



Chapter 2

Switch Concepts and Configuration

Part II

CCNA3-1

Chapter 2-2

Note for Instructors

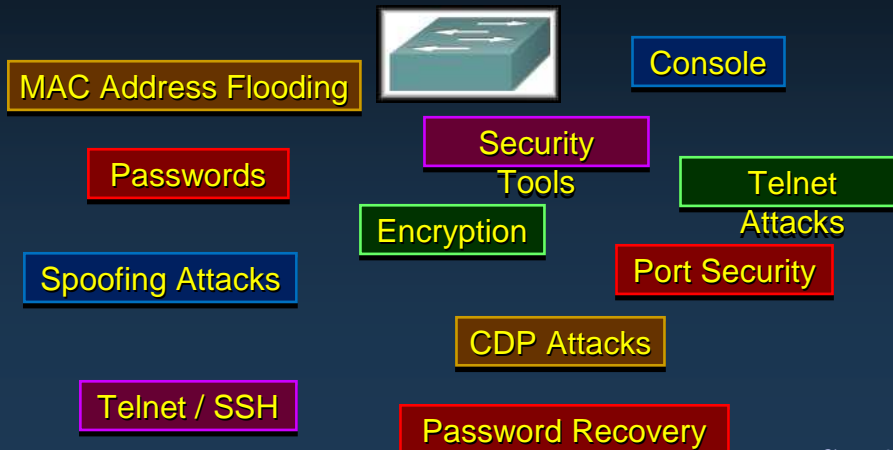
- These presentations are the result of a collaboration among the instructors at St. Clair College in Windsor, Ontario.
- Thanks must go out to Rick Graziani of Cabrillo College. His material and additional information was used as a reference in their creation.
- If anyone finds any errors or omissions, please let me know at:
 - tdame@stclaircollege.ca.

CCNA3-2

Chapter 2-2

Switch Concepts and Configuration

Configuring Switch Security



Configuring Password Options

- Securing Console Access:

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	<code>S1#configure terminal</code>
Switch from global configuration mode to line configuration mode for console 0.	<code>S1(config)#line con 0</code>
Set cisco as the password for the console 0 line on the switch.	<code>S1(config-line)#password cisco</code>
Set the console line to require the password to be entered before access is granted.	<code>S1(config-line)#login</code>
Exit from line configuration mode and return to privileged EXEC mode.	<code>S1(config-line)#end</code>

Configuring Password Options

- **Securing Virtual Terminal Access:**
 - There are 16 available default Telnet sessions as opposed to the 5 sessions set up for a router.

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1# configure terminal
Switch from global configuration mode to line configuration mode for vty lines 0 - 15	S1(config)# line vty 0 15
Set cisco as the password for the vty lines on the switch.	S1(config-line)# password cisco
Set the vty lines to require the password to be entered before access is granted.	S1(config-line)# login
Exit from line configuration mode and return to privileged EXEC mode.	S1(config-line)# end

CCNA3-5

Chapter 2-2

Configuring Password Options

- **Securing Privileged EXEC Access:**
 - Always use **enable secret** for password encryption.

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1# configure terminal
Configures the enable password to enter privileged EXEC mode.	S1(config)# enable password password
Configures the enable secret password to enter privileged EXEC mode.	S1(config)# enable secret password
Exit from line configuration mode and return to privileged EXEC mode.	S1(config)# end

CCNA3-6


Chapter 2-2

Configuring Password Options

- **Encrypting Switch Passwords:**
 - You can encrypt all passwords assigned to a switch using the **service password-encryption** command.

```
S1#config terminal
S1(config)#service password-encryption
S1(config)#end
S1#Show running-config

control-plane
!
line con 0
password 7 030752180500
login
line vty 0 4
password 7 1511021F0725
no login
line vty 5 15
password 7 1511021F0725
no login
!
end
```



CCNA3-7

Chapter 2-2

Configuring Password Options

- **Password Recovery:**
 - To recover a switch password:
 - Power up the switch with the Mode button pressed.
 - Initialize flash.
 - Load the configuration file.
 - Reconfigure the switch.
 - Reinitialize the switch.
 - Reinstall the name of the configuration file and copy it into RAM.
 - Change the password.
 - Copy to start up configuration
 - Reload the switch.

A detailed password recovery procedure will be provided on Blackboard and in the lab.

CCNA3-8

Chapter 2-2

Login Banners

- **Login Banner:**

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1# configure terminal
Configure a login banner.	S1(config)# banner login "Authorized Personnel Only!"

- **Message-Of-The-Day (MOTD) Banner:**

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1# configure terminal
Configure a MOTD login banner.	S1(config)# banner motd "Device maintenance will be occurring on Friday!"

Configure Telnet and SSH

- **Telnet:**

- Most common method.
- Virtual Terminal application.
- Send in clear text.
- Not secure.

- **Secure Shell (SSH):**

- Virtual Terminal application.
- Sends an encrypted data stream.
- Is secure.

Configure Telnet and SSH

- **Configuring Telnet:**

- Telnet is the **default transport** for the vty lines.
- No need to specify it after the initial configuration of the switch has been performed.
- **If you have switched the transport protocol on the vty lines to permit only SSH**, you need to enable the Telnet protocol to permit Telnet access.

```
S1(config)#line vty 0 15
S1(config-line)#transport input telnet
```

Configure Telnet and SSH

- **Configuring Secure Shell (SSH):**

- SSH is a cryptographic security feature that is subject to export restrictions. To use this feature, a cryptographic image must be installed on your switch.
- Perform the following to **configure SSH ONLY** Access:

```
(config)#ip domain-name mydomain.com
(config)#crypto key generate rsa
(config)#ip ssh version 2
(config)#line vty 0 15
(config-line)#transport input SSH
```

Common Security Attacks

- **MAC Address Flooding:**
 - Recall that the MAC address table in a switch:
 - Contains the MAC addresses available on a given physical port of a switch.
 - Contains the associated VLAN parameters for each.
 - Is searched for the destination address of a frame.
 - If it **IS** in the table, it is forwarded out the proper port.
 - If it **IS NOT** in the table, the frame is forwarded out all ports of the switch except the port that received the frame.

Common Security Attacks

- **MAC Address Flooding:**
 - The MAC address table is **limited in size**.
 - An intruder will use a network attack tool that continually sends bogus MAC addresses to the switch.
 - (e.g. 155,000 MAC addresses per minute)
 - The switch learns each bogus address and in a short span of time, the table becomes full.
 - *When a switch MAC table becomes full and stays full, it has no choice but to forward each frame it receives out of every port – just like a hub.*
 - The intruder can now see all the traffic on the switch.

Common Security Attacks

- **Spoofing Attacks:**
 - **Man-In-The-Middle:**
 - Intercepting network traffic.
 - DHCP or DNS spoofing.
 - The attacking device responds to DHCP or DNS requests with IP configuration or address information that points the user to the intruder's destination.
 - **DHCP Starvation:**
 - The attacking device continually requests IP addresses from a real DHCP server with continually changing MAC addresses.
 - Eventually the pool of addresses is used up and actual users cannot access the network.

CCNA3-15

Chapter 2-2

Common Security Attacks

- **CDP Attacks:**
 - Cisco Discovery Protocol (CDP) is a proprietary protocol that exchanges information among Cisco devices.
 - IP address
 - Software **Usually on by default.**
 - Platform **If you don't need it, turn it off.**
 - Capabilities
 - Native VLAN **(Trunk Links – Chapter 3).**
 - With a free network sniffer (Wireshark) an intruder could obtain this information.
 - It can be used to find ways to perform Denial Of Service (DoS) attacks and others.

CCNA3-16

Chapter 2-2

Common Security Attacks

- **Telnet Attacks:**
 - Recall that Telnet transmits in plain text and is not secure. While you may have set passwords, the following types of attacks are possible.
 - Brute force (password guessing)
 - DoS (Denial of Service)
 - With a free network sniffer (Wireshark) an intruder could obtain this information.
 - Use strong passwords and change them frequently.
 - Use SSH.

Network Security Tools

- Help you test your network for various weaknesses. They are tools that allow you to play the roles of a hacker and a network security analyst.
 - **Network Security Audits:**
 - Reveals what sort of information an attacker can gather simply by monitoring network traffic.
 - Determine MAC address table limits and age-out period.
 - **Network Penetration Testing:**
 - Identify security weaknesses.
 - Plan to avoid performance impacts.

Network Security Tools

- **Common Features:**
 - **Service Identification:**
 - IANA port numbers, discover FTP and HTTP servers, test all of the services running on a host.
 - **Support of SSL Service:**
 - Testing services that use SSL Level security.
 - HTTPS, SMTPS, IMAPS and security certificates.
 - **Non-destructive and Destructive Testing:**
 - Security audits that can degrade performance.
 - **Database of Vulnerabilities:**
 - Compile a database that can be updated over time.

Network Security Tools

- **You can use them to:**
 - Capture chat messages.
 - Capture files from NFS traffic.
 - Capture HTTP requests.
 - Capture mail messages.
 - Capture passwords.
 - Display captured URLs in a browser in real-time.
 - Flood a switched LAN with random MAC addresses.
 - Forge replies to DNS addresses.
 - Intercept packets.

Configuring Port Security

- **Implement Port Security to:**
 - *Port security is disabled by default.*
 - Limit the number of valid MAC addresses allowed on a port.
 - When you assign secure MAC addresses to a secure port, the port **does not forward** packets with **source addresses outside the group** of defined addresses.
 - Specify a group of valid MAC addresses allowed on a port.
 - **Or** Allow only one MAC address access to the port.
 - Specify that the port automatically shuts down if an invalid MAC address is detected.

Configuring Port Security

- **Secure MAC Address types:**
 - **Static:**
 - Manually specify that a specific MAC address is the **ONLY** address allowed to connect to that port.
 - They are added to the MAC address table and stored in the running configuration.
 - **Dynamic:**
 - MAC addresses are learned dynamically when a device connects to the switch.
 - They are stored in the address table and are lost when the switch reloads.

Configuring Port Security

- **Secure MAC Address types:**
 - **Sticky:**
 - Specifies that MAC addresses are:
 - Dynamically learned.
 - Added to the MAC address table.
 - Stored in the running configuration.
 - You may also manually add a MAC address.
 - MAC addresses that are “**sticky learned**” (you will hear that phrase) will be lost if you fail to save your configuration.

Configuring Port Security

- **Security Violation Modes:**
 - Violations occur when:
 - A station whose MAC address is not in the address table attempts to access the interface and the address table is full.
 - An address is being used on two secure interfaces in the same VLAN.
 - **Modes:**
 - **Protect:** drop frames – no notify
 - **Restrict:** drop frames - notify
 - **Shutdown:** disable port - notify

Configuring Port Security

- **Default Security Configuration:**

Feature	Default Setting
Port security	Disabled on a port.
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.
Sticky address learning	Disabled.

Configuring Port Security

- **Configure Static Port Security:**

- ONLY address allowed.
- Add to MAC table and running configuration.

```
s1#configure terminal
s1#(config)interface fa0/1
s1#(config-if)switchport mode access
s1#(config-if)switchport port-security
s1#(config-if)switchport port-security mac-address abcd.1234.7890
```

Configure the Interface

Enable Port Security

Specify the MAC address

Configuring Port Security

- **Configure Dynamic Port Security:**

- Dynamically learned when the device connects.
- Added to MAC table only.

Configure the Interface

```
s1#configure terminal
s1#(config)interface fa0/1
s1#(config-if)switchport mode access

s1#(config-if)switchport port-security
```

Enable Port Security

Configuring Port Security

- **Configure Sticky Port Security:**

- Dynamically learn MAC addresses.
- Add to MAC table and running configuration.

Configure the Interface

```
s1#configure terminal
s1#(config)interface fa0/1
s1#(config-if)switchport mode access

s1#(config-if)switchport port-security

s1#(config-if)switchport port-security maximum 24

s1#(config-if)switchport port-security mac-address sticky
```

Enable Port Security

Specify a maximum

Enable "sticky" learning

Verify Port Security

- Verify Port Security Settings:

```
switch#show port-security interface fastEthernet 0/18
Port Security           : Enabled
Port Status             : Secure-down
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

Verify Port Security

- Verify Secure MAC Addresses:

```
switch#show port-security address
Secure Mac Address Table
-----
Vlan  Mac Address      Type                Ports    Remaining Age (mins)
99    0050.BAA6.06CE    SecureConfigured    Fa0/18   -
-----
Total Addresses in System (excluding one mac per port)  : 0
Max Addresses limit in System (excluding one mac per port) : 8320
```

Securing Unused Ports

- **Disable unused ports:**

```
...
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
...
!
interface FastEthernet0/18
 switchport mode access
 switchport port-security
...
```

You can specify a range of interfaces.
For example, to specify the first 10 interfaces:
interface range fastethernet 0/1 - 10