - Identifies the IPv4 address of the next router to forward the packet to.
* **Route timestamp** - Identifies how much time has passed since the route was learned.
* **Outgoing interface** - Identifies the exit interface to use to forward a packet toward the final destination.

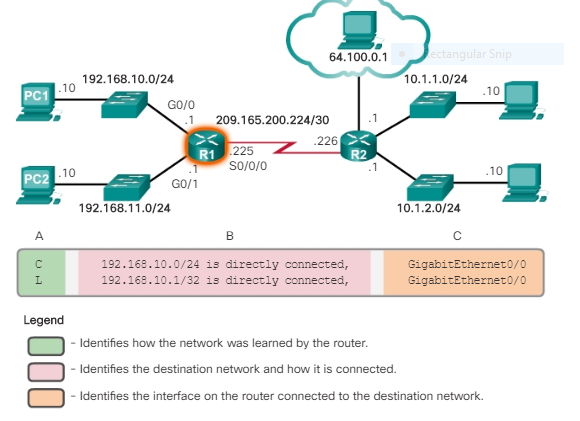


### Directly Connected Interfaces:

A newly deployed router, with no interface configured  has an empty routing table.

### Directly Connected Routing Table Entries

When the network is directly connected, directly connected interfaces have two route source codes. ‘C’ identifies a directly connected network. ’L’ identifies the IPv4 address assigned to the router’s interface.



**Destination network** - The address of the remote network.

**Outgoing interface** - Identifies the exit interface to use when forwarding packets to the destination network.

### Static Routes

Static routes are manually configured therefor the main disadvantage of using a static router is if the network topology changes the static routes should me manually re-configure unlikely dynamic routes although using static routes improved security and resource efficiency.

Static routes use less bandwidth than dynamic routing protocols, and no CPU cycles are used to calculate and communicate routes

There are two common types of static routes in the routing table:

* Static route to a specific network

A static route can be configured to reach a specific remote network. IPv4 static routes are configured using the following command:

Router(config)# **ip route** *network mask* {*next-hop-ip* | *exit-intf* }

A static route is identified in the routing table with the code ‘**S**’

* Default static route

A default static route is similar to a default gateway on a host.

The default static route specifies the exit point to use when the routing table does not contain a path for the destination network. A default static route is useful when a router has only one exit point to another router

To configure an IPv4 default static route, use the following command:

Router(config)# **ip route 0.0.0.0 0.0.0.0** { *exit-intf* | *next-hop-ip* }

### Dynamic Routing

Dynamic routers are automatically learning about the paths to different networks.Dynamic routing protocols are used by routers to share information about the reachability and status of remote networks. It performs network discovery and maintains routing tables.

**Dynamic routers has a good knowledge about all the routers around them**

If there are multiple ways to get to a network and one goes down a dynamic router can finds it way around the network automatically unlikely statistic routers.

### IPv4 Routing protocols

A router running a dynamic routing protocol does not only make a best path determination to a network, it also determines a new best path if the topology changes because the routers that use dynamic routing protocols automatically share informations with other routers

Cisco routers can support a variety of dynamic IPv4 routing protocols including:

* **EIGRP** - Enhanced Interior Gateway Routing Protocol
* **OSPF** - Open Shortest Path First
* **IS-IS** - Intermediate System-to-Intermediate System
* **RIP** - Routing Information Protocol

### IPv6 Routing Protocols

ISR devices support dynamic IPv6 routing protocols including:

* RIPng (RIP next generation)
* OSPFv3
* EIGRP for IPv6

Support for dynamic IPv6 routing protocols is dependent on hardware and IOS version.

To enable IPv6 routers to forward traffic, must configure the **ipv6 unicast-routing** global configuration command.

# Chapter 2: Static Routing

Routing is the central part of the every data in the network when sending packets, it has the fully responsible of sending and resaving packets. Routers learn about remote networks either dynamically, using routing protocols, or manually, or using static routes.

Routers use combinations of both dynamically routing protocols and static routes. **This chapter focuses on static routing**

**Reach Remote Networks**

There are two ways the router can learn about remote networks. Manually (static) and dynamically.

**Manually (Static)** - Remote networks are manually entered into the route table using static routes.

**Dynamically** - Remote routes are automatically learned using a dynamic routing protocol.

## Why Use Static Routing?

Static routing provides some advantages over dynamic routing

Advantages are:

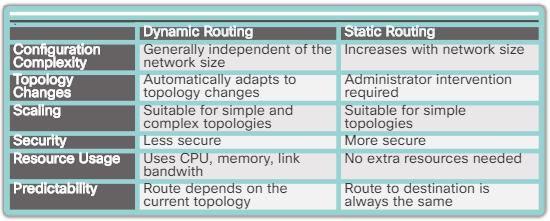
Statistic routers have a better security due to the facts the data technician has the full control of what it’s doing. The data technician chooses the path way of sending packets and Static routes are not advertised over the network.

Statistic routers use less bandwidth than dynamic routing protocols, no CPU cycles are used to calculate and communicate.

Static routing has the following disadvantages:

Initial configuration and maintains take a long time due to the fact it has to be done manually, cannot be configured to a lager network. Administration access is needed when making changes in the routing information, it’s not easy to maintain in a growing network due to the fact it doesn’t scale well in a growing network, and the administrator of the router has to learn everything about the whole network for proper implementation.

All the advantages on dynamic routing are the disadvantages on static routing.

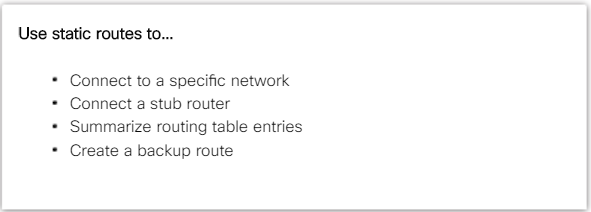


## When to Use Static Routes

Static routing has three primary uses:

* Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
* Routing to and from stub networks. A stub network is a network accessed by a single route, and the router has only one neighbor.
* Using a single default route to represent a path to any network that does not have a more specific match with another route in the routing table. Default routes are used to send traffic to any destination beyond the next upstream router.

## Static Route Applications



The static routers are commonly used for those reasons but it can also be used to:

* Reduce the number of routes advertised by summarizing several contiguous networks as one static route
* Create a backup route in case a primary route link fails

The following types of IPv4 and IPv6 static routes will be discussed:

* Standard static route
* Default static route
* Summary static route
* Floating static route

## Standard Static Route

Both IPv4 and IPv6 are support the configurations of static routers. When connecting to a specific remote network the static routers are useful.

## Default Static Route

Default routers are the router in the routing table it matches all the packets and is used by the router if a packet does not match any other. A default router can be either dynamic or static.

A default static route is simply a static route with 0.0.0.0/0 as the destination IPv4 address. Configuring a default static route creates a Gateway of Last Resort.

Default static routes are used:

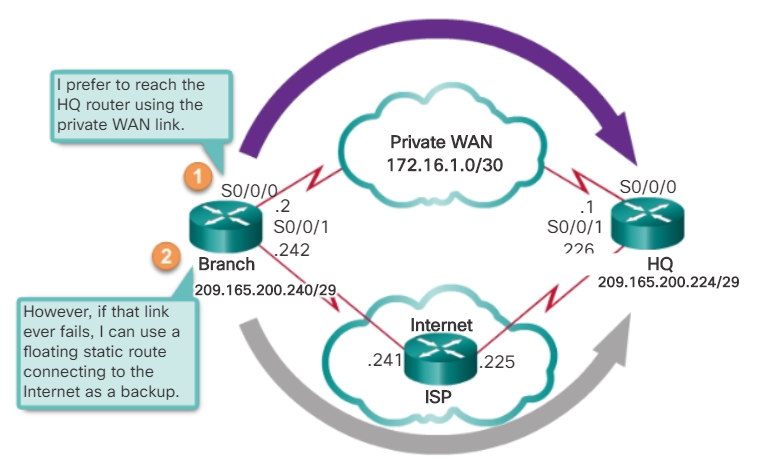
* When a more specific match does not exist in the routing table when sending a packet. A common use is when connecting a company's edge router to the ISP network
* When a router has only one other router which is connected. **the router is known as a stub router.**

## Summary Static Route

Static routers can be summarized into a single static router to reduce the number of routing table entries if the destination networks are sharing a common border and can be summarized into a single network address. And if the static routers are using the same next hop IP address.

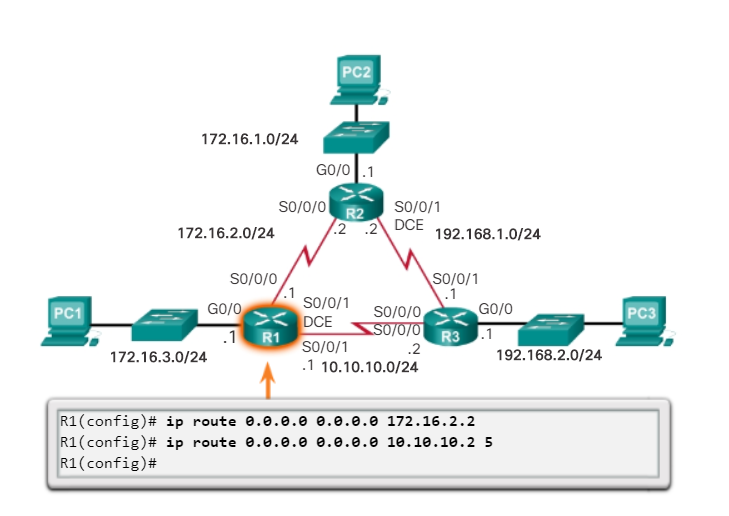
## Floating Static Route

Floating static routers are manual routers that used to provide a backup path to a primary static or dynamic route. The floating static route will be used when primary router is not available. **The floating static router has to be configured with a higher administrative distance than the primary router.** The administrative distance represents the trustworthiness of a route. If multiple paths to the destination exist, the router will choose the path with the lowest administrative distance.



## Configure an IPv4 Floating Static Route

Configure a one router to a backup router by using **“ip route” command**



## Test the IPv4 Floating Static Route

Floating static rout can be test by verifying that the routing table is using the default static rout **“show ip”**

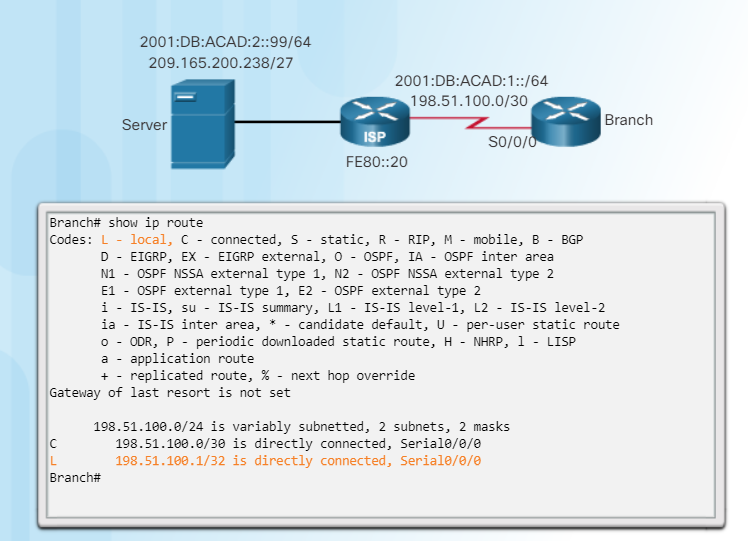
Can also can be testing by taking down the primary link pathway and see the backup pathway will kicks in

## Automatically Installed Host Routes

**A host route is an IPv4 address with a 32-bit mask or an IPv6 address with a 128-bit mask.**

This will indicate with **“L”** and it comes up when you give an IP address to the interface on your device, those are automatically be entered.

**Host routs are only for one host it is not for the network, every one of the bits will be host bits**

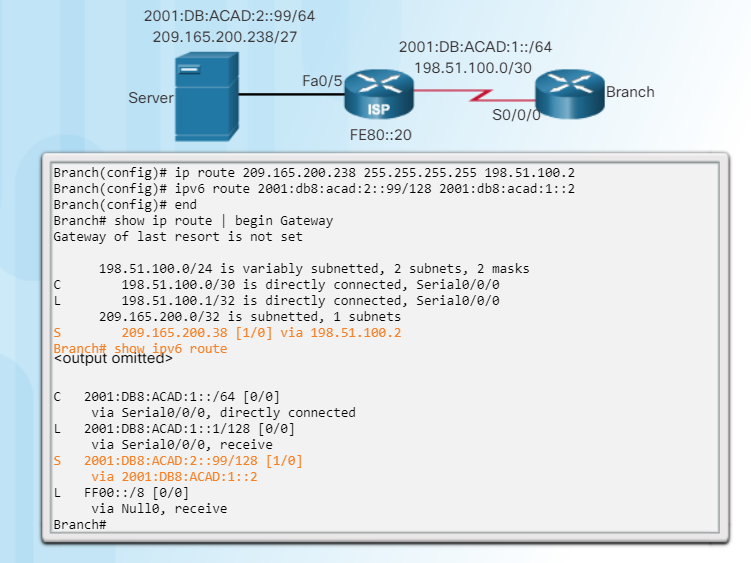


**These host addresses can be used to set up static routs.**

## Configure IPv4 and IPv6 Static Host Routes

If the branch only wants to communicate with the server, the server local can be used to make that happen.

By giving a unique network address as 255.255.255.255 to the server by doing that there will be no other room in that network so that address will only go to the its own address



It’s the same type of static entry but will just use a different sub net mask(pre fixed link)

## IP route Command

Static routes are configured using the **IP route** global configuration command

The following parameters are required to configure static routing:

* network-address - Destination network address of the remote network to be added to the routing table, often this is referred to as the prefix.
* subnet-mask - Subnet mask, or just mask, of the remote network to be added to the routing table. The subnet mask can be modified to summarize a group of networks.

One or both of the following parameters must also be used:

* IP-address - The IP address of the connecting router to use to forward the packet to the remote destination network. Commonly referred to as the next hop.
* exit-intf - The outgoing interface to use to forward the packet to the next hop.

**The distance parameter is used to create a floating static route by setting an administrative distance that is higher than a dynamically learned route.**

## Next-Hop Options

Each router has entry for only direct connection to the network and their associate local addresses. None of the routers have any knowledge about the outside networks (network beyond their directly connected interfaces.

The next hop can be identify in two ways it’s either IP address exit interface, or how the destination is specified creates according to one of the three following router types.

* Next-hop route - Only the next-hop IP address is specified
* Directly connected static route - Only the router exit interface is specified
* Fully specified static route - The next-hop IP address and exit interface are specified

## Configure a Next-Hop Static Route

In the next hop static router, only the next-hop address is specified. The exit interface is obtained from the next hop. Multiple next-hop static routers can be configured by using IP address of the next-hop.

Before any packet is forwarded by a router, the routing table process must determine the exit interface to use to forward the packet. This is known as route resolvability.

Every route that references only a next-hop IPv4 address and does not reference an exit interface must have the next-hop IPv4 address resolved using another route in the routing table with an exit interface.

It actually takes two routing table lookup processes to forward any packet to the 192.168.2.0/24 network. When the router performs multiple lookups in the routing table before forwarding a packet, it is performing a process known as a recursive lookup. Because recursive lookups consume router resources, they should be avoided when possible.

## Configure a Directly Connected Static Route

When configuring a static route, another option is to use the exit interface to specify the next-hop address. When all directly connect static routers are configured by using the exit interface the next hop can send receiving packets by look for the match in the routing table and it will sent to the it’s serial port interface. Other look ups are not needed.

Configuring a directly connected static route with an exit interface allows the routing table to resolve the exit interface in a single search, instead of two searches. Although the routing table entry indicates “directly connected”, the administrative distance of the static route is still

**Only a directly connected interface can have an administrative distance of 0**

For point-to-point interfaces, you can use static routes that point to the exit interface or to the next-hop address. For broadcast interfaces, it is more suitable to use static routes that point to a next-hop address.

## Configure a Fully Specified Static Route

Fully specified static route:

Both next-hop IP address and the exit interface are specified in a fully specified static route. **This is another type of static route** that is used in older IOSs, prior to CEF

This form of static routers are used when there are multiple access interface and it is important that there are not confusion when identify the next hop. The next-hop must be directly connected to the specified exit interface.

Suppose that the network link between R1 and R2 is an Ethernet link and that the GigabitEthernet 0/1 interface of R1 is connected to that network. CEF will not enabled. To eliminate the recursive lookup, a directly connected static route can be implemented using the following command:

R1 (config)#**ip route 192.168.2.0 255.255.255.0 GigabitEthernet 0/1**

However, this may cause unexpected or inconsistent results. The difference between an Ethernet multi-access network and a point-to-point serial network is that a point-to-point serial network has only one other device on that network, the router at the other end of the link. With Ethernet networks, there may be many different devices sharing the same multi-access network, including hosts and even multiple routers. By only designating the Ethernet exit interface in the static route, the router will not have sufficient information to determine which device is the next-hop device.

## Verify a Static Route

Along with **ping** and **traceroute**, useful commands to verify static routes include:

* show ip route
* show ip route static
* show ip route network

## Default Static Route

Default routers are usually learn from other routers using dynamic protocol. It does not require any left-most bits to match between the default route and the destination IPv4 address of the packet. If there are no specific match the default router will be used as the Gateway of the Last Resort.

Default static routes are commonly used when connecting:

* An edge router to a service provider network
* A stub router (a router with only one upstream neighbor router)

## Troubleshoot a Missing Route

Common IOS troubleshooting commands include:

* ping
* traceroute
* show ip route
* show ip interface brief
* show cdp neighbors detail

# Chapter 3: Dynamic Routing

**Dynamic Routing Protocol Evolution**

Dynamic routing protocols have be evolving since 1980s, RIPv1 was one of the first routing protocols in the world it was released on 1988 but it can be only used for simple technology when years passed by the technology evolved itself therefor other companies came up with more advance protocol types so the routing protocols can be up to date with the evolving technology .

After few years the RIPv2 was released but still is could not scale to a large network, so two other routing protocols were developed which are **Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) Cisco developed the Interior Gateway Routing Protocol (IGRP) and Enhanced IGRP (EIGRP), which also scales well in larger network implementations.**

## Dynamic Routing Protocol Components

Routing protocols is a communication system for routers so they can communicate with each router and lean about routing information

The purpose of dynamic routing protocols includes:

* Discovery of remote networks
* Maintaining up-to-date routing information
* Choosing the best path to destination networks
* Ability to find a new best path if the current path is no longer available

The main components of dynamic routing protocols include:

* Data structures - Routing protocols are keeping all the data they collect in the RAM
* Routing protocol messages – routers use unique method to communicate with other routers, routers collect accurate information about the network.
* Algorithm – routers use a specific algorithm to make things perfect(steps of rules )

**Dynamic routing protocols are making finding the best pathway to the network automatically by communicating with other routers**

## Static Routing Uses

There are benefits of using dynamic routing protocols but some network professionals sometimes use static routing protocols because there are some advantages of using static routers, and there are also disadvantages of using static routers as well.

When using a static router it’s a human brain than sit behind everything and controlling everything manually but when using a dynamic router it’s a computerized brain that works behind the everything. Using a dynamic router can be accurate sometimes but when the router has to think logically and the static routers are smarter than dynamic.

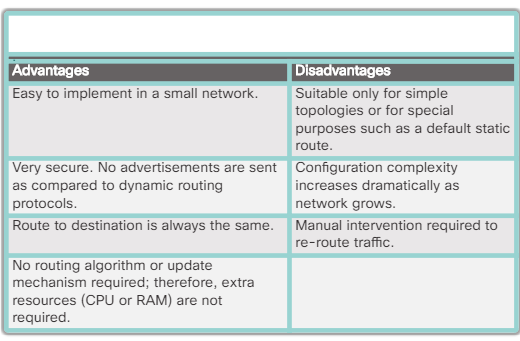
However when technicians use static routing protocol they are making sure that it won’t grow to a lager network.

Static routing has several primary uses, including:

* Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
* Routing to and from a stub network, which is a network with only one default route out and no knowledge of any remote networks.
* Accessing a single default route (which is used to represent a path to any network that does not have a more specific match with another route in the routing table).

## Static Routing Advantages and Disadvantages

Static routers are easy to implement in a small network and its configurations won’t change automatic therefor it’s easy to trouble shoot.

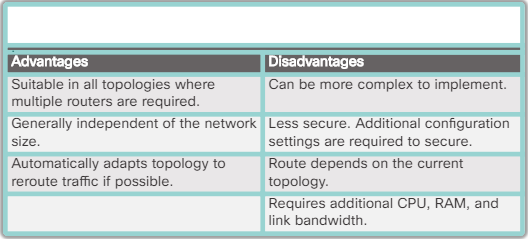


## Dynamic Routing Protocols Uses

Dynamic routing protocols helps the network administrator to maintain the network; therefore the large networks use dynamic routing protocols because if there are like 100+ routers and the link went down it won’t be easy to troubleshoot. Dynamic routing protocols can automatically fix problems like that.

## Dynamic Routing Advantages and Disadvantages

Dynamic routing protocols works well in all kinds of network if there are more than one router, dynamic routers are stable and can automatically determine better routers if the topology changers.



## Advertise Networks

By entering the RIP router configuration mood the will be able to run RIPv1 but the router still needs a logical interface to communicate with other routers and as well connected to a logical network.

To enable RIP routing for a network, **“network** *network-address****”*** *router*configuration *mode command**can* be used.

 Enter the classful network address for each directly connected network. This command:

* Enables RIP on all interfaces that belong to a specific network. Associated interfaces now both send and receive RIP updates.
* Advertises the specified network in RIP routing updates sent to other routers every 30 seconds.

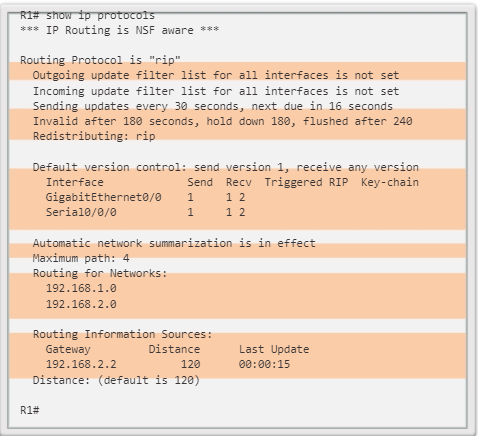
**Note**: RIPv1 is a classful routing protocol for IPv4. Therefore, if a subnet address is entered, the IOS automatically converts it to the classful network address. For example, entering the**network 192.168.1.32**command would automatically be converted to**network 192.168.1.0**in the running configuration file. The IOS does not give an error message, but instead corrects the input and enters the classful network address.

## Verify RIP Routing

The **“show ip protocols”** command displays the IPv4 routing protocol settings that are configured at the moment

“show ip protocols” command shows :

* Which routing protocol is running.
* The values of various timers.
* The version of the running protocol.
* Summary at the classful network boundary
* The classful networks are advertised. These are the networks that includes in its RIP updates.
* The list of RIP neighbors .



## Enabling and verify RIPv2

Now days the RIPv1 is not being used as much, it’s an old version. Version one is a classsful routing protocol it does not use it does not use sider notation and subnet mask. RIPv2 can be activated be using the command “**version 2**” RIPv1 will send classful routing updates but can receive v1 or v2 updates but v2 can only receive v2 routing updates

## Disable Auto Summarization

RIPv2 automatically summarizes networks at major network boundaries by default, just like RIPv1.

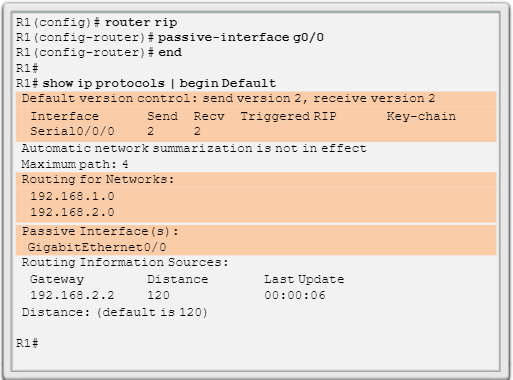
To modify the default RIPv2 behavior of automatic summarization, use the no auto-summary router configuration mode command.

When there are overlapping networks the no auto-summary router command can be used because summary blog can be too big and cost problems on the routing process. That’s why turn off the automatic summary.

## Configure Passive Interfaces

It means that you don’t want to share routing updates through some interface. Because more use share the more bandwidth (wasting bandwidth) you use so if there are no need to share routing update then better not to send it.

The process of blocking sharing routing updates can be done by using the commands shown in the figure down below.

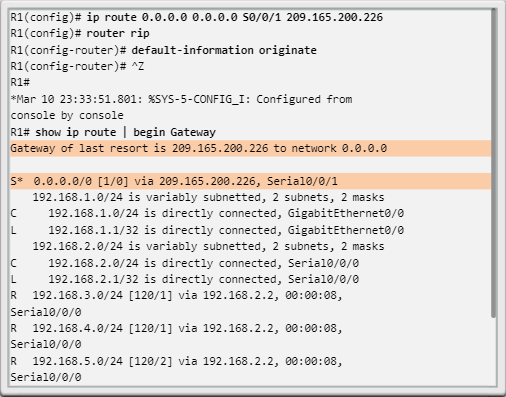


## Propagate a Default Route

If you want to share a default rout with other devices of the network, basically send all the traffic that doesn’t match any data in the routing table, so the default route will make a default dissection with the data.

When you make a one default rout it can be used by all the devices in the network.

To set up default rout these commands can be used.



To propagate a default route in RIP, the edge router must be configured with:

A default static route using the ip route 0.0.0.0 0.0.0.0 command.

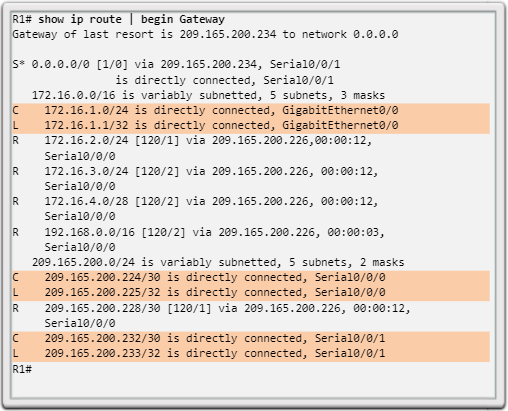
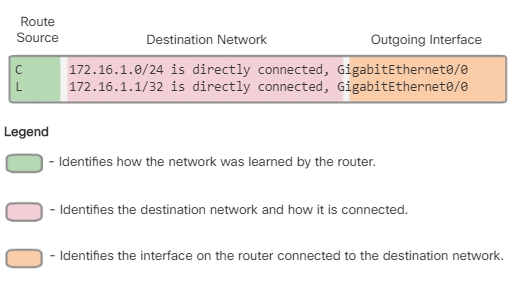
The default-information originate router configuration command. This instructs R1 to originate default information, by propagating the static default route in RIP updates.

## Routing Table Entries

The edge router which is directly connected to the internet propagating a default static route and then share it with the other routers in the network.

## Directly Connected Entries

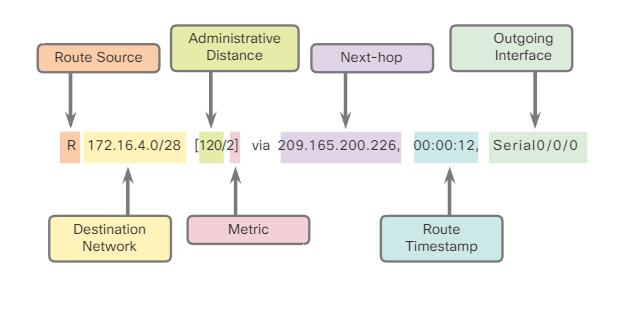
As highlighted in Figure, the routing table of R1 contains three directly connected networks. Notice that two routing table entries are automatically created when an active router interface is configured with an IP address and subnet mask.



## Remote Network Entries

The entry identifies the following information:

* **Route source** - Identifies how the route was learned.
* **Destination network** - Identifies the address of the remote network.
* **Administrative distance (AD)** - Identifies the trustworthiness of the route source. The AD for static routes is 1 and the AD for connected routes is 0. Dynamic routing protocols have an AD higher than 1 depending upon the protocol.
* **Metric** - Identifies the value assigned to reach the remote network. Lower values indicate preferred routes. The metric for static and connected routes is 0.
* **Next hop** - Identifies the IPv4 address of the next router to forward the packet to.
* **Route timestamp** - Identifies from when the route was last heard.
* **Outgoing interface** - Identifies the exit interface to use to forward a packet toward the final destination.



**This is an IPv4 rioting table entry on R1 route to remote network 172.16.4.0 on R3**

## Routing Table Terms

Routes are discussed in terms of:

* Ultimate route – has a way off the device, whether a next-hop or interface to exit
* Level 1 route -
* Level 1 parent route – not an untimed route (all the thing that are left a line before)
* Level 2 child routes - (all the thing that are left a line after)

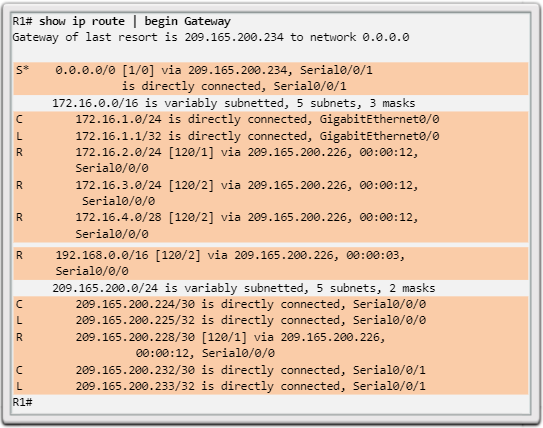
Everything but a parent route is a ultimate route.

Level 2 child routes are sub netted from the parent routes level 1 route, parent route always have child routs if there are no child routs underneath then there are no parent routs it can just be a level 1 route (ultimate route)



## Ultimate Route

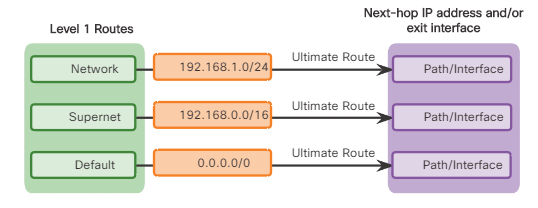
An ultimate route is a routing table entry that contains either a next-hop IPv4 address or an exit interface. Directly connected, dynamically learned, and local routes are ultimate routes.



## Level 1 Route

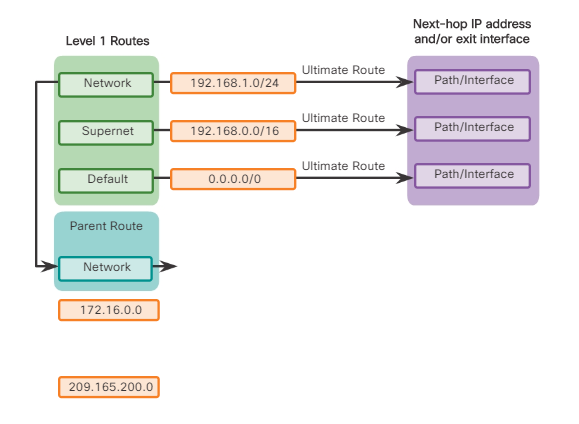
level 1 route can be a:

* **Network route** - A network route that has a subnet mask equal to that of the classful mask.
* **Supernet route** - A supernet route is a network address with a mask less than the classful mask, for example, a summary address.
* **Default route** - A default route is a static route with the address 0.0.0.0/0.



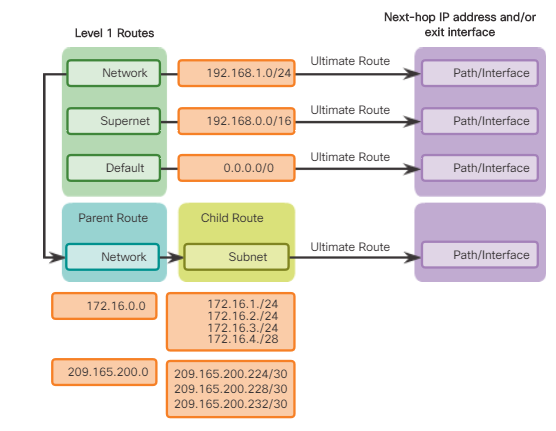
## Level 1 Parent Route

A parent route can never be an ultimate route.



## Level 2 Child Route

A level 2 child route is a route that is a subnet of a classful network address and Level 1 parent routes contain level 2 child routes. Like a level 1 route, the source of a level 2 route can be a directly connected network, a static route, or a dynamically learned route. Level 2 child routes are also ultimate routes.



## Router look up process

Router is going to best match as a level one ultimate router.

If the best match is a level 1 parent route, proceed to the next step.

The router examines child routes (the subnet routes) of the parent route for a best match.

If there is a best math with a level 2 child rout, that subnet is used to forward the packet.

If there is not a match with any of the level 2 child routes, proceed to the next step.

Router will continue to find a match on level 1 supernet routes

## Best routs == longest match

Longest distance available route will be admin distance

## IPv6 routing table entries

Everything in the IPv6 routing table is ultimate route.

# Chapter 4: switched networks

## Growing complexity of networks

Everything is connected.

Can be gain access to the information from anywhere in the world, network is no longer a physical office.

## Elements of a converged Network

All kind of the data being sent along the same networking type. Different protocols will keep the data separate

* Call control - Telephone call processing, caller ID, call transfer, hold, and conference
* Voice messaging - Voicemail
* Mobility - Receive important calls wherever you are
* Automated attendant - Serve customers faster by routing calls directly to the right department or individual

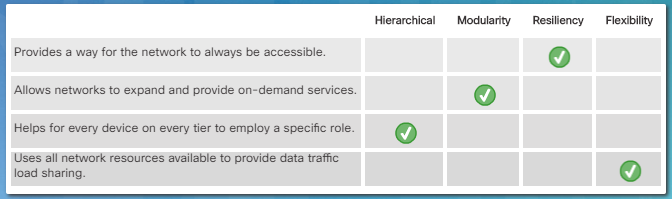
## Cisco Borderless Networks

There are no borders in the network there are different portals from everywhere network policy can control set up the network privet but other than that the network is open for everyone

## Hierarchy in the Borderless Switched Network

There are access layers to make the network accurate. Creating a borderless switched network requires that sound network design principles are used to ensure maximum availability, flexibility, security, and manageability. **(High-speed routers “layer 3 switchers”) it can function routing functions.**

* Hierarchical - Facilitates understanding the role of each device at every tier, simplifies deployment, operation, and management, and reduces fault domains at every tier
* Modularity - Allows seamless network expansion and integrated service enablement on an on-demand basis
* Resiliency - Satisfies user expectations for keeping the network always on
* Flexibility - Allows intelligent traffic load sharing by using all network resources



## Access, Distribution, and Core Layers

**Access Layer**

The access layer represents the network edge, where traffic enters or exits the campus network.

**Distribution Layer**

The distribution layer interfaces between the access layer and the core layer to provide many important functions, including:

* Aggregating large-scale wiring closet networks
* Aggregating Layer 2 broadcast domains and Layer 3 routing boundaries
* Providing intelligent switching, routing, and network access policy functions to access the rest of the network
* Providing high availability through redundant distribution layer switches to the end-user and equal cost paths to the core
* Providing differentiated services to various classes of service applications at the edge of the network

Core Layer

The core layer is the network backbone. It connects several layers of the company network and hold then tight together.

## Role of Switched Networks

They make sure the traffic will be sent only to the destination device.

A switched LAN allows more flexibility, traffic management, and additional features:

* Quality of service
* Additional security
* Support for wireless networking and connectivity
* Support for new technologies, such as IP telephony and mobility services

## Form Factors

There are few different kind of switchers:

**Fixed configuration switches**: normal switch.. Fixed configuration switches do not support features or options beyond those that originally came with the switch

**Modular configuration switches:** can add more port and is expensive but also add more flexibility

**Stackable Configuration Switches**: can act like one switch Stackable configuration switches can be interconnected using a special cable that provides high-bandwidth throughput between the switches. A modular switch with a single 24-port line card could have an additional 24-port line card installed to bring the total number of ports up to 48.

Switches can be stacked one on top of the other with cables connecting the switches in a daisy chain fashion. Makes dissections faster than other switch

## Switching as a General Concept in Networking and Telecommunications

Switchers are making dissections when frame forwarding by learning about MAC addresses through ingress and a destination port.

## Dynamically Populating a Switch MAC Address Table

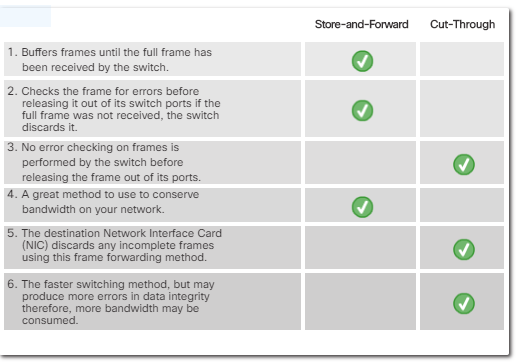
Switches use MAC addresses to direct network communications through the switch, to the appropriate port, toward the destination.

## Switch Forwarding Methods

There are two methods to forward data

Store and forward methods: A switch using store-and-forward switching performs an error check on an incoming frame. After receiving the entire frame on the ingress port, as shown in the figure, the switch compares the frame-check-sequence (FCS) value in the last field of the datagram against its own FCS calculations. And there are automatic buffering. This is a bit slow.

Cut through: An advantage to cut-through switching is the ability of the switch to start forwarding a frame earlier than store-and-forward switching. Fragment free switching is a modified form of cut-through switching in which the switch waits for the collision window (64 bytes) to pass before forwarding the frame.



## Collision Domains

Each port on a switch is a collision domain **collision domain is when a segment or device is compete to communicate.**

This problem does not matter if the router is configured to full duplex

## Broadcast Domains

Each network is there broadcast domain.

## Alleviating Network Congestion

LAN switches have special characteristics that make them effective at alleviating network congestion. By default, interconnected switch ports attempt to establish a link in full duplex, therefore eliminating collision domains.

The following are some important characteristics of switches that contribute to alleviating network congestion:

* High port density - Switches have high-port densities: 24- and 48-port switches are often just a single rack unit and operate at speeds of 100 Mb/s, 1 Gb/s, and 10 Gb/s. Large enterprise switches may support many hundreds of ports.
* Large frame buffers - The ability to store more received frames before having to start dropping them is useful, particularly when there may be congested ports to servers or other parts of the network.
* Port speed - Depending on the cost of a switch, it may be possible to support a mixture of speeds. Ports of 100 Mb/s, and 1 or 10 Gb/s are common (100 Gb/s is also possible).
* Fast internal switching - Having fast internal forwarding capabilities allows high performance. The method that is used may be a fast internal bus or shared memory, which affects the overall performance of the switch.
* Low per-port cost - Switches provide high-port density at a lower cost.

# Chapter 5: Switch Configuration

Switch Boot Sequence

After a Cisco switch is powered on, it goes through the following boot sequence:

First the cisco switch will run a test and run all the configurations that is stored in the ROM, **Next** the switch will boot load the software (it’s a small program that stored in ROM) the boot loader initializes the flash file system in the system board.

Finally, the boot loader locates and loads a default IOS operating system software image into memory and gives control of the switch over to the IOS.

## Recovering From a System Crash

The boot loader provides access into the switch if the operating system cannot be used because of missing or damaged system files.

The boot loader can be accessed through a console connection following these steps:

* Step 1. Connect a PC by console cable to the switch console port. Configure terminal emulation software to connect to the switch.
* Step 2. Unplug the switch power cord.
* Step 3. Reconnect the power cord to the switch and, within 15 seconds, press and hold down the Mode button while the System LED is still flashing green.
* Step 4. Continue pressing the Mode button until the System LED turns briefly amber and then solid green; then release the Mode button.
* Step 5. The boot loader switch: prompt appears in the terminal emulation software on the PC.

## Switch LED Indicators

Cisco Catalyst switches have several status LED indicator lights. Switch lights can be used to monitor switch activity and performance.

**System LED**- Shows whether the system is receiving power and is functioning properly

**Redundant Power System (RPS) LED**- Shows the RPS status

**Port Status LED**- Indicates that the port status mode is selected when the LED is green.

**Port Duplex LED**- Indicates the port duplex mode is selected when the LED is green

**Port Speed LED**- Indicates the port speed mode is selected.

**Power over Ethernet (PoE) Mode LED**- If PoE is supported; a PoE mode LED will be present.

## Preparing for Basic Switch Management

Switchers are configured by a remote devices fx. A router or a host computer. The switch must be configured with an ip address and a subnet mask

**Switchers have an interface VLAN**

## Configuring Basic Switch Management Access with IPv4

**Step 1. Configure Management Interface**

An ip address and a subnet mask has to be configured to the interface VLAN first and then use the “no shut “ command to enable the interface. **The SVI for VLAN 99 will not appear as "up/up" until VLAN 99 is created and there is a device connected to a switch port associated with VLAN**

S1(config)# **vlan***vlan\_id*

S1(config-vlan)# **name***vlan\_name*

S1(config-vlan)# **exit**

S1(config)# **interface***interface\_id*

S1(config-if)# **switchport access vlan***vlan\_id*

**Step 2. Configure Default Gateway**

R1 is the default gateway for S1

To configure the default gateway for the switch, use the**ip default-gateway**command.

Enter the IPv4 address of the default gateway.

 Use the**copy running-config startup-config**command to back up your configuration.

**Step 3. Verify Configuration**

The**show ip interface brief**command is useful when determining the status of both physical and virtual interfaces

## Duplex Communication

Full-duplex communication improves the performance of a switched LAN and it increases effective bandwidth by allowing both ends of a connection to transmit and receive data simultaneously. **This is also known as bidirectional communication.**

Unlike full-duplex communication, half-duplex communication is unidirectional. Sending and receiving data does not occur at the same time. Half-duplex communication creates performance issues because data can flow in only one direction at a time,

**Gigabit Ethernet and 10Gb NICs require full-duplex connections to operate.**

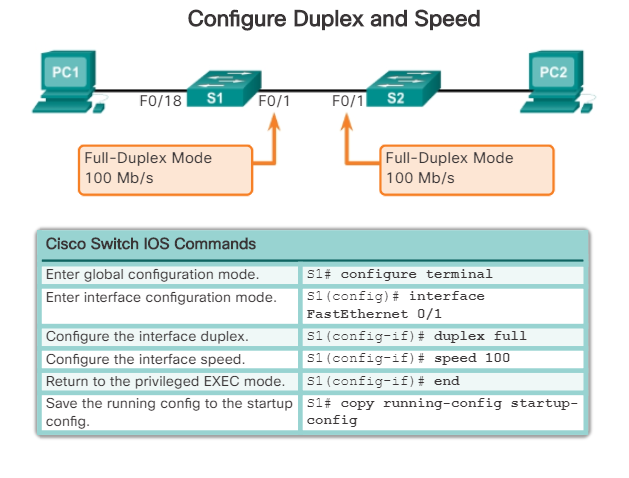
## Configure Switch Ports at the Physical Layer

**Duplex and Speed**

Switch ports can be manually configured with specific duplex and speed settings.

Use the**duplex**interface configuration mode command to manually specify the duplex mode for a switch port

Use the **speed** interface configuration mode command to manually specify the speed for a switch port



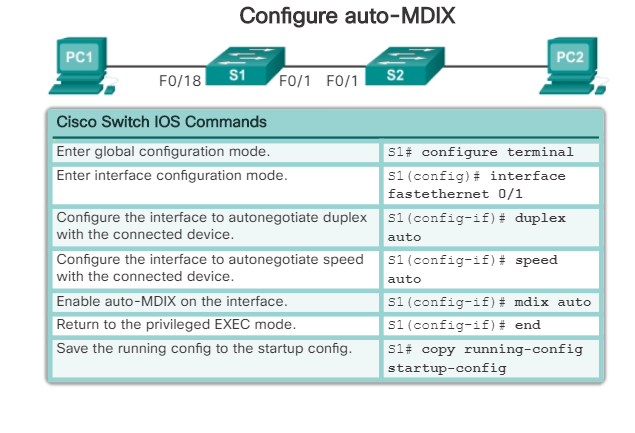
## Auto-MDIX

Until recently, certain cable types (straight-through or crossover) were required when connecting devices.

When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately.

When connecting to switches without the auto-MDIX feature, straight-through cables must be used to connect to devices such as servers, workstations, or routers.

To examine the auto-MDIX setting for a specific interface, use the**show controllers ethernet-controller**command with the**phy**keyword. To limit the output to lines referencing auto-MDIX, use the**include Auto-MDIX**filter.

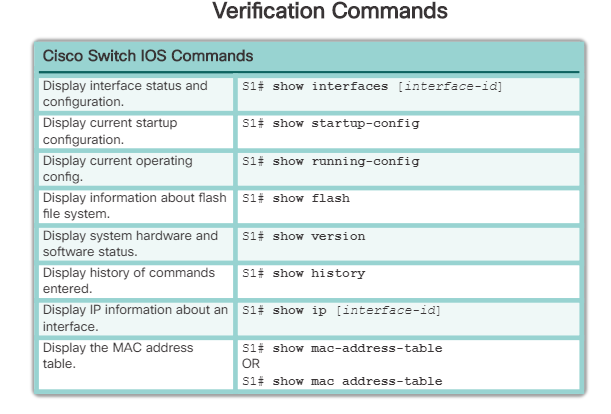


## Verifying Switch Port Configuration

**show**command is helpful in verifying common configurable switch features.

Use **show running-config** to verify that the switch has been correctly configured.

Other commands:

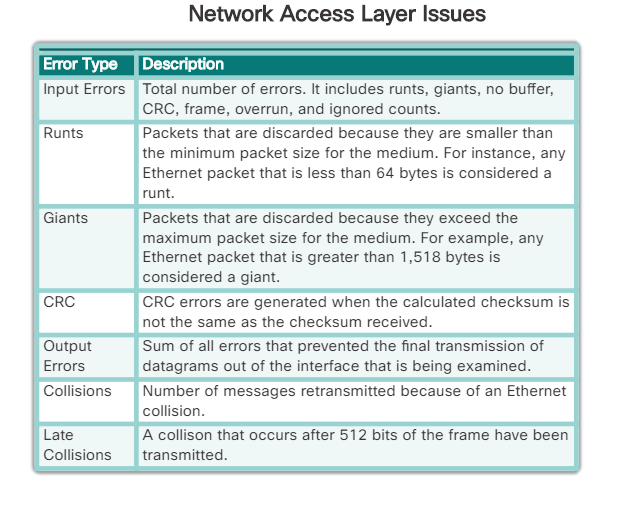


## Network Access Layer Issues

The output from the**show interfaces**command can be used to detect common media issues.

Based on the output of the**show interfaces**command, possible problems can be fixed as follows:

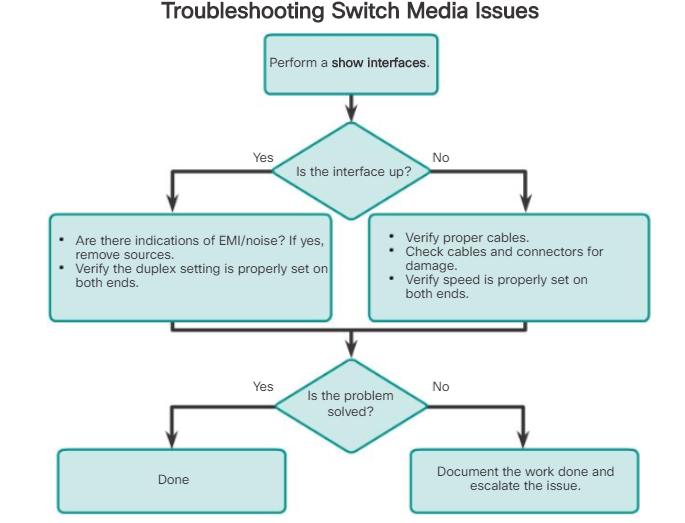
* If the interface is up and the line protocol is down, a problem exists. There could be an encapsulation type mismatch, the interface on the other end could be error-disabled, or there could be a hardware problem.
* If the line protocol and the interface are both down, a cable is not attached or some other interface problem exists. For example, in a back-to-back connection, the other end of the connection may be administratively down.
* If the interface is administratively down, it has been manually disabled (the**shutdown**command has been issued) in the active configuration.



**show interfaces**command include the following: “Input errors

* **Runt Frames** - Ethernet frames that are shorter than the 64-byte minimum allowed length are called runts. Malfunctioning NICs are the usual cause of excessive runt frames, but they can also be caused by collisions.
* **Giants** - Ethernet frames that are larger than the maximum allowed size are called giants.
* **CRC errors** - On Ethernet and serial interfaces, CRC errors usually indicate a media or cable error. Common causes include electrical interference, loose or damaged connections, or incorrect cabling. If you see many CRC errors, there is too much noise on the link and you should inspect the cable. You should also search for and eliminate noise sources.

## Troubleshooting Network Access Layer Issues



## SSH Operation

Secure Shell (SSH) is a protocol that provides a secure (encrypted) management connection to a remote device.

SSH provides security for remote connections by providing strong encryption when a device is authenticated (username and password) and also for the transmitted data between the communicating devices. SSH is assigned to TCP port 22. Telnet is assigned to TCP port 23.

To enable SSH on a Catalyst 2960 switch, the switch must be using a version of the IOS software including cryptographic (encrypted) features and capabilities. **“show version**command”

## Configuring SSH

Before configuring SSH, the switch must be minimally configured with a unique hostname and the correct network connectivity settings.

**Step 1. Verify SSH support.**

Use the**show ip ssh**command to verify that the switch supports SSH.

**Step 2. Configure the IP domain.**

Configure the IP domain name of the network using the**ip domain-name***domain-name*global configuration mode command.

**Step 3. Generate RSA key pairs.**

Not all versions of the IOS default to SSH version 2, and SSH version 1 has known security flaws. To configure SSH version 2, issue the**ip ssh version 2**global configuration mode command. Generating an RSA key pair automatically enables SSH. Use the**crypto key generate rsa**global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. When generating RSA keys, the administrator is prompted to enter a modulus length.

**Note: To delete the RSA key pair, use the crypto key zeroize rsa global configuration mode command. After the RSA key pair is deleted, the SSH server is automatically disabled.**

**Step 4. Configure user authentication.**

The SSH server can authenticate users locally or using an authentication server. To use the local authentication method, create a username and password pair using the**username***username***secret***password*global configuration mode command. In the example, the user**admin**is assigned the password**ccna**.

**Step 5. Configure the vty lines.**

Enable the SSH protocol on the vty lines using the**transport input ssh**line configuration mode command.

Use the**line vty**global configuration mode command and then the**login local**line configuration mode command to require local authentication for SSH connections from the local username database.

**Step 6. Enable SSH version 2.**

By default, SSH supports both versions 1 and 2. When supporting both versions, this is shown in the**show ip ssh**output as supporting version 1.99. Version 1 has known vulnerabilities. For this reason, it is recommended to enable only version 2. Enable SSH version using the**ip ssh version 2**global configuration command.

## Verifying SSH

On a PC, an SSH client such as PuTTY, is used to connect to an SSH server.

* SSH enabled on switch S1
* Interface VLAN 99 (SVI) with IPv4 address 172.17.99.11 on switch S1
* PC1 with IPv4 address 172.17.99.21

## Secure Unused Ports

**Disable Unused Ports**

A simple method that many administrators use to help secure the network from unauthorized access is to disable all unused ports on a switch

Navigate to each unused port and issue the Cisco IOS**shutdown**command. If, later on, a port must be reactivated, it can be enabled with the**no shutdown**command.

It is simple to make configuration changes to multiple ports on a switch. If a range of ports must be configured, use the**interface range**command.

## Port Security: Operation

**Port Security**

All switch ports (interfaces) should be secured before the switch is deployed for production use.





## Port Security: Violation Modes

An interface can be configured for one of three violation modes, specifying the action to be taken if a violation occurs.

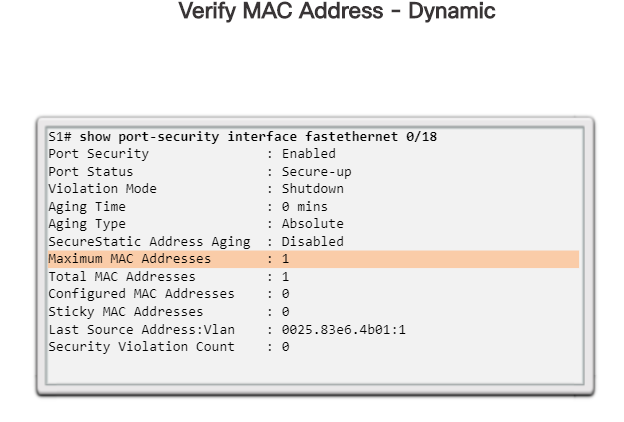
* **Protect**- When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. There is no notification that a security violation has occurred.
* **Restrict**- When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. In this mode, there is a notification that a security violation has occurred.
* **Shutdown**- In this (default) mode, a port security violation causes the interface to immediately become error-disabled and turns off the port LED. It increments the violation counter. When a secure port is in the error-disabled state, it can be brought out of this state by entering the**shutdown**interface configuration mode command followed by the**no shutdown**command.

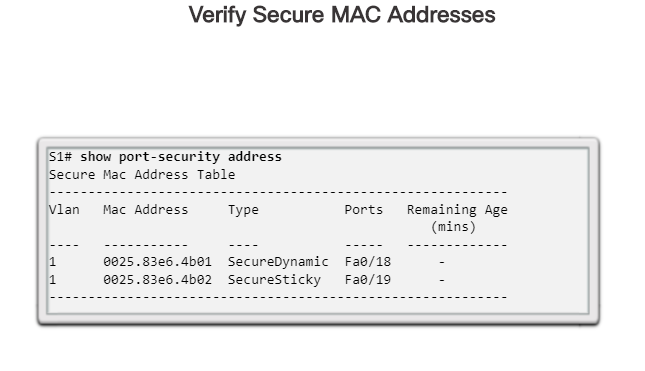
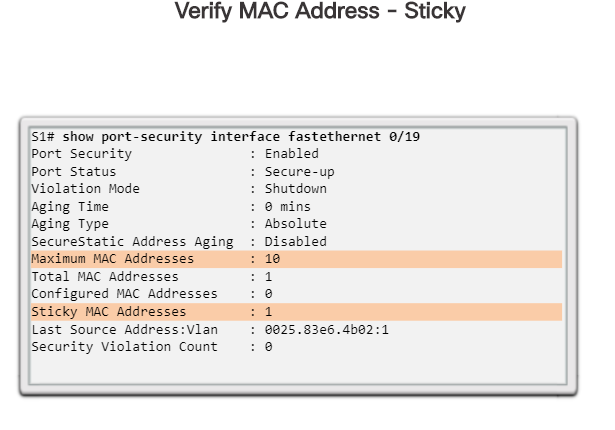
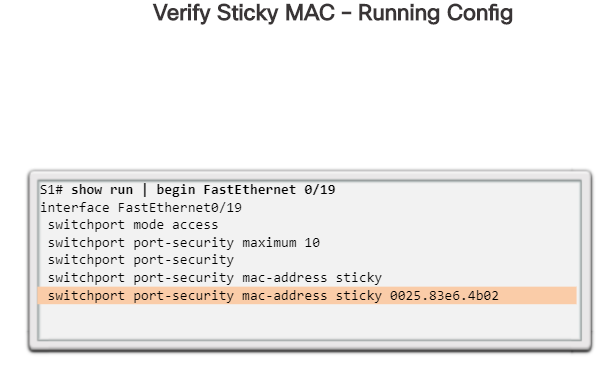
To change the violation mode on a switch port, use the**switchport port-security violation**{**protect**|**restrict**|**shutdown**} interface configuration mode command.

## Port Security: Verifying

After configuring port security on a switch, check each interface to verify that the port security is set correctly, and check to ensure that the static MAC addresses have been configured correctly.

**Note**: The MAC address is identified as a sticky MAC.





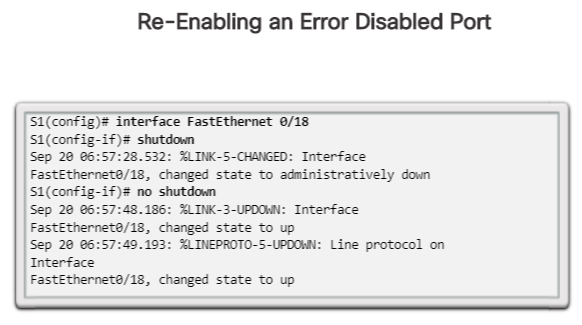
## Ports in Error Disabled State

When a port is configured with port security, a violation can cause the port to become error disabled.

When a port is error disabled, it is effectively shut down and no traffic is sent or received on that port. A series of port security related messages display on the console

The administrator should determine what caused the security violation before re-enabling the port. If an unauthorized device is connected to a secure port, the port should not be re-enabled until the security threat is eliminated.

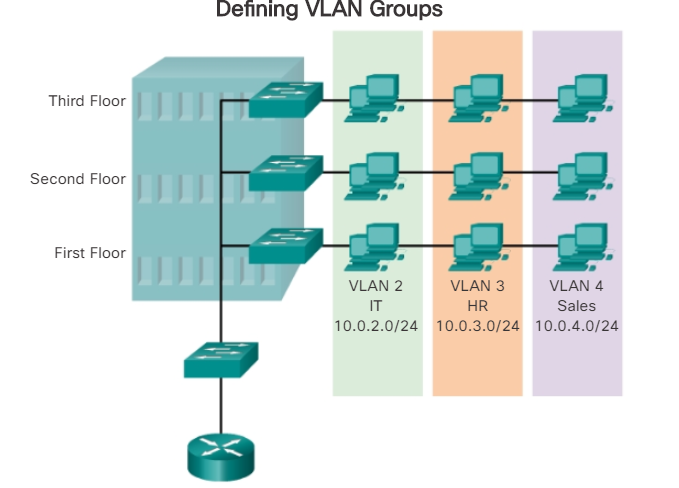
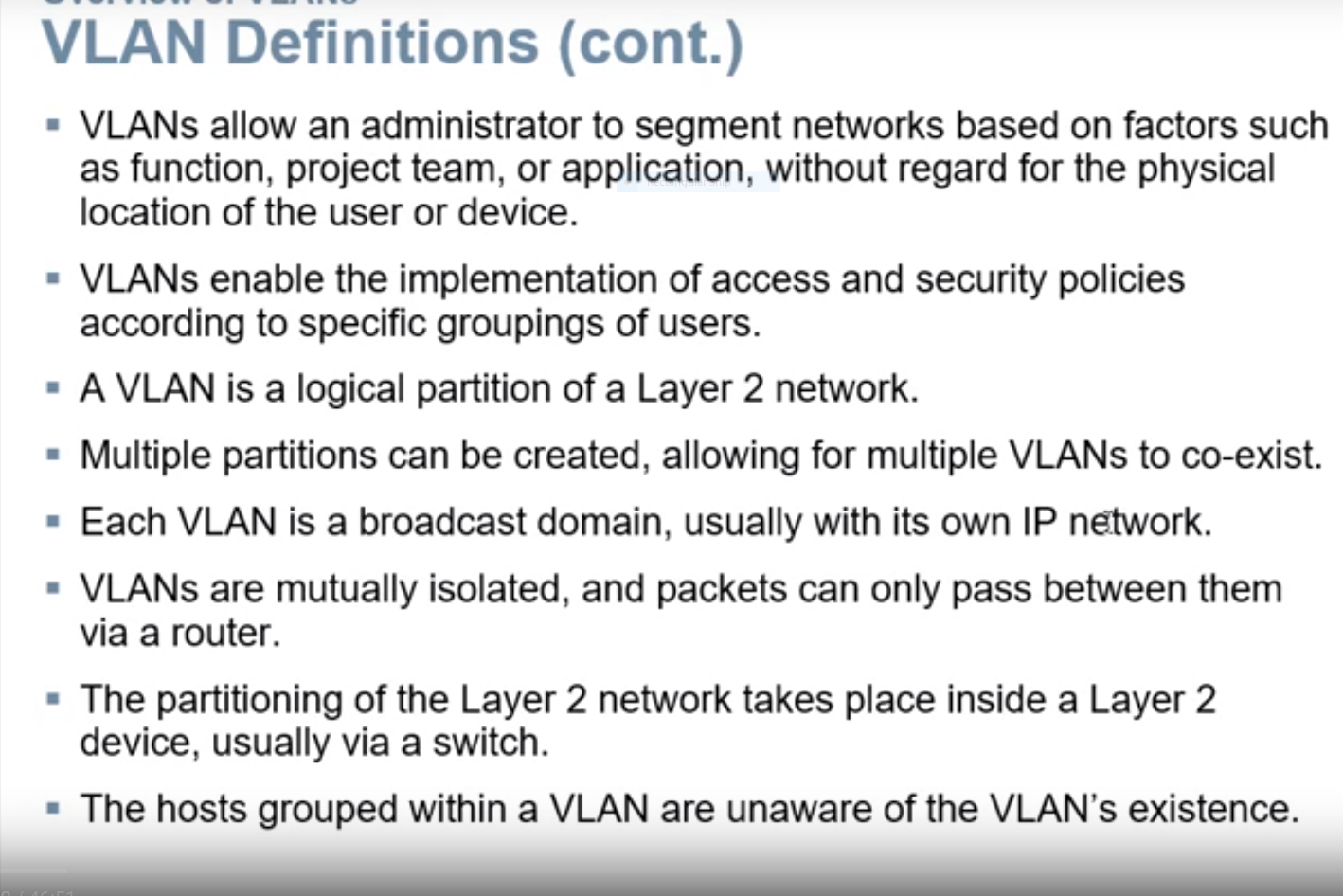
To re-enable the port, use the**shutdown**interface configuration mode command. Then, use the**no shutdown**interface configuration command to make the port operational.



# Chapter 6: VLANs

**VLAN Definitions**

Having more broadcast domain will slow the network down so odder to solve it we can create VLAN.



## Benefits of VLANs

* Improve security
* Reduce cost
* Better performance
* Smaller broadcast domains
* IT efficiency
* Management Efficiency
* Simpler project and application management

## Types of VLANs

**Data VLAN-** user generated traffic

**Default VLAN**- all switch ports become part of this VLAN until switch is configured, **show vlan brief**

**Native VLAN**- used for untagged traffic

**Management VLAN**-used to access management capabilities

## Voice VLANs

A separate VLAN is needed to support Voice over IP (VoIP). VoIP traffic requires:

* Assured bandwidth to ensure voice quality
* Transmission priority over other types of network traffic
* Ability to be routed around congested areas on the network
* Delay of less than 150 ms across the network

IT’S OWN VLAN

## VLAN Trunks

A trunk is a point-to-point link between two network devices that carries more than one VLAN. A VLAN trunk extends VLANs across an entire network.

VLANs would not be very useful without VLAN trunks

A VLAN trunk does not belong to a specific VLAN; rather, it is a conduit for multiple VLANs between switches and routers.

**This network could not function without VLAN trunks.**

## Controlling Broadcast Domains with VLANs

* VLANs can be used to limit the reach of broadcast frames.
* A VLAN is a Broadcast domain of its own.
* A broadcast frame sent by a device in a specific VLAN is forwarded within that VLAN only.
* VLANs help control the reach of broadcast frames and their impact in the network.
* Unicast and multicast frames are forwarded within the originating VLAN.

## Tagging Ethernet Frames for VLAN Identification

* Frame tagging is the process of adding a VLAN identification header to the frame.
* It is used to properly transmit multiple VLAN frames through a trunk link.
* Switches tag frames to identify the VLAN to which they belong.
* Different tagging protocols exist;
* IEEE 802.1Q is a very popular example.
* The protocol defines the structure of the tagging header added to the frame.
* Switches add VLAN tags to the frames before placing them into truck links and remove the tags before forwarding frames through non-trunk ports.
* When properly tagged, the frame can transverse any number of switches via trunk link and still be forwarded within the correct VLAN at the destination

**VLAN Tag Field Details**

The VLAN tag field consists of a Type field, a Priority field, a Canonical Format Identifier field, and VLAN ID field:

* **Type** - A 2-byte value called the tag protocol ID (TPID) value. For Ethernet, it is set to hexadecimal 0x8100.
* **User priority** - A 3-bit value that supports level or service implementation.
* **Canonical Format Identifier (CFI)** - A 1-bit identifier that enables Token Ring frames to be carried across Ethernet links.
* **VLAN ID (VID)** - A 12-bit VLAN identification number that supports up to 4096 VLAN IDs.

## Native VLANs and 802.1Q Tagging

* Control traffic sent on the native VLAN should nit be tagged
* Frames received untagged, remain untagged and are placed in the native VLAN when forwarded.
* If there are no ports associated to the native VLAN and no other trunk links, an untagged frame is dropped.
* When configuring a switch port on a cisco switch, configure devices so that they do not send tagged frames on the native VLAN.
* In cisco switches, native VLAN is VLAN 1, by default

## Voice VLAN Tagging

Recall that to support VoIP, a separate voice VLAN is required.

The link between the switch and the IP phone acts as a trunk to carry both voice VLAN traffic and data VLAN traffic.

The Cisco IP Phone contains an integrated three-port 10/100 switch. The ports provide dedicerede connections to these devices:

* Port 1 connects to the switch or other VoIP device.
* Port 2 is an internal 10/100 interface that carries the IP phone traffic.
* Port 3 (access port) connects to a PC or other device.

On the switch, the access is configured to send Cisco Discovery Protocol (CDP) packets that instruct an attached IP phone to send voice traffic to the switch in one of three ways, depending on the type of traffic:

* In a voice VLAN tagged with a Layer 2 class of service (CoS) priority value
* In an access VLAN tagged with a Layer 2 CoS priority value
* In an access VLAN, untagged (no Layer 2 CoS priority value)

## VLAN Ranges on Catalyst Switches

Different Cisco Catalyst switches support various numbers of VLANs. The number of supported VLANs is large enough to accommodate the needs of most organizations.

**Normal Range VLANs**

* Used in small- and medium-sized business and enterprise networks.
* Identified by a VLAN ID between 1 and 1005.
* IDs 1002 through 1005 are reserved for Token Ring and Fiber Distributed Data Interface (FDDI) VLANs.
* IDs 1 and 1002 to 1005 are automatically created and cannot be removed.
* Configurations are stored within a VLAN database file, called vlan.dat. The vlan.dat file is located in the flash memory of the switch.
* The VLAN Trunking Protocol (VTP), which helps manage VLAN configurations between switches, can only learn and store normal range VLANs.

**Extended Range VLANs**

* Enable service providers to extend their infrastructure to a greater number of customers. Some global enterprises could be large enough to need extended range VLAN IDs.
* Are identified by a VLAN ID between 1006 and 4094.
* Configurations are not written to the vlan.dat file.
* Support fewer VLAN features than normal range VLANs.
* Saved, by default, in the running configuration file.
* VTP does not learn extended range VLANs.

## Creating a VLAN

When configuring normal range VLANs, the configuration details are stored in flash memory on the switch, in a file called vlan.dat. Flash memory is persistent and does not require the**copy running-config startup-config**command.

In addition to entering a single VLAN ID, a series of VLAN IDs can be entered separated by commas, or a range of VLAN IDs separated by hyphens using the**vlan***vlan-id*command. For example, use the following command to create VLANs 100, 102, 105, 106, and 107:

S1(config)# **vlan 100,102,105-107**

## Assigning Ports to VLANs

After creating a VLAN, the next step is to assign ports to the VLAN. An access port can belong to only one VLAN at a time. One exception to this rule is that of a port connected to an IP phone, in which case, there are two VLANs associated with the port: one for voice and one for data.

Use the**interface range** command to simultaneously configure multiple interfaces.

The**switchport access vlan**command forces the creation of a VLAN if it does not already exist on the switch.

## Changing VLAN Port Membership

*Display the brief vlan information.*

S1# show vlan brief

*Remove F0/18 from vlan 20. Use the 'do' form of the 'show' command to display the brief vlan information after removal.*

S1# configure terminal

S1(config)# interface F0/18

S1(config-if)# no switchport access vlan

S1(config-if)# do show vlan brief

*Set F0/11 to access mode and assign it to vlan 20. Return directly to privileged EXEC mode when complete.*

S1(config-if)# interface F0/11

S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 20

S1(config-if)# end

*Display the brief vlan information.*

S1# show vlan brief

*Verify the switchport status of F0/18.*

S1# show interfaces F0/18 switchport

## Deleting VLANs

The **no vlan** vlan-id global configuration mode command is used to remove VLAN 20 from the switch.

Alternatively, the entire vlan.dat file can be deleted using the**delete flash:vlan.dat**privileged EXEC mode command. The abbreviated command version (**delete vlan.dat**) can be used if the vlan.dat file has not been moved from its default location.

**Note**: For a Catalyst switch, the**erase startup-config**command must accompany the**delete vlan.dat**command prior to reload to restore the switch to its factory default condition.

## Verifying VLAN Information

*Ports F0/11 and F0/18 have been assigned to VLAN 20. Display the vlan information specifically for the Student vlan.*

S1# show vlan name student

*Display summary information for VLANs.*

S1# show vlan summary

*Display the interface information for VLAN 20*.

S1# show interfaces vlan 20

*Display the switchport information for F0/18.*

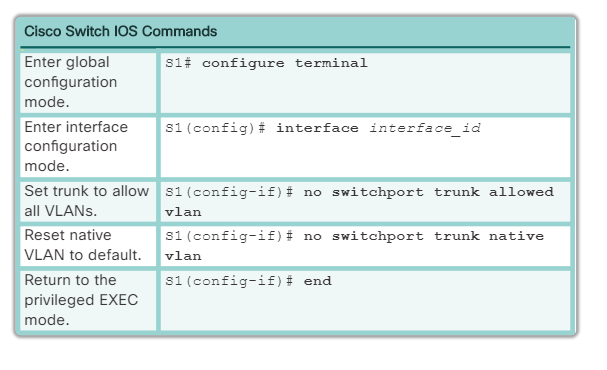
S1# show interfaces F0/18 switchport

## Configuring IEEE 802.1Q Trunk Links

A VLAN trunk is an OSI Layer 2 link between two switches that carries traffic for all VLANs (unless the allowed VLAN list is restricted manually or dynamically)

To configure a switch port on one end of a trunk link, use the **switchport mode trunk** command. With this command, the interface changes to permanent trunking mode

## Resetting the Trunk to Default State



## Verifying Trunk Configuration

*Configure port f0/1 to be an 802.1q trunk. Use VLAN 99 as the native VLAN.*

S1(config)# interface f0/1

S1(config-if)# switchport mode trunk

S1(config-if)# switchport trunk native vlan 99

*Return directly to privileged EXEC mode. Display the switchport status of f0/1.*

S1(config-if)# end

S1# show interfaces f0/1 switchport

## IP Addressing Issues with VLAN

* It is a common practice to associate a VLAN with an IP network.
* Because different IP networks only communicate through a router, all

devices within a VLAN must be part of the same IP network to

communicate.

* The figure displays that PC1 cannot communicate to the server because

it has a wrong IP address configured.

## Missing VLANs

If all the IP address mismatches have been solved, but the device still

cannot connect, check if the VLAN exists in the switch.

## Missing VLANs (cont.)

* If the VLAN to which a port belongs is deleted, the port becomes inactive. All ports

belonging to the VLAN that was deleted are unable to communicate with the rest of the

network.

* Not functional until the missing VLAN is created using the vlan vlan\_id global

configuration.

## Introduction to Troubleshooting Trunks

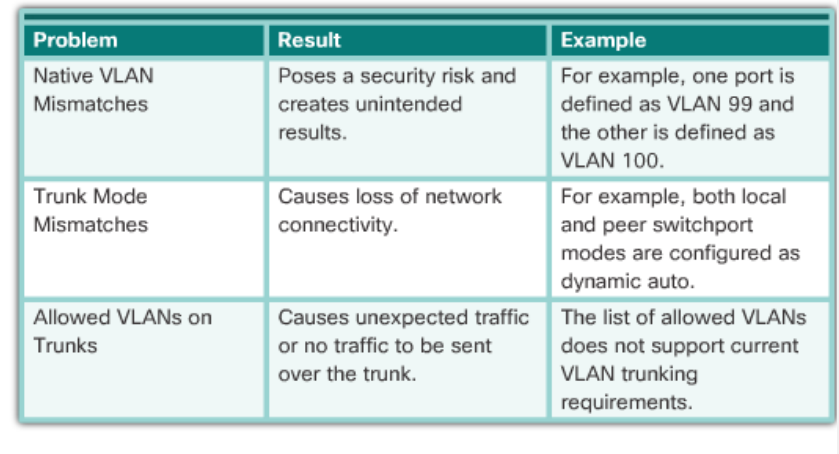
To solve a native VLAN mismatch, configure the native VLAN to be the same VLAN on both sides of the link.

## Common Problems with Trunks

* Trunking issues are usually associated with incorrect configurations.
* The most common type of trunk configuration errors are:
* Native VLAN mismatches
* Trunk mode mismatches
* Allowed VLANs on trunks
* If a trunk problem is detected, the best practice guidelines

recommend to troubleshoot in the order shown above.

## Common Problems with Trunks (cont.)



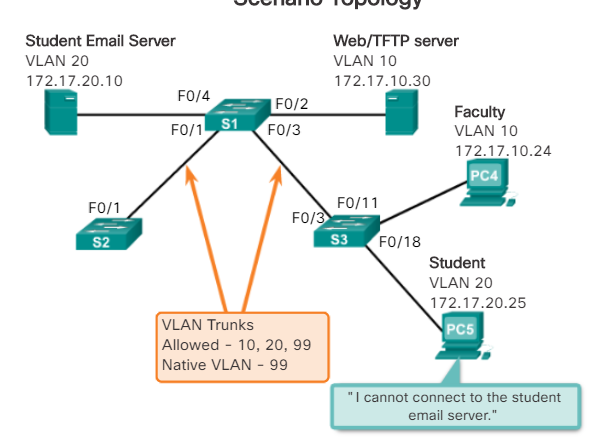
## Incorrect Port Mode

Trunk links are normally configured statically with the**switchport mode trunk**command.

When a port on a trunk link is configured with a trunk mode that is incompatible with the neighboring trunk port, a trunk link fails to form between the two switches.

## Incorrect VLAN List

For traffic from a VLAN to be transmitted across a trunk, it must be allowed on the trunk. To do so, use the**switchport trunk allowed vlan***vlan-id* command.



What is Inter-VLAN Routing?

There are three options for inter-VLAN routing :

* Legacy inter-VLAN routing
* Router-on-a-Stick
* Layer 3 switching using SVIs

## Legacy Inter-VLAN Routing

Historically, the first solution for inter-VLAN routing relied on routers with multiple physical interfaces. Each interface had to be connected to a separate network and configured with a distinct subnet.

1. PC1 on VLAN 10 is communicating with PC3 on VLAN 30 through router R1.

2. PC1 and PC3 are on different VLANs and have IPv4 addresses on different subnets.

3. Router R1 has a separate interface configured for each of the VLANs.

4. PC1 sends unicast traffic destined for PC3 to switch S2 on VLAN 10, where it is then forwarded out the trunk interface to switch S1.

5. Switch S1 then forwards the unicast traffic through its interface F0/3 to interface G0/0 on router R1.

6. The router routes the unicast traffic through its interface G0/1, which is connected to VLAN 30.

7. The router forwards the unicast traffic to switch S1 on VLAN 30.

8. Switch S1 then forwards the unicast traffic to switch S2 through the active trunk link, after which switch S2 can then forward the unicast traffic to PC3 on VLAN 30.

In this example, the router was configured with two separate physical interfaces to interact with the different VLANs and perform the routing

## Router-on-a-Stick Inter-VLAN Routing

While legacy inter-VLAN routing requires multiple physical interfaces on both the router and the switch, a more common, present-day implementation of inter-VLAN routing does not.

‘Router-on-a-stick’ is a type of router configuration in which a single physical interface routes traffic between multiple VLANs on a network

1. PC1 on VLAN 10 is communicating with PC3 on VLAN 30 through router R1 using a single, physical router interface.

2. PC1 sends its unicast traffic to switch S2.

3. Switch S2 then tags the unicast traffic as originating on VLAN 10 and forwards the unicast traffic out its trunk link to switch S1.

4. Switch S1 forwards the tagged traffic out the other trunk interface on port F0/3 to the interface on router R1.

5. Router R1 accepts the tagged unicast traffic on VLAN 10 and routes it to VLAN 30 using its configured subinterfaces.

6. The unicast traffic is tagged with VLAN 30 as it is sent out the router interface to switch S1.

7. Switch S1 forwards the tagged unicast traffic out the other trunk link to switch S2.

8. Switch S2 removes the VLAN tag of the unicast frame and forwards the frame out to PC3 on port F0/23.

## Configure Legacy Inter-VLAN Routing: Preparation

Legacy inter-VLAN routing requires routers to have multiple physical interfaces. The router accomplishes the routing by having each of its physical interfaces connected to a unique VLAN.  Each interface is also configured with an IPv4 address for the subnet associated with the particular VLAN to which it is connected.

Even though there are many steps in the process of inter-VLAN routing, when two devices on different VLANs communicate through a router, the entire process happens in a fraction of a second.

## Configure Legacy Inter-VLAN Routing: Switch Configuration

To configure legacy inter-VLAN routing, start by configuring the switch.

Use the**vlan***vlan\_id*global configuration mode command to create VLANs. In this example, VLANs 10 and 30 were created on switch S1.

After the VLANs have been created, the switch ports are assigned to the appropriate VLANs. The**switchport access vlan***vlan\_id*command is executed from interface configuration mode on the switch for each interface to which the router connects.

In this example, interfaces F0/4 and F0/11 have been assigned to VLAN 10 using the**switchport access vlan 10** command. The same process is used to assign interface F0/5 and F0/6 on switch S1 to VLAN 30.

Finally, to protect the configuration so that it is not lost after a reload of the switch, the**copy running-config startup-config**command is executed to back up the running configuration to the startup configuration.

## Configure Legacy Inter-VLAN Routing: Router Interface Configuration

Now the router can be configured to perform inter-VLAN routing.

Router interfaces are disabled by default and must be enabled using the**no shutdown**command before they are used. After the**no shutdown**interface configuration mode command has been issued, a notification displays, indicating that the interface state has changed to up. This indicates that the interface is now enabled.

Examine the routing table using the**show ip route**command.

## Configure Router-on-a-Stick: Preparation

Legacy inter-VLAN routing using physical interfaces has a significant limitation. Routers have a limited number of physical interfaces to connect to different VLANs. As the number of VLANs increases on a network, having one physical router interface per VLAN quickly exhausts the physical interface capacity of a router.

**The term prefix length can be used to refer to the IPv4 subnet mask when associated with an IPv4 address, and the IPv6 prefix length when associated with an IPv6 address.**

## Configure Router-on-a-Stick: Switch Configuration

To enable inter-VLAN routing using router-on-a stick, start by enabling trunking on the switch port that is connected to the router.

Because switch port F0/5 is configured as a trunk port, the port does not need to be assigned to any VLAN. To configure switch port F0/5 as a trunk port, execute the**switchport mode trunk**command in interface configuration mode for port F0/5.

## Configure Router-on-a-Stick: Router Subinterface Configuration

The configuration of the router is different when a router-on-a-stick configuration is used, compared to legacy inter-VLAN routing. The figure shows that multiple subinterfaces are configured.

Each subinterface is created using the**interface***interface\_id subinterface\_id*global configuration mode command. The syntax for the subinterface is the physical interface, in this case g0/0, followed by a period and a subinterface number. As shown in the figure subinterface GigabitEthernet0/0.10 is created using the**interface g0/0.10 global**configuration mode command. The subinterface number is typically configured to reflect the VLAN number.

**Note:** There is a**native**keyword option that can be appended to this command to set the IEEE 802.1Q native VLAN. In this example, the**native**keyword option was excluded to leave the native VLAN default as VLAN 1.

## Configure Router-on-a-Stick: Verifying Subinterfaces

By default, Cisco routers are configured to route traffic between local subinterfaces. As a result, routing does not specifically need to be enabled.

## Configure Router-on-a-Stick: Verifying Routing

After the router and switch have been configured to perform inter-VLAN routing, the next step is to verify host-to-host connectivity. Access to devices on remote VLANs can be tested using the**ping**command.

For the example shown in the figure, a**ping**and a**tracert**are initiated from PC1 to the destination address of PC3.

**Ping Test**

The **ping** command sends an ICMP echo request to the destination address. When a host receives an ICMP echo request, it responds with an ICMP echo reply to confirm that it received the ICMP echo request. The **ping** command calculates the elapsed time using the difference between the time the echo request was sent and the time the echo reply was received. This elapsed time is used to determine the latency of the connection. Successfully receiving a reply confirms that there is a path between the sending device and the receiving device.

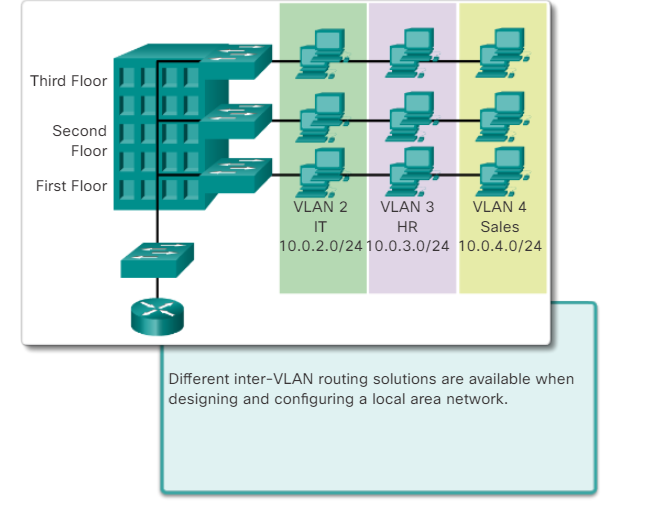
**Tracert Test**

Tracert is a useful utility for confirming the routed path taken between two devices. On UNIX systems, the utility is specified by**traceroute.**Tracert also uses ICMP to determine the path taken, but it uses ICMP echo requests with specific time-to-live values defined on the frame.

## The Inside Track

Your company has just purchased a three-level building. You are the network administrator and must design the company inter-VLAN routing network scheme to serve a few employees on each floor.

Floor 1 is occupied by the HR Department, Floor 2 is occupied by the IT Department, and Floor 3 is occupied by the Sales Department. All Departments must be able to communicate with each other, but at the same time have their own separate, working networks.



# Chapter 7: Access Control Lists

By default a router does not filter traffic. Traffic that enters the router is routed solely based on information within the routing table.

Packet filtering controls access to a network by analyzing the incoming and outgoing packets and passing or dropping them based on criteria such as the source IP address, destination IP addresses, and the protocol carried within the packet. A packet-filtering router uses rules to determine whether to permit or deny traffic. A router can also perform packet filtering at Layer 4, the transport layer.

An ACL is a sequential list of permit or deny statements. The last statement of an ACL is always an implicit deny which blocks all traffic. To prevent the implied deny any statement at the end of the ACL from blocking all traffic, the**permit any**statement can be added.

When network traffic passes through an interface configured with an ACL, the router compares the information within the packet against each entry, in sequential order, to determine whether the packet matches one of the statements. If a match is found, the packet is processed accordingly.

ACLs are configured to apply to inbound traffic or to apply to outbound traffic.

Standard ACLs can be used to permit or deny traffic only from source IPv4 addresses. The destination of the packet and the ports involved are not evaluated. The basic rule for placing a standard ACL is to place it close to the destination.

Extended ACLs filter packets based on several attributes: protocol type, source or destination IPv4 address, and source or destination ports. The basic rule for placing an extended ACL is to place it as close to the source as possible.

The**access-list**global configuration command defines a standard ACL with a number in the range of 1 through 99The**ip access-list standard***name*is used to create a standard named ACL.

After an ACL is configured, it is linked to an interface using the**ip access-group**command in interface configuration mode. Remember these rules: one ACL per protocol, one ACL per direction, one ACL per interface.

To remove an ACL from an interface, first enter the**no ip access-group**command on the interface, and then enter the global **no access-list** command to remove the entire ACL.

The**show running-config**and**show access-lists**commands are used to verify ACL configuration. The**show ip interface**command is used to verify the ACL on the interface and the direction in which it was applied.

The**access-class**command configured in line configuration mode restricts incoming and outgoing connections between a particular VTY and the addresses in an access list.

## FTP Denied

**Scenario**

It was recently reported that viruses are on the rise within your small- to medium-sized business network. Your network administrator has been tracking network performance and has determined that one particular host is constantly downloading files from a remote FTP server. This host just may be the virus source perpetuating throughout the network!

Use Packet Tracer to complete this activity. Write a named ACL to deny the host access to the FTP server. Apply the ACL to the most effective interface on the router.

To complete the physical topology, you must use:

* One PC host station
* Two switches
* One Cisco 1941 series Integrated Services Router
* One server

Using the Packet Tracer text tool, record the ACL you prepared. Validate that the ACL works to deny access to the FTP server by trying to access the FTP server’s address. Observe what happens while in simulation mode.

Save your file and be prepared to share it with another student, or with the entire class.

# Chapter 8: DHCP

## Class Activity - IoE and DHCP

With the advent of the Internet of Everything (IoE), any device in your home capable of wired or wireless connectivity to a network will be able to be accessed from just about anywhere.

Using Packet Tracer for this modeling activity, perform the following tasks:

* Configure a Cisco 1941 router (or DHCP-server-capable ISR device) for IPv4 or IPv6 DHCP addressing.
* Think of five devices in your home you would like to receive IP addresses from the router’s DHCP service. Set the end devices to claim DHCP addresses from the DHCP server.
* Show output validating that each end device secures an IP address from the server. Save your output information via a screen capture program or use the **PrtScrn**key command.
* Present your findings to a fellow classmate or to the class.

All nodes on a network require a unique IP address to communicate with other devices. The static assignment of IP addressing information on a large network results in an administrative burden that can be eliminated by using DHCPv4 and DHCPv6 to dynamically assign IPv4 and IPv6 addressing information, respectively.

* DHCPv4 dynamically assigns, or leases, an IPv4 address from a pool of addresses for a limited period of time, as configured on the server, or until the client no longer needs the address.

DHCPv4 involves the exchange of several different packets between the DHCPv4 server and the DHCPv4 client resulting in the lease of valid addressing information for a predefined period of time.

Messages originating from the client (DHCPDISCOVER, DHCPREQUEST) are broadcast to allow all DHCPv4 servers on the network to hear the client request for, and receipt of, addressing information. Messages originating from the DHCPv4 server (DHCPOFFER, DHCPACK) are sent as unicasts directly to the client.

There are two methods available for the dynamic configuration of IPv6 global unicast addresses.

* Stateless Address Autoconfiguration (SLAAC)
* Dynamic Host Configuration Protocol for IPv6 (Stateful DHCPv6)

With stateless autoconfiguration, the client uses information provided by the IPv6 RA message to automatically select and configure a unique IPv6 address. The stateless DHCPv6 option informs the client to use the information in the RA message for addressing, but additional configuration parameters are available from a DHCPv6 server.

Stateful DHCPv6 is similar to DHCPv4. In this case, the RA message informs the client not to use the information in the RA message. All addressing information and DNS configuration information is obtained from a stateful DHCPv6 server. The DHCPv6 server maintains IPv6 state information similar to a DHCPv4 server allocating addresses for IPv4.

If the DHCP server is located on a different network segment than the DHCP client then it is necessary to configure a relay agent. The relay agent forwards specific broadcast or multicast messages, including DHCP messages, originating from a host on a LAN segment and destined for a specific server located on a different LAN segment.

Troubleshooting issues with DHCPv4 and DHCPv6 involve the same tasks:

* Resolve Address Conflicts
* Verify Physical Connectivity
* Test Connectivity using a Static IP Address
* Verify Switch Port Configuration
* Test Operation on the Same Subnet or VLAN

# Chapter 9: NAT for IPv4

## NAT Check

**Scenario**

Network address translation is not currently included in your company’s network design. It has been decided to configure some devices to use NAT services for connecting to the mail server.

Before deploying NAT live on the network, you prototype it using a network simulation program.

For further instructions, refer to the PDF which accompanies this activity.

## Packet Tracer - Skills Integration Challenge

**Scenario**

This culminating activity includes many of the skills that you have acquired during this course. First, you will complete the documentation for the network. So make sure you have a printed version of the instructions. During implementation, you will configure VLANs, trunking, port security, and SSH remote access on a switch. Then, you will implement inter-VLAN routing and NAT on a router. Finally, you will use your documentation to verify your implementation by testing end-to-end connectivity.

This chapter has outlined how NAT is used to help alleviate the depletion of IPv4 address space. NAT for IPv4 allows network administrators to use RFC 1918 private address space while providing connectivity to the Internet, using a single or limited number of public addresses.

NAT conserves public address space and saves considerable administrative overhead in managing adds, moves, and changes. NAT and PAT can be implemented to conserve public address space without affecting the ISP connection. However, NAT has drawbacks in terms of its negative effects on device performance, mobility, and end-to-end connectivity and should be considered a short term implementation for address exhaustion with the long term solution being IPv6.

This chapter discussed NAT for IPv4, including:

* NAT characteristics, terminology, and general operations
* The different types of NAT including static NAT, dynamic NAT, and PAT
* The benefits and disadvantages of NAT
* The configuration, verification, and analysis of static NAT, dynamic NAT, and PAT
* How port forwarding can be used to access an internal device from the Internet
* Why NAT is available but not integral to IPv6 networking
* Troubleshooting NAT using**show**and**debug**commands

# Chapter 10: Device Discovery, Management, and Maintenance

In this chapter, you learned and practice skills that network administrators use for device discovery, management, and maintenance.

CDP is a Cisco proprietary protocol for network discovery on the data link layer. It can share information such as device names and IOS versions, with other physically connected Cisco devices. LLDP is vendor-neutral protocol on the data link layer for network discovery. The network devices advertise information, such as their identities and capabilities to their neighbors.

NTP synchronizes the time of day among a set of distributed time servers and clients. This allows networking devices to agree on the time a specific event occurred, such as the lose of connectivity between a router and a switch. Syslog messages can be trapped and sent to a syslog server where the network administrator can investigate when the link failed.

Device maintenance includes the tasks of backing up, restoring, and upgrading IOS images and configuration files. Upgrading an IOS image also includes tasks related to software licensing.