Cisco

# Cisco Information

*Note: Whenever there is a command you have to type, it will be surrounded in “ ` ` ” so that is what you will have to type. Whenever something is in between <> that is a value that YOU have to supply. Any optional parameters will be in []. You can just type shortcuts for the command. So for the `enable` command if you type `ena` it will still work.*

## Privilege ModesAD

### User EXEC Mode:

* Limited capabilities
* Useful for basic operations
* Basic monitoring commands and does not allow commands that can change configuration
* Referred to as a ‘view-only’ mode
* If the prompt ends with: ‘>’ then it is in User EXEC Mode

#### Navigation

* + `enable` to enter privileged EXEC Mode

### Privileged EXEC Mode:

* Executes configuration commands
* Higher privilege modes like Global Configuration Mode can only be accessed from this mode
* Allows access to all commands and features
* Prompt ends with #

#### Navigation

* + `disable` to go down to User EXEC Mode
  + `configure terminal` to enter Global Configuration Mode

### Global Configuration Mode:

* Configuration changes are made that affect the operation of the device as a whole
* Prompt ends in: (config)#
* This is accessed before other specific configuration modes
* Is like the gateway to different sub-configuration modes
* Sub-configuration modes allows the configuration of a particular part of function of the IOS device
* Common sub-configuration modes include:
  + Line Configuration Mode
    - Used to configure console, SSH, Telnet, or AUX access
  + Interface Configuration Mode
    - Like a port for example an IP Port
* The mode is identified by the prompt that is unique to that mode, by default it begins with the device name. For example default for line is: (config-line)# and the default for interface configuration mode is: (config-if)#

#### Navigation

* + `exit global` to go back to Privileged EXEC Mode
  + Sub-configuration mode varies. Most of the time it follows the format: `line/interface <interface\_name> <interface\_number>`. For example to access console you would do: `line console 0`. The interface number can be found when you hover over the device. *You choose `line` or `interface` depending on what you are trying to configure.*
  + To exit sub-configuration mode to Global Configuration Mode you just have to type `exit`
  + To exit sub-configuration mode to Privileged EXEC Mode type `end`
  + To change from one interface to another interface you would just do: `line/interface <interface\_name> <interface\_number>. For example, to switch to FastEthernet you would do: `interface FastEthernet 0/1`. *You choose `line` or `interface` depending on what you are trying to configure.*

## Configuration Files

### Startup Configuration File

The file stored in Non-volatile Random Access Memory (NVRAM) that contains all of the commands that will be used by the device upon startup or reboot. NVRAM does not lose its contents when the device is powered off.

### Running Configuration File

The file stored in Random Access Memory (RAM) that reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device immediately. RAM is volatile memory. It loses all of its content when the device is powered off or restarted.

### Commands Related to Configuration Files:

#### Writing to Memory

In Privileged EXEC Mode (Prompt with ‘#’), execute: `write memory`

#### Show Running Config

In Privileged EXEC mode run:

`show running-config`

#### Show Startup Config

In Privileged EXEC mode run:

`show startup-config`

#### Save Running Config File

To save it, in privileged EXEC mode run:

`copy running-config startup-config`

### Altering the Config Files

* In privileged EXEC mode run: `reload`
  + The above command will reload the switch which will restart the running config file
* If changes were made to the startup config file that you need to remove run: `erase startup-config`
  + The above command will erase the startup config and reloading the switch will set all the config back to default.

## Basic IOS Command Structure

General Syntax is the command followed by appropriate keywords and arguments

The keyword is a specific parameter defined in the operating system.

The argument is not predefined and is a value or variable defined by the user

If you ever need help, just type a ? at the CLI and it will give you anything. You can even keep the ? at any time in a command if you forgot the exact command

Make sure that when you are naming the Cisco devices that it has a meaning. It is also case sensitive

## To configure the hostname:

Go into global configuration mode and type:

`hostname <name>`

## To remove the hostname:

Go into global configuration mode and type:

`no hostname`

## VLANs

VLANs are a way to improve network performance by:

* The separation of large broadcast domains into smaller ones

VLANs provide a way to group devices within a LAN

VLANs are based on logical connections, instead of physical connections

Devices within a VLAN act as if they are in their own independent network

Each VLAN is considered a separate logical network, and packets destined for another VLAN are forwarded to a device that supports routing

### Benefits of VLANs

#### Security

Groups with sensitive data are separated from the rest of the network

This decreases the chances of confidential information being leaked

#### Cost Reduction

Results form reduced need for expensive network upgrades and more efficient use of existing bandwidth and uplinks

#### Better Performance

Divides Layer 2 networks into multiple logical workgroups

* Broadcast domains

Reduces unnecessary traffic and boosts performance

#### Shrink Broadcast Domains

Reduces number of devices in the broadcast domain

#### Improved IT Staff Efficiency

VLANs make is easier to manage the network

When a new switch is added all policies and procedures are already configured

Easy for the IT staff to isolate the problem

#### Simpler Project and Application Management

Having separate functions makes managing a project or working with a specialized application easier

VLAN design must take into consideration the implementation of a hierarchical network-addressing scheme.

Hierarchical network addressing - IP network numbers are applied to network segments or VLANs in an orderly fashion that takes the network as a whole into consideration

Blocks of contiguous network addresses are reserved for and configured on devices in a specific area of the network

### Types of VLANs

VLAN types can be defined by traffic classes or specific function that they serve

#### Data VLAN

* A VLAN that is configured to carry user-generated traffic. A VLAN carrying voice or management traffic would not be a data VLAN.
* Sometimes referred to as a user VLAN
* Data VLANs are used to separate the network into groups of users or devices

#### Default VLAN

* All switch ports become a part of the default VLAN
* Switch ports that participate in the default VLAN are part of the same broadcast domain
* Allows any device connected to any switch port to communicate with other devices on other switch ports.
* Default for Cisco Switches is VLAN 1
* VLAN 1 has all the same features of any VLAN but cannot be renamed

#### Native VLAN

* Is assigned to an 802.1Q trunk port
* Trunk ports are the links between switches that support the transmission of traffic associated with more than one VLAN
* 802.1Q trunk port supports traffic from many VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic)
* Tagged traffic refers to traffic that has a 4-byte tag inserted within the original Ethernet frame header, specifying the VLAN to which the frame belongs to
* The 802.1Q trunk port places untagged traffic on the native VLAN which by default if VLAN 1
* Native VLANs are defined in IEEE 802.1Q specification
* A native VLAN serves as a common identifier on opposite ends of a trunk link
* Best practice to configure the native VLAN as an unused VLAN, distinct from VLAN 1 and other VLANs.
* Not unusual to dedicate a fixed VLAN to serve the role of the native VLAN for all trunk ports in the switched domain

#### Management VLAN

* A VLAN configured to access the management capabilities of a switch
* VLAN 1 is the management VLAN by default
* To create, the switch virtual interface (SVI) of that VLAN is assigned an IP address and subnet mask, allowing the switch to be managed via HTTP, Telnet, SSH, or SNMP.
* VLAN 1 would be a bad choice for the management VLAN

If the native VLAN (VLAN 1) is the same as the management VLAN it is considered a security risk

#### 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

### VLAN Trunks

* A trunk is a point-to-point link between two network devices that carries more than one VLAN
* If you have one switch with multiple VLANS connecting to another switch, trunks will enable all the VLANs to communicate using only one wire
* VLAN trunks allow all VLAN traffic to propagate between switches, so that devices which are in the same VLAn, but connected to different switches, can communicate without the intervention of a router.
* A VLAN trunk does not belong to a specific VLAN
* A trunk can be used on any device equipped with an appropriate 802.1Q-capable NIC
* Without VLANs when a switch receives a broadcast frame on one of its ports then it broadcasts on all its ports except the one it received it from
* With VLANs when a switch receives a broadcast frame on one of its ports then it broadcasts it only on the ports with that VLAN enabled.

When you are talking about tagged and untagged it just means if the ethernet frame header has a 4 byte tag inserted within the original Ethernet frame header specifying which VLAN it belongs to

### Native VLANs and 802.1Q Tagging

#### Tagged Frames on the Native VLAN

* Some devices add a VLAN tag to native VLAN traffic. This should not be tagged and if a 802.1Q trunk port receives a tagged frame with the VLAN ID the same as the Native VLAN it drops the frame. So you have to configure the device not to do that
  + Devices from other vendors that support tagged frames include IP Phones, servers, routers, and non-Cisco switches

#### Untagged Frames on the Native VLAN

* On a well designed network should not be possible
* In case it does, it forwards the frames to the native VLAN if there are no devices associated with the native VLAN and there are no other trunk ports (both of which is not unusual) then the frame is dropped
* When configuring an 802.1Q trunk port a default Port VLAN ID (PVID) is assigned the value of the native VLAN ID and all untagged traffic coming or out is forwarded based on the PVID value.

### Voice VLAN Tagging

Separate voice VLAN required

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

Cisco IP Phone contains 3 ports:

* 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)

The VLAN file is in flash under the name of vlan.dat

### VLAN Ranges

#### Normal Range VLANs

* Use 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 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 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 have larger VLANs
* Are identified by VLAN ID between 1006 and 4094
* Configurations are not written to vlan.dat file
* Support fewer VLAN features than normal range VLANs
* Are, by default, save in the running configuration file
* VTP does not learn extended range VLANs

### Verifying Trunk Configuration

After running: `show interfaces <interface-id> switchport` if:

* Administrative Mode: trunk
* Operational Mode: trunk
* Administrative Trunking Encapsulation: dot1q
* Operational Trunking Encapsulation: dot1q
* Trunking Native Mode VLAN: 99 (VLAN0099) (that vlan should be the default you set)
* Administrative Native VLAN tagging: enabled
* Trunking VLANs Enabled: ALL

### Introduction to DTP

* Ethernet trunk interfaces support different trunking modes
  + Can be set to trunking or nontrunking, or to negotiate trunking with the neighbor interface
* Trunk negotiation is managed by Dynamic Trunking Protocol (DTP) which operates on a point-to-point basis between network devices
* DTP is a Cisco proprietary protocol that is enabled on certain Switches

### Commands for VLAN Stuff

`delete flash:vlan.dat` - this command deletes the vlan.dat file

`show interface trunk` - shows all the trunk port information of the switch

#### Verifying VLAN Information

##### `show vlan [brief | id <vlan-id> | name <vlan-name> | summary]`

* Running `show vlan brief` will Display one line for each VLAN with the VLAN name, status, and its ports
* Running `show vlan id <vlan-id>` will display information about a single VLAN identified by VLAN ID number
* Running `show vlan name <vlan-name>` will display the same information as above but is identified by the VLAN name
* Running `show vlan summary` will display VLAN summary information

##### `show interfaces [<interface-id> | vlan <vlan-id> | switchport ] `

* Running `show interfaces <interface-id> switchport` will display the administrative and operational status of a switching port, including port blocking and port protection settings
* Running `show interfaces vlan <vlan-id> switchport` will display the administrative and operational status of a switching port, including port blocking and port protection settings

#### Creating a VLAN

In global configuration mode (`configure terminal`):

* Create a VLAN with a valid id number: `vlan <vlan-id>`
  + To create multiple, you separate by commas. To create VLANs 100,102, 105, 106, and 107: `vlan 100,102,105-107`
* In the VLAN interface mode execute: `name <vlan-name>` to give the vlan a name
* Then type: `end` to return to privileged EXEC mode

#### Assigning Ports to VLANs

In global configuration mode (`configure terminal`):

* Go to the port interface that the VLAN is going to be on. To access it run: `interface <interface\_id>`
* Set the port to access mode for security reasons: `switchport mode access`
* Assign the port to a VLAN: `switchport access vlan <vlan\_id>`
* Return to the privileged EXEC Mode: `end`

#### Remove VLAN Assignment

* In the interface configuration mode run: `no switchport access vlan`

#### Deleting VLANs

In global configuration mode (`configure terminal`) run: `no vlan <vlan-id>`

Make sure that no port is associated with that otherwise it won’t work until given access to a working VLAN

#### Configuring IEEE 802.1Q Trunk Links

Enter global configuration mode: `configure terminal`

Enter interface configuration mode: `interface <interface\_id>`

Force the link to be a trunk link: `switchport mode trunk`

Specify a native VLAN for untagged 802.1Q trunks: `switchport trunk native vlan <vlan-id>`

Specify the list of VLANs to be allowed on the trunk link: `switchport trunk allowed vlan <vlan-list>`

Return to privileged EXEC mode: `end`

The command `switchport trunk native vlan <vlan-id>` sets the native VLAN for all the untagged traffic on the network.

#### Resetting the Trunk to Default State

Enter global configuration mode: `configure terminal`

Enter interface configuration mode: `interface <interface-id>`

Set trunk to allow all VLANs: `no switchport trunk allowed vlan`

Reset native VLAN to default: `no switchport trunk native vlan`

Return to the privileged EXEC mode: `end`

#### To enable trunking from Cisco Switch to a device that supports DTP

Run:

* `switchport mode trunk`
* `switchport nonegotiate`

#### Negotiated Interface Modes

* `switchport mode access`
  + Puts the interface into permanent non trunking modes and negotiates to convert the link into a non trunk link
* `switchport mode dynamic auto`
  + Makes the interface able to convert the link to a trunk link if the neighboring interface is set to trunk or desirable mode.
* `switchport mode dynamic desirable`
  + Makes the interface actively attempt to convert the link to a trunk link.
  + Interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode.
* `switchport mode trunk`
  + Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link
* `switchport nonegotiate`
  + Prevents interface from generating DTP frames

Each VLAN must correspond to a unique IP subnet

Easy to solve by identifying the incorrect configuration and changing the subnet address to the correct one

Use `show mac address-table` to check which addresses were learned on a particular ports of the switch and to which VLAN that port is assigned.

Use `show vlan` or `show interfaces switchport` to make sure the port is not inactive

Sometimes a switch port may behave like a trunk port even if it is not a trunk port

VLAN Leaking - an access port might accept frames from VLANs different from the VLAN to which it is assigned

#### Troubleshooting Trunks

Use `show interfaces trunk` command to check whether the local and peer native VLANs match. If the native VLAN does not match on both sides, VLAN leaking occurs.

Then Use the `show interfaces trunk` command to check whether a trunk has been established between switches. Statically configure trunk links whenever possible.

Make sure the native VLAN on both sides of the Trunk is the same

#### Common Problems with Trunks

* Native VLAN mismatches
  + Trunk ports are configured with different native VLANs
* Trunk mode mismatches
  + One trunk port is configured in a mode that is not compatible for trunking on the corresponding peer port
* Allowed VLANs on trunks
  + List of allowed VLANs on a trunk has not been updated with the current VLAN trunking requirements

The best way to prevent a basic switch spoofing is to turn off trunking on all ports, except the ones that specifically require trunking. On the required trunking ports disable DTP and manually enable trunking

## Inter-VLAN Routing

This is routing between VLANs and how to do it. (mind blown)

### Commands / How to do stuff in this

#### Legacy

When configuring legacy, each VLAN has its own port on the router and the switch.

That means that on the router, one port will be for one VLAN and another port for another VLAN and same on the switch

This also means that each port gets its own ip address but it is within the same subnet as the VLAN ip addresses

#### Router-on-a-stick

When configuring the switch, make sure that you make the mode of the port connected to the router as trunk with in the interface of the port that is the trunk:

`switchport mode trunk`

Also make sure you specify the VLANs that are supposed to go through this one port.

When configuring the router, there is a long process:

Go to global configuration mode and when accessing the interface of the port that is connected to the switch run this command:

`interface <ip-address>.<subinterface>`

The subinterface part of the command is just a number and generally it is the VLAN id

Once in that subinterface run these commands:

`encapsulation dot1q <vlan\_id>`

`ip address <ip-address> <subnet-mask>`

`no shutdown`

You can also run `no shutdown` on the interface itself instead of the sub interface

In order to verify the subinterfaces on the router run this command:

`show vlan`

#### Multilayer Switch

# Types of Routing

## Static Routing

Static Routing is when the network administrator manually fills in the routing table of a router.

These are configured so that a router can learn about a remote network

### Advantages of Static Routing

* Better Security - They don’t broadcast themselves over the network
* Use less bandwidth, no CPU cycles are used to calculate and comunicate routes
* Path it uses to send data is known

### Disadvantages of Static Routing

* Initial configuration and maintenance is time-consuming
* Configuration is error-prone, especially in large networks
* Administrator intervention is required to maintain changing router information
* Does not scale well with growing networks; maintenance becomes cumbersome
* Requires complete knowledge of the whole network for proper implementation.

### Uses of Static Routing

* Connect to a specific network
* Connect a stub router
  + A stub router is a router that is connected to a stub network. A stub network is a network that has no knowledge of other networks, that will typically send much or all of its non-local traffic out via a single path, with the network aware only of a default route to non-local destinations.
* Summarize routing table entries
* Create a backup route

### Types of Static Routing

1. Standard static route
   1. Static routes are useful when connecting to a specific remote network
2. Default static route
   1. A route that matches all packets. A default route identifies the gateway IP address to which the router sends all IP packets that it does not have a learned or static route.
   2. Used:
      1. When no other routes match the packet destination address. Common use is when connecting a company’s edge router to the ISP network
      2. Has only one other router it is connected to. Known as a stub router
3. Summary static route
   1. To reduce the size of the routing table, multiple static routes can be summarized into a single static route if:
      1. The destination networks are contiguous and can be summarized into a single network address
      2. The multiple static routes all use the same exit interface or next-hop IP address
   2. For example, the IP addresses:
      1. 172.20.0.0/16
      2. 172.21.0.0/16
      3. 172.22.0.0/16
      4. 172.23.0.0/16
   3. The above IP addresses can all be summarized as: 172.20.0.0/14
4. Floating static route
   1. This is a route that is a backup path to a primary static or dynamic route (Check dynamic routing for more details).
   2. It is configured with a higher Administrative Distance (AD) than the primary route.

### CIDR and VLSM

### Commands for Static Routing:

For the following commands these are what the parameters mean:

Network-address is the parameter for the destination network address of the remote network to be added to the routing table

Subnet-mask is the parameter is the subnet mask of the remote network being added to the routing table. It can be modified to summarize a group of networks.

Ip-address is the next-hop router’s IP address. Commonly creates a recursive lookup

Exit-interface is the interface the is responsible for forwarding packets to the destination network.

#### To configure a Next-Hop Static Route:

`ip route <network-address> <subnet-mask> <ip-address>`

#### To configure a Directly Connected Static Route:

`ip route <network-address> <subnet-mask> <exit-interface>`

#### To configure a Fully Specified Static Route:

`ip route <network-address> <subnet-mask> <exit-interface> <ip-address>`

#### To configure a Floating Static Route:

`ip route <network-address> <subnet-mask> {<ip-address> | <exit-interface>} [administrative-distance]`

#### To configure a Default Static Route:

`ip route 0.0.0.0 0.0.0.0 {<ip-address> | <exit-interface>}`

**WHEN THE EXIT INTERFACE IS IN AN ETHERNET NETWORK, USE A FULLY SPECIFIED STATIC ROUTE WITH BOTH EXIT INTERFACE AND IP ADDRESS, IN THAT ORDER.**

#### Verifying Static Route Configuration

`show ip route`

`show ip route static`

`show ip route <network>`

#### Verifying a Default Static Route Configuration:

Run `show ip route static`

If one of the entries has S\* before it, it means that it is the default route

#### Troubleshooting a Missing Route

`ping`

`traceroute`

`show ip route`

`show ip interface brief`

`show cdp neighbors detail`

## Dynamic Routing

Automatically updates its routing table based on the routers around it.

It learns about the different remote networks via different routing protocols and algorithms

### Routing Protocols

#### IPv4 Protocols

* EIGRP (Enhanced Interior Gateway Routing Protocol)
* RIPv2 (Router Interface Protocol)
* IS-IS (Intermediate System-to-Intermediate System)
* OSPFv2 (Open Shortest Path First)
* BGP-4 (Broadway Gate Protocol)

#### IPv6 Protocols

* RIPng (Router Interface Protocol)
* EIGRP for IPv6
* OSPFv3
* IS-IS for IPv6
* BGP-MP

Routing Protocols are used to facilitate the exchange of routing information between routers.

A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information

### Purpose

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

### Main Components

* Data Structures:
  + Routing protocols typically use tables or databases for its operations. This information is kept in RAM
* Routing Protocol Messages
  + Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network
* Algorithm
  + An algorithm is a finite list of steps used to accomplish a task. Routing protocols use algorithms for facilitating routing information and for best path determination

Routing protocols automatically add information about remote networks to their own routing tables.

Routing protocols determine the best path, or route, to each network. That route is then added to the routing table.

Routers automatically exchange routing information when there is a topology change

### Operation of Dynamic Routing Protocol

1. The router sends and receives routing messages on its interfaces
2. The router shares routing messages and routing information with other routers that are using the same routing protocol
3. Routers exchange routing information to learn about remote networks
4. When a router detects a topology change the routing protocol can advertise this change to other routers

On boot up of router, it knows nothing about the network. The only information it has is from its own saved configuration file stored in NVRAM. If the IP addressing is configured correctly, then the router initially discovers its own directly connected networks

If a router protocol is configured, then it sends out and receives and update packet.

Distance vector routing protocols typically implement a routing loop prevention technique known as split horizon. Split horizon prevents information being sent out the same interface from which it was received.

##### Network Convergence - When all the routers in the network know about everything around and in the network

### Classifying Protocols by Classless Behavior

### Distance Vector Routing Protocols

### Line-State Routing Protocols

A router configured with one of these protocols can create a complete view or topology of the network by gathering information from all of the other routers

Is like having a complete map of the network topology.

After network convergence, routers only send updated when the topology changes.

Best work where:

* The network design is hierarchical, usually occurring in large networks
* Fast convergence of the network is critical
* The administrators have good knowledge of the implemented link-state routing protocol

### Classful Routing Protocols

Classful Routing protocols do not send subnet mask information in their routing updates

Classless routing protocols include subnet mask information in the routing updates

Because RIPv1 and IGRP do not include subnet mask information in their updates, they cannot provide variable-length subnet masks(VLSMs) and classless interdomain routing (CIDR)

### Routing Protocol Characteristics

* **Speed of convergence** - how quickly the routers in the network topology share routing information and reach a state of consistent knowledge.
* **Scalability** - How large a network can become, based on the routing protocol that is deployed. The larger the network is, the more scalable the routing protocol needs to be
* **Classful or Classless (Use of VLSM)** - Classful routing protocols do not include subnet mask and can’t support VLSM. Classes routing protocols include the subnet mask and support VLSM and better route summarization
* **Resource Usage** - Resource usage includes the requirements of a routing protocol such as RAM, CPU utilization, and link bandwidth utilization.
* **Implementation and Maintenance** - Describes the level of knowledge that is required for a network administrator to implement and maintain the network based on the routing protocol deployed

### Routing Protocol Metrics

### Distance Vector Technologies

Distance vector routing protocols share updates between neighbors periodically even if the topology does not change.

### Distance Vector Algorithm

The algorithm used defines the following processes:

* Mechanism for sending and receiving routing information
* Mechanism for calculating the best paths and installing routes in the routing table
* Mechanism for detecting and reacting to topology changes

Different protocols use different algorithms

* RIP uses the Bellman-Ford algorithm.
* IGRP and EIGRP use the Diffusing Update Algorithm (DUAL)

### Routing Information Protocol

RIP was a first generation routing protocol for IPv4; easy to configure; good choice for small networks

RIPv1 was updated to RIPv2 which is a classless routing protocol; so it supports VLSM and CIDR

RIPv2 also has increased efficiency, reduced routing entries, and its secure.

RIPng is the version that has support for IPv6

#### Commands for Configuration of RIP

##### To Enable RIP:

Run `router rip` in the global configuration mode. This is where you configure the settings for RIP

##### To Disable and Eliminate RIP:

Run `no router rip` in the global configuration mode. This command stops the RIP process and erases all existing RIP configurations

##### To Enable RIP Routing for a Network:

Use: `network <network-address>`. For network-address 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

##### Verifying RIP Settings:

The `show ip protocols` command displays the IPv4 routing protocol settings currently configured on the router.

The `show ip route` command displays the RIP routes installed in the routing table.

##### Enabling RIPv2:

By default, when a RIP process is configured on a Cisco router, it is running RIPv1. However, even though it sends only RIPv1 messages it can interpret both versions’ messages.

When in the router configuration mode [prompt ending in: (config-router)] run `version 2`

##### Disabling Auto Summarization:

RIPv2 automatically summarizes networks at major network boundaries by default

Use the `no auto-summary` router configuration mode command.

##### Configuring Passive Interfaces:

By default, RIP updates are forwarded out all RIP enabled interfaces, but you only need to send it out the interfaces connected to other RIP routers.

Sending out unneeded updates on a LAN that has no RIP router impacts the network in three ways:

* Wasted Bandwidth
* Wasted Resources
* Security Risk

Use the `passive-interface <router-interface>` to set that interface as a passive interface

Use `passive-interface default` to set the passive interfaces to the default

##### Propagating a Default Route:

If there is an edge router that is connected to another network or the internet via only one line and you have to set that as the default gateway the best way to do it is:

* Set the default route using: `ip route 0.0.0.0 0.0.0.0 {<exit-interface> | <next-hop-ip>}
* Then run `default-information originate` as a router configuration command
* You can also run `show ip route` to verify that the Gateway of last resort is the correct default gateway

### Enhanced Interior-Gateway Routing Protocol

The IGRP was the first proprietary IPv4 routing protocol developed by Cisco.

IGRP was replaced with EIGRP in 1992.

EIGRP also introduced support for VLSM and CIDR. It also increases efficiency, reduces routing updates, and supports secure message exchange

EIGRP also introduced:

* Bounded triggered updates -
* Hello keepalive mechanism
* Maintains a topology table
* Rapid convergence
* Multiple network layer protocol support

### Shortest Path First Protocols

Link-state routing protocols are also called shortest path first protocols because they are built around Edsger Dijkstra’s shortest path first (SPF) algorithm

Open Shortest Path First (OSPF)

Intermediate System-to-Intermediate System (IS-IS)

Link-state routing protocols have the reputation of being more complex than their distance vector counterparts. However the basic functionality and configuration is equally straight forward

### Dijkstra’s Algorithm

All link-state routing protocols use this algorithm to calculate the best path route.

It involves adding up the costs of a path, from source to destination, to determine the total cost of a route

Each router calculates the SPF algorithm and determines the cost from its own perspective

### Link-State Routing Process

A link is an interface on a router

Information about the state of those links is known as link-states

All routers in an OSPF area will complete the following generic link-state routing process:

1. Each router learns about its own links and its own directly connected networks
2. Each router is responsible for “saying hello” to its neighbors on directly connected networks
3. Each router builds a Link-State Packet (LSP) containing the state of each directly connected link
4. Each router floods the LSP to all neighbors who then store all LSP’s received in a database
5. Each router uses the database to construct a complete map of the topology and computes the best path to each destination network

Then Network Convergence is reached.

#### Link and Link-States

The router first looks at all the interfaces configured in the configuration file and figures out the different links and states of those links

#### Say Hello

* Routers with link-state routing protocols use a Hello packet to discover neighbors on its links
* A neighbor is any other router that is enabled with the same routing protocol
* When two link-state routers learn that they are neighbors, they form an adjacency . These Hello packets continue to be exchanged between the two and serve as a keepalive function to monitor the state of the neighbor.
* If a router stops receiving Hello packets from its neighbor, that neighbor is considered unreachable and the adjacency is broken

#### Building the LSP

* Each router builds a link-state packet containing the state of each directly connected link

#### Flooding the LSP

* Each router floods its link-state information to all other link-state routers in the routing area.
* Whenever a router receives an LSP from a neighboring router, it immediately sends that LSP out all other interfaces except the one it arrived in.
* An LSP is sent:
  + During initial startup of the routing protocol process on that router
  + Whenever there is a change in the topology

#### Building the Link-State Database

* Each router uses the database to construct a map of the topology and computes the best path to each destination network
* Eventually, all routers receive an LSP from every other link-state router in the routing area. These are stored in the link-state database

#### Building the SPF Tree

* To begin the SPF algorithm interpress each router’s LSP to identify networks and associated costs
* The SPF algorithm then calculates the shortest paths to reach each individual network resulting in a SPF tree, which looks like the topology of the network.
* Each router constructs its own SPF tree independently from all other routers.
* To ensure proper routing, the link-state databases used to construct those trees must be identical on all routers.

### OSPF (Open Shortest Path First)

A link-state routing protocol that developed as a replacement for the distance vector routing protocol: RIP.

OSPF is a classless routing protocol that uses the concept of areas for scalability.

OSPFv2 is the current version with significant technical improvements over OSPFv1

OSPFv3 is the version for IPv6

#### Features of OSPF

* **Classless** - It is classless by design; therefore, it supports VLSM and CIDR
* **Efficient** - Routing changes trigger routing updates. It uses the SPF algorithm to choose the best path
* **Fast convergence** - It quickly propagates network changes
* **Scalable** - It works well with small and large network sizes. Routers can be grouped into areas to support a hierarchical system
* **Secure -** It supports Message Digest 5 (MD5) authentication. When enabled, OSPF routers only accept encrypted routing updates from peers with the same pre-shared password.

#### Components of OSPF

##### Data Structures

* + OSPF creates and maintains three databases
    - Adjacency Database - Creates the neighbor table
    - Link-state Database (LSDB) - Creates the topology table
    - Forwarding Database - Creates the routing table
  + These tables contain a list of neighboring routers to exchange routing information with and are kept and maintained in RAM

##### Routing Protocol Messages

* + OSPF exchanges messages to convey routing information using five types of packets
    - Hello packet
    - Database description packet
    - Link-state request packet
    - Link-state update packet
    - Link-state acknowledgment packet
  + These packets are used to discover neighboring routers and also to exchange routing information to maintain accurate routing information about the network

##### Algorithm

* + The CPU processes the neighbor and topology tables using Dijkstra’s SPF algorithm. The SPF algorithm is based on the cumulative cost to reach a destination
  + The SPF algorithm creates an SPF tree by placing each router at the root of the tree
  + Then it calculates the shortest path to each node.

#### Single-Area and Multiarea OSPF

To make OSPF more efficient and scalable, OSPF supports hierarchical routing using areas.

An OSPF area is a group of routers that share the same link-state information in their LSDBs

Can be implemented one of two ways:

* Single-Area OSPF - all routers are in one area called the backbone area (Area 0)
* Multiarea OSPF - All areas must connect to the backbone area (Area 0). Routers interconnecting the areas are referred to as Area Border Routers (ABR)

With multiarea OSPF, OSPF can divide one large autonomous system (AS) into smaller areas.

### OSPF Packets

* Type 1: Hello packet - Used to establish and maintain adjacency with other routers
  + Hello packets are sent at an interval that is used as an keepalive function
  + If the router doesn’t get a response in some time it will declare the neighbor dead and remove it from the adjacency table
* TYpe 2: Database Description (DBD) packet - Contains an abbreviated list of the sending router’s LSDB for the receiving router to check against their LSDB to make sure that all the Link State Databases across the routers are the same
* Type 3: Link-State Request (LSR) packet - Receiving routers can then request more information about any entry in the DBD by sending an LSR
* Type 4: Link-State Update (LSU) packet - Used to reply to LSRs and to announce new information. LSUs contain seven different types of LSAs
* Type 5: Link-State Acknowledgment (LSAck) packet - When an LSU is received, the router sends an LSAck to confirm receipt of the LSU. The LSAck data field is empty.

### Router IDs

A router ID is an IP address assigned to identify a specific router among OSPF peers

When a neighboring OSPF enabled router receives a Hello packet with a router ID that is not within its neighbor list, the receiving router attempts to establish an adjacency with the initiating router

Every router requires a router ID to participate in an OSPF domain.

The router ID is used by the OSPF-enabled router to:

* Uniquely identify the router - The router ID is used by other routers to uniquely identify each router within the OSPF domain and all packets that originate from them
* Participate in the election of the DR - In a multiaccess LAN, the election occurs during the establishment of the OSPF network. When OSPF links become active, the routing device configured with the highest priority is elected the DR. Assuming there is no priority configured, or there is a tie, then the router with the highest router ID is elected the DR. The routing device with the second highest router ID is elected the BDR.

The router can derive the router ID based on one of three criteria, in the following preferential order:

* The router ID is explicitly configured using OSPF `router-id <rid>` The rid value is any 32-bit value expressed as an IPv4 address.
* If the router ID is not explicitly configured, router chooses highest IPv4 address of any of configured loopback interfaces.
* If no loopback is configured, then the router chooses highest active IPv4 address of any of its physical interfaces.

### Commands for Configuring OSPF

##### Enter and Enable OSPF Configuration:

Just like you used `router rip` to enter the configuration mode for RIP you have to use `router ospf <process-id>` in global configuration mode. The process-id value is locally significant and represents a number between 1 and 65,535. It does not have to be the same value on the other OSPF routers to establish adjacencies with those neighbors.

##### Configuring Router ID

Use the `router-id <rid>` and assign an IPv4 address.

##### Advertise Networks:

Use the `network <network-address>` to advertise all the networks connected to the router.

##### Verifying the Router ID

Use `show

## Access Control Lists (ACLs)

### Module 13

#### Access Control Lists

* + Spot traffic or permit only specific traffic on networks
  + A sequential list of the permit or deny statements that apply to addresses or upper-layer protocols

#### What is an ACL?

* + Series of IOS commands that control whether a router forwards or drops packets based on information found in the packet header

#### When configured they perform these tasks:

* + Limit network traffic to increase network performance
  + Provide traffic flow control
    - Restrict the delivery of routing updates
      * If updates aren’t required because of network conditions, bandwidth is preserved
  + Provide a basic level of security for network access
    - Allow one host to access part of the network and prevent another
  + Filter traffic
  + Screen hosts to permit or deny access to network services.

#### By default, a router doesn’t have ACLs configured

* + Doesn’t filter traffic
    - Traffic that entered is solely based on information within the routing table

#### TCP Conversation

* + TCP Communication
    - Requests data, IP manages the communicator between the PC (source) and the server (destination). TCP manages the communications between the web browse an (application) and the network server software
  + TCP is responsible for breaking data down into segments
  + Provides a connection-oriented, reliable, byte stream service.
    - Connection-oriented = two applications must establish a TCP connection prior to exchanging data.
  + TCP is a full-duplex protocol
    - Each connection supports a pair of byte streams, each stream flowing on one direction
      * Includes a flow control mechanism for each byte (limit how much data the sender can transmit)
    - Implements a congestion-control mechanism

#### Packet Filtering

* + Packet filtering(static packet filtering) controls access to a network by analyzing the incoming and outgoing packets and passing or dropping them based on given criteria
    - Source IP address
    - Destination IP addresses
    - Protocol carried within the packet
* A router acts as a packet filter
* Layer 4 = transport layer
* A router can filter packets based on the source port and destination port of the TCP or UDP segment. (Defined using ACLs)

#### ACEs also called ACL. ACEs can be created to filter traffic based on certain criteria

* + Source address
  + Destination address
  + The protocol
  + Port numbers

#### To evaluate network traffic, the ACL extracts the following info from the Layer 3 packet header:

* + Source IP address
  + Destination IP address
  + ICMP message type

#### ACL also extracts upper layer info from Layer 4 header:

* + TCP/UDP source port
  + TCP/UDP destination port

#### ACL Operation

* + Define the set of rules that give added control for packets that enter inbound interfaces, packets that relay through the router, and packets that exit outbound interfaces of the router.
  + ACLs configured to apply to inbound traffic or apply to outbound traffic
    - Inbound ACLS:
      * Incoming packets are processed before routed to the outbound interface. An inbound is efficient since it saves the overhead of routing loops if the packet is discarded.
      * Best used to filter packets when the network attached to an inbound interface is the only source of the packets
    - Outbound ACLs
      * Incoming packets are routed to the outbound interface. Processed through the outbound ACL
      * Bes used when the same filter will be applied to packets coming from multiple inbound interfaces before exiting the same outbound interface
  + The last statement of ACL is an implicit deny.
    - Statement automatically inserted at the end of each ACL
    - Implicit deny blocks all traffic
    - An ACL that doesn’t have one permit statement will block on traffic

#### Types of Cisco IPv4 ACLs

* + Two types: Standard and extended
  + Standard
    - Used to permit or deny traffic only from source IPv4 addresses.
      * Destination of the pack/ports are not evaluated
      * Created in global config mode
  + Extended
    - Filter IPv4 packets based on:
      * Protocol type
      * Source IPv4 address
      * Destination IPv4 address
      * Source TCP or UDP ports
      * Destination TCP or UDP ports
      * Optional protocol type information for finer control

#### Numbering and Naming ACLs

* + Usinger numbered is effective for determining ACL type on smaller networks
    - Does not provide information about the purpose of ACL
  + Numbers 200 to 1299 are off limits because they are used by other protocols (legacy or obsolete)

#### Introducing ACL Wildcard Masking

* + IPv4 ACEs have wildcard masks
    - A string of 32 binary digits used by a router to determine which bits of the address to examine for a match
  + 1 and 0 identify how to treat corresponding IP address bits
  + Subnet = binary
    - Identify network, subnet, host of an IP
  + Wildcat uses binary
    - Filter individual IP addresses or groups of IP addresses to permit or deny access to resources
  + Wildcard mask bit 0 = match the corresponding bit value in the address
  + Wildcard mask bit 1 = ignore the corresponding bit value in the address
    - (Inverse mask)

#### General Guidelines for Creating ACLs

* + Using ACLs in firewall routers positioned between your internal network and an external network such as the Internet
  + Use ACLs on a router positioned between two parts of your network to control traffic entering or exiting a specific part of your internal network
  + Configure ACLs on border routers, that is, routers situated at the edges of your networks This provides a very basic buffer from the outside network, or between a less controlled area of your own network and a more sensitive area of your network
  + Configure ACLs for each network protocol configured on the border router interfaces
  + Configure ACL per protocol, per direction, per interface
    - One ACL per protocol
      * To control traffic flow on the interface. Must be defined for each protocol and enabled on the interface
    - One ACL per direction
      * Control traffic in one direction at a time. Two separate ACLs to control inbound and outbound traffic
    - One ACL per interface
      * Control traffic for interface

#### Where to Place ACLs

* + Extended ACLs
    - Locate as close as possible to the source of traffic to be filtered (undesirable traffic is closer to the source network without crossing the network infrastructure
  + Standard ACLS
    - Close to the destination. Effectively prevent traffic from reaching any other network
  + Can also Depend on:
    - The extent of network admin control
    - Bandwidth
    - Ease of configuration
  + Standard
    - As close as possible to the destination network

#### Extended ACLs

* + Extended IPv4 ACLS can be used for more precise traffic-filtering control
    - Number 100 to 199 and 2000 to 2699
      * 799 possible extended numbered ACLS
  + Used more often than standard ACLS
    - Greater degree of control
  + Extended ACLS check:
    - Source addresses of packets
    - Destination address
    - Protocols
    - Port numbers (or services)
  + Testing for Ports and Services
    - Filter on protocol and port number allows network admin to build specific extended ACLS
      * Can be specified by configuring port number or name of a well-known port

#### Configuring Extended ACLs

* + Same as standard
  + First configured then activated on an interface

#### Inbound and Outbound ACL Logic

* + Inbound
    - When information in a packet header and an ACL statement match, the rest of the statements in the list are skipped
      * The packet is permitted or denied as specified by the matched statement
    - If the header doesn’t match the statement the packet is tested against the next statement.
    - ACL statement
      * At the end of the statement there is an ‘implicit deny any statement’
        + Not shown in output
      * Final implied statement applied to all packets for which conditions did not test true
    - Final Test Statement
      * Matches all other packets and results in a ‘deny’ action
        + Instead of proceeding in or out of an interface, the router drops all of these remaining packets
      * Final statement or ‘implicit deny any statement’ or ‘deny all traffic’ statement
    - An ACL should have 1 permit statement otherwise all traffic is blocked
  + Outbound
    - Before packet is forwarded to an outbound interface, router checks the table to see if the packet is routable
      * If not routable, it is dropped and not tested against ACEs
      * Router checks to see if outbound interface is grouped in an ACL
        + If not grouped, the packet can be sent to output buffer
    - Outbound ACL Operation
      * No ACL applied to interface
        + Not grouped to an outbound ACL packet is sent directly to outbound interface
      * ACL applied to the interface
        + If grouped to an outbound ACL, the packet is not sent out on the outbound interface until tested by ACEs that are associated with the interface

Based on the ACL test the packet is permitted or denied

\*Permit = send packet to output buffer

\*Deny = discard packet

#### ACL Logic Operations

* + When packet arrives at router interface, the process is the same whether ACLs are used or not
    - As frame enters the router checks to see the destination Layer 2 address matches its interface Layer 2 address or if its broadcast frame
  + If frame address is accepted, the information is taken off and router checks for ACL on inbound
    - If exists packet is tested against the statements in list
  + If packet matches statement, either permitted or denied
    - Accepted: then checked against routing table to determine destination
      * If routing table exists for destination packet is then switched to outgoing interface, or the packet will drop
    - Router checks outgoing interface has an ACL
      * If exists, packet is tested against statements
        + If packet matches it is permitted or denied
      * If no ACL or packet is permitted, the packet is encapsulated in the new Layer 2 protocol and forwarded out the interface to the net device.

#### Standard ACL Decision Process

* + Standard only examine the source IPv4 address
    - Destination and ports aren’t considered

#### Extended ACL Decision Process

* + Built to filter on source and destination addresses, protocol and port numbers

#### Type of IPv6 ACLs

* + Similar to IPv4 both operation and configuration.
  + Only 1 type of ACL
    - Equivalent to extended in IPv4
  + No numbered ACLs
  + Summary:
    - Named ACLs only
    - Equivalent to the functionality of an IPv4 Extended ACL
  + IPv4 and IPv6 can’t share the same name
  + Comparing IPv4 and IPv6
    - Three Major Differences
      * Applying an IPv6 ACL
      * No Wildcard masks
        + IPv6 ACLs do not use wildcard masks. Preix-length is used to indicate an IPv6 source or destination address
      * Additional Default Statements
        + Two implicit permit statements at the end of each IPv6 access list

#### Summary

* + A default router does not filter traffic. It enters solely based on information within a routing table
  + Packet filtering controls access to a network by analyzing the incoming and outgoing packets and passing or dropping them based on criteria
    - IP address
    - Destination IP addresses
    - Protocol carried within packet
  + ACL
    - A sequential list of permit or deny statements
      * Last statement is always an implicit deny which blocks all traffic
    - When network goes through an interface with an ACL, router compares information ithin packet against each entry in sequential order and determines if the packet matches one of the statements
      * If found the packet proceeds
    - ACLS are configured to apply inbound traffic or outbound traffic
  + Standard ACLs
    - Used to permit or deny traffic only from a source IPv4 address
      * Destination of packet and ports are not evaluated
    - Place close to destination
  + Extended ACLs
    - Filter packets based on:
      * Protocol type
      * Source
      * Destination IPv4 address
      * Source or destination ports
    - Place close to source

### Commands for ACLs

#### Standard Numbered ACLs

To configure an ACL run the following command in Global Configuration Mode:

`access-list <access-list-number> { deny | permit } <source-ip-addr> [ <source-wildcard> ] [log]

Access-list-number has to be a number 1-99 or 1300-1999

Use the keyword any in place of source-ip-addr to use any ip-addr

To add a remark/comment to an ACL run the following command in Global Configuration Mode:

`access-list remark <remark>`

To enable an access list, go to the interface configuration mode for the interface the ACL will reside on and run the following command:

`ip access-group <access-list-number> {in | out}

The above global commands are considered old-style configuration commands. A new style is by using the command for Named ACLs but using a number instead of a name there.

IOS will still store all the new-style commands as old-style commands.

#### Extended Numbered ACLs

Note: the access-list-number for extended numbered ACLs have to be between 100-199 or 2000-2699

To configure an ACL using only source IP and destination IP with wildcard masks run the following command in Global Configuration Mode:

`access-list <access-list-number> { deny | permit } <packet-type> <source-ip-addr> <source-wildcard> <destination-ip-addr> <destination-wildcard> [log]

When configuring an extended ACL to deny or permit a specific ip address make sure you put host before it like so:

‘access-list 1 deny ip host 192.168.0.1 host 192.168.0.2’

When using a packet-type of UDP or TCP you can also use source and destination ports with this command:

`access-list <access-list-number> {deny | permit } { tcp | udp } <source-ip-addr> <source-wildcard> [ { eq | ne | lt | gt | range} <source-port> ] <destination-ip-addr> <destination-wildcard> [ { eq | ne | lt | gt | range} <destination-port> ] `

Either of the ports are optional.

To add a remark/comment to an ACL run the following command in Global Configuration Mode:

`access-list remark <remark>`

To enable an access list, go to the interface configuration mode for the interface the ACL will reside on and run the following command:

`ip access-group <access-list-number> {in | out}

#### Named ACLs

To create a named ACL run the following command in Global Configuration Mode:

`ip access-list { standard | extended } <name>`

That sends you into ACL configuration mode. In there you can do the same access-list commands as before minus the access-list keyword. You can write the same permit, deny, or remark commands as above in the same format as a standard ACL or extended ACL depending on your configuration

To remove a line, you have to copy the line and put `no` before it to remove it.

Editing an ACL can also be done with sequence numbers.

To create a new line with a sequence number, just put the sequence number before the permit or deny command

To remove a line with a sequence number just do: `no <sequence-number>`

The above editing commands work for named and numbered ACLs

#### Troubleshooting and Verifying ACLs

`show running-config` and look for ip access-group commands under each interface

`show ip interfaces` to find which ACLs are enabled on which interfaces

Then do the more specific `show ip interface <interface>`

`show access-lists` or `show ip access-lists` to show the configuration of an ACL; the latter shows only IP Access Lists.

## Network Address Translation for IPv4

### Module 15

#### Introduction

* + All IPv4 addresses that traverse the internet must be registered with Regional Internet Registry (RIR)
  + Can lease public addresses from an ISP
  + Solutions
    - IETF
    - Network Address Translation (NAT)
    - RFC 1918 private IPv4 addresses

#### IPv4 Private Address Space

* + Private Addresses
    - Within organization to allow devices to communicate locally
    - Can’t be routed over internet
    - To allow a private IPv4 address
      * Private address must first be translated to a public address
  + NAT provides translation of private to public addresses
  + Private IPv4 address to access resources outside of the network

#### What is NAT

* + It conserves public IPv4 addresses
    - Allows networks to use private IPv4 addresses internally
  + NAT - enabled
    - router can be configured with 1 or more valid public addresses
      * Known as NAT pool
    - Internal device sends traffic out the router translates the internal address to public address
  + NAT router operates at border of stub network
    - Stub network
      * Network with a single connection to its neighboring network
        + 1 way in and 1 way out
  + Device inside stub network wants to communicate outside
    - Packet is forwarded to border router
      * Performs the NAT process

#### NAT Terminology

* + Four types of addresses
    - Inside local address
      * Address of source as seen from inside the network
        + Ex: 192.168.10.10 assigned to PC1
    - Inside global address
      * Address of source as seen from outside network
    - Outside local address
      * Address of destination seen from inside network
    - Outside global address
      * Address of destination as seen from outside network
      * Most local and outside global address are the same
  + Inside address is the address of the device being translated by NAT
  + Outside address is the address of the destination device
  + Local address is any address that appears on the inside portion of network
  + Global address is any address that appears on the outside of the network

#### Static NAT

* + Three types of NAT translation
    - Static address translation
      * 1 to 1 address mapping between local and global addresses
    - Dynamic Address translation
      * Many to many between local and global
    - Port Address Translation
      * Many to 1 between local and global. Also known as overloading
  + Static nat is 1 to 1 and are configured by network administrator and remain constant
  + Requires that enough public addresses are available to satisfy the total number of user sessions

#### Dynamic NAT

* + Uses pool of public address to assign, first come first serve

#### Port Address Translation (PAT)

* + Multiple private IPv4 addresses to single public addresses
  + Most home routers
  + ISP assigns 1 address to router
  + Each private address is tracked by port number.
    - Device initiates TCP/IP session
      * Generates TCP or UDP source port
  + PAT ensures that devices use different TCP port number for each session
    - Response comes back from server, source port number becomes destination port number on return trip
      * Determines which device the router forwards the packets
  + Validates incoming packets were requested

#### Next Available Port

* + PAT attempts to preserve original source port
    - If already used than port number is assigned from appropriate group
      * 0-511
      * 512-1023
      * 1024-65535
    - No more ports and no more than 1 external address, PAT moves to the address to try to allocate original source port

#### Benefits of NAT

* + Conserves legally registered addressing by allowing privatization of intranets
    - Conserves addressing through application port-level multiplexing
  + Increases flexibility of connections
    - Multiple pools
    - Backup pools
    - Load balancing pools
  + Provides consistency for internal network addressing schemes
  + Provides network security
  + Conserves the legally registered addressing scheme
  + Increases the flexibility of connections to the public network
  + Provides consistency for internal network addressing schemes
  + Provides network security

#### Disadvantages of NAT

* + Performance is degraded
  + End to end functionality is degraded
  + End to end IP traceability is lost
  + Tunneling becomes more complicated
  + Initiating TCP connections can be disrupted
  + NAT increases witching delays between translation of each address within packet headers

#### Configuring Static NAT

* + Step 1
    - Create a mapping inside local address and inside global address
  + Step 2
    - After mapping, interfaces participate in the translation of inside or outside relative to NAT

#### Dynamic NAT Operation

* + Static provides permanent mapping between inside local and inside global
  + Dynamic has automatic mapping on inside local and inside global
  + Uses a group, or pool of public IPv4 addresses for translation
  + Requires configuration of inside and outside interfaces

#### Configuring PAT: Address Pool

* + PAT (NAT overload) conserves addresses in the inside global address pool by allowing the router to use one inside global address for many inside local address
    - Single public IPv4 address can be used for a lot of internal private IPv4 address
  + Router maintains enough info from higher-level protocols (TCP or UDP port numbers) in order to translate the inside global back into inside local

#### Single Address

* + Step 1
    - Define ACL to permit traffic translation
  + Step 2
    - Configure source translation
  + Step 3
    - Identify which interfaces are inside
  + Step 4
    - Identify the interfaces outside

#### Port Forwarding

* + Tunneling
  + The act of forwarding traffic addressed to a specific network port from one network node to another
    - Allows external user to reach port on private IPv4 address from outside
  + Port forwarding allows users on internet to access internal servers by using WAN port

#### Troubleshooting NAT

* + Step 1
    - Define what NAT is suppose to achieve
  + Step 2
    - Verify correct stranslations
      * Show ip nat translations
  + Step 3
    - Use clear and debug command to verify NAT is operating
      * Check dynamic entries
  + Step 4
    - Review what's happening to packet

#### Debug command

* + Debug ip nat
    - Verifies the operation of NAT feature by showing info about every packet
  + Debug ip nat detailed
    - Generates description of each packet
    - Provides info about certain errors
  + Output of command
    - \* = indicates that the translation is occuring in the fast switched past
      * First packet is always process-switched (slower) remaining packets go through fast switched
    - s = - Source of IP address
    - A.b.c.d ----> w.x.y.z - Indicates source address translated to
    - d= - Destination IP address
    - [xxxx] = Value inside is IP identification number

#### Summary

* + NAT is used to alleviate the depletion of IPv4 address space
    - Allows network admin to ue RFC 1918 private address space while providing internet
      * Single or limited number of public addresses
  + Conserves public address space
  + NAT and PAT can be implemented to conserve public address space and build private secure intranets without affecting ISP
  + Drawbacks
    - Negative effects on
      * Device performance
      * Security
      * Mobility
      * End to end connectivity

### Commands for NAT

Use the command: `ip nat inside` in interface configuration mode to specify which interface is the inside local interface

Use the command: `ip nat outside` interface configuration command to specify which interface is the inside global interface

#### Static NAT

Use the following global configuration command to map an inside local private ip address to a public inside global ip address:

`ip nat inside source static <local-ip-address> <global-ip-address>`

#### Dynamic NAT

Use the following global configuration command to configure pools and how to configure the ACL.

1. Configure an pool of ip addresses for the NAT to use. Use the following command:
   1. `ip nat pool <name> <start-address> <end-address> { netmask <mask-address> | prefix-length /<prefix-length> }
   2. In the ACL just do a permit on all the different ip local addresses
   3. Lastly run the following command:
      1. `ip nat inside source list { <acl-number> | <acl-name> } pool <pool-name>`

#### PAT

The first steps are the same as dynamic NAT but you have 2 options. If you have a pool of addresses run the following command:

`ip nat inside source list { <acl-number> | <acl-name> } pool <pool-name> overload`

If you have only one inside global then run the following command:

`ip nat inside source list { <acl-number> | <acl-name> } interface <interface> overload`

#### Troubleshooting and Verifying

`show ip nat translations`

`show ip nat statistics`

To clear all NAT entries run the following command:

`clear ip nat translation \*`

To clear certain IP NAT entries:

`clear ip nat translation inside <global-ip> <local-ip>`

`clear ip nat translation outside <local-ip> <global-ip>`

To clear the ports:

`clear ip nat translation <protocol> inside <global-ip> <global-port> <local-ip> <local-port>`

`clear ip nat translation <protocol> outside <local-ip> <global-ip>`

To enable debugging:

`debug ip nat`

## Dynamic Host Configuration Protocol (DHCP)

### Module 14

#### Introduction for DHCPv4

* + DHCPv4 assigns IPv4 addresses and other network configuration info dynamically
  + A dedicated DHCPv4
    - Scalable
    - Relatively easy to manage
  + DHCPv4 has three different address allocation mechanism to provide flexibility
    - Manual Allocation
      * Admin assign a pre-allocated IPv4 address
      * Communicates only the IPv4 address to the device
    - Automatic Allocation
      * Assigns a static IPv4 address automatically and permanently
        + Selecting from a pool of available addresses
      * No lease and the address is permanently assigned
    - Dynamic Allocation
      * Dynamically assigns or leases an IPv4 address from pool of addresses for a limited amount of time chosen by server or until the client doesn’t need it.
  + Dynamic allocation is the most commonly used DHCPv4 mechanism
    - Clients lease info from server for a defined time

#### DHCPv4 Operation

* + Works in client/server mode
  + Client communicates with DHCPv4 server, server assigns or leases IPv4 address to the client
  + Client connects to network with the leased IP address until it expires
  + Client must contact the server to extend the lease
  + DHCP Discover (DHCPDISCOVER)
    - Finds DHCPv4 servers on network. No valid IPv4 info at bootup it uses Layer 2 and Layer 3 broadcast addresses to communicate
  + DHCP Offer (DHCPOFFER)
    - When server receives DHCPDISOCVER message, reserves an addresses to lease
    - Server creates an ARP entry with a MAC address of the requesting client and leased IPv4 of client
  + DHCP Request (DHCPREQUEST)
    - When clients gets an offer it sends back a request message. Used for lease origination and lease renewal.
      * When used for lease origination the request serves as a binding acceptance
  + DHCP Acknowledgement (DHCPACK)
    - When a request message is received the server verifies the lease with ICMP ping and create a new ARP for the client lease and replies with DHCPACK message
      * DHCPACK message is a duplicate of DHCPOFFER, expect with a change in message type field.

#### DHCPv4 Message Format

* + This format is used for all transactions
    - DHCPv4 messages are encapsulated within UDP transport protocol
    - Message sent from client use UDP source port 68 and destination port 67
    - Server to client uses the same ports
  + Fields
    - Operation (OP) Code
      * Specifies the type of message
      * Value 1 = request message
      * Value 2 = reply message
    - Hardware Type
      * Identifies type of hardware in network
      * Same codes used in ARP messages
    - Hardware Address Length
      * Specifies length of address
    - Hops
      * Control forwarding messages
      * Set to 0 before transmitting a request
    - Transaction Identifier
      * Used by client to match request with replies received from server
    - Seconds
      * The number of seconds elapsed since client attempted to renew/acquire lease
      * Prioritizes replies
    - Flags
      * Used by client during lease renewal when address is valid and usable
    - Your IP address
      * Used by server to assign IPv4 address to client
    - Server IP address
      * Used by server to identify address of the server that the client should use for next step
    - Gateway IP address
      * Routes DHCPv4 messages when relay agents are involved.
      * Gateway address facilitates communications of requests and replies
    - Client Hardware Address
      * Specifies the physical layer of the client
    - Server Name
      * Used by server sending an offer and a DHCPACK.
    - Boot Filename
      * Optinional
      * Used by client to request a particular type of boot file in discover message.
      * Used by server for DHCPOFFER to fully specify boot file directory and filename
    - DHCP Options
      * Holds DHCP options
        + Parameters for required DHCP operation
        + Variable length
      * Used by client and server

#### DHCPv4 Discover and Offer Messages

* + Client is configured to receive IPv4 settings dynamically
    - Requests addressing values from DHCPv4 server
    - Client transmits DHCPDISCOVER on local network
      * This message is an IPv4 broadcast
        + Destination IPv4 address of 255.255.255.255
      * Client hasn’t configured, IPv4 address is 0.0.0.0
  + DHCPv4 server gets a DHCPDISCOVERR
    - Responds with DHCPOFFER
      * Contains initial configuration info
        + IPv4 address
        + Subnet mask
        + Lease duration
        + IPv4 address of DHCPv4 server making offer
      * Can have other information (configured)
        + Lease renewal time
        + DNS address
  + DHCP server responds to DHCPDISCOVER by assigning values to CIADDR and subnet mask
    - Frame is constructed using CHADDR (client hardware address)
      * Sent to requesting client

#### Configuring a Basic DHCPv4 Server

* + Step 1: Excluding IPv4 Addresses
    - DHCPv4 Server assigns all IPv4 address in a DHCPv4 address pool
      * Excluding specific addresses
        + Ip dhcp excluded-address
    - Single address or range can be excluded (low-address and high-address range)
  + Step 2: Configuring a DHCPv4 Pool
    - Ip dhcp pool pool-name
      * Creates a pool with specific name and puts router into DHCPv4 configuration mode
        + Identified: Router (dhcpconfig)#
  + Step 3: Configuring Specific Tasks
    - Address pool and default gateway router must be configured
      * Network statement to define the range of addresses
    - Define default gateway router
      * Default-router
    - Typically gateway
      * LAN interface
      * 1 gateway is required
        + Up to 8 addresses if multiple gateways
  + Disabling DHCPv4
    - Service is enabled by default
      * To disable: no service dhcp
        + global config mode
      * Service dhcp
        + Global config mode
        + Re-enabling DHCPv4 server process
      * Enabling service has no effect if parameters are not configured

#### Verifying DHCPv4

* + Show running- config | section dhcp
    - Displays DHCPv4 commands configured
  + Operation of DHCPv4
    - Show ip dhcp binding
      * Displays a list of IPv4 address to MAC address bindings that have been provided by server
  + Show ip dhcp server statistics
    - Verify messages are being received or sent by router
      * Displays count info regarding the number of DHCPv4 messages that are being sent and received

#### DHCPv4 Relay

* + A hierarchical network made up of servers located on a server farm
    - May provide
      * DHCP
      * DNS
      * TFTP
      * FTP
  + Ipconfig /release
    - Renew its IPv4 address, the address is released and the address is 0.0.0.0
  + Ipconfig /renew
    - A DHCPDISCOVER message is broadcasted
  + Admin needs to add DHCPv4 serves on subnets
  + Configure CISCO IOS helper address
    - Enables router to forward broadcasts to server

#### Configuring a Router as DHCPv4 Client

* + Configure ethernet interface on DHCP client
    - Ip address dhcp
      * Interface config mode

#### Configuring a Wireless Router as a DHCPv4 Client

* + Connect to ISP using DSL or cable modem
  + Set to receive IPv4 addressing info automatically from ISP

#### Troubleshooting Tasks

* + Task 1: Resolve IPv4 Address Conflicts - Resolve address conflicts
    - Lease can expire on client but still be connected
    - If the lease isn’t renewed
      * DHCPv4 server can reassign the address to someone else
    - Show ip dhcp conflict
      * Displays all address conflicts
    - Client uses Address Resolution Protocol (ARP) to detect conflicts
  + Task 2: Verify Physical Connectivity - Verify physical connectivity
    - Show interfaces interface
      * Confirms router interface is acting as default gateway
  + Task 3: Test Connectivity using a Static IP Address - Test with a static IPv4 address
    - Verify network connectivity by configuring static IPv4 address info on client workstation
  + Task 4: Verify Switch Port Configuration - Verify switch port configuration
    - Client is unable to get an address on startup, get address by manually forcing a DHCPv4 request to be sent
  + Task 5: Test DHCPv4 Operation on the Same Subnet or VLAN - Test from the same subnet or VLAN
    - When client is on same subnet or VLAN as the DHCPv4 server
* Verify Router DHCPv4 Configuration
  + When server is on a separate LAN, router interface facing client must be configured to relay requests
  + Step 1
    - ip helper-address
      * Configured on correct interface
      * Must be directed to the correct DHCPv4 server
    - Show running-config
      * To check
    - Show ip interface
      * Verify DHCPv4 relay on interface
  + Step 2
    - No service dhcp
      * Global configuration
      * Has not been configured
      * Disables all DHCP server and relay functionality on router
    - Service dhcp
      * Default configuration

#### Debugging DHCPv4

* + Router configured as DHCPv4 server, without requests from client is fails
    - Verify router is receiving requests
  + Typical ports when sending messages
    - 67 and 68
  + Extended ACL displays only DHCPv4 messages
    - Debug ip packet
  + Debug ip dhcp server events
    - Reports server events

#### Summary

* + All nodes on network need a unique IP address to communicate
  + Static assignment of IP addressing info on large network results in administrative burden, eliminated by DHCPv4 and DHCPv6
  + DHCPv5
    - Three different address allocation mechanisms
      * Manual Allocation
        + Admin assigns pre-allocated address and DHCPv5 communicates only with the address
      * Automatic Allocation
        + DHCPv4 automatically assigns static address permanently to device

From pool of available devices

* + - * + No lease and address is permanent
      * Dynamic Allocation
        + Dynamically assigns or leases an address from pool with a limited period of time
    - Dynamic is most common and involves the exchange of several packets
    - Messages from client
      * DHCPDISCOVER and DHCPREQUEST
      * Broadcasted to allow servers on network to hear the request for addressing info
    - Messages from server
      * DHCPOFFER and DHCPACK
        + Sent as unicasts directly to client

### Commands for DHCP

#### DHCP Relay

When the DHCP server is on a different subnet or not in the same LAN as the clients then the router connected to the clients has to have this command run on all interfaces that have a client connection required:

`ip helper-address <ip-addr>`

#### DHCP Router Server

You can also configure a router to be a DHCP server with the following commands. The first two:

1. `ip dchp excluded-address <start-ip> <end-ip>`
2. `ip dchp pool <name>` <- that command sends you into DHCP configuration mode
3. `network <subnet-ID> <netmask>` or `network <subnet-ID> <prefix-length>`
4. `default-router <addr1> [ <addr2> ]`
5. `dns-server <addr1> [ <addr2> ]`
6. `lease <days> <hours> <minutes>`
7. `domain-name <name>`
8. `next-server <ip-address>` <- this is for a TFTP server for IP phones

#### Troubleshooting and Verifying

`show ip dhcp binding` <- shows the different IP addresses assigned

`show ip dhcp pool <pool-name>` <- shows the information about the pool

`show ip dhcp server statistics` <- gives statistics about the server

`show ip interface <interface>` <- can you show the helper address set on the interface

`show ip dhcp conflict` <- will show any conflicts between the same IP address being used.

## Securing Network Devices

### Module 16

#### Securing the Network Infrastructure

* + Infrastructure includes routers, switches, servers, endpoints and others
  + Shoulder surfer
    - Easy way for an attacker to gain unauthorized access
  + Routers are the primary target
  + Edge router
    - Last router between the internal network and un untrusted network (internet)
    - All internet traffic goes through edge router, first and last line of defense.

#### Implementing Security

* + Single router Approach
    - A single router connects the protected network or internal LAN to the Internet.
    - Security policies are configured on this device.
    - Commonly in smaller sites
    - The required security features can be supported by Integrated Services Routers (ISRs) without impeding the router’s performance capabilities
  + Defense-in-Depth Approach
    - More secure than single router approach
    - It has multiple layers of security prior to traffic entering the protected LAN
    - There are three primary layers of defense
      * Edge router, firewall, internal router that connects to the protected LAN
    - Edge Router = first line, also known as screening router. Passes all connections that are intended for the internal LAN to the firewall
    - Firewall = second line. Picks up where the edgerouter leaves off and performs more filtering. Provides additional access control by tracking the state of the connections and acts as a checkpoint
    - Edge router has specific rules on what traffic is allowed/denied
    - Default = firewall denies the initiation of connections from outside, untrusted, networks to the inside, trusted, network
      * Allows users to establish connections to untrusted networks, permits the responses to come back
      * Perform user authentication (authentication proxy), users must be authenticated to gain access to network resources
    - Intrusion Protection Systems (IPS) can also be used, not just routers
  + DMZ Approach
    - Similar to defense-in-depth, but includes demilitarized zone (DMZ)
      * Used for serves that must be accessible from the internet or some other external network
    - DMZ is set up between two routers
      * Internal: Connecting to the protected network
      * External: Connecting to unprotected network
    - Can also be an additional port off a single router
      * Firewall is located between the protected/unprotected networks.
        + Set up to permit required connections (HTTP)
      * Firewall serves as primary protection
      * Router provides protection by filtering some traffic, but leaving the bulk of it to firewall

#### Securing Routers

* + The edge router needs to be secure.
  + Physical Security
    - Put router and physical devices in locked room, accessible only to authorized personnel, free of electrostatic or magnetic interference, fire suppression, controls for temperature and humidity
    - Install UPS (uninterruptible power supply), keep spare component available
  + Operating System Security
    - Configure router with maximum amount of memory
      * Can protect from DoS attacks, and supporting the widest range of security services
    - Latest, stable version of operating system
    - Keep secure copy of router operating system image and router configuration file as backup
  + Router Hardening (unused ports and services)
    - Secure admin control. Make sure only authorized people have access
    - Disable the unused ports and interface. Less ways for a device to be accessed
    - Disable unnecessary services.

#### Secure Administrative Access

* + Admin access is required for router management purposes.
  + Restrict device accessibility
    - Limit access to ports, restrict the permitted communicators and restrict the permitted methods of access
  + Log and account for all access
    - Auditing purposes, record anyone who excessed device
  + Authenticate access
    - Ensure access is granted only to authenticated users, groups and services
    - Limit number of failed login attempts and time between login
  + Authorized actions
    - Restrict actions and views
  + Present legal notification
    - Display legal notice, developed in conjunction with company legal counsel, for interactive sessions
  + Ensure the confidentiality of data
    - Protect locally stored sensitive data from viewing and copying
    - Consider vulnerability of data in transit over a communication channel to sniffing, session hijacking and man-in-the-middle attacks (MITM)

#### Secure Local and Remote Access

* + Local Access
    - Network infrastructure devices can be accessed locally
    - Requires a direct connection to a console port on router using computer that is running terminal emulation software
    - Admin must have physical access to router and connect using a console cable to console port
    - Typically used for initially configuring a device
  + Remote Access
    - Admins have access to infrastructure remotely. Most common remote access involves Telnet, SSH, HTTP, HTTPS or SNMP
    - COmputer can be on same subnet or different subnet
    - Some protocols send data (usernames/passwords) in plaintext
      * Encrypt all traffic between admin computer and router
        + Telnet → SSH
        + HTTP → HTTPS
      * Establish dedicated management network
      * Management network only identified admins hosts and connections to dedicated interface on the router
      * Configure packet filter to allow identified admin hosts and protocols

#### Securing Administrative Access

* + Several network devices, a central terminal access controller access - control system Plus (TACACS+) or remote authentication dial in user service (RADIUS) authentication server, such as Cisco secure Access Control Server (ACS) should be used to store all admin usernames and passwords. Local database is al recommend as back up if access to an authentication, authorization and accounting (AAA) server is unavailable
  + Securing Local Access
    - Console port does not require a password for console admin access
    - Secure local access is configured using a console port line password
      * line console 0, followed by password and login subcommands
  + Securing Remote Access
    - Involves securing the vty lines and aux port
    - Cisco Routers support up to 5 simultaneous vty lines for Telnet or SSH
      * Vty ports are 0 - 4
        + line vty 0 4

Password and login

* + - Auxiliary port (aux port), dial up modem can also be used for remote access
      * Cisco auxiliary port doesn’t require a password
        + Secure = line aux 0

Password and login

* + Securing Privileged EXEC Mode Access
    - enable secret password in global configuration restricts access to privileged EXEC mode
      * Always hashed inside router configuration using a hashing algorithm
        + SHA256 hashing algorithm instead of weaker MD5 algorithm

#### Increase Password Security

* + To increase
    - Enforce minimum password lengths
    - Disable unattended connections
    - Encrypt all passwords in the configuration file
  + Minimum Character Length
    - Set minimum password length from 0 to 16
      * security passwords min-length length
        + Global configuration
      * Default is 6
      * Should be 10
  + Disable Unattended Connections
    - Default = stays active and logged in for 10 minutes after last session activity
      * exec-timeout minutes [seconds]
    - Disable EXEC process like aux port
      * no exec
  + Encrypt All Passwords
    - Enable secret
      * Cisco router passwords are stored in plaintext in the router startup and running configuration files
    - service password-encryption
    - Stop encrypting passwords, use no form of command, only passwords created after the no will be unencrypted

#### Configuring Secure Local Database Entries

* + username name password password
  + username name secret password
    - More secure, MD5 hashing
  + Console, vty and aux ports must be configured to require a username and password combination form the local database
    - Login command must be changed to login local

#### Enhancing the Login Process

* + Virtual Login Security Enhancements
    - Implement delays between successive login attempts
    - Enable login shutdown if DoS attacks are suspected
    - Generate system-logging messages for login detection
  + By enabling a detection profile, a network device can be configured to react to repeated failed login attempts by refusing further connection requests or login blocking. Configured for a period of time = quiet period

#### Configuring Login Enhancement Features

* + By enabling the login process with the following specific parameters
    - Delays between successive login attempts
    - Login shutdown if DoS attacks are suspected
    - Generation of system login messages for login detection
  + To enhance login features
    - Router(config)# login block-for seconds attempts tries within seconds
    - Router(config)# login quiet-mode access-class { acl-name | acl-number }
    - Router(config)# login delay seconds
    - Router(config)# login on-success log { every login }
    - Router(config)# login on-failure log { every login }

#### Enable Login Enhancements

* + To provide DoS detection
    - login block-for, which must be configured to enable login enhancements. All other enhancement features are disabled until the command is configured
  + Operates in two modes
    - Normal mode
      * Watch mode, router keeps count of the number of failed login attempts within an identified amount of time
    - Quiet mode
      * Quiet period, number of failed logins exceeds the configured threshold, all login attempts using Telnet, SSH and HTTP are denied for the time specified in the login block-for command
        + When enabled, all login attempts including valid admin access are not permitted
        + login quiet-mode access-class
  + Default, Cisco accept connections such as Telnet, SSH and HTTP.
  + Delay time between login attempts using login delay

#### Logging Failed Attempts

* + Commands that can be configured to help an admin detect a password attack. Enables a device to generate syslog messages for failed or successful login attempts
    - login on-success and login on-failure log
      * Generates syslog messages for failed login requests.
    - security authentication failure rate
      * Configured to generate a log message when the login failure rate is exceeded
    - show login to verify login block-for
      * Command settings and current mode. Router is in either normal or quite mode, depending on whether login thresholds were exceeded

#### Provide Legal Notification

* + Banner messages present legal notification to potential intruders
  + Banners are disabled by default
    - Banner global configuration
* Configuring Before SSH is implemented
  + Usually remote access was configured on routers using Telnet on TCP port 23
    - Telnet traffic is forwarded in plaintext
  + SSH has replaced Telnet
    - Functionality that is similar to an outbound telnet connection, but the connection is encrypted and operates on port 22
      * Authentication and encryption
  + Prior to configuring routers
    - Ensure target routers are running IOS supporting SSH
    - Ensure each router has a unique hostname
    - Ensure each target routers use correct domain name of network
    - Target routers configured for local authentication or AAA services
* Connecting to an SSH-Enabled Router
  + Two ways to connect
    - Connect using SSH-enabled cisco router
    - Connect using a publicly and commercially available SSH client running on host
* Limiting Command Availability
  + Security Operator Privileges
    - Configure AAA
    - Issue show commands
    - Configure firewall
    - Configure IDS/IPS
    - Configure NetFlow
  + WAN engineer privileges
    - Configure routing
    - Configure interfaces
    - Issue show commands
* Privilege Levels
  + 16 privilege levels: 0, 1, 15 have predefined settings
    - 0 = Predefined for user-level access privileges.
      * Disable, enable, exit, help and logout
    - 1 = Default level for logging with the router prompt. User can’t make any changes or view the running configuration file
    - 2 - 14 = May be customized for user-level privileges
    - 15 = Reserved for the enable mode privileges. Users can change configuration and view configuration files
* Configuring Privilege LEvels
  + A USER account is level 1 and does not include ping
  + SUPPORT account requiring all level 1 and 5 access, plus ping command
  + JR-ADMIN account requires all level 1 and 5 access plus reload command
  + An ADMIN account requires complete access
* Limitations of Privilege Levels
  + No access control to specific interfaces, ports, logical interfaces and slots on routers
  + Commands available at lower levels are always executable at higher levels
  + Commands specifically for higher levels are not available for lower users
  + Assigning a command with many keywords to a specific level assigns all commands associated with first keywords to same level
  + Admin must create user account that has access to most but not all commands
    - Statements must be configured for every command
* Role-Based CLI Access
  + Security
    - Enhances security of device by define the set of CLI commands by specific user
    - Admin can control user access to specific ports, logical interfaces and slots on router
    - Prevents user from changing configuration or collecting info that shouldn’t have
  + Availability
    - Prevents unintentional execution of commands by unauthorized people.
  + Operational Efficiency
    - Users can only see commands applicable to ports. Router appears less complex
  + Role-Based Views
    - Three types
      * Root view
        + Configure any view from system
        + Admin must be root view
        + Same access privileges as user who has level 15 privileges
        + Only root user can configure a new view + add/remove commands from existing views
      * CLI View
        + Specific commands can be placed into a CLI view
        + No command hierarchy, no higher or lower views
        + Must be assigned all commands associated with view
      * Super view
        + One or more CLI views
        + Admin can define which commands are accepted and which configuration info is visible
        + Allows network admin to assign users and groups
        + Single CLI view can be shared within multiple superviews
        + Commands can’t be configured for sueperview, admin must add them
        + Users who are logged into superview can access all commands in any of the CLI views apart of superview
        + Each one has a password used
* Configuring Role-Based Views
  + Enable [view [view-name] ]
    - Used to enter CLI view.
  + Parser view view-name
    - Creates a view and enters view configuration mode
  + Secret encrypted-password
    - Sets a password to protect access to the view
    - Passwords must be created immediately after creating a view, otherwise an error message will happen
* Verify Role-Based CLI views
  + Verify view = enable view
  + Enable view USER
    - Enables USER superview and lists commands available in view
  + Enable view SUPPORT
    - Enables SUPPORT superview and lists commands available
  + Enable view JR-ADMIN
    - Enables JR-ADMIN and lists commands
* Cisco IOS Resilient Configuration feature
  + Startup configuration file is in NVRAM
  + CISCO IOS resilient allows router to withstand malicious attempts by securing router image and maintaining a secure working copy of configuration
  + Denies all requests to copy, modify or delete
    - Secure copy is stored in flash with secure IOS image
  + Only available that support PCMCIA Advanced Technology Attachment (ATA) flash interface
  + Global configuration commands
    - Secure boot-image = secures the router IOS image
    - Secure boot-config = secures the startup configuration file
* Management Access
  + Info flow between management hosts and the managed devices can take two paths
    - In band
      * Info flows across enterprise network, the internet or both using data channels (regular)
      * Apply only to devices that need to be managed or monitored
      * Use IPsec, SSH or SSL
      * Decide when the channel needs to be open at all times
      * Cost-effective security
    - Out of band (OOB)
      * Info flows on dedicated management network, no production traffic
      * Provide the highest level of security
      * Mitigate the risk of passing insecure management protocols over the production network
      * OOB management network remains unaffected by the downed link
* Introduction to Syslog
  + The most common method for getting access to system messages provided by networking devices is syslog (a standard and protocol developed for standard)
  + UDP port 514 to send event notification messages across IP networks
    - Routers, switches, application servers, firewall
  + Three Functions
    - Ability to gather logging info for monitoring/troubleshooting
    - Select type of logging info being captured
    - Specify destinations of messages
* Syslog Operation
  + The protocol sends system messages and debug output to local internal logging process
  + Can also be sent to internal buffer
    - Only viewable through CLI
  + Specify the system messages and where they are sent
  + Locations
    - Logging buffer
      * Useful security tool, log messages are stored in router memory. Events are cleared whenever the router is rebooted
    - Console
      * On by default
      * Messages log to the console and wll be viewed when modified or tested in the router using terminal emulation.
    - Terminal lines
      * Enabled EXEC sessions
        + Configured to receive log messages
        + Not stored on router, only valuable to user on line
    - Syslog server
      * Forward log messages to external syslog service
      * Reside on any number of servers or workstations
      * Most popular message logging
      * Long term log storage and central location for all router messages.
* Syslog Message
  + Produced as a result of network events
  + Smaller numerical levels are more critical
  + Meanings
    - Warnings, errors, critical, alerts and emergency levels
      * Error messages about software/hardware. Functionality of device is affected
    - Debugging level
      * Indicates that the messages are output from the debug commands
    - Notification level
      * Only for information
      * Device functionality is not affected
      * Interface up or down and system restart messages
  + Syslog facilities are service identifiers that identify and categorize system state data for error and event message
  + Syslog message facilities reported on routers
    - IP
    - OSPF protocol
    - SYS operating system
    - IP security (IPsec)
    - Interface IP (IF)
  + Most Common
    - Link up and link down messages, messages that a device produces when it exits from configuration mode.
* Syslog systems
  + Two types
    - Syslog servers
      * Log hosts, accept and process log messages from syslog clients
    - Syslog clients
      * Routers that generate and forward log messages to the servers
  + Protocol allows login message to be sent from the client to server
* Introduction to SNMP
  + Simple Network Management protocol
    - Allow admin to manage nodes (servers, workstations, routers, switches and security appliances). Enables network admin to manage network performance
    - SNMP application layer protocol, a message format for communication between managers and agents
  + Three elements
    - SNMP manager
      * Part of a network management system (NMS)
      * managements software for SNMP.
      * Collect information from SNMP agent (get action)
      * Change configuration on agent (set action)
      * Agent can forward info to NMS (traps action)
    - SNMP agents (managed node)
      * Networking device clients
      * Switches, routers, servers, firewall and workstations.
      * Access to local MIB of objects that reflect the resources and activity
    - Management information Base (MIB)
      * Networking device clients
      * Store data about device operation. Authentic remote users
  + Defines how management infor is enhanced
  + UDP, port 162 to retrieve and send management information
* SNMP Operation
  + Agents on managed devices collect and store info about device and its operation.
  + Stored by the agent locally in MIB. The manager uses the agent to access info within MIB
  + Two main SNMP manager requests, get and set
    - Get = used by NMS to query device for data.
    - Set = used by NMS to change configuration variable in agent device. Initiate actions within device
  + SNMP agent responds to SNMP manager
    - Get an MIB variable
      * SNMP agent performs function in repose to GetRequest-PDU from NMS
      * Agent retrieves value of request MIB variable and responds to NMS with value
    - Set an MIB variable
      * Performs function in response to SetRequest-PDU from NMS.
      * Agent changes the value of MIB variable to value specified by NMS.
      * Agent replies to set request including the new settings
* SNMP Vulnerabilities
  + Manager node runs SNMP management software (at least one)
    - Switches, routers, servers and workstations are equipped with SNMP agent software
    - Agent is responsible for providing access to MIB
      * Store data about device operation, meant to authenticate remote users
  + SNMP manager can get info from agent, and change or set, infor in the agent
* SNMP Community Strings
  + The SNMP management must have correct string for SNMP agents to accept them
  + Two types
    - Read-only community strings
      * Provide read only access to all objects in the MIB except community strings
      * When sent can get info but not set info
    - Read-write community strings
      * Provides read-write access to all objects in MIB, except community strings
      * When sent it can get or set info
  + Used to authenticate messages between a management station and an SNMPv1 or SNMPv2 engine
  + Read-write strings can get and set information in an agent
  + Set access is equivalent to having the enable password for a device
  + By default most are public as community string
* SNMPv3
  + Standards-based protocol for network management
  + Authenticates and encrypts packets over network
  + Security features
    - Message integrity and authentication
      * Makes sure that packet hasn’t been tampered within transit
      * Transmissions from manager to agent may be authenticated to guarantee the identity of the sender and the integrity and timeliness of a message
    - Encryption
      * Scrambles contents of packet
    - Access control
      * Restricts each principal to certain actions on specific portions of data
      * Agent may enforce access control to restrict each principal to certain actions on specific portions of data
* Enabling SNMP Using CCP
  + Security levels
    - noAuth
      * Authenticates packet by string match of username/community string
    - auth
      * Authenticates packet by using Hashed Message Authentication Code (HMAC) with MD5 or SHA
    - Priv
      * Uses HMAC MD% or HMAC SHA and encrypts packet using Data Encryption Standard (DES), triple DES (3DES) or Advanced Encryption standard (AES)
* Network Time Protocol
  + Date and time settings of router
    - Manually editing date and time
    - Configuring the Network Time Protocol (NTP)
  + NTP
    - Allows router to synchronize time settings with NTP server
    - NTP clients obtain time and date info from single source
    - Uses UDP port 123 and is documented in RFC 1305
* NTP Server
  + When there is a private master clock it needs to be synchronized to Coordinated Universal Time (UTC) through satellite or radio
  + Communications (associations) between machines running NTP are usually statically configured
    - Given the IP address of NTP masters
* NTP Authentication
  + Two security mechanisms
    - ACL - based restriction scheme
    - Encrypted authentication mechanism offered by NTP version 3 or later
  + Version 3 + later, has a cryptographic authentication mechanism between NTP peers
* Cisco Discovery Protocol
  + CDP
    - Enabled by default
    - Used to obtain protocol addresses of nearby cisco devices
* Protocols and Services Default Settings
  + Proprietary protocols
    - Cisco discovery protocol
  + Globally available protocols
    - ICMP and other scanning tools
  + Security
    - Disable unnecessary services and interfaces
    - Disable and restrict commonly configured management services such as SNMP
    - Disable probes and scans like ICMP . Ensure terminal access security
    - Disable IP-directed broadcasts
* Cisco IOS Security Tools
  + Security audit tool performs checks on security level of a configuration
  + Audit Tools
    - Security audit wizard
      * Provided through CCP
      * A list of vulnerabilities and allows admin to choose which potential security related configuration changes should be implemented
      * Tests router configuration
        + Presents screen for admin
      * Compares router against recommended settings and does the following
        + Huts down unneeded servers
        + Disable unneeded services
        + Applies the firewall to the outside interfaces
        + Disables or hardens SNMP
        + Shuts down unused interfaces
        + Checks password strength
        + Enforce the use of ACLs
      * Optional automatic
    - Cisco AutoSecure
      * Available through Cisco IOS CLI
        + Auto secure
      * Initiates security audit and allows for changes
        + Can be automatic or require admin
      * Executes a script
      * First makes recommendations then modifies the security configuration of the router
      * Lock down management plane functions and forwarding plane services and functions of a router
        + Logical path of all traffic

Control all other functions of routing

* + - * Management Plan services and functions
        + Secure BOOTP, CDP, FTP, TFTP, PAD, UDP, TCP small servers. MOP, ICMP, IP source routing, Finger, password encryption, TCP keepalives gratuitous ARP, proxy ARP and directed broadcast
        + Legal notification using banner
        + Secure password and login functions
        + Secure NTP
        + Secure SSH access
        + TCP intercept services
      * Forwarding plane is responsible for
        + Packet forwarding
        + Packet switching
      * Three forwarding plane services that are enabled
        + Cisco Express forwarding (CEF)
        + Traffic filtering with ACLs
        + Cisco IOS firewall inspection for common protocols
      * Provide baseline security policies
    - One-Step lockdown
      * Provided through CCP
        + Provides list of vulnerabilities and automatically makes all recommended changes
      * Tests router configuration for potential security problems and fixes them automatically
      * Disables
        + Finger service
        + PAD service
        + TCP small servers service
        + UDP small servers service
        + IP BOOTP server service
        + IP identification service
        + Cisco Discovery Protocol
        + IP source router
        + IP GARPs
        + SNMP
        + IP redirects
        + IP proxy ARP
        + IP directed broadcast
        + MOP service
        + IP unreachables
        + IP mask reply
        + IP unreachables on null interface
      * Enables
        + Password encryption service
        + TCP keepalives for inbound and outbound telnet sessions
        + Sequence numbers and timestamps on debugs
        + Cisco express forwarding with integrated netFlow switching
        + Unicast reverse path forwarding (RPF) on outside interfaces
        + Firewall on all outside interfaces
        + SSH for access to the router
        + AAA
      * Configures
        + Minimum password length to six characters
        + Authentication failure rate to less than three retries
        + TCP synwait time
        + Notification banner
        + Logging parameters
        + Enable secret password
        + Scheduler interval
        + Scheduler allocate
        + Users
        + Telnet settings
        + Access class on HTTP server service
        + Access class on vty lines
* Cisco AutoSecure vs. CCP One-Step Lockdown
  + These features are in Cisco AutoSecure but not CCP one-step lockdown
    - Disabling NTP
      * Disables it, or configured with MD5 authentication
      * CCP does not support disabling NTP
    - Configuring AAA
      * Not configured, the local AAA will be configured. Prompts for local username and password database
      * CCP doesn’t support AAA configuration
    - Setting selective packet discard (SPD) values
    - Enabling TCP intercepts
    - Configuring anti spoofing ACLs on the outside interfaces
      * Creates three named access lists to prevent spoofing source addresses
  + These features are implemented differently in Cisco AutoSecure than CCP
    - Enabling SSH for access to the router
      * CCP enables and configures SSH that have IPsec feature set
        + Doesn’t enable Secure Copy Protocol (SCP) or disables other access and file transfer services (FTP)
      * Disabling SNMP
        + CCP disables SNMP

Doesn’t provide configuring for SNMPv3

* Summary
  + Device hardening
    - Securing network perimeter
    - Securing admin access to infrastructure devices
    - Enhancing virtual login security
    - Secure protocols
      * SSH instead of telnet
      * HTTPS instead of HTTP
  + Limiting admin
    - Provide access to infrastructure devices based on levels and implement role-based CLI to create a hierarchical admin access
  + IOS images and configuration files should be protected
    - Cisco IOS resilient configuration feature
    - Network monitoring
      * Syslog, SNMP, NTP

### 

# Securing Network Devices

## Some Methods and Recommended Practices

* Securing administrative access
* Including maintaining passwords
* Configuring enhanced virtual login features
* Implementing SSH (Secure Shell)
* Securing syslog
* Using Simple Network Management Protocol (SNMP)
* Configuring Network Time Protocol (NTP)

## Implementing Security

### Single Router Approach

* A single router connects the protected network, or internal LAN, to the internet
* Has all the security policies configured on this device
* More commonly deployed on smaller sites
* Required security features can be supported by Integrated Services Routers without impeding the router’s performance capabilities

### Defense-in-Depth Approach

* More secure than the single router approach
* Uses multiple layers of security prior to traffic entering the protected LAN
* Three primary layers of defense
  + Edge router
  + Firewall
  + Internal Router
* Edge router acts as the first line of defense AKA screening router
* Passes all connections intended for internal LAN to the firewall
* Second line of defense is the firewall. Typically picks up where edgerouter leaves off and performs additional filtering
* Provides additional access control by tracking the state of the connections and acts as a checkpoint device
* Edge router has a set of rules specifying traffic to allow or deny
* By default, firewall denies connections from the outside untrusted network to the inside trusted network.
* Allows internal users to establish connections to untrusted networks
* Also performs user authentication (authentication proxy) where users must be authenticated to gain access to network resources
* Routers are not the only devices that can be used in a defense-in-depth approach. Other security tools, such as Intrusion Protection Systems (IPS) can also be implemented.

### DMZ (Demilitarized Zone) Approach

* Variation of the defense-in-depth approach
* Includes an intermediate zone called a demilitarized zone
* DMZ can be used for servers that must be accessible from the Internet or some other external network
* DMZ can be set up between 2 routers, with an internal router connecting to the protected network and an external router connecting to the unprotected network
* Or, the DMZ can simply be an additional port off a single router
* The firewall, located between the protected and unprotected networks, is set up to permit the required connections like HTTP, from the outside networks to the public servers in the DMZ
* Firewall serves as the primary protection for all devices in the DMZ
* In DMZ approach the router provides some protection by filtering some traffic, but leaves the bulk of the protection to firewall

### Securing Routers

#### Physical Security

* + Provides physical security for the routers
  + Place router and physical devices that connect to it in a secure locked room that is accessible only to authorized personnel
    - Should be free of electrostatic or magnetic interference, has fire suppression, and has controls for temperature and humidity
  + Install an uninterruptible power supply (UPS) and keep spare components available. This reduces the possibility of a network outage from power loss

#### Operating System Security

* + Secure features and performance of the router OS
    - Configure the router with maximum amount of memory possible
    - Availability of memory can help protect the network from some DoS attacks, while supporting the widest range of security services
    - Use the latest, stable version of the OS that meets feature requirements of the network
    - Security features in an OS are improved and updated over time
    - Keep a secure copy of the router OS image and router configuration file as a backup

#### Router Hardening

* + Eliminate potential abuse of unused ports and services
    - Secure administrative control; Ensure that only authorized personnel have access and that their level of access is controlled
    - Disable unused ports and interfaces. Reduce attack surface area. Reduce the number of ways a device can be accessed
    - Disable unnecessary services. Similar to many computers, a router has services that are enabled by default
      * Some of these services are unnecessary and can be used by an attacker to gather information or for exploitation

### Secure Administrative Access

* Administrative access is required for router management purposes
* This securing is an extremely important security task
* If an unauthorized person gains administrative access to a router, the person could:
  + Alter routing parameters
  + Disable routing functions
  + Or Discover and gain access to other systems within the network
* Several important tasks are outline below
  + Restrict device accessibility
    - Limit the accessible ports, restrict the permitted communicators, and restrict the permitted methods of access.
  + Log and account for all access
    - For auditing purposes, record anyone who accesses a device, including what occurs and when
  + Authenticate access
    - Ensure that access is granted only to authenticated users, groups, and services. Limit the number of failed login attempts and the time between logins
  + Authorize actions
    - Restrict the actions and views permitted by any particular user, group or service
  + Present legal notification
    - Display a legal notice, developed in conjunction with company legal counsel, for interactive sessions
  + Ensure the confidentiality of data
    - Protect locally stored sensitive data from viewing and copying
    - Consider the vulnerability of data in transit over a communication to sniffing, session hijacking, and man-in-the-middle (MITM) attacks.
* Access via all access ports on a router, including console, auxiliary port, and virtual terminal connections should require a secure password
* All routers must be configured with the user and privileged EXEC passwords.
* Using a password and assigning privilege levels is a simple way to provide terminal access control in a network
* When managing several network devices a central Terminal Access Controller Access-Control System Plus (TACACS+) or Remote Authentication Dial in User Service (RADIUS) authentication server, such as the Cisco Secure Access Control Server (ACS) should be used to store all administrative usernames and passwords
* A local username database is also recommended as backup if access to an authentication, authorization, and accounting (AAA) server is unavailable

### Securing Local and Remote Access

* Router can be accessed locally or remotely

#### Local Access

* + All network devices can be accessed locally
  + Access to a router usually requires an direct connection to a console port on a router using a computer with a terminal emulation software
  + Administrator must have physical access to the router and connect using a console cable to the console port on the router.
  + Local access is typically for configuration of the device

#### Remote Access

* + Administrators can also access devices remotely
  + Although aux port is open most common remote access method involves allowing Telnet, SSH, HTTP, HTTPS, or SNMP connection from the computer to the router
  + Computer can be on the same subnet or different subnet
* Some remote access protocols like Telnet send data, including usernames and password in plaintext
* If an attacker can intercept this connection then they can steal the data
* Thus, it is preferable to allow only local access.
* When accessing remotely a few precautions should be taken:
  + Encrypt all traffic between administrator computer and router. Instead of Telnet use SSH; or use HTTPS instead of HTTP
  + Establish a dedicated management network. Should include only identified administration hosts and connections to a dedicated interface on the router
  + Configure a packet filter to allow only authorized administration hosts and preferred protocols to access the router. For example, permit only SSH requests from IP address of authorized administration host.
* These precautions are valuable, but do not protect network completely.
* Other methods must be implemented. Like securing passwords

### Securing Passwords

* Attackers have various methods of discovering passwords
* Administrators should have strong passwords to protect assets like routers and switches
* Here are some guidelines:
  + Password length of 10 or more characters. Longer is better
  + Complex Passwords; Mix of uppercase letters, lowercase letters, numbers, symbols, and spaces
  + Avoid easy to associate or dictionary word passwords.
  + Deliberately misspell a password. For example, Smith = Smyth = 5mYth
  + Change passwords often
  + Do not write passwords down and leave them in obvious places
* A passphrase is often easier to remember and longer and harder to guess. Consists of many words separated by spaces.

### Configuring Secure Local Database Entries

* One way of increasing authentication security from only a password is to configure a requirement of username and a password on the local and remote access lines.
* In order to do this, local database entries consisting of usernames and password combinations are created locally on each device.
* Then the local and remote access lines are configured to refer to the local database when authenticating a user

### Enhancing the Login Process

* Assigning passwords and local authentication will not prevent any attacks
* The network must have systems in place to detect and prevent these attacks
* Cisco IOS login enhancements feature provides more security when creating a virtual connection by slowing down attacks, such as dictionary attacks and DoS attacks.
* Virtual Login Security Enhancements:
  + Implement delays between successive login attempts
  + Enable login shutdown if DoS attacks are suspected
  + Generate system-logging messages for login detection
* By enabling a detection profile, a network device can be configured to react to repeated failed login attempts by refusing further connection requests, or login blocking.
* This block can be configured for a period of time called a quiet period
* Legitimate connection attempts can still be permitted during a quiet period by configuring an ACL with the addresses that are known to be associated with system administrators
* These enhancements do not apply to console connections only remote connections.
* It is assumed that only authorized personnel have access to console connections

### Provide Legal Notification

* Use banner messages to present legal notification to intruders
* Legal notices are important because intruders have won court cases because they did not encounter appropriate warning messages
* Can also tell remote administration of limitations
* Choosing appropriate wording is important and should be reviewed by legal counsel before putting on network routers.
* Never use the word ‘welcome’ or other inviting words that could be misleading and could be like an invitation to use the network
* Banners are disabled by default; must be explicitly enabled

### Configuring Before SSH Is Implemented

* Telnet was used a long time ago but it is incredibly insecure.
* SSH is the alternative for this. Runs on port 22 and allows for secure communication
* Four steps must be completed prior to configuring routers for the SSH protocol
  + Ensure that the target routers are running a Cisco IOS release that supports SSH
  + Ensure that each of the target routers has a unique hostname
  + Ensure that each of the target routers is using the correct domain name of the network
  + Ensure that the the target routers are configured for local authentication or AAA services for username and password authentication. This is mandatory for a router-to-router SSH connection

## Assigning Administrative Roles

### Limiting Command Availability

* Most company employees require only specific areas of access to the network
* Not all job functions in an IT department should have the same level of access to the infrastructure devices
* Configuring privilege levels is the next step for the system administrator to secure the network
* Privilege levels determine who should be allowed to connect to the device and what that person should be able to do with it
* Cisco IOS has 2 levels of access to commands:
  + User EXEC mode (**privilege level 1**) - Provides lowest EXEC mode user privileges and allows only user-level commands available at the “router>” prompt
  + Privileged EXEC mode (**privilege level 5**) - Includes all enable-level commands at the “router#” prompt
* Sometimes a more precise level of control is required. Cisco IOS has two methods of providing infrastructure access: privilege level and role-based CLI

#### Privilege Levels

* Cisco routers enable an administrator to configure multiple privilege levels.
* Especially useful in a desktop environment where one admin needs to configure (level 15) but others only need to monitor with customized levels 2 to 14
* 16 total privilege levels in total; Levels 0, 1, and 15 are predefined:
  + Level 0 - Predefined user-level access privileges. Seldom used. Includes: disable, enable, exit, help, and logout
  + Level 1 - Default level for login with router prompt “Router>”. User cannot make changes or view the running-configuration file
  + Level 2-14 - Can be customized for user-level privileges. Commands from lower levels can go to higher levels and vice versa
  + Level 15 - Reserved for the enable mode privileges (enable command). Users can change configurations and view configuration files
* Administrator can define multiple customized privilege levels and assign different commands to each level.
* The higher the privilege level the more router access a user has
* Privileges at higher levels also encompass the lower levels. So commands from low levels can be run in higher levels

#### Limitations of Privilege Levels

* No access control to specific interfaces, ports, logical interfaces, and slots on routers
* Commands available at lower privilege levels are always executable at higher levels
* Commends specifically set on a higher privilege level are not available for lower privileged users
* Assigning a command with multiple keywords to a specific privilege level also assigns all commands associated with the first keywords to the same privilege level. An example is the `show ip route` command
* Biggest limitations is: if an administrator must create a user account that has access to most but not all commands, `privilege exec` must be configured for every command that must be executed at a privilege level lower than 15. Can be super tedious

#### Role-Based CLI Access

* To provide more flexibility, Cisco introduced the role-based CLI access feature in Cisco IOS 12.3(11)T
* This feature provides finer, more granular access by controlling specifically which commands are available to specific roles
* Enables network administrator to create different views of router configurations for different users. Each view defines the CLI commands that each user can access.

##### Security

* + Role-based CLI access enhances the security of the device by defining the set of CLI commands accessible by a specific user
  + Administrators can also control user access to specific ports, logical interfaces, and slots on a router.
  + Prevents a user from accidentally or purposely changing a configuration or collecting information to which they should not have access.

##### Availability

* + Prevents unintentional execution of CLI commands by unauthorized people, which could result in undesirable results, and minimizes downtime

##### Operational Efficiency

* + Users can only see CLI commands applicable to the ports and CLI to which they have access
  + So the router seems to be less complex, and commands are easier to identify when using the help feature

#### Role-Based Views

Three types of views:

* Root View
* CLI View
* Superview

##### Root View

* Administrator must be in root view in order to configure any other view
* Same privileges as a user who has a privilege level of 15
* However, a root view is not the same as a level 15 user
* Only a root view user can configure a new view and add or remove commands from the existing views

##### CLI View

* Specific set of commands can be bundled into a CLI View
* Unlike privilege levels, a CLI view has no command hierarchy and therefore no higher or lower views
* Each view must be assign all commands associated with that view
* A view does not inherit commands from other views
* Same commands can be used in multiple views

##### Superview

* Consists of one or more CLI views
* Administrators can define which commands are accepted and which configuration information is available
* Allows a network administrator to assign users and groups of users multiple CLI views at once, instead of having to assign a single CLI view per user with all commands associated to that one CLI View
* Have the following characteristics:
  + Single CLI view can be shared within multiple superviews
  + Commands cannot be configured for a superview. Administrator must add commands to CLI view and add that to a superview
  + Users who are logged into a superview can access all the commands configured for any of the CLI views that are part of the superview
  + Each superview has a password that is used to switch between superviews or from a CLI view to another superview
* Deleting a superview does not delete the associated CLI views. They remain to be used by other superviews

## Monitoring and Managing Devices

### Securing Cisco IOS Image and Configuration Files

#### Cisco IOS Resilient Configuration Feature

If attackers gain access to a router, they could alter traffic flows, alter configurations, and even erase the startup configuration file and the Cisco IOS image.

If configuration or image is erased, operator might need to retrieve an archived copy and restore the router, after which the recovery process will commence

Cisco IOS resilient configuration feature allows for faster recovery.

This feature allows a router to withstand malicious attempts at erasing files by securing the image and maintaining a secure working copy of the running configuration

When an image is secured, the feature denies all requests to copy, modify, or delete it.

Secure copy of the startup configuration is stored in flash with the secure IOS image.

This set of Cisco IOS images and router running configuration files is referred to as the bootset

This feature is only available for systems that support a PCMCIA Advanced Technology Attachment (ATA) flash interface

The Cisco IOS image and backup configuration on the Flash drive are hidden from view

The configuration file in the primary bootset is a copy of the running configuration that was in the router when the feature was first enabled.

Feature secures the smallest working set of files to preserve persistent storage space. No extra space is required

Feature automatically detects image or configuration version mismatch

Only local storage is used for securing files, eliminating scalability maintenance challenges from storing multiple images and configurations on TFTP servers

Feature can be disabled only through a console session

### Secure Management and Reporting

#### Managing and Monitoring Network Devices

Processing log messages in an enterprise network can be challenging

When a network is under attack, it is important to now the state of critical network devices and when the last known modifications

Configuration change management also includes ensuring that the right people have access when new management methodologies are adopted.

At a minimum, record changes using authentication systems on devices and archive configurations using FTP or TFTP

Automated logging and reporting of information from identified devices to management hosts are also important considerations

These logs and reports can include content flow, configuration changes, and new software installs, to name a few.

Data from any device can be sent to an analysis host for viewing. This data can be viewed in real time, on demand, and in scheduled reports

There are various logging levels to ensure that the correct amount of data is sent. It is also possible to flag device log data within the analysis software to permit granular viewing and reporting.

#### Management Access

Information flow between management hosts and managed devices can take two paths:

* In-band: Information flows across an enterprise production network, the Internet, or both using regular data channels
* Out-of-band (OOB): Information flows on a dedicated management network on which no production traffic resides

In layman's terms:

In-band management means that the management packets are going through a live network which means there are other packets going through

Out-of-band management means that the management packets are not going through a live network which means that only management packets are travelling on that network

Generally in-band management is the usage of software like SSH, Telnet, VNC, etc. to manage a network device

Meanwhile out-of-band management is when it is like a direct connection to a network device to manage it

In-band management occurs only when a management application does not use OOB or does not physically have enough interfaces

If a device must contact a management host by sending data across the production network, that traffic should be sent securely using a private encrypted tunnel or VPN tunnel

OOB is appropriate for large enterprise networks.

OOB provides the highest level of security

OOB mitigates the risk of passing insecure management protocols over the production network

In-band management is also recommended in smaller networks as a means of achieving a more cost-effective security deployment.

Apply in-band management only to devices that need to be managed or monitored

Use IPsec, SSH, or SSl when possible

Decide whether the management channel needs to be open at all times

### Using Syslog for Network Security

When certain events occur on a network, networking devices have trusted mechanisms to notify the administrator with detailed system messages

Network administrators have a variety of options for storing, interpreting, and displaying these messages, and for being alerted to those messages could have the greatest impact on the network infrastructure

Most common method of accessing system messages is to use a protocol called syslog

Syslog is a term used to describe a standard. Also used to describe the protocol for that standard

Syslog uses UDP port 514 to send event notifications across IP networks to even message collectors

Many networking devices support syslog and allows network devices to send their system messages across the network to syslog servers

Several different syslog server software packages for Windows and UNIX, many being freeware

The syslog logging service provides three primary functions:

* The ability to gather logging information for monitoring and troubleshooting
* The ability to select the type of logging information that is captured
* The ability to specify the destinations of captured syslog messages

Syslog protocol starts by sending system messages and `debug` output to a local logging process internal to the device

How the process manages these messages is based on device configurations

For example, syslog messages may be sent across the network to an external syslog server. These messages can be retrieved without the need of accessing the actual device. Log messages and outputs stored on the external server can be pulled into various reports for easier reading

Syslog messages can also be sent to an internal buffer. Messages sent to the internal buffer are only viewable through the CLI of the device

Network administrator may specify that only certain types of system messages are sent to various destinations.

For example, the device may be configured to forward all system messages to an external syslog server but debug-level messages are forwarded to the internal buffer and accessible only by the administrator from the CLI

Cisco routers can log information regarding configuration changes, ACL violations, interface status, and many other types of events. Can send log messages to several different facilities

Router can be configured to send syslog messages to one or more of the following locations:

* Logging buffer - Logging buffer is a useful security tool because log messages are stored in router memory for a time. Events are cleared whenever router is rebooted
* Console - Console logging is on by default. Messages log to the console and can be viewed when modifying or testing the router using terminal emulation software while connected to the console port
* Terminal lines - Enabled EXEC sessions can be configured to receive log messages on any terminal lines. Similar to console logging, not stored by the router and is only valuable to the user on that line
* Syslog server - Cisco routers can be configured to forward log messages to an external syslog service. This service can reside on any number of servers or workstations, including Windows and Unix-based systems. Most popular logging facility, because it provides long-term log storage capabilities and a central location for all router messages

Cisco devices produce syslog messages as a result of network events.

Every syslog message contains a severity level and facility

Smaller numerical levels are the more critical syslog alarms.

Severity level of messages can be set to control where each type of message is displayed.

| Level | Keyword | Description | Definition |
| --- | --- | --- | --- |
| 0 | emergencies | System is unusable | LOG\_EMERG |
| 1 | alert | Immediate action is needed | LOG\_ALERT |
| 2 | critical | Critical conditions exist | LOC\_CRIT |
| 3 | errors | Error conditions exist | LOG\_ERR |
| 4 | warnings | Warning conditions exist | LOG\_WARNING |
| 5 | notifications | Normal but significant condition | LOG\_NOTICE |
| 6 | informational | Informational messages only | LOG\_INFO |
| 7 | debugging | Debugging messages | LOG\_DEBUG |

Each syslog level has its own meaning:

Warning, errors, critical, alerts, and emergency levels - These messages are error messages about software or hardware malfunctions; these types of messages mean that the functionality of the device is affected. Severity of issue determines the actual syslog level applied

Debugging level - This level indicates that the messages are output generated from issuing various `debug` commands

Notification level - The notifications level is only for information, device functionality is not affected. Interface up or down transitions, and system restart messages are displayed at the notifications level

Syslog messages also contain information on the facility

Syslog facilities are service identifiers that identify and categorize system state data for error and event message reporting.

The logging facility options that are available are specific to the networking device

Common syslog message facilities reported on Cisco IOS routers include:

* IP
* OSPF Protocol
* SYS operating system
* IP Security (IPsec)
* Interface IP (IF)

Format of syslog messages on Cisco IOS software is as follows:

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

Sample output on a Cisco switch for an EtherChannel link changing state to up would be:

00:00:46: %LINK-3-UPDOWN: Interface Port-chanel1, changed state to up

Here the facility is LINK and the severity level is 3, with a MNEMONIC of UPDOWN

Most common messages are link up and down messages, and messages produced by the device when it exits from configuration mode

If ACL logging is configured, the device generates syslog messages when packet matches a condition

Syslog implementations always contain two types of systems:

* Syslog servers - AKA log hosts, these systems accept and process log messages from syslog clients
* Syslog clients - Routers or other types of equipment that generate and forward log messages to syslog servers

Syslog protocol allows login messages to be sent from a client to the server

Ability to send logs to a central syslog server can be part of a security problem.

Biggest issue is the enormity of the task of evaluating the information. This includes, sifting through various logs and events, correlating the events from several different network devices and application server and determining the type of action to take based on a vulnerability assessment of the incident

### Using SNMP for Network Security

Another common monitoring tool is Simple Network Management protocol (SNMP)

SNMP was developed to allow administrators to manage nodes, such as servers, workstations, router, switches, and security appliances, on an IP network.

Enables network administrators to manage network performance, find and solve network problems, and plan for network growth

SNMP is an application layer protocol and provides a message format for communication between managers and agents

Consists of three elements:

* SNMP Manager
* SNMP Agents (managed nodes)
* Management Information Base (MIB)

In order to configure SNMP, first necessary to define relationship between the manager and the agent

SNMP manager is part of a network management system (NMS)

SNMP manager runs SNMP management software. It can collect information from an SNMP agent using the “get” action and can change configurations on an agent using the “set” action.

SNMP agents can also forward information directly to an NMS using “traps”

SNMP agent and MIB reside on networking device clients.

Network devices that must be managed, such as switches, routers, servers, firewalls, and workstations are equipped with an SNMP agent software module

MIBs store data about the device operation and are meant to be available to authenticated remote users

SNMP agent is responsible for providing access to the local MIB of objects that reflect resources and activity

SNMP defines how management information is exchanged between network management applications and management agents

SNMP uses UDP port 162 to retrieve and send management information

In SNMPv1, asynchronous event reports are called “traps” while in later versions they are called notifications

The “get” and “set” actions are the vulnerabilities that open SNMP to an attack

SNMP agents collect information about the device and its operation on which it resides

Information is stored by the agent locally in the MIB, then the SNMP manager uses SNMP agent to access information within the MIB

2 primary SNMP manager requests, get and set.

A get request is used by the NMS to query the device for data

A set request can also initiate actions within a device

For example, a set request can cause a router to reboot, send a configuration file, or receive a configuration file.

An SNMP manager uses the following operations:

| Operation | Description |
| --- | --- |
| get-request | Retrieves a value from a specific variable |
| get-next-request | Retrieves a value from a variable within a table; exact name is not required, a sequential search is performed to find required variable |
| get-bulk-request | Retrieves large blocks of data, such as multiple rows in a table. Only works with SNMPv2 or later |
| get-response | Replies to a get-request, get-next-request, and set request sent by an NMS |
| set-request | Stores a value in a specific variable |

SNMP agent responds to SNMP manager requests as follows:

* Get an MIB variable - SNMP agent performs this function in response to a GetRequest-PDU from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value
* Set an MIB variable - SNMP agent performs this function in response to a SetRequest-PDU from the NMS. The SNMP agent changes the value of the MIB variable to the value specified by the NMS. An SNMP agent reply to a set request includes the new settings in the device.

An NMS periodically polls SNMP agents by querying the device for data using the get request

This way, a network management application can collect information to monitor traffic loads and to verify device configurations of managed devices

Information can be displayed via GUI on the NMS. Averages, minimums, or maximums can be calculated, the data can be graphed, or thresholds can be set to trigger a notification process when the thresholds are exceeded.

For example, an NMS can monitor CPU utilization of a Cisco router, the SNMP manager samples the value periodically and presents this information in a graph for the network administrator to use in creating a baseline

Disadvantages with periodic polling:

* Delay between the time an event occurs and the time that it is noticed (via polling)
* Trade-off between polling frequency and bandwidth usage

To mitigate disadvantages, it is possible for SNMP agents to generate and send traps to inform the NMS immediately of certain events.

Traps are unsolicited messages alerting the SNMP manager to a condition or event on the network.

Examples of trap conditions include, but not limited to, improper user authentication, restarts, link status, either up or down, MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events

Trap-directed notifications reduce network and agent resources by eliminating the need for some of the SNMP polling requests

At least one manager node runs SNMP management software and network devices that must be managed are equipped with the SNMP agent software module

Agent is responsible for providing access to a local MIB of objects that reflects the resources and activity at its node

MIBs store data about the device operation and are meant to be available to authenticated remote users

SNMP manager can get information from the agent, and change, or set, information in the agent

Sets can change configuration variables in the agent device and can also initiate actions in devices. A reply to a set indicates the new setting in the device.

The get and set actions create vulnerabilities that open SNMP to attack

SNMP agents accept commands and requests from SNMP management systems only if those systems have a correct community string.

An SNMP community string is a text string that can authenticate messages between a management station and an SNMP agent and allow access to the information in the MIBs

Community strings are essentially used for password-only authentication of messages between the NMS and the agent

Two types:

* Read-only community strings: Provides read-only access to all objects in the MIB, except the community strings
* Read-write community strings: Provides read-write access to all objects in the MIB, except the community strings

If manager sends on of the correct read-only community strings, it can get information but not set information in an agent.

Most SNMP use “public” as a community string. If you configure an SNMP a router agent to use that commonly known public string, anyone with an SNMP system can read the router MIB

Router MIB variables can point to things such as routing tables and other security-critical parts of the router configuration, so it is extremely important that you create your own SNMP community strings.

However, these strings are sent in plaintext which is a huge vulnerability of SNMPv1 and SNMPv2

If using in-band management, to reduce security risks, SNMP management should be configured to only pull information from devices rather than being allowed to push ‘set’ changes to the device

To ensure management information is pulled, each device should be configured with a read-only SNMP community string

Keeping SNMP traffic on a management segment allows the traffic to traverse an isolated segment when management information is pulled from devices and when configuration changes are pushed to a device

Therefore, if using and OOB network, it is acceptable to configure an SNMP read-write community string. However, be aware of the increased security risk of a plaintext string that allows modification of device configurations

SNMPv3 is a standards-based protocol for network management

SNMPv3 provides the following security features:

* Message integrity and authentication - ensures that a packet has not been tampered with in transit and is from a valid source
* Encryption - scrambles the contents of a packet to prevent it from being seen by an unauthorized source
* Access control - Restricts each principal to certain actions specific portions of data

To configure SNMP use either: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_53_se/configuration/guide/2960scg/swsnmp.pdf>

Or

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swsnmp.html>

### Using NTP

Many things involved in the security of a network, such as logs, depend on an accurate date and timestamp.

When dealing with an attack, seconds matter, because it is important to identify the order in which a specified attack occurred.

To ensure log messages are accurately time stamped, clocks on hosts and network devices must be synchronized and maintained

Typically, the data and time settings of the router can be set using one of two methods:

* Manually editing the data and time
* Configuring the Network Time Protocol (NTP)

Manually configuring may work for small networks but as they get bigger it gets harder.

A better solution is to configure NTP on the network

NTP allows routers on the network to synchronize their time settings with an NTP server. A group of NTP clients that obtain time and date information from a single source have more consistent ime settings

When NTP is implemented in the network, it can be setup to synchronize to a private master clock, or it can synchronize to a publicly available NTP server on the internet.

NTP uses UDP port 123

If a private master clock is implemented, it could be synchronized to UTC via satellite or radio.

Administrator must ensure that time source is valid and from a secure site.

For example, an attacker can launch a DoS attack by sending bogus NTP data across the internet to the network in an attempt to change the clocks on network devices, possibly causing digital certificates to become invalid

Pulling the clock time from the internet means allowing unsecured packets through the firewall, so the NTP server must be trusted is reliable, valid, and secure

The communications (known as associations) between machines that run NTP are usually statically configured. Each device is given the IP address of NTP masters

Accurate time keeping is possible by exchanging NTP messages between each pair of machines with an association

The time of a device is critical; thus the security features of NTP should be used to avoid the accidental or malicious setting of incorrect times

2 Security Mechanisms available:

* ACL-based restriction scheme
* Encrypted authentication mechanism offered by NTP version 3 or later

NTPv3, and later, support a cryptographic authentication mechanism between NTP peers.

This authentication mechanism, in addition to ACLs that specify which network devices are allowed to synchronize with other network devices, can be used to help mitigate an attack

### Performing a Security Audit

#### Cisco Discovery Protocol

Cisco routers are initially deployed with many services that are enabled by default

Done for convenience and to simplify configuration process

Some of these services can make the devices vulnerable to attack if not secured.

The Cisco Discovery Protocol (CDP) is an example that is enabled by default

It is used primarily to obtain protocol addresses of neighboring Cisco devices and to discover the devices on the local network.

Attackers don’t need CDP-enabled information to gain the information

CDP was created to make it easier for administrators to discover and troubleshoot other Cisco devices.

Edge devices are an example of a device that should have this feature disabled

#### Protocols and Services Default Settings

Depending on the security needs of an organization, many of these services should be disabled or, at a minimum, restricted

These features range from Cisco proprietary protocols such as the CDP, to globally available protocols such as ICMP

| Feature | Default |
| --- | --- |
| Cisco Discovery Protocol (CDP) | Enabled |
| Configuration autoloading | Disabled |
| FTP server | Disabled |
| TFTP server | Disabled |
| NTP service | Disabled |
| Packet assembler/disassembler (PAD) service | Enabled |
| TCP and UDP minor services | Enabled in versions 11.3 and later |
| Maintenance Operation Protocol (MOP) service | Enabled on most Ethernet interfaces |
| SNMP | Enabled |
| HTTP or HTTPS configuration and monitoring | Setting is Cisco device dependent |
| DNS | Enabled |
| Internet Control Message Protocol (ICMP) redirects | Enabled |

| Feature | Recommendation |
| --- | --- |
| CDP | Should be disabled globally or per interface if not required |
| Configuration autoloading | Should remain disabled when not in use by the router |
| FTP server | Should be disabled when it is not required |
| TFTP server | Should be disabled when not required |
| NTP | Should remain disabled when not required |
| PAD service | It should be explicitly disabled when not in use |
| TCP and UDP minor services | Disable explicitly |
| MOP service | Should be explicitly disabled when not in use |
| SNMP | Disabled when not required |
| HTTP or HTTPS configuration and monitoring | Disable if not required. If required, restrict access to the router HTTP or HTTPS service using ACLs |
| DNS | Disable when not required. DNS lookup service is required, ensure server address is set explicitly |
| ICMP redirects | Disabled when not required |
| IP source routing | Disabled when not required |
| Finger service | Disable when not required |
| ICMP unreachable notifications | Disable on interfaces to untrusted networks |
| ICMP mask reply | Disable on interfaces to untrusted networks |
| IP identification service | Should be explicitly disabled |
| TCP keepalives | Should be enabled globally to manage TCP connections and prevent certain DoS attacks. Service is enabled before Cisco IOS 12.0 and disabled 12.0 and later. Disable when not required |
| Gratuitous ARP (GARP) | Disabled on each router interface unless service is needed |
| Proxy ARP | Disable on each interface unless router is being used as a LAN bridge |

In order to secure network devices, administrators must find the vulnerabilities existing in the current configuration.

Best way to accomplish this is through a security audit tool.

A security audit tool performs checks on the security level of a configuration by comparing that configuration to recommended settings and tracking discrepancies

After vulnerabilities are identified, configurations must be modified to reduce or eliminate those vulnerabilities

Three security audit tools are available:

* Security audit wizard - Provided through CCP. Provides a list of vulnerabilities and then allows administrator to choose which potential security-related configuration changes to implement on a router
* Cisco AutoSecure - Available through CLI. `auto secure` command initiates a security audit and then allows for configuration changes. Based on mode selected, configuration changes can be automatic or require administrator input
* One-Step lockdown - Provided through CCP. Provided a list of vulnerabilities and then automatically makes all recommended security-related configuration changes

#### Cisco AutoSecure

AutoSecure released in IOS version 12.3 and is initiated from the CLI and executes a script

First makes recommendations for fixing security vulnerabilities and then modifies the security configuration of the router

Can lockdown the management plane functions and the forwarding plane services and functions of a router

The management plane is the logical path of all traffic related to the management of a routing platform. Is used to control all other functions of routing and to manage a device through its connection to the network.

Several management plane services and functions:

* Secure BOOTP, CDP, FTP, TFTP, PAD, UDP, and TCP small servers, MOP, ICMP (redirects, mask-replies), IP source routing, Finger, password encryption, TCP keepalives, gratuitous ARP, proxy ARP, and directed broadcast
* Legal notification using a banner
* Secure password and login functions
* Secure NTP
* Secure SSH access
* TCP intercept services

Forwarding plane is responsible for packet forwarding.

Three forwarding plane services and functions that AutoSecure enables:

* Cisco Express Forwarding (CEF)
* Traffic filtering with ACLs
* Cisco IOS firewall inspection for common protocols

AutoSecure is often used to provide a baseline security policy on a new router. Features can then be altered for the organization

## Commands for Securing Administrative Access

### Securing Local Access

* By default console port does not require a password for console administrative access
* To secure local access, it should always be configured using a console port line password. Run the following commands:
  + `line console 0` <- Interface configuration mode
  + `password <password>`
  + `login`

### Securing Remote Access

* Securing remote access involves securing vty lines and aux port. By default, Cisco routers support up to 5 simultaneous vty lines for Telnet or SSH
* Many Cisco routers have vty ports numbered 0 to 4. Run the following commands to secure it:
  + `line vty 0 4` <- Interface configuration mode
  + `password <password>`
  + `login`
* NOTE: Some Cisco devices have more than 5 vty lines. Check running config to check number of vty lines
* The aux port and dial-up modem can also be used to provide remote access. Does not require a password for remote admin access by default
* To secure, run the following commands:
  + `line aux 0` <- Interface configuration mode
  + `password <password>`
  + `login`

### Securing Privileged EXEC Mode Access

* Run `enable secret <password>` in global configuration mode
* The above command uses the SHA256 hashing algorithm in IOS 15.0(1)S and later
* Older ones use MD5
* If password is lost or forgotten, it must be replaced using Cisco router password recovery procedure

### Increase Password Security

#### Minimum Character Length

* After Cisco IOS Release 12.3(1) and later, admins can set minimum character length for all router passwords from 0 to 16 characters using
  + `security passwords min-length <length>` in global configuration mode.
* Default setting is 6. Command affects user passwords, enable secret passwords and line passwords created after execution
* Existing router passwords remain unaffected
* **STRONGLY RECOMMENDED THAT THE MINIMUM PASSWORD LENGTH BE SET TO AT LEAST 10 CHARACTERS**
* Any password that fails the length results in an error message.

#### Disable Unattended Connections

* By default, an administrative interface stays active and logged in for 10 minutes after the last session activity.
* After the time, the interface times out and logs out the session
* **IT IS RECOMMENDED THAT THE TIMEOUT PERIOD IS REDUCED TO 2 OR 3 MINUTES**
* Timeout period can be adjusted using `exec-timeout <minutes> [<seconds>]` in line configuration mode for each of the line types used
* Can also disable EXEC mode on certain lines using the `no exec` command. This command allows you to disable the EXEC process for connections that may attempt to send unsolicited data to the router

#### Encrypt All Passwords

* By default, with the exception of `enable secret`, all passwords are stored on the router as plaintext
* However you can encrypt it with `service password-encryption` which hashes current and future plain text passwords
* However, this is only meant to prevent against shoulder surfing and can be cracked very easily with an online application
* To stop encrypting passwords run `no service password-encryption`
* Future passwords will then be plaintext but current passwords will remain encrypted
* `enable secret` is far more secure

### Configuring Secure Local Database Entries

* Can use either:
  + `username <name> password <password>`
  + `username <name> secret <password>` or `username <name> secret {[0] <password> | 5 <encrypted-secret>}`
    - To use SHA256 run the following command: `username <name> algorithm-type sha256 secret <password>`
  + `username secret` command is more secure .
  + When configuring `login` on the console, vty, and aux ports you should now use `login local` to tell that port to use the local database.

### Configuring Login Enhancement Features

* NOTE: The enhancements are available only if local and remote access uses the local database for authentication. If they use password authentication then login enhancement features will not be enabled
* The following commands can be used to enhance login features:
  + `login block-for <seconds> attempts <tries> within <seconds>`
    - Provides DoS detection
    - This command must be configured to enable login enhancements
    - All other features are disabled until this command is configured
    - This command monitors login device activity and operates in two modes:
      * Normal mode - AKA watch mode. Router keeps count of the number of failed login attempts within an identified amount of time
      * Quiet mode - AKA quiet period. If number of failed logins exceeds the configured threshold, all login attempts are designed for the time specified
  + `login quiet-mode access-class { <acl-name> | <acl-number> }`
    - Sets the admins who can access during quiet period
  + `login delay <seconds>`
    - This command delays the time between the amount of login attempts
  + `login on-success log { every <login> }`
    - The every login part specifies the number of login attempts before a logging message is generated
  + `login on-failure log { every <login> }`
    - The every login part specifies the number of login attempts before a logging message is generated
  + `security authentication failure rate`
    - Can be configured to generate a log message when the login failure rate is exceeded
  + `show login`
    - The above command can be used to verify the `login block-for` command
  + `show login failures`
    - Displays information regarding failed attempts

### Setting a Banner / Providing a Legal Notification

* `banner {motd | exec | login} <delimiter> <message> <delimiter>`
  + For example: `banner motd # its a message #`
  + Option command tokens can be used within the message section of the banner command:
    - $(hostname) - Displays hostname of router
    - $(domain) - Displays domain name of router
    - $(line) - Displays vty or tty (asyncrhonous) line number
    - $(line-desc) - Displays description attached to the line
  + Should be included with caution

### Configuring SSH

* Four steps when using CLI:
  + 1. If router has a unique hostname, configure the IP domain name of the network using the `ip domain-name <domain-name>` command in global configuration mode
  + 2. One-way secret keys must be generated for a router to encrypt SSH traffic. These keys are reffered to as asymmetric keys. Cisco IOS uses Rivest, Shamir, and Adleman (RSA) algorithm to generate keys. To create the RSA key use:  
     `crypto key generate rsa general-keys modulus <modulus-size>`  
    Run that in global configuration mode and the modulus determines the size of the RSA key and can be configured from 360 bits to 2,048 bits. The larger the modulus the more secure; however, larger modules take slightly longer to generate and encrypt and decrypt. Minimum recommended is 1,024 bits
  + Note: SSH is automatically enabled after RSA keys are generated
  + 3. Ensure that there is a valid local database username entry. If not, create one
  + 4. Enable vty inbound SSH sessions using the line vty commands:  
     `login local`  
     `transport input ssh`
* To verify SSH and display generated keys use the following command:   
   `show crypto key mypubkey rsa` in privileged EXEC mode
* If there are existing key pairs it is recommended that they are overwritten using the   
   `crypto key zeroize rsa`
* Cisco routers support two versions of SSH:
  + SSH version 1 - original version but has known vulnerabilities
  + SSH version 2 - provides better security using the Diffie-Hellman key
* Default is SSH version 1.99. AKA compatibility mode and is merely an indication that the server supports V2 and V1.
* However best practice is to enable v2
  + Use the following command to specify a version:   
     `ip ssh version {1 | 2}`   
    in global configuration mode
* Time interval that the router waits for the SSH client to respond during the SSH negotiation phase can be configured using:  
   `ip ssh time-out <seconds>`  
  In global configuration mode
* The default is 120 seconds and is not the same as the `exec-timeout` value, which is the amount of time that SSH takes to authenticate a user. When the EXEC session starts, the standard `exec-timeout` value configured for the vty applies
* By default, a user logging in has 3 attempts before being disconnected.
* To configure a different number of consecutive SSH retries use:  
   `ip ssh authentication-retries <integer>`  
  Global configuration command
* To verify the option SSH command settings use the following command:  
   `show ip ssh` command

### Connecting to an SSH-Enabled Router

* `ssh -l <username> <ip-address>` to connect to a router. Privileged EXEC Mode
* `show ssh` in privileged EXEC mode to show current SSH sessions

### Configuring Privilege Levels

* Execute the following command in Global Configuration mode:  
   `privilege <mode> {level <level> | reset} <command>`
  + The <mode> parameter specifies the configuration mode. Use the `privilege ?` command to see a complete list of router configuration modes available
  + The optional level parameter enables setting a privilege level with a specified command
  + The optional <level> parameter is the privilege level associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15
  + The reset option parameter resets the privilege level of a command
  + The optional <command> for which you want to reset the privilege level. Allows the user to use that command if reset is not set
* If you assign `show ip route` then it also applies the `show` and `show ip` command
* There are 2 methods for assigning passwords to the different levels:
  + To the privilege level itself, use:  
     `enable secret level <level> <password>`
  + To a user that is granted a specific privilege level use:  
     `username <name> privilege <level> secret <password>`
* NOTE: When a command is assigned at a specific level, access to that command is removed from any lower level.
* For example, to assign level 5 access to the `ping` command but not anything below use the following:  
   `privilege exec level 5 ping`
* Now, anyone from levels 1-4 can’t use `ping`
* To assign a password to level 5 use the following command:  
   `enable secret level 5 cisco5
* The privilege level can also be assigned to a user in the local database. To assign a specific username to privilege level 5, enter the following command:  
   `username SUPPORT privilege 5 secret cisco5`
* To access established privilege level enter:  
   `enable <level>`
* Command from user mode and enter the password that was assigned to the custom privilege level.
  + If no privilege level is specified, it is assumed to be level 15
* Sometimes easy to forget, so to display and confirm the current privilege level use:  
   `show privilege`  
  Remember that higher privilege levels automatically inherit the command access of lower levels

### Configuring Role-Based Views

* Before you can create a view, AAA must be enabled using  
   `aaa new-model`  
  Or using CCP
* `enable [view [<view-name]]`
  + The above command is used to enter CLI view. Enter the name root for <view-name> or a specific view-name.
  + If no name is specified, root is assumed
  + Must configure `aaa new-model` before using
* 5 steps to create and manage a specific view:

1. Enable AAA with   
    `aaa new-model`  
   global configuration mode command. Exit and enter root view with  
    `enable view`  
   command.
2. Create a view with the following command in router configuration mode:  
    `parser view <view-name>`  
   This creates a view and enters view configuration mode. Excluding the root view, there is a maximum limit of 15 views in total
3. Assign a secret password to the view using the following command:  
    `secret <password>`  
   Sets password to protect access to the view. Password must be created immediately after creating a view; otherwise an error message will appear
4. Assign commands to the selected view using the following command:  
    `commands <parser-mode> {include | include-exclusive | exclude} [all] {interface <interface-name> | <command>}`
   1. The <parser-mode> parameter specifies the mode in which the specified command exists; for example, EXEC mode
   2. The `include` parameter adds a command or an interface to the view and allows it to be used for other views
   3. The `include-exclusive` parameter adds a command or an interface to the view but will NOT allow it to be used for other views
   4. The `exclusive` command excludes a command or an interface from the view
   5. The `all` keyword is a “wildcard” that allows every command in a specified configuration mode that begins with the same keyword or every subinterface for a specified interface to be part of the view
5. Exit view configuration mode by typing:  
    `exit`

### Configuring Role-Based CLI Superviews

Steps to configure a superview are essentially the same as configuring a CLI view.

`view <view-name>` is used to assign commands/views to the superview.

Administrator must be in root view to configure a superview

To confirm that root view is being used, use either  
 `enable view` or `enable view root`

When prompted, enter the secret password.

Four steps to create and manage a superview:

1. Create a view and enter superview configuration mode using the following command:  
    `parser view <view-name> superview`
2. Assign a secret password to the view using the following command:  
    `secret <encrypted-password>`
3. Assign an existing view using the following command:  
    `view <view-name>`
4. Exit by typing `exit`

More than one view can be assigned to a superview, and views can be shared between superviews

To access existing views, enter the following command in user mode and enter the password assigned to that custom view:

`enable view <view-name>`

### Verifying Role-Based CLI Views

To verify a view use the following command:

`enable view <view-name>`

Provide password to log into the view

Use the question mark command to verify that the commands available in the view are correct

From the root view, use:

`show parser view all`

To see a summary of all views

### Commands for Cisco IOS Resilient Configuration Feature

The following commands are available in global configuration mode:

`secure boot-image` - Secures the router IOS Image

`secure boot-config` - Secures the startup configuration file

#### Verifying Bootset Files

`show secure bootset` to verify existence of the archive

#### Restoring the Bootset Files

1. Reload the router with the `reload` command
2. From ROMmon mode, enter the `dir` command to list contents of the device that contains the secure bootset file.
3. From the CLI the device name can be found in the output of the `show secure bootset` command
4. Boot the router using the `boot <filename>` command. The file name can be found from step 2. Once booted, change to privileged EXEC mode and restore configuration
5. Enter global configuration mode
6. Restore secure configuration to the supplied filename using the `secure boot-config restore <filename>` command

#### Recovering a Router Password

Password recovery requires the administrator to have physical access to the router through a console cable for security reasons

1. Connect to the console port
2. Use `show version` to view and record the configuration register
   1. Configuration register is similar to BIOS setting of a computer which controls the boot process
   2. Represented by a single hexadecimal value
3. Power cycle the router using power switch
4. Issue the break sequence. Must be done within 60 seconds of power up to put router into ROMmon mode
5. Change default configuration register with the `confreg 0x2142` command at the rommon 1> prompt. This changes the default configuration register and causes the router to bypass the startup configuration where the forgotten `enable` password is stored
6. Reboot the router. Type `reset` at the rommon 2> prompt. The router reboots, but ignores the saved configuration
7. Press Ctrl-C to skip initial setup procedure.
8. Put router into privileged EXEC mode
9. Copy startup configuration to the running configuration
10. Verify configuration.
11. Change the enable secret password
12. Enable all interfaces
13. Change the config-register with the `config-register <configuration-register\_setting>` The configuration register setting is the value in step 2 or 0x2102
14. Save configuration settings by `copy running-config startup-config`

Using the command `no service password-recovery` will disable the entire process above

All access to ROMmon mode is disabled with the above command

To recover a device after the above command is entered, initiate break sequence within 5 seconds after image decompresses during boot

### Configuring System Logging

1. Set the destination logging host using the following command:  
    `logging host [<hostname> | <ip-address>]
2. (Optional) Set the log severity (trap) level using the following command:  
    `logging trap <level>`  
    Level is one of the level numbers or level names specified above
3. Set source interface using the following command. This command specifies that syslog packets contain the IPv4 or IPV6 address of a specific interface, regardless of which interface the packet uses to exit the router:  
    `logging source-interface <interface-type> <interface-number>`
   1. Interface-type specifies the interface type. For example, FastEthernet
   2. Interface-number specifies the interface number. For example, 0/1
4. Enable logging with the following command:  
    `logging on`
   1. Logging can also be turned on and off for specific destinations using the following commands  
       `logging buffered`  
       `logging monitor`  
       `logging`  
      However if `logging on` is disabled, no messages are sent to those destinations, only the console receives messages

### Manually Setting the Time

Use the following command in privileged EXEC mode:

`clock set <time> <month> <day> <year>`

For example:

`clock set 10:28:00 DEC 16 2008`

Will set the time to 10:28 December 16th 2008

### Configuring NTP

#### NTP Server

In an NTP configured network, one or more routers are designated as the master clock keeper AKA NTP master using the following command in global configuration command:  
 `ntp master [<stratum>]`

The stratum number is the number of hops away from an authoritative source such as an atomic clock

NTP clients either contact the master or listen for messages from the master to synchronize their clocks. In order to contact the master use the following command:  
 `ntp server {<ip-address> | <hostname>} [version <number>] [key <keyid>] [source <interface>] [prefer]`

Although `ntp server <ip-address>` is good enough

In a LAN environment, NTP can be configured to use IP broadcast messages instead by using the following command in interface configuration mode:

`ntp broadcast client`

The above command configures devices to receive NTP broadcast messages on the interface

That command reduces configuration complexity because each machine can be configured to send or receive broadcast messages. The accuracy of timekeeping is marginally reduced because the information flow is one-way only

You can use the `show clock` method in order to view the time

#### NTP Authentication

Use the following commands on the NTP master and the NTP client:

* `ntp authenticate`
* `ntp authentication-key <key-number> md5 <password>`
* `ntp trusted-key <key-number>`
  + The key-number here corresponds the key-number from the above command

Use `show ntp associations detail` to confirm that the server is an authenticated source

#### Cisco AutoSecure

`auto secure [no-interact | full] [forwarding | management] [ntp | login | ssh | firewall | tcp-intercept]`

You can run the above command in privileged EXEC mode. Here are the meanings for each term:

* No-interact: The router will automatically configure everything like CCP One-Step Lockdown
* Full: This is the default setting, user will be prompted
* Forwarding: only the forwarding plane will be secured
* Management: only the management place will be secured
* Ntp: specifies the configuration of the NTP feature
* Login: specifies the configuration of the login feature
* Ssh: specifies the configuration of the SSH feature
* Firewall: specifies the configuration of the firewall feature
* Tcp-intercept: specifies the configuration of the TCP-Intercept feature

## Authentication, Authorization and Accounting

### Module 17

* Introduction
  + AAA protocol provides the necessary framework to enable scalable access security
    - Configured to access a local username and password database
    - Access a cisco secure access control server (ACS)
* Authentication without AAA
  + Passwords
    - Login and password combination console
      * Vty lines and aux ports
* AAA components
  + Who is permitted to access a network, what they can do while they are there and to audit what actions they perform
  + Authentication
    - Users and admins must prove who they are
    - Username and password, challenge and response questions, token cards
  + Authorization
    - Determine which resources user has access to
  + Accounting and Auditing
    - What the user does.
* Authentication Modes
  + Two access modes
    - Character mode
      * User sends request to establish EXEC mode process with router
    - Packet mode
      * User sends a request to establish connection through router with device on network
  + Two methods of implementing
    - Local AAA Authentication
      * Uses local database
        + Stores usernames and passwords locally on router.
        + Users authenticate against database
        + Small networks
    - Server-Based AAA Authentication
      * External database service that leverages RADIUS and TACACS+ protocols
        + ACS
* Authorization
  + Typically implemented using server-based solution
* Accounting
  + Collects and reports usage data
  + Implemented using server-based solution
  + Statistics go back to ACS server
* Authenticating Administrative Access
  + Local AAA Authentication or self-contained authentication
  + One or two routers providing access to limited number of users
    - Local usernames and passwords stored on router
  + System admin must populate local security database by saying a username and password
* Comparing Local AAA and Server-Based AAA Implementations
  + Local
    - User establishes connection with router
    - Router prompts user for username and password, using local database
  + Serve-based
    - User establishes connection with router
    - Prompts for username and password
    - Rouer passes username and password to Cisco Secure ACS
    - ACS authenticates user
* Introducing Cisco Secure Access Control Server
  + ACS family of products supports Terminal Access Control Access Control Server Plus (TACACS+) and Remote Authentication Dial-In User Services (RADIUS)
    - TACACS+ is considered more of a security protocol when communicating between client and AAA servers
      * Exchanges are encrypted
      * RADIUS only encrypts password
* Introducing TACACS+ and RADIUS
  + Both authentication protocols
  + Critical Factors for TACACS+
    - Incompatible with TACACS and XTACACS
    - Separates authentication and authorization
    - Encrypts all communications
    - Uses TCP port 49
  + Critical Factors for RADIUS
    - Uses proxy servers for scalability
    - Combines authentication and authorization into one process
    - Encrypts only passwords
    - Uses UDP
    - Supports remote-access technologies and Session Initiation Protocol (SIP)
* TACACS+ Authentication
  + Provides separate AA services.
    - Provides flexibility in implementation
      * Can be used for authorization and accounting while using another method for authentication
    - More types of authentication requests and response codes
* RADIUS Authentication
  + Open IETF standard AAA protocol
  + Defined by RFCs 2865, 2866, 2867, 2868
  + Hides passwords during transmission with Password Authentication Protocol (PAP)
    - Using MD5 hashing and shared secret
      * Rest of packet is plaintext
  + VoIP service providers
  + Common authentication protocol using 802.1X security standard
  + Diameter Protocol is planned replacement for RADIUS
    - New transport protocol called Stream Control Transmission Protocol (SCTP), TCP instead of UDP
    - Released as IETF protocol
* TACACS+ and RADIUS with Cisco Secure ACS
  + Cisco Secure ACS for windows server is a single solution offering AAA for both
  + Highly scalable, high performance access control server
  + Benefits
    - Extended access security
      * Authentication, user access and administrator access are combined in a centralized identity networking solution
    - Allows more flexibility and mobility
    - Uniform security policy for all users
    - Reduces admin and management burden
      * Scales user and network admin access to network
* Cisco Secure ACS Features
  + Authenticate users using internal Cisco Secure user database or configured to leverage external databases that are centrally managed
  + Advanced Features
    - Automatic service monitoring
    - Database synchronization and importing of tools for large-scale deployments
    - LDAP user authentication support
    - User and admin access reporting
    - Restrictions to network access based on criteria such as the time of day and day of week
    - User and device group profiles
* Cisco Secure ACS as a TrustSec Component
  + Core component, includes
    - Cisco Network Admission Control (NAC)
    - Cisco NAC Guest Server
    - Cisco NAC Profiler
    - Cisco Secure ACS
  + Offers two deployment options
    - ACS 802.1X- Based infrastructure solution
      * Cisco ACS policy server authenticates users connecting to the network
      * Central management of access policies
      * Supports RADIUS and TACACS+
    - NAC Appliance-Based Overlay solution
      * NAC manager is the policy server works to authenticate users and their devices over wired, wireless and VPN connections
      * Cisco NAC profiler and Cisco NAC Guest server
* Cisco Secure ACS, High-performance and Scalability
  + Ease of use
    - Web based user interface
  + Scalability
    - Large networked environments with redundant servers, remote databases and database replication/backup services
  + Extensibility
    - LDAP authentication forwarding supports the authentication of user profiles
  + Management
    - Microsoft Windows Active Directory support consolidates windows username and passwords
  + Administration
    - Different access levels
    - Easier and more flexible
  + Product flexibility
    - Support for AAA
  + Integration
  + Third-party support
    - Offers token server support for any one-time password (OTP)
  + Control
    - Dynamic quotas to restrict access
      * Time of day, network use, number of logged sessions and day of the week
* Cisco Secure ACS Software and Hardware Implementation Options
  + Installed on Windows Server or on 1U, rack-mountable, security-hardened server (ACS Solution Engine)
* Software and Network Requirements for Cisco Secure ACS
  + Before installing Cisco Secure ACS you have to prepare
  + Network and Port Prerequisites
    - Cisco devices not Cisco IOS AAA, must be configured with TACACS+, RADIUS or both
    - Dial-in, VPN or wireless must be able to connect to AAA clients
    - Computer must be able to reach all AAA clients using ping
    - Gateway devices and other network devices must permit communication over ports
    - Supported web browser must be installed
    - NICs in computer must be enabled
* Cisco Secure ACS Home Page
  + Buttons
    - User setup
    - Group setup
    - Shared profile components
    - Network configuration
    - System configuration
    - Interface Configuration
    - Administration control
    - External user databases
    - Posture validation
    - Network access profiles
    - Reports and activity
    - Online documentations
* Cisco Secure ACS Databases
  + Can be configured to forward authentication of users to one or more external user databases
  + Three major configuration options for ACS external databases
    - Unknown User Policy
      * Authentication procedure for users not in Cisco Secure ACS database
    - Database Group Mappings
      * Group privileges on external database users
    - Database Configuration
      * External servers
      * Parameters of external servers
        + RSA securID token server
        + RADIUS token server
        + External ODBC database
        + Windows database
        + LEAP proxy RADIUS server
        + Generic LDAP
* Cisco Secure ACS User Database Setup
  + Configured to communicate with an external user database
    - By specific user assignment
      * Specific users
    - By unknown user policy
      * Users no found in Cisco Secure user database
* Monitoring Authentication Traffic
  + Debug aaa authentication
    - Troubleshooting
  + Command indicates a status message of PASS when a TACACS+ login attempt is successful
* Introduction to Server-Based AAA Authorization
  + TACACS+ establishes a new TCP session for every authorization request
* AAA Authorization Types
  + Service type can specify the types of commands or services
    - Commands level
      * Exec (shell) commands
    - Exec
      * Starting an exec (shell)
    - Network
      * Network services (PPP, SLIP, ARAP)
  + Not enabled all users are allowed full access
* Introduction to Server-Based AAA Accounting
  + Enables usage tracking, dial-in access, log the data gathered to a database, produce reports on data gathered
  + Create a list of changes, and the exact nature of the changes. Knowing this information helps the troubleshooting process if the changes cause unexpected results
* AAA Accounting Configuration with the CLI
  + Network
    - Accounting for all network related service requests
      * Serial line internet protocol (SLIP)
      * PPP
      * PPP Network Control Protocols (NCPs)
  + Exec
    - Accounting for EXEC shell session
  + Connection
    - Accounting on all outbound connections
      * Telnet
      * Local area transport (LAT)
  + Default
    - Listed accounting methods follow keyword as default list of methods
  + List-name
    - Character string used to name a custom accounting method list
  + Start-stop
    - Sends “start” accounting notice at beginning and “stop” accounting at the end
  + Stop-only
    - Sends “stop” accounting record for all causes like authentication failure
  + None
    - Disables accounting services on a line or interface
  + Broadcast
    - Enables sending accounting records to multiple servers
* Summary
  + AAA provides a scalable framework for enabling administrative access
  + Controls who is allowed to connect to the network
  + Small or simple networks, AAA can be implemented using local database
  + Larger of complex, AAA can be implemented using server-based AAA
  + Servers can use RADIUS or TACACS+ to communicate with client routers
  + Cisco Access COntrol Server (ACS) can be used to provide AAA server services

# Authentication, Authorization, and Accounting

Network must be designed to control who is allowed to connect and what they can do when connected

These design specifications are identified in the network policy

The policy specifies how people like administrators, users, and clients can access network resources.

Policy can also mandate an accounting system that tracks people logging in and what they did

Managing a network using only user mode or privilege mode password commands is limited and does not scale well.

Using the Authentication, Authorization, and Accounting (AAA) protocol provides necessary framework to enable scalable access security

Routers can be configured to use AAA to access a local username and password database which provides greater security

Router can also be configured to access a Cisco Secure Access Control Server (ACS).

Using ACS is scalable because all infrastructure devices access a central server. Is also fault tolerant because multiple servers can be configured. Used by large organizations

One way of protecting from intruders is to access the control that certain people have and allowing only certain people.

That can be done with many different types of authentication. Simplest form is using passwords configuring a login and password combination on console, vty, and aux ports.

The above method is implemented but is also the weakest and least secure, these passwords are very vulnerable to brute-force attacks, and provides no accountability

To help provide accountability use local database authentication

This method provides user accounts with an password which makes it a little more secure because attackers need to know the username

It also provides more accountability cause it records when a user logs in

Local database method does have some limitations:

* User accounts must be configured locally on each device
* With large networks, it can take time to implement and change local database
* No fallback authentication method is administrator forgets username and password. Thus, password recovery becomes the only option

Better solution is to have all devices refer to the same database from a central server which is where AAA comes in.

## AAA Components

AAA provides the primary framework to set up access control on a network device.

Provides higher degree of scalability than methods described before

The functional components:

* Authentication - Users and administrators must prove that they are who they are. Can be established using username and password combinations, challenge and response questions, token cards, and other methods.
* Authorization - After user gets authenticated, this determines what they have access to and what they can do
* Accounting and auditing - Records whatever the user does, including what is accessed, amount of time the resource is accessed, and any changes that were made. Keeps track of how network resources are used

## AAA Characteristics

### Authentication Modes

Can be used to authenticate users for administrative access or remote network access. The 2 access methods use different modes to request AAA services:

| Access Type | Modes | Router Ports | Common AAA commands |
| --- | --- | --- | --- |
| Remote administrative access | Character Mode provides user and privileged EXEC access | Console, vty, aux, and tty | `login`, `exec`, and `enable` commands |
| Remote network access | Packet Mode provides access to network resources | Dial-up and VPN access | `ppp` and `network` commands |

Character mode - A user sends a request to establish an EXEC mode process with the router for administrative purposes

Packet mode - A user sends a request to establish a connection through the router with a device on the network

Except for accounting commands, all AAA commands apply to both character mode and packet mode

Two methods of implementing AAA services:

* Local AAA Authentication
  + Uses the local database for authentication. Ideal for small networks
* Server-Based AAA Authentication
  + Uses an external database server resource that leverages RADIUS or TACACS+ protocols
  + Examples include Cisco ACS for Windows Server.
  + If there are more routers, server-based AAA is more appropriate

### Authorization

After users are successfully authentication, they are then authorized for specific network resources

What a user can and cannot do on the network after that user is authentication

Typically implemented using a AAA server-based solution

Uses a created set of attributes that describes the user’s access to the network

These attributes are compared to the information in the AAA database, and determined what the user can or cannot do and sent to the local router

Authorization is automatic and does not require users to perform additional steps and is implemented immediately after login

### Accounting

Collects and reports usage data so it can be used for purposes such as auditing or billing

Collected data might include the start and stop connection times, executed commands, number of packets, and number of bytes

Implemented using an AAA server-based solution and sent to the ACS server

One widely deployed use of accounting is combining it with AAA authentication for managing access to devices

Accounting provides more security than just authentication

Logs are extremely detailed on the ACS server

### Introduction to Server-Based AAA Authorization

* Authentication is concerned with ensuring that the device or end user is legitimate
* Authorization is concerned with allowing and disallowing authenticated users access to certain areas and programs on the network.
* TACACS+ allows the separate of authentication from authorization
* A router can be configured to restrict the user to performing only certain functions after successful authentication and can be configured for both character mode (exec authorization) and packet mode (network authorization).
* RADIUS does not separate the authentication and authorization processes
* Gives the ability to control user access to specific services
* If the command is allowed for a user then there is a ACCEPT response from the ACS otherwise there is a REJECT response from the ACS
* By default TACACS+ establishes a new TCP session for every authorization request, which can lead to delays when users enter commands
* Cisco Secure ACS supports persistent TCP sessions to improve performance

### Introduction to Server-Based AAA Accounting

* Often need to keep track of which resources individuals or groups use.
* AAA Accounting enables usage tracking, such as dial-in access, to log the data gathered to a database, and to produce reports on the data gathered
* Accounting is generally considered a network management or financial management issue.
* One security issue that is addressed by accounting is the creation of a list of users and the time of day they dialed into the system.
* Creates a list of changes occuring on the network, the user that made the changes, and the exact nature of the changes
* Cisco Secure ACS serves as a central repository for accounting information, essentially tracking events that occur on the network
* Each session that is established can be fully accounted for and stored on the server
* Like authentication and authorization method lists, method lists for accounting define the way accounting is performed and the sequence in which these methods are performed
* After it is enabled, the default accounting method list is automatically applied to all interfaces, except those that have a user-defined, or custom, accounting method list explicitly defined

## Configuring AAA

### Local AAA Authentication

Also referred to as self-contained authentication

The Local AAA Authentication method is similar to using `login local` command with one exception, it also provides a way to configure backup methods of authentication

Configuring local AAA services to authenticate administrator access (character mode access) requires a few basic steps:

1. Add usernames and passwords to the local router database for users that need administrative access to the router
2. Enable AAA globally on the router
   1. `aaa new-model`
3. Configure AAA parameters on the router
   1. `aaa authentication login default local-case`
   2. `aaa local authentication attempts max-fail 10`
   3. The `default` keyword specifies that it applies to all lines
4. Confirm and troubleshoot the AAA configuration

To enable AAA use: `aaa new-model` and to disable use: `no aaa new-model`

After AAA is enabled, to configure authentication on vty ports, asynchronous lines (tty), the aux port, or the console port, define a named list of authentication methods and then apply that list to the various interfaces

To define a named list usr the following command:

`aaa authentication login {default | <list-name>} <method1> … [<method4>]`

* The default keyword means to use the listed authentication methods that follow this keyword as the default list of methods when a user logs in. It also applies the method list to all interfaces and lines
* <list-name> is the Character string used to name the list of authentication methods activated when a user logs in
* <method1> … [<method4>] identifies the list of methods that the AAA authentication process will query in the given sequence. At least one method must be specified. A maximum of four methods may be specified

The method list is a sequential list describing the authentication methods to be queried for authenticating a user and enabled an administrator to designate one or more security protocols for authentication and using more than one protocol provides a backup system for authentication

| Method Type Keywords | Description |
| --- | --- |
| `enable` | Uses the enable password for authentication |
| `krb5` | Uses Kerberos 5 for authentication |
| `krb5-telnet` | Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router |
| `line` | Uses the line password for authentication |
| `local` | Uses the local username database for authentication |
| `local-case` | Uses case-sensitive local username authentication |
| `none` | Uses no authentication |
| `cache <group-name>` | Uses a cache server group for authentication |
| `group radius` | Uses the list of all RADIUS servers for authentication |
| `group tacacs+` | Uses the list of all TACACS+ servers for authentication |
| `group <group-name>` | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the `aaa group server radius` or `aaa group server tacacs+` command |

The list of authentication methods above must be applied to specific interfaces or lines.

To enable on a line or interface use the following command:

`login authentication <list-name>`

Additional security can implemented on the line using the following global configuration command:

`aaa local authentication attempts max-fail <number-of-unsuccessful-attempts>`

The above command secures AAA user accounts by locking them out.

To display a list of all locked-out users use:

`show aaa local user lockout`

Use the following command to unlock a specific user or all locked user:

`clear aaa local user lockout {username <username> | all}`

To show attributes that are collected for a AAA session:

`show aaa user {all | <unique-id>}`

The following command can be used to show the unique ID of a session:

`show aaa session`

#### Debug Options

You can use:

`debug aaa <type>`

To figure out type you can just type a ?

To disable prepend `no` or use `undebug all`

### Configuring Server-Based AAA Authentication

1. Globally enable AAA
2. Specify the Cisco Secure ACS that will provide AAA services for the router. Can be a TACACS+ or RADIUS server.
3. Configure the encryption key needed to encrypt the data transfer between the network access server and Cisco Secure ACS
4. Configure the AAA authentication method list to refer to the TACACS+ or RADIUS server. For redundancy, it is possible to configure more than one server

#### Configure a TACACS+ Server and Encryption Key

##### To configure a TACACS+ Server

`tacacs-server host <ip-address> single-connection` or `tacacs server host <ip-address> single-connection`

* Single-connection keyword enhances TCP performance by maintaining a single TCP connection for the life of the session. Otherwise, by default, a TCP connection is opened and closed for each session. If required, multiple TACACS+ servers can be identified by entering their respective IP address using the `tacacs-server-host` command

##### Configuring an Encryption Key

`tacacs-server key <key>` or `tacacs server key <key>`

Use that command to configure the shared secret key to encrypt the data transfer between the router and the server. This key must be the same as the TACACS+ server

### Configure a RADIUS server and Encryption key

##### Configuring an RADIUS Server

`radius-server host <ip-address>` or `radius server host <ip-address>`

Because RADIUS uses UDP, there is no equivalent `single-connection` keyword

#### Configuring an RADIUS encryption key

`radius-server key <key>` or `radius server key <key>`

### Configuring Authentication to Use the AAA Server

`aaa authentication login <type> { default | <list-name>} <memory1> … [<memory4>]`

EX: `aaa authentication login default group tacacs+ group radius local-case

### Troubleshooting Server-Based AAA Authentication

`debug aaa authentication`

The above command indicates a status message of PASS when a TACACS+ login attempt is successful

`debug radius ` and `debug tacacs` are both useful commands

### Configuring Server-Based AAA Authorization

`aaa authorization { network | exec | commands <level> } { default | <list-name>} <method1> … [<method4>]`

* commands <level> - for exec (shell) commands
* exec - for starting an exec (shell)
* network - for network services (PPP, SLIP, ARAP)

When AAA authorization is not enabled, all users are allowed full access. After authentication is started, the default changes to allow no access

Thus, the administrator must create a user with full access rights before authorization is enabled.

Only way to recover from that is a reboot

To enable on an interface use:

`authorization`

### Configuring Server-Based AAA Accounting

`aaa accounting {network | exec | connection} {default | <list-name>} {start-stop | stop-only | none } [broadcast] <method1> … [<method4>]`

* Network - runs accounting for all network-related service requests, including SLIP, PPP, and NCPs
* Exec - runs accounting for the EXEC shell session
* Connection - Runs accounting on all outbound connections made from the network access server, such as Telnet or local-area transport (LAT)
* Default - Uses the listed accounting methods that follow this keyword as the default list of methods
* List-name - Character string used to name a custom accounting method list
* Start-stop - senda a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process
* Stop-only - Sends a “stop” accounting record for all cases including authentication failure
* None - Disabled accounting services on a line or interface
* Broadcast (optional) - Enables sending accounting records to multiple AAA servers

# Implementing Virtual Private Networks

### Module 18

* Introduction
  + Use VPNs to create an end to end private network connection over third-party networks (internets or extranets)
  + Eliminates distance barrier and enables remote user to access central site network resources
  + IP security (IPsec) protocol provides framework for configuring secure VPNs. Reliable way to maintain communication privacy while streamlining operations, reducing costs and allowing flexible network administration
  + Secure site to site VPNs between central and remote sites can be used using IPsec or Secure Sockets Layer (SSL)
* Introducing VPNs
  + VPN is a private network that is created through tunneling over a public network (internet) instead of using a dedicated physical connection. Uses virtual connections routed through the internet from the organization to a remote site.
  + Carries information within a private network
    - Actually transported over a public network
  + VPN is private in that the traffic is encrypted to keep data confidential
  + Multiple benefits
    - Cost Savings
      * Enable organizations to use cost-effective, third-party internet transport to connect remote offices and remote users
      * Eliminate expensive WAN links and modern banks
      * Advent of cost-effective, high bandwidth technologies (DSL)
    - Security
      * Provide highest level of security by using advanced encryption and authentication
    - Scalability
      * Enable corporations to use internet infrastructure within ISPs
        + Make new users
    - Compatibility with broadband technology
      * Allow mobile workers, telecommuters and people who want to extend
      * Take advantage of high-speed, broadband connectivity
* Types of VPNs
  + Connects two endpoints
  + Logical connections can be made of Layer 2 or Layer 3
  + Layer 3 VPNs
    - Generic routing encapsulation (GRE)
      * Standardized as RFC 1701
      * Delivery header for GRE is defined in RFC 1702
      * Private data is encapsulated in GRE header
    - MPLS
      * Tag switching and later standardized through the IETF
      * Use labels to encapsulate original data
    - IPsec
      * Backing of IETF
      * Provide significant cost savings
      * Allow authentication, integrity, access control and confidentiality
      * Can be encrypted and verified
    - Point to point site (GRE/IPsec)
    - Any to any connectivity to many sites (MPLS)
* Site to Site and Remote Access VPNs
  + Site to site
    - Connection devices on both sides are aware of VPN configuration
    - Remains static
    - Internal hosts have no knowledge
    - Frame Relay, ATM, GRE and MPLS
  + Remote access
    - Info is not statically set up
    - Allows dynamic changing
      * Can be enabled/disabled
* Site to Site VPN
  + Extension of classic WAN
  + Connects entire networks to each other
  + Hosts send and receive normal TCP/IP traffic through gateway (router, firewall, Cisco VPN concentrator or Cisco ASA)
    - Encapsulating and encrypting outbound traffic
* Remote Access VPN
  + Evolution of circuit switching networks
    - Plain old telephone service (POTS)
    - Integrated services for digital network (ISDN)
  + Support client/server architecture VPN client (remote host) requires secure access
* VPN Client Software options
  + Each host has Cisco VPN client software
    - When host sends traffic for VPN the software encapsulates and encrypts traffic
* Cisco IOS SSL VPN
  + Provides remote-access connectivity with a web browser and native SSL encryption
  + Provides flexibility to support secure access
  + Three modes
    - Clientless
    - Thin Client
    - Full Client
  + Allow user to access web pages and services
    - Accessing files, sending and receiving email and running TCP-based application without IPsec
  + Primary benefits
    - Dynamic multipoint VPNs (DMVPNs)
    - Cisco IOS firewalls, IPsec
    - Intrusion prevention systems (IPSs)
    - Cisco Easy VPN
    - Network Address translation (NAT)
* Cisco VPN Product Lines
  + Several devices to support remote and site to site VPN
    - Cisco VPN enabled routers and switches
    - Cisco PIX 500 series security appliances
      * Robust, enterprise class, integrated network security services, including stateful inspection firewall, deep protocol and application inspection and IPsec VPN
      * End of sale and end of life
    - Cisco ASA
      * All in one security appliances that deliver enterprise-class security and IPsec VPN to small and medium business
      * Wide range of security services
        + Firewall, IPS, VPN
    - Cisco VPN 3000 series concentrators
      * Offers both IPsec and SSL
      * End of sale and end of life
    - SOHO routers
      * Broadband home routers
        + Cisco 850 Series ISR, Linksys routers
* Cisco IOS VPN Feature Support
  + Provides a suite of VPN-optimized routers
  + Adds strong security using encryption and authentication
  + Provide high performance for site to site, intranet and extranet
  + VPN Features
    - Voice and Video Enabled VPN (V3PN)
      * Integrates IP telephony, QoS and IPsec
      * End to end VPN service
      * Timely delivery of latency sensitive applications (voice and video)
    - IPsec stateful failover
      * Fast and scalable network resiliency for sessions between remote and central sites
      * Stateless and stateful failover solutions available
        + Hot Standby Router Protocol (HSRP)
      * Ensures maximum uptime of mission-critical applications
    - Dynamic Multipoint Virtual Private Network (DMVPN)
      * Enables auto-provisioning of site to site IPsec
      * Three Cisco IOS software features: NExt Hop Resolution Protocol (NHRP), multipoint GRE, IPsec VPN
    - IPsec and MPLS integration
      * Enables ISPs to map IPsec sessions
      * Colocated edge routers connected to MPLS provider edge (PE) network
      * Enables ISP to securely extend
    - Cisco Easy VPN
      * Simpilies VPN deployment to remote offices and teleworkers
      * Centralizes management
      * Reducing management complexity
* VPN Services with Cisco ASA
  + Features of Cisco ASA provides
    - Flexible platform
      * Offers IPsec and SSL VPN on single platform
      * Application inspection firewall and intrusion prevention services
    - Resilient clustering
      * Remote-access deployments
    - Cisco Easy VPN
      * Scalable, cost effective and easy to manage remote access
    - Automatic Cisco VPN client updates
      * Enables software operating on remote desktops to automatically update
    - Cisco IOS SSL VPN
      * Clientless and thing client capabilities
    - VPN infrastructure for contemporary applications
      * Enables converged voice, video and data across secure IPsec network
        + Combine site to site VPN support
    - Integrated web-based management
      * Provides management
      * Using integrated web-based Cisco Adaptive Security Device Manager (ASDM)
    - Cisco ASA 5505
      * 10 IPsec
      * 25 SSL VPN peers
      * 25 VPN peers
    - Cisco ASA 5510
      * 250 VPN peers
    - Cisco ASA 5520
      * 750 VPN peers
    - Cisco ASA 5540
      * 5,000 IPsec peers and 2500 SSL VPN peers
    - Cisco ASA 5550
      * 5,000 VPN peers
    - Cisco ASA 5585-X
      * 10,000 VPN peers
* Cisco IPsec VPN clients
  + Three IPsec clients
    - Cisco VPN client software
      * Installed on PC or laptop
      * Organizations to establish end to end encrypted VPN tunnels
      * Client receives security policies from the central site VPN device
    - Cisco Remote Router VPN Client
      * Remote router connects to small offices LANs to the VPN
    - Cisco AnyConnect Secure Mobility Client
      * Provide remote users with secure connections
      * Available for windows, mac, linux
      * Some smart devices
* Cisco VPN Hardware modules
  + VPN advanced integration module (AIM)
    - Broad range of cisco routers are equipped with it
    - Installed inside ISR chassis to offload encryption from CPU
  + Cisco IPsec VPN shared port adapter (SPA)
    - Scalable and cost effective VPN performance
      * Cisco Catalyst 6500 series switches
      * Cisco 7600 series/catalyst 6500 series services SPA carrier-400
  + CIsco VPN accelerator module 2+ VAM2+
    - Encryption/compression
    - Key generation services (IPsec applications)
      * Instals in Cisco 7204VXR, 7206VXR and 7301 routers
* Introduction to GRE Tunnels
  + Defined in RFC 1702 and RFC 2784
  + Creating a virtual point to point link at remote points over an IP internet work
  + Supports multi protocol tunneling
  + Encapsulate multiple OSI Layer 3 protocol
  + Stateless, endpoint keeps no info about the state or availability of the remote tunnel endpoint
  + Service providers (SPs)
* GRE Header
  + Encapsulates entire original IP packet with standard IP header and GRE header
  + Two 2-byte mandatory fields
    - GRE flag
    - Protocol type
  + Type field in header supports encapsulation of an OSI Layer 3
  + 24 bytes of additional overhead for tunneled packets
* Configuring GRE
  + It is up if
    - Tunnel source and destination are configured
    - Tunnel destination is in routing table
    - GRE keepalives are received (if used)
    - GRE is the default mode
* GRE with IPsec
  + Can be used to tunnel non-IP traffic over an IP network
  + Only supports unicast traffic (IPsec)
  + GRE supports multicast and broadcast traffic over link
  + Doesn’t provide encryptions
* IPsec as an IETF Standard
  + IETF standard (RFC 2401-2412)
    - Defines how VPN can be configured using IP addressing
  + Provides data confidentiality, data integrity and origin authentication
  + Not bound by any specific encryption, authentication, security algorithms or keying technology
  + Works on network layer
  + Implemented from Layer 4 - Layer 7
  + Plaintext layer 3 header
  + Functions over all Layer 2 protocols
    - Ethernet, ATM, Frame Relay, synchronous data link control (SDLC) and high level data link control (HDLC)
  + Five Building Blocks
    - First
      * IPsec protocol
        + Authentication Header (AH)
        + Encapsulation Security Protocol (ESP)
    - Second
      * Type of confidentiality implemented using encryption
        + Data encryption Standard (DES)
        + Triple DES (3DES)
        + Advanced Encryption Standard (AES)
        + Software optimized encryption algorithm (SEAL)
    - Third
      * Integrity that can be implemented using message digest 5 (MD5) or Secure Hash Algorithm (SHA)
    - Fourth
      * Shared secret key is established
      * Preshared keys (PSK) or digitally signed using RSA
    - Fifth
      * Diffie-hellman (DH) algorithm group
      * Four separate DH key exchange algorithm to choose from
        + DH1, DH2, DH5 and DH7
  + IPsec can secure a path between pair of gateways, a pairs of hosts or a gateway and host
  + Security functions
    - Confidentiality
      * Ipsec ensures confidentiality by using encryption
      * Achieved through encryption of traffic as it travels
      * Encryption algorithms and key lengths
        + DES

56 bit key

High performance encryption

Symmetric key cryptosystem

* + - * + 3DES

Variant 64 bit DES

Three independent 56 bit encryption per 64 block

Stronger encryption

Symmetric key cryptosystem

* + - * + AES

Stronger security (DES)

Computationally more effective (3DES)

Three different key lengths

128, 192, 265

Symmetric key cryptosystem

* + - * + Software-optimized Encryption Algorithm (SEAL)

160 bit key

Symmetric key cryptosystem

* + - Integrity
      * IPsec ensures data arrives unchanged
      * HMAC, Hashed Message Authentication Code, guarantees integrity of message using hash value
      * Two HMAC
        + HMAC Message Digest %

128 bit shared secret key

* + - * + HMAC Secure HAsh Algorithm 1

160 bit

Considered stronger

* + - Authentication
      * Uses internet Key exchange (IKE) to authenticate users and devices
      * Usernames, password, one time password, biometric, pre shared keys and digital certificates
      * Two primary methods of configuring peer authentication
        + Pre-shared Keys (PSKs)

Pre shared secret key in each peer manually used to authenticate peer

COmbine with other info to form authentication key

* + - * + RSA signatures

Exchange of digital certificates authenticates peers

Derives hash and encrypts it with private key

* + - Secure Key exchange
      * Uses DH algorithm to provide a public key exchange method for two peers to established a shared secret key
      * Several DH groups
        + DH 1, 2, 5

Support exponentiation over a prim modulus with 768 bits, 1024 bits and 1536 bits

* + - * + DH 14, 15, 16

2048 bits, 3072 bits, 4096 bits

* + - * + DH 19, 20, 24

Support Elliptical Curve Cryptography (ECC)

256 bits, 384 bits, 2048 bits

* IPsec Framework Protocols
  + Open standards
  + Spends it the messaging to secure the communications
  + Authentication Header(AH) and Encapsulation Security Protocol (ESP)
  + AH
    - IP protocol 51
    - Confidentiality is not required or permitted
    - Data authentication and integrity between two systems
    - No encryption
  + ESP
    - IP protocol 50
    - Confidentiality and authentication
      * Encryption and authentication for inner IP packet and ESP header
    - Data origin authentication and data integrity
    - Encryption and authentication are option in ESP, but one must be selected
* Authentication Header
  + AH applies a keyed one way hash function to a packet to create hash/message digest
  + Order
    - IP header and data payload are hashed using the secret key
    - Hash builds a new AH header
    - New packet is transmitted to IPsec peer router
    - Peer router hashes IP header and data payload, extracts transmitted hash and compares
* ESP
  + Provides confidentiality by encrypting payload
  + Supports multiple symmetric encryption algorithms
  + Default is 56 bit DES
  + Provide integrity and authentication
    - Payload is encrypted
    - Encrypted payload is sent through hash algorithm
  + ESP can enforce anti-replay protection
    - Each packet is unique and not duplicated
* Transport and Tunnel Modes
  + ESP and AH can be applied to IP packets to modes
    - Transport Mode
      * Only for transport layer of OSI model and above
      * Protects payload of packet and leaves original IP address in plaintext
        + Used to route the packet
      * Used between hosts. Works well with GRE
    - Tunnel Mode
      * Security for completel original IP packet
      * Encrypted and then encapsulated
      * Ip in IP encryption
        + Ip address on the outside of IP packet is used to rout packet
      * Between host and a security gateway or between two security gateways
* Security Associations
  + Solution negotiates key exchange parameters establishes a shared key, authenticate the peer and negotiate the encryption parameters
    - Security Association (SA)
      * Basic building block of IPsec
        + Maintained in SA database (SADB)
      * IKE calculates shared keys based on exchange of series of data packets
        + Disables third party from decrypting the keys
        + Layered on UDP and uses UDP port 500 to exchange IKE info
      * IKE is defined in RFC 2409
        + Hybrid: Internet Security Association and Key Management Protocol (ISAKMP) and Oakley and Skeme Key exchange methods

ISAKMP = message format

* + - * + Oakley supports

Group 1, 758 bit, Group 2, 1024 bit, group 5, 1536 bit

* IKE Phase 1 and Phase 2
  + Phase 1
    - Two IPsec peers perform initial negotiation of SAs
      * Policy sets, authenticate peers and set up secure channel
    - Transform sets, hash methods are determined
  + Phase 2
    - SAs are negotiated by IKE process ISAKMP
* Three Key Exchanges
  + First
    - Between initiator and responder establishes basic security policy
    - Peer negotiate and agree
    - Protocols are group into sets, IKE policy sets
  + Second
    - Creates and exchanges DH public keys between two endpoints
  + Third
    - Each end device must authenticate the other end
    - Initiator and recipient authenticate each other
    - Three data origin authentication
      * PSK
      * RSA signature
      * RSA encrypted nonce
* Aggressive Mode
  + Three exchanges occurred during main mode
    - Outcome = secure communication path for subsequent exchanges between peers
  + Aggressive mode is faster, fewer exchanges
  + Main modes requires three exchanges with six packs
  + Aggressive mode packets
    - First
      * Intiaitor packages, needed for SA negotiate in first message, DH public key
    - Second
      * Recipient responds with the parameters, authentication information and DH public key
    - Third
      * Initiator sends a confirmation that it received info
* IKE Phase 2
  + Negotiate the IPsec security parameters to secure IPsec tunnel, called quick mode. Only occur after IKE has established secure tunnel
  + SAs are negotiated
  + Phase 2 performs
    - Negotiates IPsec security parameters, IPsec transform sets
    - Establishes unidirectional IPsec SAs
    - Periodically renegotiates IPsec SAs to ensure security
    - OPtionally performs additional DH exchange
* IPsec VPN Negotiation
  + VPN = communication channel between two endpoints
    - Don’t necessarily include encryption or authentication
  + IPsec VPNs rely on IKE protocol to establish secure connections
  + IPsec negotiation involves 5 steps
  + 1. IPsec tunnel is initiated, traffic travels between peers and meets criteria
  + 2. IKE Phase 1 begins. Peers negotiate the established IKE SA policy, secure tunnel is created using ISAKMP
  + 3. IKE PHase 2 begins. Use authenticated secure tunnel to negotiate IPsec SA transform.
  + 4. IPsec tunnel is created, data is transferred
  + 5. IPsec terminates
* Protocols 50 and 51 and UDP Port 500
  + Configuring Cisco IOS ISAKMP ensure existing ACLs on perimeter routers, firewalls do not block IPsec traffic
  + Not blocked
    - ESP is assigned IP protocol number 50
    - AH is assigned IP protocol number 51
    - ISAKMP uses UDP port 500
* Negotiating ISAKMP Policies
  + Two endpoints must negotiate the policies
  + Peer that initiates negotiate sends all policies to remote peer. Remote peer tries to find match with policies
  + Match is made when both policies have same encryption, ash, authentication, DH parameter value and when policy of remote peer specifies a lifetime less or equal to that being compared
* Defining Transform sets
  + Combination of individual IPsec transforms that are designed to enact a specific security policy
  + COnsist of AH transform, ESP transform and IPsec mode
  + Limited to one AH and one or two ESP
* Configuring Transform Sets
  + Negotiated during IKE Phase 2 quick mode
* Defining Crypto ACLs
  + Crypto ACLs identify traffic flow to protect
    - Outbound select outbound traffic that IPsec should protect
  + Traffic not selected is sent in plaintext
  + Inbound can create filter and discard traffic
  + Extended IP ACLs select IP traffic to encrypt, Ip address, network, subnet and port
* Symmetric Crypto ACLs
  + Must be configured for use by IPsec
  + Decrypt by viewing source and destination in ACL in reverse order
  + Applied to forward direction to traffic exiting router and backward direction to traffic entering
    - Outbound ACL source become inbound ACL destination
* Defining Crypto Maps
  + Created for IPsec combine the needed configuration parameter of IPsec SA’s
    - Which traffic to protect
    - Granularity of flow to be protected by set of SAs
    - Who the remote IPsec peers are. Determining where the IPsec-protected traffic is sent
    - Local address used for IPsec traffic (optional)
    - Which type of Ipsec security is applied
      * Choosing from list, one or more transform sets
    - Key management method
    - SA lifetimes
  + Only one crypt map can include a combination of Cisco Encryption Technology (CET) and Ipsec using IKE
  + Create multiple crypto map entries for a given interface if
    - Separate IPsec peers handled different data flows
    - Different IPsec security must be applied to different types of traffic to same or separate IPsec peers
  + IKE not used to establish a particular set of SA’s and multiple ACL must be specified
* CCP VPN Wizards
  + VPN folder, subfolders
    - SSL VPN
      * Used to configure SSL VPNs parameters
    - The GET VPN
      * Used to configure GET VPN parameters
    - VPN components
      * Used to configure VPN components
        + IPsec, IKE, Easy VPN server group policies and browser proxy settings and VPN keys encryption
* Quick setup and step by step wizard
  + Quick setup uses CCP default IKE policies and IPsec transform sets
    - Enables junior admin
  + Step by step
    - Allows admin to specify details of IPsec VPN, IKE and Ipsec policy configuration steps
* Quick setup
  + Parameters
    - Interface to use for VPN connection (outside interface)
    - Peer identity info, type of peer and Ip address of the peer
    - Authentication method
      * PSKs, you specify the secret
      * Digital certifications, you choose certificate that has been created before
    - Traffic to encrypt identifying source interface and destination IP subnet
* Step by Step wizard
  + Parameters
    - Connection settings (outside interface, peer identify and authentication credentials)
    - IKE proposal (priority, encryption , HMAC algorithm, IKE authentication method, DH group and IKE lifetime)
    - IPsec transform set info (name, integrity algorithm, encryption algorithm, mode of operation and compression)
    - Traffic to protect, identify single source and destination subnets or defining an ACL for se of more complex VPNS
* Advantages of Telecommuting
  + Sometimes called telworking
  + Have flexibility in location and hours
  + Save on real estate, utility and other costs
* Benefits of Telecommuting
  + Offers organization, social and environmental benefits
* Teleworker WAN connection options
  + Typically need high speed access
    - Broadband connections (DSL, Cable or satellite)
  + DSL = 200 kb/s
    - Homes use asymmetric DSL
  + Cable = 200 kb/s
    - Not affected by distance to ISP
    - Shared service. Degree of number of subscribers in the network
  + Satellite internet = 128 kbps to 512 kb/s
  + May require a VoIP
* Remote-Access VPN Options
  + Two Primary Methods for deploying remote-access
    - IPsec
    - SSL
      * Doesn’t require software client to be preinstalled on endpoint host
      * Integrate security and routing. Browser based network
      * Supports multiple cryptographic algorithms
        + Authenticating server and client, transmitting certificates and establishing session keys
      * Feature and benefits
        + Web based clientless access and full network access without preinstalled software

Based on user and security requirements minimizes support costs

* + - * + Protect against viruses, worms, spyware and hackers

Integrating network and endpoint security

* + - * + Simple, flexible cost effective

Uses single license

* + - * + Single device for both SSL VPN and IPsec VPN

Reduces costs

* + - * Types
        + Clientless Access Mode

Remote user accesses internal or corporate network using web browser

No specialized VPN software

All traffic is transmitted and delivered through standard web browsers

* + - * + Thin Client

TCP port forwarding

CLient application uses TCP to connect to server and port

Download Java applet, acts as TCP proxy.

Starts a new SSL connection for every client connection

Initiates HTTP request from remote user to SSL gateway

Referred as type of clientless mode. Extends functions of web browser to enable TCP stuff, POP3, SMTP, IMAP, Telnet and SSH

* + - * + Full client

Enables complete access to network over SSL tunnel

Move data at the Network (IP) Layer

Java applet is downloaded to handle tunneling

* + SSL VPN Design
    - Considerations
      * User connectivity
        + Determine whether users connect corporate network
      * Router feature
        + Router can run various features, Ipsec VPN tunnels, routing engines, firewall process
      * Router Hardware
        + Fairly CPU and memory intensive
      * Infrastructure Planning
        + COnsider placement of VPN termination devices
      * Implementation Scope
        + Network security admin need to determine size
* Introducing Cisco Easy VPN
  + Three components
    - Cisco Easy VPN Server
      * Router or Firewall acting as VPN head-end device in site to site or remote access VPNs
    - Cisco Easy VPN remote
      * Router or firewall acting as remote VPn client
    - Cisco VPN client
      * Application supported on PC used to access server
    - Cisco Easy VPN
      * Negotiates tunnel parameters
      * Establishes tunnels according to set parameters
      * Automatically creates a NAT / PAT and associated ACL
      * Authenticates users by usernames, group names and passwords
      * Manages security keys for encryption and decryption
      * Authentication encrypts and decrypts data through the tunnel
* Initial Easy VPN Server Steps
  + - Needed specified custom policies
      * Interface on which client connections terminate
      * IKE policy
      * Authentication (PRE\_SHARE or RSA\_SIG)
      * D-H group (1, 2, 5)
      * Encryptionalgorithm (DES, 3DES, AES)
      * Hash (SHA\_1 or MD5)
      * IKE lifetime
* Selecting the Transform Set
  + Transform set name
  + Encryption algorithm such as DES, 3DES, AES or SEAL
  + HMAC, SHA\_1 or MD5
  + Optional compression
  + Mode of operation, tunnel/transport
* Group Authorization and Group Policy Lookup
  + Local
    - All groups are in router configured in NVRAM
  + RADIUS
    - Router uses RADIUS server for authorization
  + RADIUS and local
    - Can look up policies stored in AAA server database, reached through RADIUS
* Easy VPN Server summary
  + Presents summary of parameters
  + Can then be verified
* Introducing Cisco VPN client
  + Can establish end to end, encrypted VPN tunnels for secure connectivity
* Summary
  + VPN is a private network created through tunneling over a public network
  + Typically site to site VPNS and remote access VPNs are used
  + GRE
    - Tunneling protocol
      * Used to create point to point link to routers
    - Supports multi protocol tunneling
      * IP included
    - Does not support routing protocols
      * Require multicast or broadcasts
    - Supports multicast or broadcast traffic
      * Often used with IPsec
  + VPNs require modern encryption to make sure the information is secure
    - IPsec framework of open standards
    - Relies on existing algorithms
      * Achieves encryption, authentication and key exchange
    - Can encapsulate a packet using Authentication Header (AAH) or other options, ESP
  + IPsec uses LIKE to establish key exchange. Site to site VPN requires
    - Ensure existing ACL’s, firewalls, routers, etc don’t block traffic
    - Define parameters within policy. Used to negotiate for ISAKMP peering
    - Define IPsec transform set
      * Combination of AH transform, ESP transform and IPsec mode
    - COnfigure crypto ACL, defining what traffic is protected through IPsec
    - Apply a crypto map specifies parameters of IPsec SAs
  + Remote access connections can be provided using IPsec VPN solution or SSL VPN
    - SSL provides remote access from an internet enabled location with web browsers and SSL encryption
  + Access Requirements Determine Remote-Access VPN
    - IPsec is better because
      * Number of applications supported
      * Strength of encryption
      * Strength of authentication
      * Overall security

## Commands for configuring VPNs

### Configuring a Site-to-Site GRE Tunnel

Originally developed for Cisco by creating a virtual point-to-point link to Cisco routers at remote points over and IP internetwork

Supports multi protocol tunneling. It can encapsulate multiple OSI Layer 3 protocol packet types inside an IP tunnel.

Adding an additional GRE header between the payload and the tunneling IP header provides the multi protocol functionality

IP tunneling using GRE enables network expansion by connecting multiprotocol subnetworks across a single-protocol backbone environment and supports IP multicast tunneling

Routing protocols that are used across the tunnel enable dynamic exchange of routing information in the virtual network

GRE tunnels are stateless and each tunnel endpoint keeps no information about the state or availability of the remote tunnel endpoint

This feature helps Service Providers provide IP tunnels to customers who are not concerned about the internal tunneling architecture at the SP end. Customers then have the flexibility to configure or reconfigure their IP architecture, but still maintain connectivity

It creates a virtual point-to-point link to routers at remote points over an IP internetwork and does no include any strong security mechanisms to protect its payload

#### GRE Header

GRE encapsulates the entire original IP packet with a standard IP header and GRE header.

A GRE tunnel header contains at least two 2-byte mandatory fields:

* GRE flag
  + Identifies the presence of optional header fields
* Protocol Type
  + Identifies the type of payload; EtherType

GRE uses a protocol type field in the header to support the encapsulation of any OSI Layer 3 protocol

The header along with the tunneling IP header, creates at least 24 bytes of additional overhead for tunneled packets

#### Configuring GRE

5 Steps:

1. Create a tunnel interface using the `interface tunnel 0` command
2. Assign the tunnel an IP address
3. Identify the source tunnel using the `tunnel source` command
4. Identify the destination of the tunnel using the `tunnel destination` command
5. Configure which protocol GRE encapsulates using the `tunnel mode gre` command

NOTE: Also network the VPN network if using OSPF

| Command | Description |
| --- | --- |
| `tunnel mode gre ip` | Specifies that the mode of the tunnel interface is FRE over IP |
| `tunnel source <ip\_address>` | Specifies the tunnel source address |
| `tunnel destination <ip\_address>` | Specifies the tunnel destination address |
| `ip address <ip\_address> <mask>` | Specifies the IP address of the tunnel interface |

##### Commands to Verify

`show ip interface brief`

`show interface tunnel`

#### GRE with IPSec

The advantage of GRE is that it can be used to tunnel non-IP traffic over an IP network.

Unlike IPSec, which only supports unicast traffic, GRE supports multicast and broadcast traffic over the tunnel link. Therefore, routing protocols are supported

GRE does not provide encryption; if that is needed, IPSec should be configured

### Configuring a Site-to-Site IPSec VPN

Configuration Tasks:

1. Ensure that ACLs configured on interfaces are compatible with the IPsec configuration. Usually there are restrictions on the interface that the VPN traffic uses. For example, block all traffic that is no IPsec or IKE
2. Create an ISAKMP policy. This policy determines the ISAKMP parameters that will be used to establish the tunnel
3. Configure the IPsec transform set. The transform set defines the parameters that IPsec tunnel uses. The set can include the encryption and integrity algorithms
4. Create a crypto ACL. The crypto ACL defines which traffic is sent through the IPsec tunnel and protected by the IPsec process
5. Create and apply a crypto map. The crypto map groups the previously configured parameters together and defines the IPsec peer devices. The crypto map is applied ot the outgoing interface of the VPN device

#### Task 1

First step in configuring Cisco IOS ISAKMP is to ensure that the existing ACLs do no block IPsec traffic. Perimeter routers typically implement a restrictive security policy with ACLs, where only specific traffic is permitted, and all other traffic is denied. Such a restrictive policy blocks IPsec traffic. Therefore, specific permit statements must be added

Ensure that the ACLs are configured like so:

* ESP is assigned IP protocol number 50
* AH is assigned IP protocol number 51
* ISAKMP uses UDP port 500

To permit AH trafffic use:

`access-list <acl> permit ahp <source> <wildcard> <destination> <wildcard>`

To permit ESP traffic use:

`access-list <acl> permit esp <source> <wilcard> <destination> <wildcard>`

To permit ISAKMP traffic use:

`access-list <acl> permit udp <source> <wildcrad> <destination> <wildcard> eq isakmp`

Use `show access-lists` to verify

#### Task 2

Next step, is to define the paramaters within the IKE policy.

IKE uses these parameters during negotiation to establish ISAKMP peering between two IPsec endpoints

Multiple ISAKKMP policies can be configured. When configuring policies, each policy must be given a unique priority number.

##### Set Priority

Use the command:

`crypto isakmp policy <priority>`

The priority value can be between 1 and 10,000 with 1 being the higest priority and 10,000 being the lowest

##### Invokke ISAKMP Policy Configuration Command Mode

`crypto isakmp policy`

You can set the parameters in the mode above. If not explicitly configured, defaults are used

###### ISAKMP Parameters in Configuration Command Mode

`encryption <encryption-type>`

Encryption Type can be:

* Des
* 3des
* Aes
* Aes 192
* Aes 256

`hash <hash>`

Hash:

* Sha
* Md5

`authentication <authentication>`

Authentication:

* Pre-share
* Rsa-encr
* rsa-sig

`group <group\_num>`

Group\_num:

* 1
* 2
* 5

`lifetime <seconds>` the number of any seconds. Default is: 86,400 (one day)

##### Negotiating ISAKMP policies

2 endpoints must negotiate policies before they agree on the SA to use for IPsec

If a match is not made negotiation is cancelled

##### Pre-Shared Keys

PSKs must be configured if `authentication pre-share` is set.

At a given peer, the same key can be configured to be shared with multiple remote peers.

A more secure approach is to specify different keys to share between different pairs of peers

###### Configure a PSK

`crypto isakmp key <keystring> hostname <hostname>` or `crypto isakmp key <keystring> address <peer-address>`

Keystring - specifies the PSK. Use any combination of alphanumeric character up to 128 bytes. MUST BE THE SAME ON BOTH SIDES

Peer-address - specifies the IP address of the remote peer

Hostname - Specifies the hostname of the remoote peer. Concateneated with its domain name (for example, myhost.domain.com)

To use the <hostname> parameter. The following command must be used:

`crypto isakmp identity hostname`

#### Task 3

A transform set is a combination of individual IPsec transforms that are designed to enact a specific security policy for traffic.

During IKE phase 2 quick mode, the peers agree to use a particular transform set for protecting a particular data flow

Transform sets constist of a combination of an AH transform, an ESP transform, and the IPsec mode.

Limited to one AH transform and one or two ESP transforms

Multiple transform sets can be configured and can be specified in a crypto map entry

##### Defining a Transform Set

Specify one to four using the following command:

`crypto ipsec transform-set <transform-set-name> <transform1> [<transform2>] [<transform3>] [<transform4>]`

The above command invokes crypto-transform configuration mode

<transform-set-name> - This parameter specifies the name of the transform set to create or modify

<transform1>, etc - Type of transform set. Specify up to 4: One AH, One ESP encryption, One ESP authentication and optionally IP compression. These transforms define the IPsec security protocols and algorithms

##### Commands Within the Configuration Mode

###### AH Commands

`ah-md5-hmac` - AH with the MD5 authentication algorithm

`ah-sha-hmac` - AH with the SHA algorithm

###### ESP Commands

Note: If an ESP protocol is specified in a transform set, an ESP encryption transform set or an ESP encryption transform set and an ESP authentication transform set must be specified

Specifying the transform type:

`esp-md5-hmac`

`esp-sha-hmac`

Specifying the encryption type:

`esp-aes`

`esp-aes 192`

`esp-aes 256`

`esp-des`

`esp-3des`

`esp-null`

`esp-seal`

##### Type `tunnel` at the end of the configuration mode

#### Task 4

Crypto ACLs identify the traffic flows to protect. Outbound crypto ACLs select outbound traffic that IPsec should protect. Traffic that is not selected is sent in plaintext. If desired, inbound ACLs can be created to filter and discard traffic that should have been protected by IPsec

Extended IP ACLs select IP traffic to encrypt based on protocol, IP address, network, subnet, and port.

Although ACL syntax is unchanged from extended IP ACLs, the meanings are slightly different for crypto ACLs

For example, the permit statement specifies that matching packets must be encrypted and deny specifies that matching packets are not encrypted.

##### Crypto ACL Syntax

`access-list <acl-number> {deny | permit| <protocol> <source> <wildcard> <destination> <wildcard>`

Outbound crypto ACLs define the interesting traffic to be encrypted. All other traffix passes as plaintext

Inbound crypto ACLs inform the router of which traffic should be received as encrypted trafffic. When traffic matches the permit statement, the router expects that traffic to be encrypted. If inbound plaintext traffic is received that matches a permit statement in the crypto ACL, that traffic is dropped. This drop occurs because the plaintext traffic was expected to be protected by IPsec and encrypted but it was not

You can have multiple crypto ACLs defined for specific traffic to receive specific IPsec protection, then different crypto map entries use these entries to specify different IPsec policies.

Try to be as restrictive as possible when defining a crypto ACL. Using `any` is not recommended

Symmetric Crypto ACLs must be configured.

Outbound ACL source becomes the inbound ACL destination.

#### Task 5

Crypto map entries that are created for IPsec combine the needed configuration parameters of IPsec SAs, including the following parameters:

* Which traffic to protect using a crypto ACL
* Granularity of the flow to be protected by a set of SAs
* Who the remote IPsec peers are, which determine where the IPsec-protected traffic is sent
* Local address used for IPsec traffic (optional)
* Which type of IPsec security is applied to this traffic, choosing from a list of one or more transform sets
* Key management menthod
* SA lifetimes

Crypto map entries with the same crypto map name but different map sequence numbers are grouped into a crypto map set

Only one crypto map can be set to a single interface

Multiple interfaces can share the same crypto map set if the same policy is applied to multiple interfaces

If more than one crypto map entry is created for a given in terface, use the sequence number of each map entry to rank the map entries. The smaller the seqeunce number, the higher the priority

Create multiple crypto map entries for a gien interface if any of these conditions exist:

* Separate IPSec peers handle different data flows.
* Different IPsec security must be applied to different types of traffic, to the same or separate IPsec peers.

IKE is not used to establish a particular set of SAs and multiple ACL entries must be specified, create separate ACLs, one per permit entry, and specify a separate crypto map entry for each ACL

##### Crypto Map Syntax

`crypto map <map-name> <seq-num> ipsec-manual`

`crypto map <map-name> <seq-num> ipsec-isakmp [dynamic <dynamic-map-name>]`

<map-name> - The name of the crypto map to set or edit

<seq-num> - Number assigned to the entry

Ipsec-manual - Indicates that ISAKMP will not be used to establish the IPsec SAs

Ipsec-isakmp - Indicates that ISAKMP will be used to establish the IPSec SAs

Dynamic (optional) - specifies that this entry references a preexisting static crypto map entry

<dynamic-map-name> - Specifies the name of the dynamic crypto map set that should be used as the policy template.

##### Crypto Map Configuration Mode Commands

| Command | Description |
| --- | --- |
| `set` | Used with the `peer`, `pfs`, `transform-set`, and `security-association` commands |
| `peer [<hostname> | <ip-address>]` | Specifies the allowed IPsec peer by IP address or hostname |
| `pfs [group1 | group2]` | Specifies DH Group 1 or DH Group 2 |
| `transform-set [<set\_name(s)>]` | Specify list of transform sets in priority order. When the `ipsec-manual` is used, only one transform set can be defined.  When using `ipsec-isakmp` up to 6 can be specified |
| `security-association lifetime` | Sets SA lifetime parameters in seconds or kilobytes |
| `match address [<access-list-id | name]` | Identifies the ACL by name or number. Value should match the number or name argument of a previously defined IP-extended ACL being matched |
| `no` | Used to delete commands entered with the `set` command |
| `exit` | Exits crypto map configuration mode |

##### Applying the Crypto Map

In the interface you are applying it to, run the following command:

`crypto map <map-name>`

### Verifying and Troubleshooting IPsec Configuration

| Show Command | Description |
| --- | --- |
| `show crypto map` | Displays configured crypto maps |
| `show crypto isakmp policy` | Displays IKE policies |
| `show crypto ipsec sa` | Displays established IPsec tunnels |
| `show crypto ipsec transform-set` | Displays configured IPsec transform sets |
| `debug crypto isakmp` | Debugs IKE events |
| `debug crypto ipsec` | Debugs IPsec events |
| `show crypto isakmp sa` | Displays all current IKE SAs |

`show running-config` also helps a lot

# Implementing Cisco Adaptive Security Appliance

### Commands for Configuring Cisco ASA

| IOS Commands | ASA Commands |
| --- | --- |
| `erase startup-config` | `write erase` |
| `enable secret` | `enable password` |
| `line con 0`  `password password`  `login` | `passwd password` |
| `show ip interfaces brief`` | `show interfaces ip brief` |
| `show ip route` | `show route` |
| `show ip nat translations` | `show xlate` |
| `show vlan` | `show switch vlan` |
| `ip route` | `route outside` |
| Ctrl+C | Q |

# Commands to do Things:

## Setting Passwords:

### Set password to access Privileged EXEC Mode:

Go to global configure mode and then type the following command:

`enable secret <password>`

### Set a password for User EXEC Mode:

#### For console access:

Enter the console interface configuration mode and then enable password by entering the following commands:

`line console 0`

`password <password>`

`login`

`exit`

#### For SSH and Telnet and Remote Access:

Enter the vty interface configuration mode and then enable the password by entering the following commands:

`line vty 0 15`

`password <password>`

`login`

`exit`

By doing “0 15” you are telling the OS to gather all the VTY lines so all the remote access lines and sets a password for every single one of them

### Encrypting the Password

In Global Config mode run:

`service password-encryption`

## Other Things:

### Disable DNS Lookup:

Enter global configuration mode: `configure terminal`

And execute `no ip domain-lookup`

### Configuring the IP Address of an Interface

In the interface configuration, run: `ip address <ipaddr> <subnetmask>`

After executing that line run: `no shutdown`

### Configuring a Static Default Route pointing to the next hop ISP router

`ip route 0.0.0.0 0.0.0.0 <ipaddr>`

### Setting Default Gateway

In Global Configuration Mode (prompt ending in ‘(config)’) execute `ip default-gateway <ipaddr>` or `ip route 0.0.0.0 0.0.0.0 <ipaddr>`

### Adding an Interface to Another Interface

In the interface mode, type: `switchport access vlan <vlan\_number>`

### Set the Message of the Day (Banner)

In Global Config Mode run the command:

`banner motd # <message\_of\_the\_day> #`

### Showing Condition of Interfaces

`show ip interface brief`

### To remove the IP address

`no ip address` in the interface configuration mode

### Show the contents of the flash memory

`show flash`

### Show IPTables / Routing Tables on Routers

`show ip route`

### Show Time Set on Router

`show clock`