Achievable

CCNA DUMP SHEET

Device and Layer 2 security

How IOS stores a password

Type	Stored as	From
0	Clear text	The `password` keyword
7	Weak, reversible	`service password-encryption`
5	Salted MD5 hash	The `secret` keyword
9	SCRYPT, newer IOS	The `secret` keyword

- **Both set:** `enable secret` beats `enable password`
- **Type 7:** only slows shoulder surfing. Secrets are always hashed

TACACS+ vs RADIUS

	TACACS+	RADIUS
Origin	Cisco proprietary	Industry standard
Ports	TCP 49	UDP 1812, 1813 (accounting)
Encrypts	Entire packet body	Password only
AAA	Separates all three	Combines the first two
Used for	Device administration	End users: VPNs, wireless

Console and VTY access

```
R1(config)# enable secret cisco123
R1(config)# username admin privilege 15 secret cisco
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# line vty 0 15
R1(config-line)# login local
```

- **Local accounts:** unused until the line has `login local`
- **Line password:** `password cisco`, `login`. Not recommended
- **Privilege:** default 1. 15 skips `enable`, straight to privileged EXEC

Port security

`switchport mode access`	First step
`switchport port-security`	Turns it on
`switchport port-security maximum 2`	Default 1
`switchport port-security mac-address <mac>`	Static MAC
`switchport port-security mac-address sticky`	Learned
`switchport port-security violation restrict`	Sets mode
`show port-security [interface g0/1]`	All, or one
`show interfaces status err-disabled`	Disabled

- **Dynamic port:** refused, so set access or trunk first
- **Phone with a PC:** maximum of at least 2

Port security violations

Mode	Offender	Port	Syslog, SNMP	Counter
`protect`	Dropped	Stays up	No	No
`restrict`	Dropped	Stays up	Yes	Yes
`shutdown`	Dropped	Err-disabled	Yes	Yes

- **Defaults:** maximum 1 MAC, mode `shutdown`
- **Violation:** a source MAC not allowed, or over the maximum
- **Sticky:** MACs join running-config. Save, or lost on reload
- **Recover:** `shutdown`, then `no shutdown` on the interface
- **Auto:** `errdisable recovery cause psecure-violation`
- **Port Status:** `Secure-up`, `Secure-shutdown`

DHCP snooping

```
SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 10
SW1(config)# interface g0/1
SW1(config-if)# ip dhcp snooping trust
SW1(config-if)# interface g0/2
SW1(config-if)# ip dhcp snooping limit rate 10
```

- **Needs both:** the global command and a VLAN
- **Untrusted (default):** drops server messages, OFFER and ACK
- **Trusted:** toward the DHCP server or a relay
- **Client checks:** DISCOVER, REQUEST: source MAC equals chaddr. RELEASE, DECLINE: match the binding table
- **Binding table:** IP, MAC, VLAN, port
- **Option 82:** on by default. Turn it off on a Layer 2 switch that isn't a relay: `no ip dhcp snooping information option`
- **Limit:** none by default. Over it: err-disabled
- **Verify:** `show ip dhcp snooping`, add `binding`

Dynamic ARP Inspection (DAI)

```
SW1(config)# ip arp inspection vlan 10
SW1(config)# interface g0/1
SW1(config-if)# ip arp inspection trust
```

- **First:** DHCP snooping. DAI reads its binding table
- **Checks:** ARP sender IP and MAC on untrusted ports, or drops
- **Static IP hosts:** not in the table, so use an ARP ACL
- **Trust:** switch and router links. All ports untrusted by default
- **Port limit:** `ip arp inspection limit rate 25`
- **Default limit:** 15 pps on untrusted ports. Over it: err-disabled
- **Verify:** `show ip arp inspection`, add `statistics`