BRYANT CCNA 2018 SECTION 5 - MEMORY, BOOT, PASSWORDS

Memory 1: Mem contents and boot process.

ROM - Stores bootstrap startup program, OS software, and power-on diagnostic test programs (POST)
Flash Memory - Stores IOS image ~~and config files~~
RAM: Stores operational info like routing/switching tables and the running config file
NVRAM: Non-Volatile RAM. Holds startup config file

IOS Image search order:
1. Flash (default)
2. TFTP
3. ROM

Memory 2: Setup Mode

ctrl-c to exit dialog

MEMORY 3: Enable secret/Password

enable secret - sets secret, which always overrides the password.
enable password - also used for auth, probably for backward compatibility? Not used if secret set.

Memory 4: Console Port Single Password

```
(config)# line con 0
(config-line)# login
            # password cisco
```

Memory 5: Console Port Username/Password DB

So far we have a password, but:
- no accountability. no usernames are asked for
- password is easier to crack than username/pw
- passwords are shared by people who shouldn't share

- To add a username/password:

```
(config)# username admin password cisco
```

- To enable login:

```
          # line con 0
(config-line)# login local
```

To automatically encrypt all passwords:

```
(config)# service password-encryption
```

Memory 6: Port Security Success Fundamentals

AKA "The Enemy Within"

Port Security - Abasic Cisco Security feature that uses the source MAC address of incoming frames.

First: check ports to verify things are on the right port.

```
# show cdp neighbors
```

Then, to enable on an interface:

```
(config)# int fast 0/1
(config-if)# switch port port-security
```

NOTE: port must be in access mode for port security!

```
(config-if) switchport mode access
```

Port Security Options!

```
sw1(config-if)# switchport port-security aging time?
 <1-1440> Aging time in minutes
Aging type:
  absolute:   Absolute Aging (default)
  inactivity: Aging based on inactivity time period
```

```
port-security maximum?
  <1-6144>  Maximum MAC Addresses
```

```
port-security mac-address?
   H.H.H   48 bit MAC address
   sticky  Configure dynamic secure addresses as sticky
```

```
switchport port-security violation?
    protect    security violation protect mode
    restrict   security violation restrict mode
    shutdown   security violation shutdown mode
```

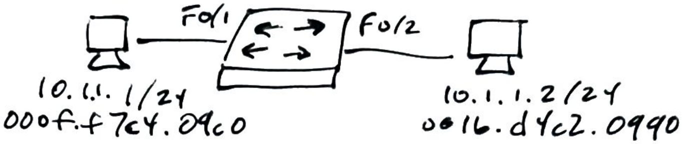
Shutdown - puts port into error-disable mode, and generates SNMP message

Restrict - generates SNMP / syslog message.

Protect - only drops frame. nothing else.

~~Memory 21: Port Security options~~

Memory 8: Port Security Static Lab Begins



Enable port security

```
sw1(config)# int fo/1
   (config-if)# switchport port-security
```

(must be an access port, 'switchport mode access')

```
#switchport port-security mac-adress
                        aaaa.bbbb.cccc
```

This is not the right MAC, so the interface will now be down for more info:

```
# show port-security
# show int fo/1
# show port-security int fo/1   ← ✱
```

Steps to Fix:

1. Resolve the issue first
2. Then reset the port

} order is important. If you reset the port first it will error again

fix port-security

```
# inf fast 0/1
#^no switch~~mode~~ port-securnty- mac-address ....
# switchport port-security mac-address
                       000f.f7c4.09c0
```

reset port

```
# shut
# no shot
```

Memory 10: Port Security Dynamic Lab

By just turning on port-security without a MAC:

→ (config-if)# switchport port-security

Once the port goes up, it will take the connected MAC.
you can view the addresses with

→ # show port-security address

To add another address, or allow dynamic learning with an address assigned, change the max.

→ (config-if)# switchport port-security maximum 2

Now you can add up to two addressed, or learn dynamically

Memory 11: Port Security Sticky Address

- Dynamic Entries Lost if port shut down
- Sticky sets the MAC to be stored.

```
# int f0/1
# switch-port port-security mac-address sticky
```

That's all! Now any Dynamically learned MAC addresses are markedas sticky and will be stored.

Errdisable recovery

```
(config)# err disable recovery cause psecure-violation
```

★ not supported in packet tracer

```
# err disable recovery interval 30
```

seconds- minimum 30 seconds