Cisco Security

User and access management

Enable secret takes precedence over enable password.

```
enable password potato
enable secret potato2

enable password = potato2
```

Enable AAA (allow user with privilege 15 to login straight into enable mode)

```
conf t
aaa new-model
aaa authentication login default group local
aaa authorization exec default group local
```

Create user with default privilege 15 level

```
conf t
username $USERNAME privilege 15 secret $PASSWORD
```

login = password and username of the vty itself.
login local = Local username database

```
conf t
line con 0
login local
exec-timeout 0 0
logging synchronous
```

Line VTY user are set to privilege 15 automatically.

```
conf t
line vty 0 15
privilege level 15
```

"Encrypt" passwords in the startup-config.

```
service password-encryption
```

Port-Security

Enabling port security on port
Cannot be enabled on a trunk/dynamic/auto port. Must be an access port.

```
conf t
interface gigabitethernet0/1
switchport port-security
```

Keep MAC addresses when port-shutdown or switch reload.

```
conf t
interface gigabitethernet0/1
switchport port-security
switchport port-security mac-address sticky
```

MAC aging

Dynamic MAC aging default = 0
absolute timer = Counts down irregardless of traffic
inactivity timer = resets when traffic is seen from MAC.
maximum - Default 1
If you raise the number of max MAC addresses on a port, you can run static and dynamic MAC detection.

MAC address conversion

Character	HEX
a	10
b	11
c	12
d	13
e	14
f	15

- One digit hex ---> 0-9 or A-F
- Two digit hex ---> Left to Right, units of 16 ---> units of 1.

Hexadecimal A7 to decimal
A = 10 units of 16 (A=16) ---> 160
7 = 7 units of 1 ---> 7
160 + 7 = 167

Decimal 241 to Hexadecimal

1. f = 15 * 16
2. 1 = 1 * 1
3. F1

Violation option

protect - Drops traffic, no SYSLOG, no SNMP Trap, no counters increased
restrict - Drops traffic, generate SNMP trap, generate SYSLOG.
shutdown - Default, increase violation counters, Port shutdown in error-disabled.

Show port-security commands

```
show port-security interface fastethernet 0/1
```

```
show port-security address
```

Error disabled recovery
Default recovery 300 seconds

```
conf t
errordisable recovery cause ?
errordisable recovery cause psecure-violation
errdisable recovery interval 30
```

```
show errdisable recovery
```

VLAN interfaces (SVI)

- Layer 2 vlan must exist
- Physical interface with vlan attached to must be in UP and UP.
    - Can be a trunk with vlan allowed or an access port with the vlan.

Autonegociation - Speed and Duplex

- Highest speed supported by both is used.
- Full duplex supported by both is used.
- **DO NOT** set one side auto and the other side forced.
- Symptoms --> Slow Upload, irregular speed, packet loss, CRC/Runt frames errors on the interface

Interface range

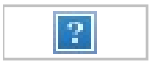
```
interface range fastethernet 0/1-24
interface range fastethernet 0/1-24,25,26
```

TCP and UDP

TCP

- Guarantees delivery of segments
- Error Detection and recovery
    - Sequence numbers and ACK to recover from lost/corrupt packets
- TCP Windowing
- Connection-oriented
    - Three-way handshake
    - SYN FLAG / ACK FLAG
    - Source ---> Destination : SYN
    - Destination ---> Source : SYN-ACK
    - Source ---> Destination : ACK
    - Connection Established
- When connection is terminated - 4 Way Handshake
    - Client ---> Server : FIN, ACK
    - Client <--- Server : ACK
    - Client <--- Server : ACK, FIN
    - Client ---> Server : ACK
- Flow control and Windowing

- The receiver increases the Window size / controls the flow.
- The receiver asks for more data when traffic flows well --> No errors/retransmits on packets.



UDP

- "Best Effort"
- No Error Detection
- No Windowing
- Connectionless - Data is sent without the remote peer being aware.

Port Numbers

Well-known port numbers:

Protocol / Transport	Port
HTTPS / TCP	443
SNMP / UDP	161
SMTP / TCP	25
TELNET / TCP	22
SSH / TCP	23

Socket ---> Combination of an ipaddress and a port number.
192.168.1.1:10000

DHCP

DORA

1. Discover - Broadcast from client.
2. Offer - DHCP server receives Discover and sends unicast offer to client.
3. Request - Client sends request for the offered IP address.
4. Ack - DHCP server ack the client request and assigns the IP.

Routing - Static Routes

```
ip route destination_subnet destination_mask [local-router-exit-interface | next-hop-ip-address]

ip route 2.2.2.2 255.255.255.0 192.168.1.1

#Default Route
ip route 0.0.0.0 0.0.0.0 [local-router-exit-interface | next-hop-ip-address]
```

Routing - Distance Vector Protocols - RIP

RIPv1 / IGRP

- Full route table update at fixed interval. Every 30 seconds for RIP.

- Do not subnet VLSM.
- No Packet authentication.

RIPv2

- Supports VLSM.
- Multicasts from router updates - 224.0.0.9 instead of broadcast (RIPv1)
- Supports Authentication.
- Supports route summarization.

Split Horizon

- A route cannot be advertised via an interface that received the route in the first place.
- No split horizon on frame-relay.

Route Poisoning

- When all routers have the same routing table --> State of convergence
- Slow to converge
- When router removes a subnet that is local to itself.
    - Send update that shows 16 hops for the removed subnet.
    - Other routers will receive the update and remove the route from their own routing tables as 16 hops marks a subnet as unreachable.

Hops

- Metric for RIPv2.
- Measures of distance to reach a specific subnet.
- Does not care about interface speed - only hop count.

Enabling RIPv2

```
conf t
router rip

#Show protocols active on router
show ip protocols

#Enable specific version of RIPv2 per interface or global.
interface gig0/1
ip rip send version 2

conf t
router rip
rip version 2
network 10.10.10.0
network 10.10.11.0

#Disable auto summary
conf t
router rip
no auto-summary

#Enable split Horizon
interface serial0/1/0
ip split-horizon
```

Confirming that RIPV2 works.

```
show ip protocols
show ip rip database
```

Clear RIP routes.

```
clear ip route *
```

Passive interfaces

Prevents sending RIPv2 updates from interfaces where it's not necessary.

```
conf t
router rip
passive-interface fastethernet0/1
passive-interface fastethernet0/2
```

```
conf t
router rip
passive-interface default
no passive-interface fastethernet0/1
no passive-interface fastethernet0/2
```

RIP Load Balancing

1. If a subnet is reachable through two paths with the same hope count --> Load balance across the two links.

Disabling equal cost load balancing

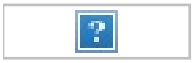
```
conf t
router rip
maximum-path 1
```

Default route in RIP

```
conf t
router rip
default-information originate
```

Routing Administrative distance

1. The prefix mask is considered first. The more specific route is installed.
2. If the prefix max is "=" ---> Administrative Distance is checked. The route with the lowest ADs wins.



Floating static routes

If a route with a lower AD is removed from the routing table, the static route will be added and become active.

```
conf t
ip route 2.2.2.0 255.255.255.0 21.1.1.2 [static route metric here | higher than
routing protocol 1-255 ]
```

Subnetting

	128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
45	0	0	0	0	1	1	0	1

200.17.100.3

	128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
200	1	1	0	0	1	0	0	0
17	0	0	0	1	0	0	0	1
100	0	1	1	0	0	1	0	0
3	0	0	0	0	0	0	1	1

11001000.00010001.01100100.00000011

Network class

	Class A	**Class B**	**Class C**
1st Octet range	1 - 126	128 - 191	192 - 223
Network Mask	255.0.0.0 - /8	255.255.0.0 - /16	255.255.255.0 - /24

Number of subnet in a network - 200.1.1.0 /27

1. Find the class of the subnet --> Class C (+192)
2. A class C is a /24 by default.
3. /27 - /24 = 3 subnet bits.
4. Number of subnet --> 2^Number_subnet_bits_remaining --> 2^3 --> 2 * 2 * 2 = 8 subnets

Number of hosts per subnet - 200.1.1.0 /27

1. Find the number of host bits --> /32 - /27 --> /5 host bits
2. Find the number of valid host per subnet - remove subnet and broadcast address.
3. (2^(number of host bits))-2 --> 2^5 --> 2 * 2 * 2 * 2 * 2 --> 32 - 2 --> 30

Find the Subnet of an IP address - 10.17.2.14/18

1. /18 = First two octets = 16 bits + 2 bits from third octet
2. 10.17.00000010
3. 10.17.**00** 000000 --> Total of 18 bits for subnet address
4. Subnet address = 10.17.0.0/18

Find the broadcast and range of valid addresses in subnet - 210.46.110.0 /25

1. /32 - /25 = last 7 bits --> host bits
2. 01111111 --> 64 + 32 +16 +8 + 4 + 2 +1 --> 96 + 16 + 15 --> 96 + 31 --> Broadcast = 210.46.110.127

Find the broadcast and range of valid addresses in subnet - 150.10.64.0 /18

1. /32 - /18 = last 14 bits --> host bits

	128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
64	0	1	0	0	0	0	0	0

2. Broadcast --> 150.10.0**1111111.11111111** --> 150.10.127.255
3. Range of valid addresses --> 150.10.64.1 to 150.10.127.254

Access Lists

- All ACL have an implicit DENY ALL ALL at the end.
- The search is done TOP to BOTTOM
- When a match is found, that's the end of the search. Any remaining lines are not examined.

Wildcard masks

- 0 --> All bits must match.
- 1 --> Does not need to match.

Standard ACL

- Can only match on the SOURCE ip address of a packet.
- Standard Access list number : 1 --> 99
- Standard expanded access list number : 1300 --> 1999

```
<1-99>       Standard IP access-list number
<1300-1999>  Standard IP access-list number (expanded range)
WORD         Access-list name
```

```
ip access-list standard 5 deny 3.3.3.0 0.0.0.255
interface fastethernet0
ip access-group 5 in
```

Extended ACL

- Can match on source AND/OR destination.

Named Extended/Standard ACL

- Allows naming of Access list instead of number.
- Valid for Standard and Extended ACL.
- Cannot have an Extended and Standard ACL with the same name.
- You need to use `ip access-list standard | extended` instead of `access-list`

```
conf t
ip access-list extended BLOCK11
deny ip 3.3.3.0 0.0.0.255 11.11.11.0 0.0.0.255
permet ip any any
```

ACL on VTY lines

```
conf t
line vty 0 14
access-class MGMT-NETWORKS in
```

ACL Sequence numbers####

- Allows moving and deletion of specific lines within the ACL.
- You cannot move or reassign a sequence number.
- You need to delete and recreate the line with the new sequence number.

```
conf t
ip access-list extended 101
no $SEQUENCE_NUMVER
```

Where to apply ACLs

- Apply Extended ACLs as close to the **source** of the traffic.
- Apply Standard ACL as close to the **destination** as possible.

NTP - Network Time Protocol

- Creates a single source of time for all device on the network.
- UDP Port 123

Stratum - Level of accuracy of the NTP server.

- 0 --> Atomic clocks
- 1 --> Gets time from a stratum 0 NTP server.

NTP Modes

- Master : Set the device itself as the master and will synch with itself to synchronize time.
- Peer : The two devices will dynamically synchronize time between the two.
- Server : The client device will ask time from the server. Does not send time synchronize requests to the server.
- Broadcast Mode : Broadcast mode for NTP packets.

```
!*** Set the device itself as the master NTP server.
conf t
ntp master
```

```
!*** Set the NTP server for the device.
conf t
ntp server ntp.nist.ca
```

```
conf t
ntp peer ntp.potato.com
```

```
!*** Show all ntp services from which the device will sync it's clock. Also
shows the preferred device.
show ntp associations

show ntp status

show clock
```

```
!*** Under device interface configuration.
!*** Sets broadcast server mode (send updates)
conf t
interface serial 0/1/0
ntp broadcast


!*** Set client broadcast mode
conf t
interface serial 0/1/0
ntp broadcast client
```

NAT / PAT - Network Address Translation / Port Address Translation

- Local --> Private address
- Global --> Public routable address
- Inside Local --> **Local Address** being translated to External.
- Inside Global --> **External Address** that is used during the NAT.
- Outside Local --> **Non-routable** addresses of the host on the remote network.

- Outside Global --> **Routable** addresses of the host on the remote network.

Static NAT

- One to one mapping of an Inside Local to a Inside Global.
    - I.E : Map a public IP to the internal IP of a server.

```
!*** Place on the interfaces closest to the hosts.
ip nat inside

!*** Place on the WAN interface.
ip nat outside

!*** Setup Static NAT / One to one mapping
ip nat inside source static 10.1.1.2 200.1.1.1


!*** Show translations
show ip nat translations

!*** Show NAT statistics
show ip nat statistics

!*** clear ip nat table to reset the NAT mappings
clear ip nat translations *
```

Dynamic NAT

Allow the NAT of a pool of internal address to a pool of outside addresses.

```
!*** Create IP NAT Pool
ip nat pool CCNA 200.1.1.1 200.1.1.5 prefix-length 24

!*** Create the access-list of internal host that will be NAT.
access-list 2 permit host 10.1.1.2
access-list 2 permit host 10.1.1.22

!*** Create the NAT function for the access-list 2 and the pool CCNA
ip nat inside source list 2 pool CCNA
```

Port address translation - NAT Overload

Allows the mapping of multiple inside addresses to a single outside address using a combination of the IP address / Port Number in ordre to uniquely identify each flow of data.

```
!*** Overload of the inside addresses to the outside address
ip nat inside source list 2 interface serial0/1/0 overload
```

IPv6

- Solution to the IPv4 exhaustion.

- 128 bit addresses
- 8 blocks of 4 HEX characters.
- No more broadcast - only multicasts.
- Easier summarization.
- Can be run without a DHCP server.
- IANA (Internet Assigned Numbers Authority) - Assigns IP blocks to RIR (Regional Internet Registry - ARIN, RIPE, AFRINIC, APNIC, LACNIC.

Compressing IPv6 addresses

- Compress consecutive blocks of 0000 with ::
    - Can only do once per IPv6 addresses
- Remove leading 0 in blocks.

Assigning IPv6 addresses to interfaces

```
!### Enable IPv6 Routing for the router.
ipv6 unicast-routing

!### Assign an IPv6 address to an interface
interface fastethernet0/1
ipv6 address 2001:1111:2222:1::1/64
```

Types of IPv6 addresses.

- There is no broadcast - only Unicast and Multicast.
- Global Unicast addresses
    - Routable public addresses
- Link-local addresses : Addresses used in links directly.
    - Routers will not route those packets.
    - Addresses will always start FE80:0000:0000:0000 (FE80:/10)
    - 64-bit interface identifier - EUI-64 process

EUI-64 Process

1. Take MAC address of the interface
2. 11-22-33-aa-bb-cc
3. Divide in half and insert FFFE.

- 11-22-33-FF-FE-AA-BB-CC
- 1122:33FF:FEAA:BBCC

4. Do the bit inversion (invert the 7th bit of the address)
5. 1122:33FF:FEAA:BBCC --> 1322:33FF:FEAA:BBCC

Use EUI-64 process for global unicast address.

```
ipv6 address 2001:1111:2222:1::/64 eui-64
```

IPv6 NDP - Neighbor Discovery Process

- Allows IPv6 enabled device to discover hosts and routers on an IPv6 enabled network. The discovery process is different for routers and hosts.

NDP - Router Discovery

1. Hosts multicast packet - Router Solicitation (RS) message - Destination address FF02::2 - All-IPv6-Routers address
2. Routers receives RS on FF02::2 and sends RA (Router Advertisement).

- If the soliciting node **HAS** an IPv6 address --> RA is unicast to the host.
- If the soliciting node **DOES NOT** have an IPv6 address --> RA is sent to FF02::1 - "All-IPV6-Nodes"
- RA are also sent to FF02::1 every 200 seconds.
    - FF02::1 --> All IPv6 hosts.

NDP - Host Discovery

- NS --> Neighbor Solicitation.
- NA --> Neighbor Advertisement.
    - NA is sent to SNMA - Solicited-node multicast address.
        - Always begin with FF02::1:FF
        - Contains the last 6 HEX characters of the interface mac address. That way only the relevant hosts will receive the requested NA.
- Host that receives the NA, add the entry to the NDP table - same purpose as the ARP table.

DHCP and IPv6

- Same basic functionality as IPv4 but two different types of DHCPv6 servers : Stateful and Stateless.

Stateful DHCP

- SARR (instead of DORA)

1. Solicit - Client
2. Advertise - Server offers the address to the Client
3. Request - Client request the previously offered lease to the server
4. Reply - The Server confirms the lease to the client

Stateful DHCP does not send "Default Gateway" in the DHCP lease. That part is discovered during the NDP process with NA and NS messages.

Stateless DHCP

- Stateless autoconfiguration - SLAAC.
- Hosts will generate their own ip addresses from information received during the RA - RS process. RA messages will contain the subnet prefix and the prefix length. The host will

then create it's own IP address adding it's own interface identifier at the end.

IPv6 - Duplicate Address Detection - DAD

Prevents duplicate addresses from being used on the network.

1. The host will send an NS (with the source address all :: - 128 zeros - unspecified ipv6 address) to the address it wants to use to FF02::1 (All IPV6 nodes)
2. If it gets a response, it means that a host is already using that address.

IPv6 Packet Header

- Version : Set to 6
- Traffic class : Replaces "Type of Service". Allow level of importance with QOS.
- Flow Label: NEW FIELD - Allow traffic priorities and categorization. Works with QOS and Traffic Class.
- Payload Length: Total length of packet
- Hop Limit : Like the TTL field of IPv4. Each hope decreases the counter by 1.
- Next Header : Equivalent to the Protocol field.
- Source Address : Source Address of the packet
- Destination Address : Destination Address of the packet

Logging and Timestamps

Change the aspect and format of timestamps for SYSLOG and DEBUG message.

```
service timestamps log datetime

!### Add year to log timestamps.
service timestamps log datetime year

!### Add millisecond to log timestamps.
service timestamps log datetime msec

service timestamps log datetime year msec show-timezone
```

Logging to remote server

Enable logging to the console.

```
logging console
```

Enable buffered logging. Local buffer on the server.

```
logging buffer
```

Enable logging to a remote server.

```
logging host $SYSLOG_SERVER_IPADDRESS
```

Enable console logging on SSH/Telnet session

```
conf t
logging monitor
exit
terminal monitor
```

Banner configuration

Three types of banners.

- Login : Shown during the login prompt. Telnet and SSH.
- Exec : Shown after the user logs in. Telnet and SSH.
- MOTD : Shown along the login prompt. SSHv2 --> SHOWN AFTER LOGIN INTO THE DEVICE WITH EXEC BANNER.

CDP - Cisco Discovery Protocol

- Default timers
- Hold Timer - 180 seconds - After 180 seconds, the entry is removed.
- Advertisement timer - 60 seconds.

```
show cdp neighbors
show cdp neighbors details
show cdp entry $REMOTE_DEVICE_HOSTNAME

!*** Enable CDP globally.
cdp run
no cdp run

!*** Enable CDP on an interface
interface fastethernet0/0
cdp enable
no cdp enable

!*** Show CDP information
show cdp information
show cdp interface fastethernet 0/0
```

LLDP - Link Layer Discovery Protocols

You can disable the received and transmit of LLDP packets per interface. That is not possible for CDP.

```
show lldp

conf t
lldp run

show lldp neighbor detail
```