

Terms, Definitions, AAA, and Multifactor Authentication

- **Vulnerability:** A weakness or flaw in a system that can be exploited to compromise security.
- **Exploit:** A method or piece of software that takes advantage of a vulnerability to gain unauthorized access or cause damage.
- **Threat:** Any potential danger that could exploit a vulnerability to cause harm to a system or network.
- **Risk:** The likelihood that a threat will exploit a vulnerability, combined with the potential impact.
- **Mitigation Technique:** A method or control implemented to reduce the risk associated with a threat, vulnerability, or exploit.
- **Awareness:** The understanding and recognition of security risks and best practices within an organization.
- **Education:** Formal instruction or courses aimed at providing users with knowledge about security principles and procedures.
- **Training:** Practical, hands-on exercises that teach users how to implement security measures effectively.
- **Security Standard:** A documented set of rules and guidelines established to enforce consistent security practices.
- **Security Policy:** A high-level document that defines an organization's approach to protecting information assets, including roles, responsibilities, and acceptable use.
- **AAA (Authentication, Authorization, Accounting):** A framework for controlling access, defining permissions, and tracking user activities.
 - **Authentication:** Verifying the identity of a user or device, often using something you know (password), something you have (token), something you are (biometrics), or somewhere you are (location).
 - **Authorization:** Defining what resources or actions an authenticated user is permitted to access or perform.
 - **Accounting:** Recording and tracking user activities and resource usage for auditing and reporting purposes.
- **Multifactor Authentication (MFA):** A security mechanism that requires users to provide two or more independent credentials (e.g., password + token) to verify identity.

Device Access, Authentication, Configuration and Verification

Console Port Configuration:

- To set a password on the console port and enable login:

```
Router> enable  
Router# configure terminal  
Router(config)# line console 0  
Router(config-line)# password YourPassword  
Router(config-line)# login  
Router(config-line)# exit
```

Auxiliary Port (AUX) Configuration:

- To set a password and enable login on the auxiliary port:

```
Router(config)# line aux 0  
Router(config-line)# password YourPassword  
Router(config-line)# login  
Router(config-line)# exit
```

VTY (Telnet/SSH) Configuration:

- To set passwords and enable remote access:

```
Router(config)# line vty 0 4  
Router(config-line)# password YourPassword  
Router(config-line)# login  
Router(config-line)# transport input telnet ssh    # Optional: specify  
allowed protocols  
Router(config-line)# exit
```

Creating a Local User for AAA and Accounting:

- To create a user with a password:

```
Router(config)# username admin secret StrongPassword
```

- Using `secret` instead of `password` ensures the password is stored in a secure, hashed form.

Enable Password (Privileged Mode):

- To set an encrypted password for privileged exec mode:

```
Router(config)# enable secret StrongSecretPassword
```

- `enable secret` uses MD5 hashing (or more secure hashing in modern IOS) and is preferred over `enable password` which stores it in plaintext.

Password Encryption and Hashing:

- **service password-encryption:**
 - Encrypts all plain-text passwords in the configuration using a weak Cisco type-7 encryption.
 - **CCNA Tip:** Do not rely on `service password-encryption` for strong security; always use `secret` for console, VTY, and enable passwords.
- Modern IOS versions support SHA-256 hashing when using `username ... secret` for local accounts.

CCNA Tips:

- Always use `secret` for enable mode passwords and local user accounts.
- Avoid storing passwords in plaintext.
- Always save your configuration with `write memory` or `copy running-config startup-config`.

Skipping Password Prompt:

- To skip entering a password, set the privilege level to 15 using `enable secret mySecretPassword` and assign users the same privilege with `username admin privilege 15 secret myUserPassword`.

Adjusting Automatic Timeout:

- To automatically adjust the session timeout, enter configuration mode with `configure terminal`, select the line with `line console 0` or `line vty 0 4`, then set the timeout using `exec-timeout 10 0` (10 minutes, 0 seconds).

SSH Requirements:

- **K9 Image** - A Cisco IOS image that includes encryption features required for SSH.
- **Hostname** - Set a unique device name with `hostname <device-name>`.
- **Domain Name** - Required for SSH key generation using `ip domain-name <domain>`.
 - Generate the crypto key with `crypto key generate rsa modulus 2048`.
- **SSH Version** - Use `ip ssh version 2` if possible for enhanced security.
- **Username | Password** - Configure local users with `username <name> secret <password>`.
- **Login Local** - Ensure console or vty lines are set to use local authentication with `login local`.
- **Transport Input** - Specify SSH access with `transport input ssh`.
 - If set to none, SSH connections will be rejected with "connection refused by remote host".

External Authentication Services:

- **RADIUS** - Remote Authentication Dial-In User Service; used for centralized authentication, authorization, and accounting. Uses UDP ports **1812** (authentication) and **1813** (accounting) by default.
- **TACACS+** - Terminal Access Controller Access-Control System Plus; provides centralized authentication, authorization, and accounting for network devices. Uses TCP port **49**.

VPN Overview:

- **VPN** - Virtual Private Network; a method of using tunneling protocols to allow private traffic to traverse a public or untrusted network such as the Internet. A VPN itself does not guarantee encryption or security—those properties depend on the tunneling or security protocol used (e.g., IPsec, SSL/TLS, GRE). VPNs are commonly used for remote access and site-to-site connectivity.
 - **Site-to-site VPN** - Connects entire networks (e.g., branch office to headquarters).
 - **Remote-access VPN** - Allows individual users to connect from a client device to the network.
- **IPsec (Internet Protocol Security)** - A suite of protocols that can provide data confidentiality, integrity, and authentication at the IP layer, commonly used to secure VPNs.
 - **Modes: tunnel mode** (encapsulates the entire IP packet; commonly used for site-to-site VPNs) and **transport mode** (protects only the IP payload; used for host-to-host scenarios).
 - **Protocols: ESP (Encapsulating Security Payload)** — can provide encryption, integrity, and authentication of packets. **AH (Authentication Header)** — provides integrity and authentication but does not encrypt payloads.
 - **IKE (Internet Key Exchange)** — protocol (IKEv1/IKEv2) used to negotiate keys and establish Security Associations (SAs); typically operates in Phase 1 (establishes secure channel) and Phase 2 (negotiates IPsec SAs).
 - **Use cases:** site-to-site VPNs, remote-access VPNs, and securing traffic between branch offices and data centers.
- **Other VPN technologies: SSL/TLS VPN** (commonly used for clientless remote access), **DMVPN**, and **GETVPN** for dynamic or group-based VPN solutions.

- **GRE (Generic Routing Encapsulation)** - A tunneling protocol developed by Cisco that encapsulates a wide variety of network layer protocols inside point-to-point connections. GRE itself does not provide encryption or strong security; it is often combined with IPsec to secure the tunnel. GRE is commonly used to carry routing protocols between sites or to tunnel non-IP traffic.
-

Port Security, DHCP Snooping, IP Source Guard, and Dynamic ARP Inspection

- By default, there is no security on a switch port.
- Any device that is connected to a switch has access to the network.
 - For security reasons, you might want to use the shutdown command on ports not being used.

Parking Lot VLAN - A VLAN used to isolate unused switch ports by assigning them to a separate, non-routed VLAN. This prevents unauthorized or accidental access to the production network if someone plugs into an unused port.

Example Configuration: (Parking Lot VLAN and Shutdown Ports)

```
Switch> enable
Switch# configure terminal

! Create the Parking Lot VLAN
Switch(config)# vlan 999
Switch(config-vlan)# name ParkingLot
Switch(config-vlan)# exit

! Assign unused interfaces to the Parking Lot VLAN
Switch(config)# interface range fa0/10 - 24
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 999
Switch(config-if-range)# shutdown
Switch(config-if-range)# exit
```

```
! (Optional) Prevent VLAN 999 from being routed  
Switch(config)# interface vlan 999  
Switch(config-if)# shutdown  
Switch(config-if)# exit  
  
Switch(config)# end  
Switch# write memory
```

This configuration creates a VLAN (999) called "ParkingLot," assigns unused interfaces to it, shuts them down, and disables the VLAN interface to ensure no traffic is routed.

Filtering for Unused Connections:

- You can identify unused switch ports with the command:
 - `show interface status` (displays connected, notconnect, err-disabled, etc.).
 - You can also filter output with `show interface status | include notconnect` to quickly list only the down/unconnected ports.
- Ports in the notconnect state are candidates for Parking Lot VLAN assignment or shutdown.
- Network management systems (like Cisco Prime, DNA Center, or third-party monitoring tools) can also help automate detection of unused ports.

Port Security - A feature on Cisco switches that allows you to restrict a switch port to allow only specific MAC addresses. This helps prevent unauthorized devices from connecting to the network.

- **Static define MAC address for port security** - Assign a specific MAC address to a port so only that device can connect:
 - `switchport port-security mac-address 0001.2345.6789`
- **Make permanent dynamic MAC address for port security** - Allow the switch to learn MAC addresses dynamically but retain them across reboots:
 - `switchport port-security mac-address sticky`

Switch Port Security Violation Types

- **Protect** - Drops packets from violating MAC addresses but does not generate a log or disable the port.
- **Restrict** - Drops packets from violating MAC addresses and generates a log message; the port remains up.
- **Shutdown** - The default violation mode; shuts down the port if a violation occurs and triggers the err-disabled state.

DHCP Spoofing - An attack where a malicious device on the network impersonates a DHCP server and assigns incorrect IP addresses or network settings to clients, potentially redirecting traffic or causing network disruptions.

DHCP Snooping - A security feature on Cisco switches that prevents DHCP spoofing by allowing only trusted ports to provide DHCP server responses and filtering out untrusted DHCP messages.

- **Enable DHCP Snooping globally:** `ip dhcp snooping`
- **Enable DHCP Snooping per VLAN:** `ip dhcp snooping vlan <vlan-id>`
 - Needs both commands to work.
- **Configure trusted interfaces (where legitimate DHCP servers are connected):**
 - `interface <interface-id>`
 - `ip dhcp snooping trust`
- **Enable DHCP Snooping on untrusted interfaces:** These are automatically untrusted by default.

ARP Spoofing - An attack where a malicious device sends falsified ARP messages onto a network, associating its MAC address with the IP address of another device, typically to intercept, modify, or stop network traffic.

Dynamic ARP Inspection (DAI) - A security feature on Cisco switches that validates ARP packets on the network, preventing ARP spoofing attacks by ensuring only valid ARP requests and responses are relayed.

- **Enable Dynamic ARP Inspection:**
 - ip arp inspection vlan <vlan-id> (on the VLAN to inspect)
- **Configure trusted interfaces (typically uplinks):**
 - interface <interface-id>
 - ip arp inspection trust
- **Enable DAI globally (if needed):**
 - ip arp inspection

IP Source Guard - A security feature on Cisco switches that works with DHCP Snooping to prevent IP address spoofing. It ensures that only packets with valid IP-MAC bindings, learned via DHCP Snooping or manually configured, are allowed on the interface.

- **Enable IP Source Guard on an interface:**
 - interface <interface-id>
 - ip verify source

IPv4 Access Control Lists (ACLs) and Wildcard Masking

IPv4 Access Control Lists (ACLs) - A set of rules applied to interfaces or devices to filter network traffic based on source and destination IP addresses, protocols, and ports. ACLs can permit or deny traffic, providing a method to implement security, traffic control, and policy enforcement on networks.

- Top Down Processing
- Immediate Execution Upon a Match
- Implicit Deny All at the Very End
- **Standard ACL** - Filters traffic based only on the source IP address. Standard ACLs are typically used to allow or deny entire subnets or hosts.
- **Extended ACL** - Filters traffic based on source and destination IP addresses, protocols (TCP, UDP, ICMP), and port numbers. Extended ACLs provide more granular control over traffic.

- **Identifying ACLs:**
 - **Numbered ACLs** - Use numeric identifiers to distinguish ACLs. Standard ACLs use 1-99, extended ACLs use 100-199 (some platforms allow 1300-1999 for extended).
 - **Named ACLs** - Use descriptive names instead of numbers, making them easier to manage and remember.
- **Common ACL Commands:**
 - `access-list` - Creates or modifies a numbered ACL
 - `ip access-list standard <name>` - Creates or modifies a named standard ACL
 - `ip access-list extended <name>` - Creates or modifies a named extended ACL
 - `permit <protocol> <source> <wildcard> [<destination> <wildcard>]` - Allows traffic matching the criteria
 - `deny <protocol> <source> <wildcard> [<destination> <wildcard>]` - Blocks traffic matching the criteria
 - `remark <text>` - Adds a comment to an ACL entry
 - `log` - Generates a log message for matching packets
 - `show access-lists` - Displays ACLs configured on the device
 - `ip access-group <ACL-name-or-number> in|out` - Applies an ACL to an interface in a specific direction

Wildcard Masking - A method used in ACLs to specify which bits of an IP address should be checked and which should be ignored. It is essentially the **inverse** of a subnet mask and is used to create flexible and precise filtering rules.

- **What the 0 means in a wildcard mask:** The corresponding bit must match exactly the value in the IP address.
- **What the 1 means in a wildcard mask:** The corresponding bit can be ignored; any value in that bit position is acceptable.

Extended IPv4 ACLs

- **Extended IPv4 ACLs** - A type of Access Control List that filters traffic based on source and destination IP addresses, protocols (such as TCP, UDP, ICMP), and port numbers. They provide granular control over network traffic, allowing administrators to permit or deny specific types of traffic between hosts or subnets.

Example of an Extended ACL by number:

```
! Deny traffic from 192.168.1.10 to 10.0.0.20 on any TCP port  
access-list 110 deny tcp 192.168.1.10 0.0.0.0 10.0.0.20 0.0.0.0
```

```
! Permit all other traffic  
access-list 110 permit ip any any
```

- In this example, 192.168.1.10 0.0.0.0 means the source IP is exactly 192.168.1.10.
- 10.0.0.20 0.0.0.0 means the destination IP is exactly 10.0.0.20.
- The 0 in the wildcard mask requires an exact match for that octet.

Example of an Extended ACL by name:

```
! Create a named extended ACL called BLOCK_TCP  
ip access-list extended BLOCK_TCP
```

```
! Deny traffic from 192.168.1.10 to 10.0.0.20 on any TCP port  
deny tcp 192.168.1.10 0.0.0.0 10.0.0.20 0.0.0.0
```

```
! Permit all other traffic  
permit ip any any
```

```
! Apply ACL to an interface in the inbound direction  
interface GigabitEthernet0/1  
ip access-group BLOCK_TCP in
```

- Named ACLs are easier to manage and remember compared to numbered ACLs.
- The syntax inside a named ACL does not require repeating the ACL number for each entry.

ACL Interface Direction (In/Out)

- **Inbound ACLs (in)** - Applied to traffic **entering** an interface. The ACL checks packets as soon as they arrive on the interface before they are routed.
 - Use inbound ACLs to filter traffic from external sources before it reaches your network.
- **Outbound ACLs (out)** - Applied to traffic **leaving** an interface. The ACL checks packets after they are routed and just before they exit the interface.
 - Use outbound ACLs to control traffic leaving your network to prevent sensitive data from leaving or to manage traffic leaving a segment.
- **Best practice:** Apply ACLs as close as possible to the source of the traffic you want to filter. For extended ACLs, this often means applying them inbound on the interface closest to the source host.
- **Note:** You can only apply **one ACL per direction per interface**.