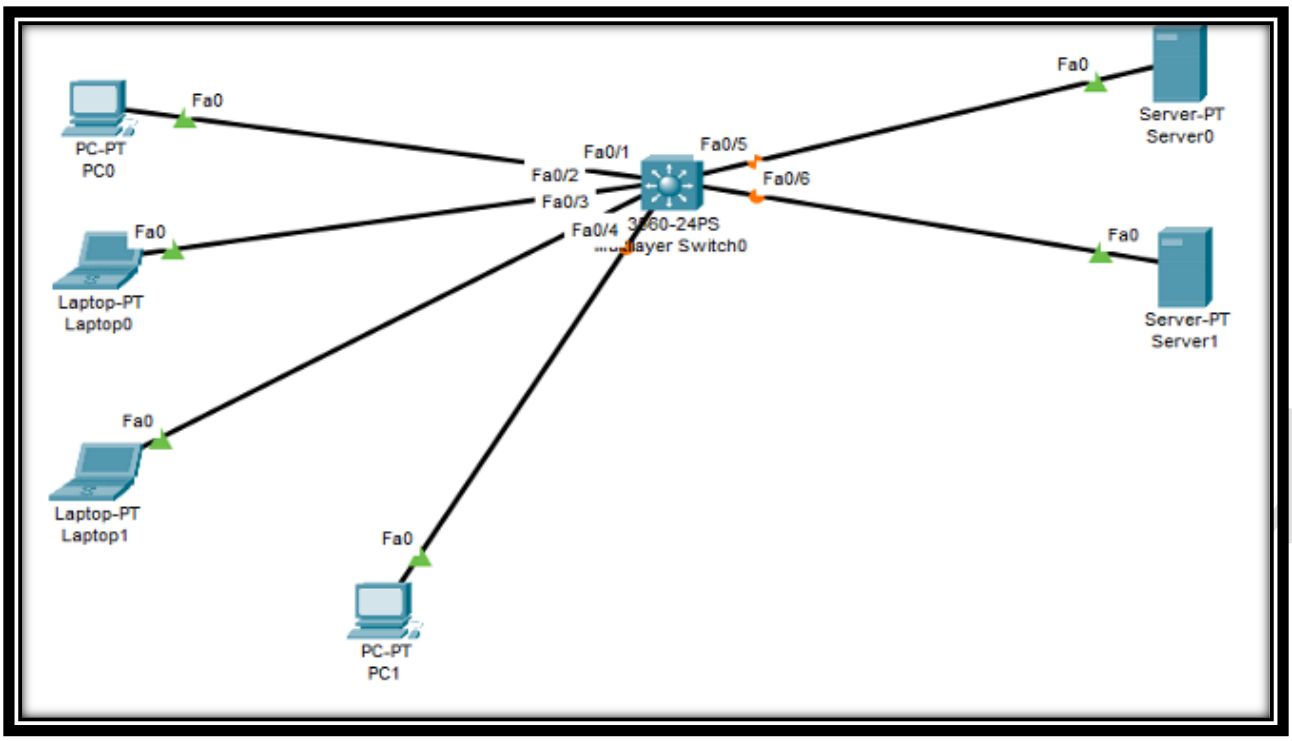
Security Fundamentals:

- Till now we learned about various networking technologies and our attention has probably been focused on using network devices to build function networks.
- Make all network is working smoothly without any issues for all users but the issues is that all users who is connected to network not all trusted to obey the rules and be good to network.



So we go for Security.

What is Security?

- We can say Security is a technique which allows the network administrator to protect the network resources from unwanted access.
- Security maintains Privacy.
- Security maintains Data Integrity (Data Integrity mean when we send data from one point to another point no one can add or remove data from that like data change by un authorized person is not allowed etc.).
- Security maintains Availability.

Vulnerabilities (Weakness):

- Network Vulnerability is a weakness or flaw in software, hardware or organizational process which when compromised by a threat can result in security breach.
- Vulnerability can be defined a weakness in a system or its design. Every system is human created and there is chances for errors or mistakes
- Vulnerability is present in Application, Network Protocols and operating system etc.

Network Vulnerabilities come in many forms but the most common types are given below:

- **Malware** such as Trojans, Viruses and worms that are installed on a user machine or a host server.
- **Social engineering attacks** that fool users into giving up personal information such as username and password etc.
- **Outdated or unpatched software** that exposes the systems running the application and potentially the entire network.
- **Misconfigured firewalls** that allow or have default policies enabled.

Exploits (Takes advantage of the Vulnerabilities):

- An Exploits is a tool or system or Method takes advantage of system Vulnerabilities.
- An Exploit can be defined as a way or method or tool which is used by an attacker on a Vulnerability to cause damage to network or system.
- Exploit can be software that may cause a buffer overflow or a method of social engineering etc.

Threat:

- Threat can be defined as anything danger to an Asset (Asset is anything which the organization is invested and which is valuable to the organization. Eg: Vehicles, Properties, Computers etc.).
- Threats can be accidentally triggered.

Mitigations Techniques:

- Attack mitigation is detection and protecting strategy use to safeguard networks servers and application
- Awareness and Countermeasures
- Application whitelisting -- Use only authorized application
- Patch applications
- User Awareness -- End User are becoming the largest security risk in any organization because it can happen anytime. Like End User Threats – Using social Media, Test Messaging, Apps download, use of email, Password creation and usages etc.
- End User Security Awareness Training (It is better to arrange a cyber security awareness training program on regular basis and should cover the following topics – cyber security and its

important, Different types of cyber Threats, How to use Internet, Email phishing and social Engineering, Device Security, Physical Security, and Password Creation and usages.

- Physical Access: Physical Access Control system that provides Network Infrastructure security with protection of digital assets as well as high priority worldwide. – CCTV, Server Rack door lock etc.

Configure device access control using local passwords

Different between Console and Aux port:

- Console port is working even router is booting
- Aux port is working after router start

Passwords:

Sh user

How to assign Console password in CISCO Switch / Router?

En
Config t
Line console 0
Password abc
login

How to assign Auxiliary password in CISCO Switch / Router?

En
Config t
Line aux 0
Password abc
login

How to assign password to VTY line?
Config t
Enable password 12345
Line vty 0 4 ---------- if we want to allow 5 person to access device remotely then we will use vty 0 4 i.e.. Qty 5
Password cisco
Login

To convert password to password 7
Service password-encryption

Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics).

Management Password- A password policy is a set of rules governing the use of passwords in the system.
Minimum Password Length – Sets the minimal length of the password.
Password Complexity Requirements- Specifies the composition of the password and its required number of characters.
Password history- Determines the number of unique password a user must use before an old password can be reused.
Maximum Password age- Determines how long a password can be used before the user is allowed or required to change it.
First Login- Determines if the user will be required to change his password upon first logging in to the system.
Multi Factor Authentication (MFA)- MFA is a security system that verifies a user's identity by requiring multiple credentials.
How does 2FA work?

- The user logs in to the website or service with their username and password.
- The password is validated by an authentication server and, if correct, the user becomes eligible for the second factor.
- The authentication server sends a unique code to the user's second factor method (like as a smartphone app).
- The user confirms their identity by providing the additional authentication for their second – factor method.

VPN (Virtual Private Network):

- It helps to establish a secure connection over insecure network, such as the Internet.
- It is a great alternative to private WAN connection since internet access is cheaper and it available everywhere.
- VPN create tunnels that allows users or systems to connect securely.
- VPN using network security protocols like IPSec to provide privacy and Data Integrity

VPNS Provides following features as given below:

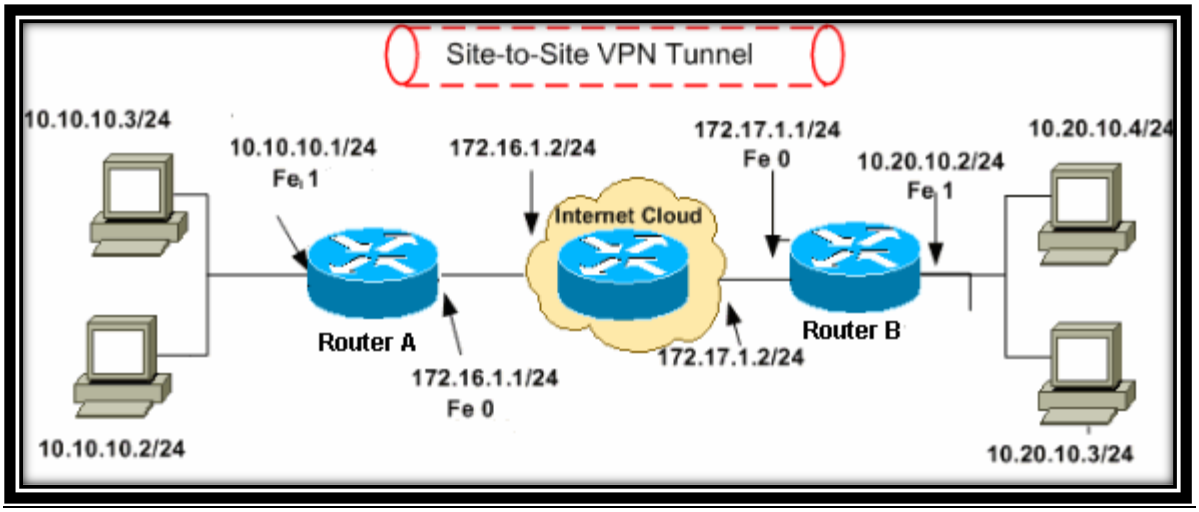
- Confidentiality: Preventing anyone to read our data -- With Encryption
- Authentication: Verifying that the router or firewall or remote user that is sending VPN traffic is authorize
- Integrity: Verifying that the VPN packet was not changed somehow during transit.
- Anti-Reply: Preventing someone from capturing traffic and resending it.

Common VPN types that we use as given below

1. Site to Site VPN
2. Remote user VPN (Client to site)

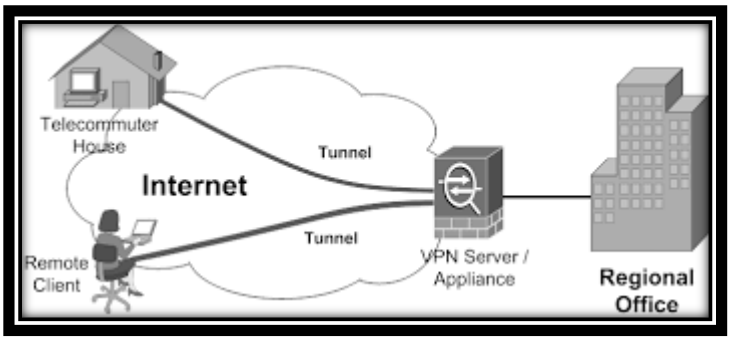
Site to Site VPN:

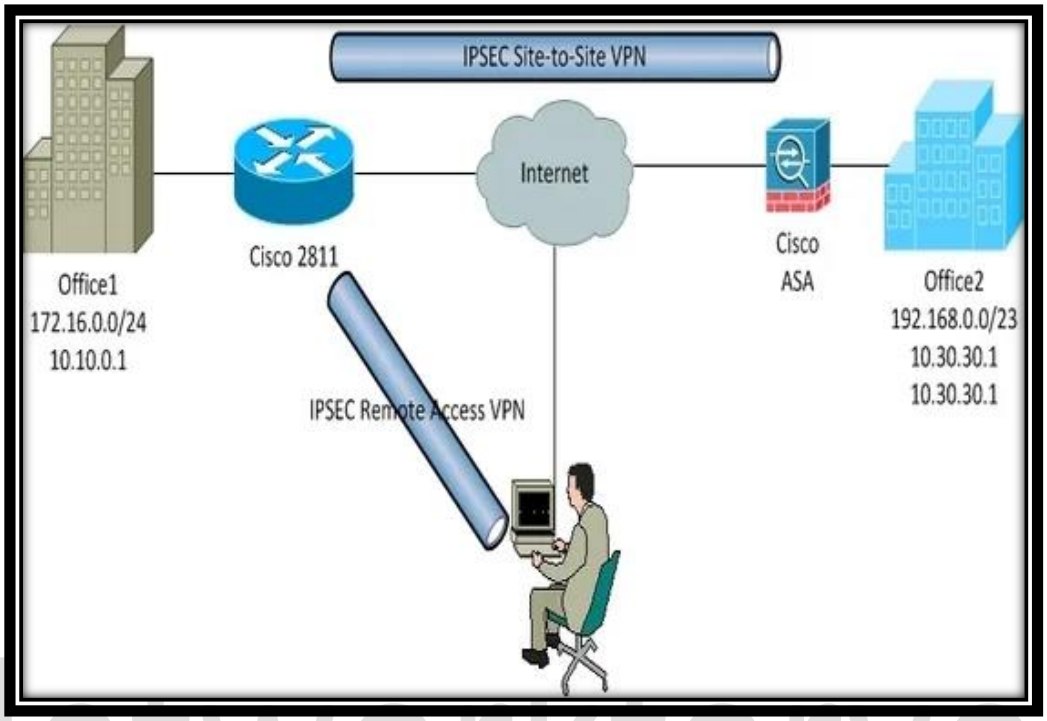
- In Site to site VPN we have a network device at each site between this network device we can build a VPN Tunnel.
- Each end of the VPN tunnel will be encrypted with original IP packet and add a VPN header a new ip header then it will forward the encrypted packet to the other end of the tunnel.
- A VPN connection that allows connecting two LANs is called a Site-to-Site VPN.
- Connect two private LAN over Public Network, Private to Private over Public Network.
- It is also called Site-to-Site VPN, LAN-to-LAN VPN or Hub-and-Spoke VPN.
- Many organizations use IPsec, GRE, and MPLS VPN as Site-to-Site VPN protocols.
- Site-to-Site VPNs can connect branch office network to company Head-Office Network.
- VPN allows secure connection of corporate office with branch offices or remote offices.
- Site-to-Site, VPN are built over Internet between two or more office locations.
- Site-to-Site Virtual Private Network (VPN) connect entire networks to each other.



Remote user VPN:

- It is also known also Client to site VPN.
- In this user installs a VPN client on his computer and VPN Tunnel is established between the user's device and the remote network device.
- Enable users to work from remote locations such as their homes & other premises.
- Remote-Access VPNs connect client devices to LAN over the Internet infrastructure.
- Individual hosts or clients, access a company network securely over the Internet.
- Each host typically has VPN client software loaded or uses a web-based client.
- Whenever the host send any information, the VPN client software encapsulates it.
- It allows individual users to establish secure connections with a remote network.
- Remote-Access VPN tunnels are formed between a VPN device & an end-user PC.
- The remote user requires the Cisco Virtual Private Network (VPN) client software.
- Remote access Virtual Private Network connect individual users to private networks.





VPN Protocols:

There are some VPN Protocols use as given below.

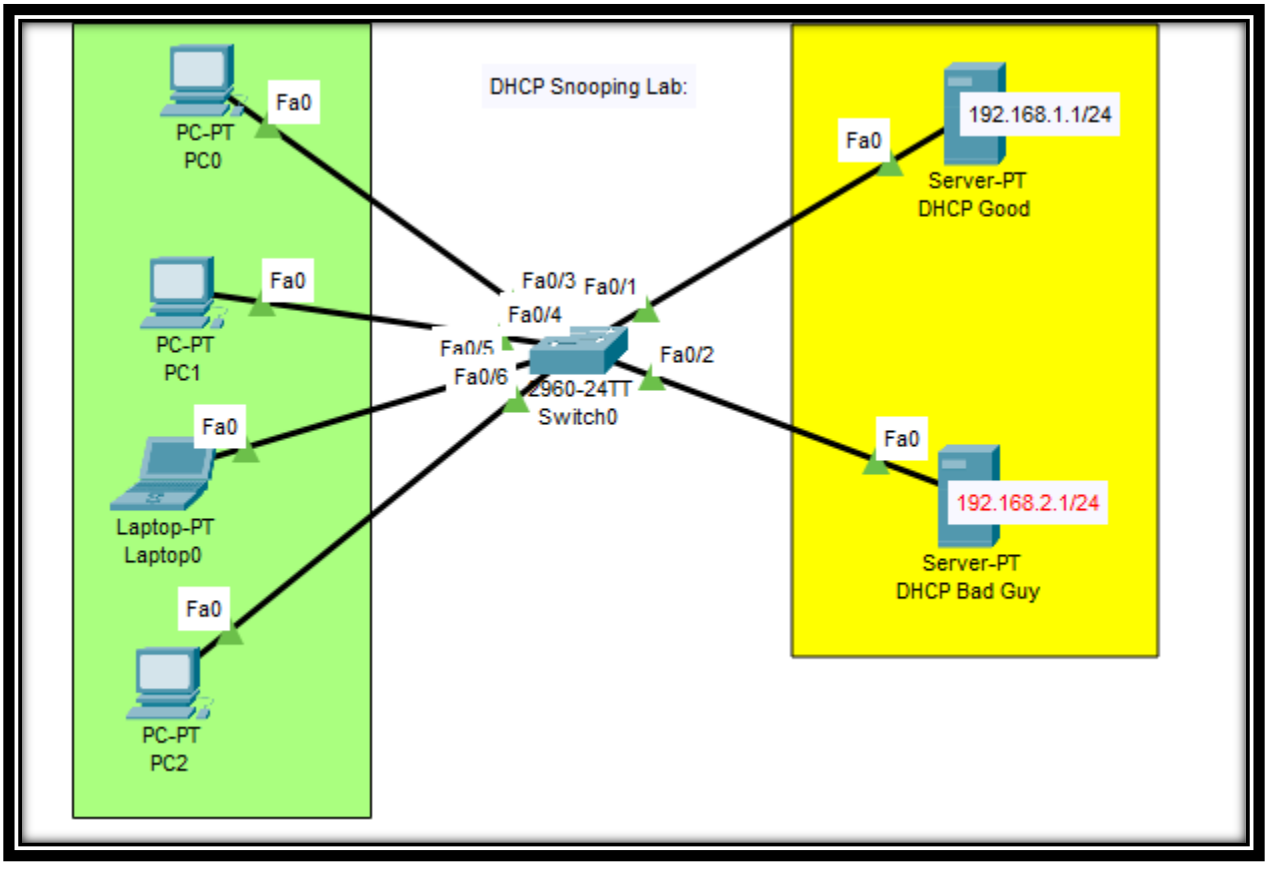
- IPSec (Internet protocol security): A Framework that provides security on layer three of the OSI Model.
- L2TP (Layer two traffic): a VPN protocol that tunnels layer two traffic does not offer any encryption so should be used together with IPsec
- SSL (Secure Socket layer): uses SSL (HTTPs) to create a secure connection with the web browser.
- PPTP (Point to point Tunneling Protocol): An old VPN Protocol that uses PPP and GRE, insecure and should not be used any more.

Advantages of VPNs:

- Cost savings
- Scalability
- Security
- Compatibility
- Better Performance
- Flexible and Reliable

DHCP Snooping:

- DHCP snooping is a security feature acts like a firewall between trusted and untrusted.
- DHCP Snooping is a technique where we configure switch to listen in on DHCP traffic and stop any malicious DHCP packets.
- DHCP snooping is like a firewall between untrusted hosts & trusted DHCP servers.
- DHCP snooping use trusted source to reply DHCP offer message.
- DHCP snooping will drop DHCP messages from a DHCP server that is not trusted.
- DHCP snooping Can be enable to disabled per VLAN basis.
- DHCP snooping feature is inactive on all VLANs by default.
- DHCP Snooping is use to prevent a man-in-the middle attack on the network.



DHCP Snooping Configuration:
en Config t hostname SW1 ip dhcp snooping ip dhcp snooping vlan 1 no ip dhcp snooping information option int f0/1 ip dhcp snooping trust ---------- To Check sh ip dhcp snooping sh ip dhcp snooping binding sh ip dhcp snooping database

Command for DHCP Snooping	Description
Ip dhcp snooping	Globally enables DHCP snooping on the device.
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.
show ip dhcp snooping	Displays general information about DHCP snooping.
sh ip dhcp snooping binding	To display IP-to-MAC address bindings for all interfaces or a specific interface,
sh ip dhcp snooping database	Displays the current operating state of the database agent and statistics associated with the transfers.

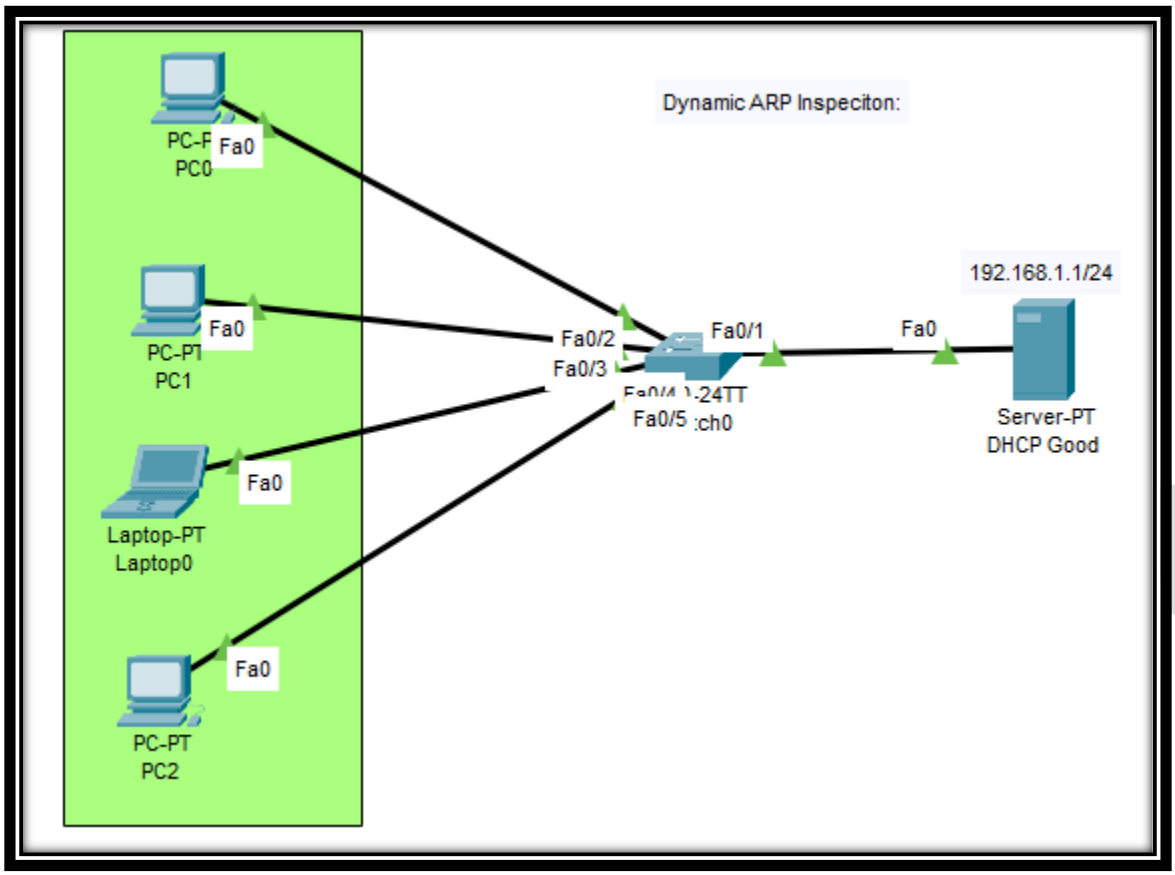
ARP (Address Resolution Protocol) is used to find the MAC address of any IP address that you are trying to reach on any your local network.

ARP Poisoning is an attack where we send fake ARP reply packets on the Network.

Dynamic ARP Inspection (DAI):

- Dynamic ARP inspection is a security feature that protect ARP poisoning Attack.
- DAI stands for Dynamic Address Resolution Protocol Inspection.
- DAI is a security feature that rejects invalid and malicious ARP packets.
- DAI feature prevents man-in-the-middle attacks such as ARP poisoning.
- DIA feature prevent man-in-the-middle attack such as ARP Spoofing.
- DHCP snooping builds bindings' database of valid MAC address, IP & VLAN interface.

- DAI uses the DHCP snooping binding database to validate bindings.
- Dynamic ARP Inspection (DAI) verifies IPv4 address to MAC address bindings.
- If mismatch happened on untrusted port, DAI will discard spoofed ARP packets.
- Dynamic ARP Inspection (DAI) only inspects ARP packets from untrusted ports.
- Dynamic ARP Inspection (DAI) can be enabled globally per VLAN.



Dynamic ARP Inspection Configuration on SW1
en **Config t** **hostname SW1** **ip dhcp snooping** **ip dhcp snooping vlan 1** **no ip dhcp snooping information option** **int f0/1** **ip dhcp snooping trust**

ip arp inspection vlan 1 **interface f0/1** **ip arp inspection trust** **----------** **To Check** **show ip arp inspection**

Port Security on Cisco Switch:

- Port security is a layer two traffic control feature on cisco switches.
- It enable an administrator configure individual switch ports to allow only a specified number of sources MAC address to connect.
- Port Security prevents unauthorized access & limit access, based on MAC address.
- Port Security is disabled by default on every interface of switch.
- Port Security can be configuring Static, Dynamic and Sticky.
- There are three different types of violation Shutdown, Protect and Restrict.

Port Security Violation Types:

There are three different types of violation Shutdown, Protect and Restrict.

Shutdown:

- Default action after violation.
- Port sends to err-disabled mode.
- For re-enable err-disabled recover, shutdown/no shutdown.
- MAC counter keeps history.

Protect:

- Need to configure for violation action.
- Traffic not sends to network from violator.
- Interface will be working even after violation.
- No MAC counter keeps history.

Restrict:

- Need to configure for violation action.
- Traffic not sends to network from violator.

- Generate log (SNMP/Syslog).
- No MAC counter keeps history.

Static:

- Static secure MAC addresses are statically configured on each switchport.
- Static secure MAC addresses are stored in the address table.
- Configuration of static secure MAC address is stored in the running configuration.
- Can be made permanent by saving them to the startup configuration.
- SW1(config-if) # **switchport port-security mac-address mac-address**

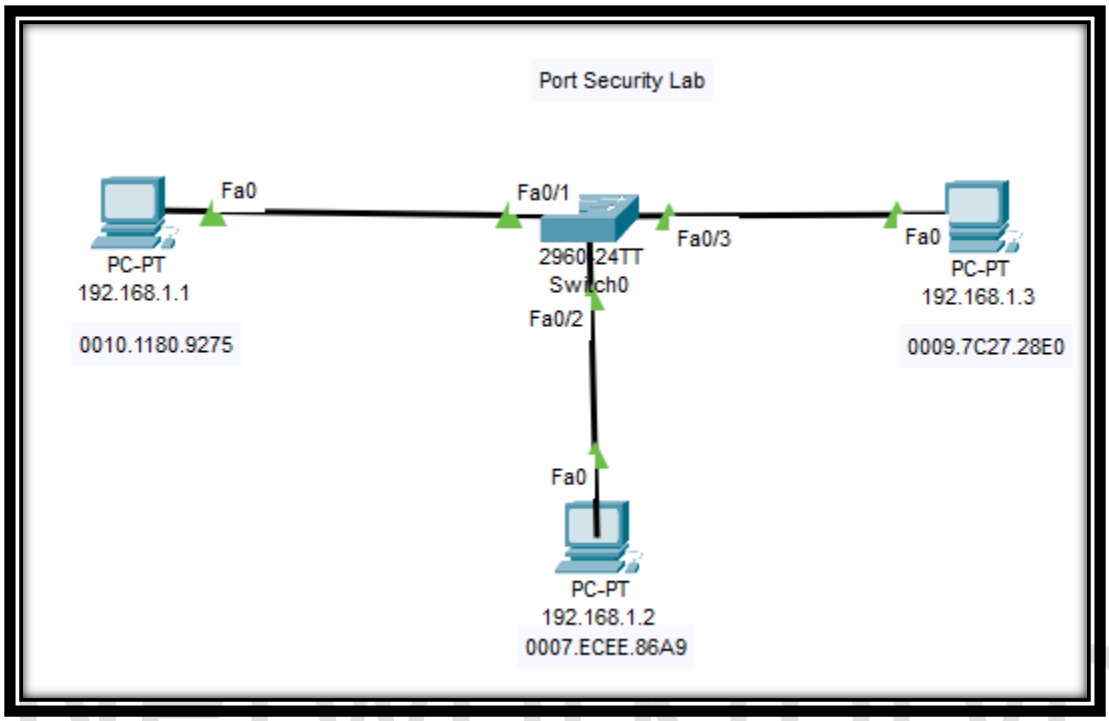
Dynamic:

- Dynamic secure MAC addresses are learned from device connected to switchport.
- Dynamic secure MAC addresses are stored in the address table only.
- Dynamic secure MAC addresses lost when the switchport state goes down.
- Dynamic secure MAC addresses also lost when the switch reboots.
- SW1(config-if) # switchport port-security
- By default, MAC addresses are learned on a switchport dynamically.
- **switchport port-security**

Sticky:

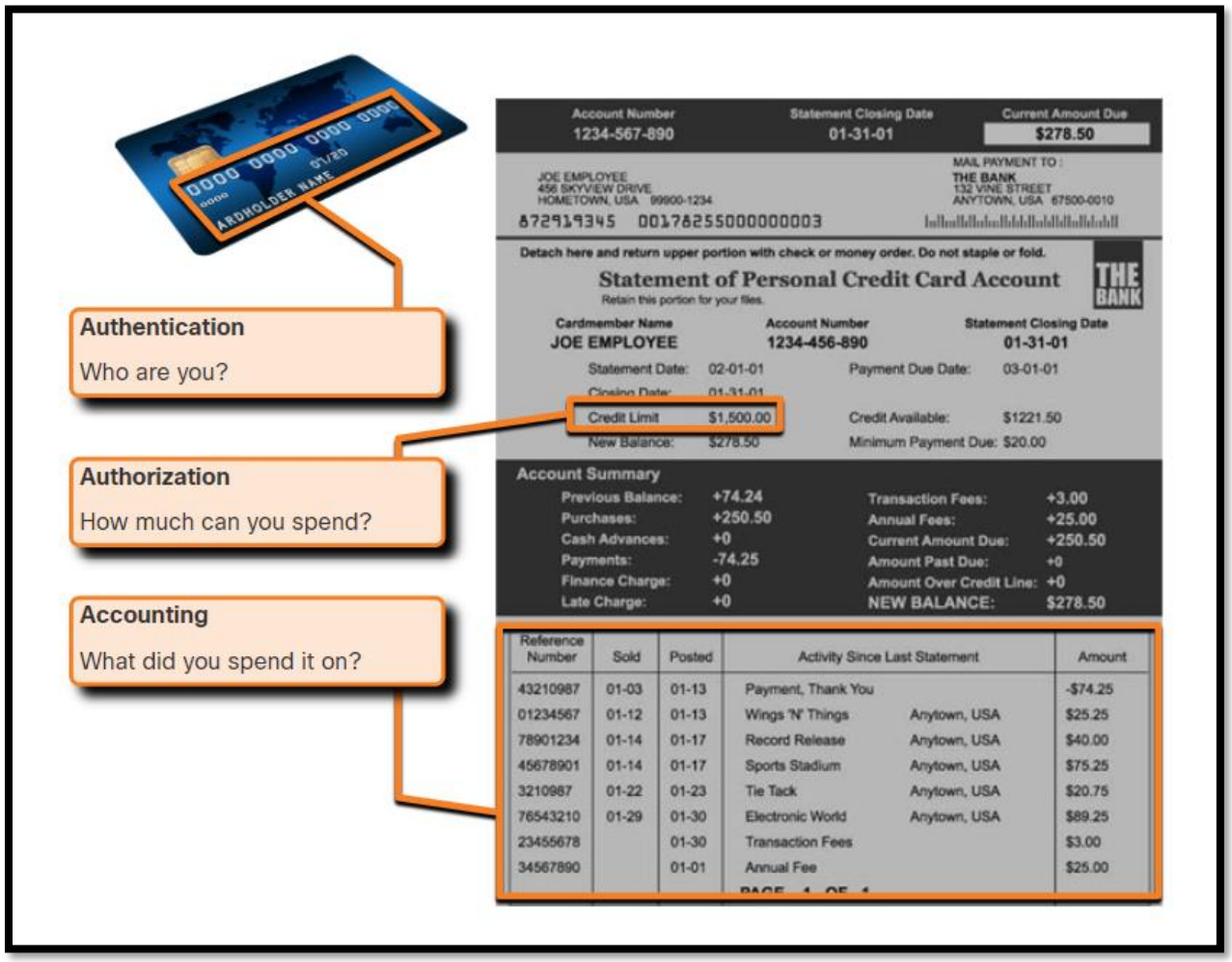
- A sticky MAC address is a hybrid between a static and dynamic MAC address.
- Dynamically learned, MAC address is automatically entered into the running configuration.
- The address is then kept in the running configuration until a reboot.
- Once the switch is reboot, the MAC address will be lost.
- To keep the MAC address across a reboot a configuration save is required.
- **switchport port-security mac-address sticky**

Lab Time:



Switchport Security Configuration:
interface f0/1 switchport mode access switchport port-security switchport port-security mac-address 0010.1180.9275 SWitchport Portt-security violation shutdown show port-security show port-security address show port-security interface f0/1
interface f0/2 switchport mode access switchport port-security switchport port-security mac-address sticky SWitchport PORt-security violation protect show port-security show port-security address show port-security interface f0/2
interface f0/3

switchport mode access
switchport port-security
SWitchport PORt-security violation restrict
show port-security
show port-security address
show port-security interface f0/3



AAA (Authentication, Authorization and Accounting):

- Authentication: Verify the identity of the user, who are you.
- Authorization: What is the user allowed to do? Example what resource he can access etc? (How much you can spend)

- Accounting: It is like all record what is done by that user it will keep all record. Example used for billing and auditing (What did you spend it on record)

AAA Stand for Authentication, Authorization and Accounting:

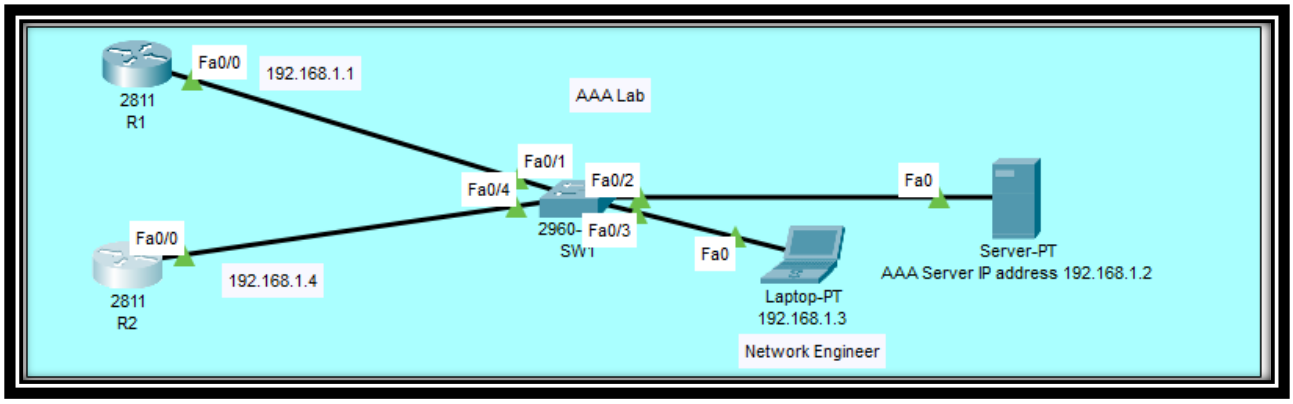
- It is a Centralized Management of users to access the network devices
- AAA Server allow setting up access control on Cisco Routers and Switches
- Like if we have 300 Switches and 10 Router in our organization then it will be very difficult to create all user in that all devices and delete when they leave organization etc. And it will take lot of memory of devise also to overcome with this type of issues we use AAA Server.
- AAA Server also control connections passing through router or switch for access network.
- When every user tries to connect to router or switch these network devices verifies by AAA Server (AAA Database)
- User Management is done with AAA Server without need to reconfigure to individual router or switch
- Like any new user came we need to configure only in AAA Server no need to add that user in Router or switch.
- AAA Server use two Main type of Protocol to configure this
- Radius Protocol (Remote Authentication Dial-in User Service)
- TACACS+ (Terminal Access Controller Access-Control System Plus)

Radius Protocol:

- It is open standard where as TACACS is Cisco Proprietary protocol.
- It uses UDP and users ports numbers 1812/1645 and 1813/1646.
- It Encrypts passwords only.
- It is light weight protocol (Consume less resources).

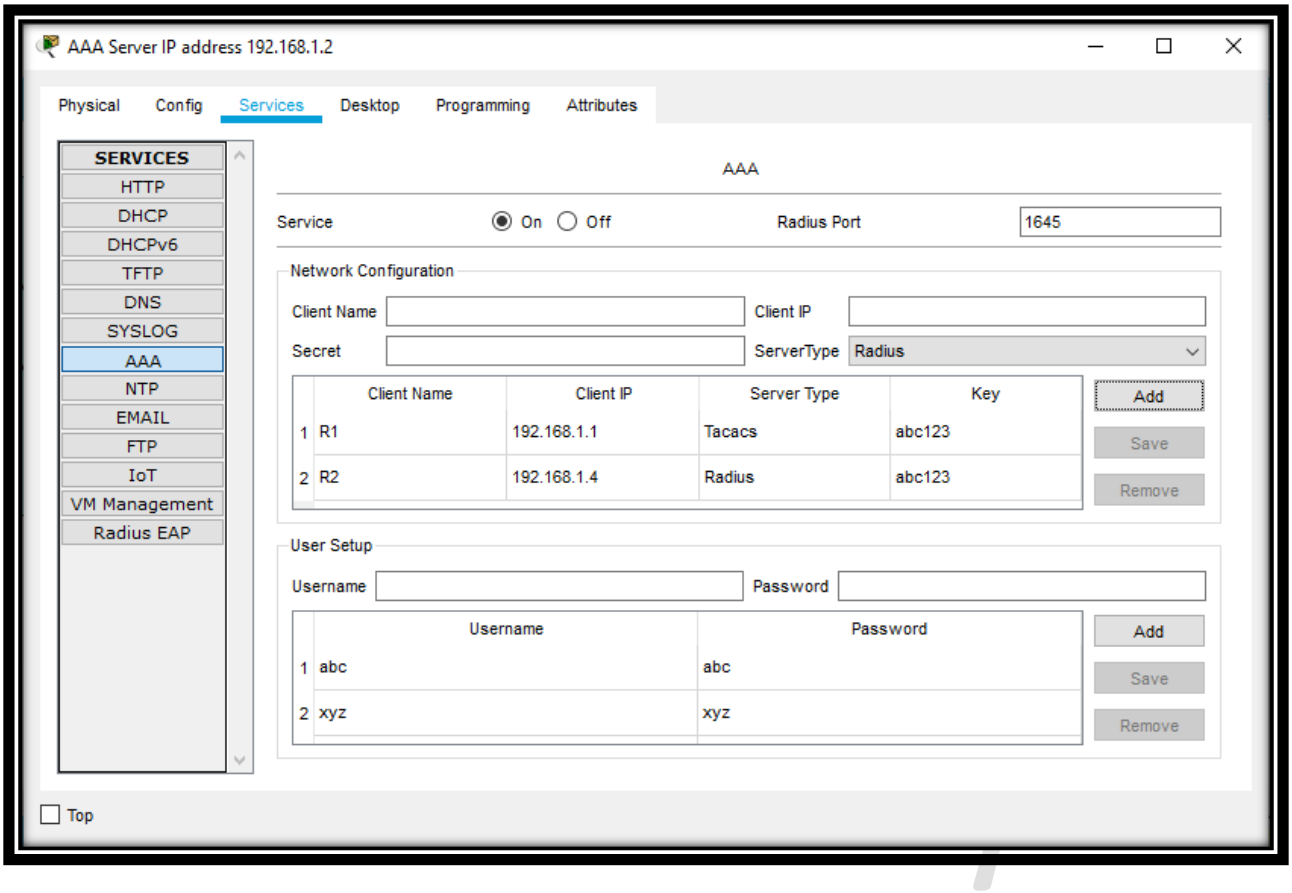
TACACS+:

- It is CISCO Proprietary protocol.
- It use TCP and port number user 49.
- It encrypts entire communication.
- It is heavy weight protocol consuming more resources.



R1 Configuration	R2 Configuration
en config t hostname R1 int f0/0 ip add 192.168.1.1 255.255.255.0 no sh aaa new-model Tacacs-server host 192.168.1.2 key abc123 aaa authentication login AAA group tacacs+ Line vty 0 1 login authentication AAA	en config t hostname R2 int f0/0 ip add 192.168.1.4 255.255.255.0 no sh aaa new-model radius-server host 192.168.1.2 key abc123 aaa authentication login AAA group radius Line vty 0 1 login authentication AAA

AAA Server Setting:



Describe wireless Security Protocols (WPA, WPA2 and WPA3):

Let discuss about security protocols for Wireless.

Now a day we use several different protocols that are used for securing a Wi fi Network.

So let's start with a secure protocol called WEP.

WEP Stand for Wired Equivalent Privacy:

- It is earliest security protocol that was used for wireless networks.
- It 32 bit key was not secure and it was easily hackable.
- That why today WEP is no longer use

WPA (Wi fi Protected Access):

- WPA stands for Wi Fi Protected Access
- It is another wireless security Protocol
- It is developed to solve the problem of WEP and it is better than WEP
- WPA is uses a stronger encryption method called TKIP (Temporal Key Integrity Protocol)
- And TKIP dynamically changes its keys as its being used
- But now WPA is outdated because TKIP did have some weakness

WPA 2 (Wi FI Protected Access 2):

- It is more strong then WPA1
- It use AES Encryption (AES stand for Advanced Encryption Standard)

Next generation of wireless security is WPA3