



Device Security

AAA



In This Section

- + Authentication, Authorization, and Accounting
- + Role Based CLI Access
- + Configuration Change Notification & Logging
- + Cisco IOS Login Enhancements

IOS AAA

- + Authentication, Authorization, & Accounting
- + Old-Model
 - + Local Authentication
 - + Local Authorization based on line/username settings
- + New-Model
 - + Supports AAA lists that define sequence of methods
 - + List can be bound to access technologies
 - + E.g. login or PPP
- + Default lists vs. explicitly assigned lists

TACACS+ and RADIUS

- + Terminal Access Controller Access-Control System (TACACS)
 - + Primarily for device authentication management
 - + E.g. IOS admins
 - + Supports per-command authorization & accounting
- + Remote Authentication Dial In User Service (RADIUS)
 - + Primarily for end user authentication management
 - + E.g. remote access VPN users
 - + Does not support per-command authorization & accounting
- + Regardless which method used, local fallback should be configured

Local Authentication

- + Default authentication method
- + Passwords are in clear-text by default
 - + service password-encryption
 - + username secret

Local Command Authorization

- + Privilege levels used to control access to exec commands
- + Default privilege levels
 - + 0 – no access
 - + 1 – user mode access
 - + 15 – privilege (enable) mode access
- + User defined privilege levels
 - + Levels 2 – 14 available for assignment

Local Command Authorization (cont.)

- + Moving command privilege down
 - + Allow privilege 1 to...
 - + run extended ping
 - + show running config
 - + Only see what you can configure
- + Moving command privilege up
 - + Revoke privilege 1 from
 - + Running show commands
 - + Using the enable command

Local Authorization (cont.)

- + Modified with privilege command
 - + exec | configure | interface | router | etc.
- + Configuration mode determines what option of privilege command to do
 - + Example:
 - + Exec command
 - + router#
 - + Configure command
 - + router(config)#
 - + Interface command
 - + router(config-if)#

Role-Based Access Control (RBAC)

- + Replacement for privilege-levels
 - + More flexible in terms of command allocation
- + Role is a group of commands
 - + Known as “parser view” in IOS
- + Roles could be
 - + Manually switched to (enable view)
 - + Assigned to users
- + Roles should be configured from root view (enable view)
- + RBAC requires AAA enabled in the router

Configuration Change Notification & Logging

- + Local command accounting
 - + Tracks users and commands issued through CLI and HTTP
- + Configured as “archive” and “log config”

Cisco IOS Login Enhancements

- + Used to protect against brute force login attacks
 - + After x number of failed attacks, delay login box
- + Configured as **login block-for**





Device Security

Control Plane Policing and Protection



Control Plane Policing (CoPP)

- + Used to protect CPU from a DoS attack
 - + E.g. flood router's CPU with routing protocol hellos
- + Configured as a QoS policing policy
 - + Not all matches supported in class-map
- + Applied under control-plane
 - + **control-plane**
 - + **service-policy** input





Switch Security

Switch Access Lists



In This Section

- + Port Based Access Lists (PACL)
- + VLAN Based Access Lists (VACL)

Catalyst PACL

- + Port ACLs
 - + Applies to layer 2 switchports
 - + Apply ingress only
 - + Filter transit traffic
 - + Traffic ingress on the VLAN/port
 - + Could be IP or MAC based
 - + MAC ACLs only affect non-IP traffic

Catalyst RACL

- + Routed ACL
 - + Same as PACL but only apply to L3 traffic
 - + Apply to L3 ports or SVIs
 - + Ingress or Egress unlike PACL
 - + Can only filter using IPv4 standard/extended ACLs

Catalyst VACL

- + VLAN ACL or VLAN map
- + Apply to an VLAN/SVI
 - + Effective for all ports in this VLAN
 - + Access and Trunk ports
 - + May inspect both IP and non IP traffic
 - + Matching based on IP or MAC ACL
 - + Configuring an IP/MAC entry activates implicit deny

VACL Considerations

- + Good to affect all future ports in VLAN
- + Don't use implicit deny
 - + You may block STP or ARP
- + Be careful when filtering L2 traffic
 - + STP & ARP could be easily blocked
- + Account for the fact that ALL transit traffic is affected
 - + Be careful when filtering transit VLANs





Switch Security

Port Based Traffic Control



In This Section

- + Port Security
- + Port Protection
- + Static CAM entries
- + Storm Control

Port-Security

- + Used to limit access to a port based on MAC address
- + Violation modes
 - + Shutdown (default)
 - + Send port to err-disable
 - + Protect
 - + Violators cannot send traffic in
 - + Restrict
 - + Violators cannot send traffic in
 - + Switch generates SNMP / Syslog message

Port-Security (cont.)

- + Applies to access and trunk ports, but not dynamic
 - + Ensure port mode is statically defined
- + Secure MAC addresses
 - + Can only belong to one port
 - + Static
 - + Learned (dynamic)
 - + Sticky
- + Trunk ports
 - + Support per-VLAN limits (default unlimited)
 - + Port limit is aggregate across all VLANs

Port-Security (cont.)

- + Remember that you can change device MACs
- + Keep in mind port-security and HSRP interaction
 - + HSRP/VRRP/GLBP add virtual MACs
 - + Two solutions
 - + Standby use-bia
 - + Allowing the virtual MAC
- + Avoid using “protected” mode on trunks
 - + Disables MAC learning once limit is reached for any VLAN
- + Consider additional MACs with IP Phones

Protected Ports

- + Protected ports cannot exchange L2 frames
 - + Used to prevent devices on the same VLAN from communicating at layer 3
 - + switchport protected
 - + Limited to one switch
 - + Example: Prevent compromised WWW server from launching DoS at servers on the same VLAN
 - + Unknown unicast and multicast packets are allowed
 - + Could be disabled explicitly

Static CAM Entries

- + Switch learns MAC addresses dynamically
 - + Learning can be disabled, e.g. on P2P VLANs
- + Static MAC entry can be configured
 - + Points to a fixed port
- + Static CAM entries can be used for “null-routing”

Storm-Control

- + Limit the amount of unicast / broadcast / multicast accepted in a port
 - + Ingress rate-limiting only
- + **storm-control {broadcast | multicast | unicast} level {level [level-low] | pps pps [pps-low]}**
 - + Level is a % of interface speed, not bandwidth
 - + 10/100/1000 issue





Switch Security

First Hop Security



In This Section

- + DHCP Snooping
- + Dynamic ARP Inspection
- + IP Source Guard

DHCP Snooping

- + Prevents DHCP server spoofing and exhaustion attack
- + Enforces DHCP server role on ports
 - + Only trusted ports may respond to DHCP DISCOVERs
- + Maintains IP, MAC, and port binding
 - + Could be used for security enforcement
- + Three main commands
 - + **ip dhcp snooping**
 - + **ip dhcp snooping VLAN x**
 - + **ip dhcp snooping trust** (interface)

DHCP Snooping Caveats

- + Don't forget to trust port to the DHCP server
 - + In multi-switch scenarios trust trunks as well
- + Keep in mind that DHCP snooping inserts information option
 - + Adds empty "giaddr" field, IOS rejects such packets
- + Information Option insertion could be disabled
 - + **no ip dhcp snooping information-option**
 - + Alternative is configure server to trust empty giaddr

Dynamic ARP Inspection (DAI)

- + Prevents ARP poisoning attack
- + Inspects ARP requests/Responses
 - + **ip arp inspection VLAN X**
 - + **ip arp inspection trust** (port command)
- + Enforces IP to MAC bindings based on DHCP snooping database

Dynamic ARP Inspection

- + If DHCP is not used static ARP mappings could be configured
 - + Takes precedence over dynamic entries
 - + Configured using ARP inspection ACL
 - + **arp access-list X**
 - + **permit ip host <IP> mac host <MAC>**
- + Applied to a VLAN
 - + **ip arp inspection filter <NAME> VLAN y**

IP Source Guard

- + Prevents IP address spoofing
- + Uses DHCP Snooping database to filter IP's on the port dynamically
 - + **ip verify source** (interface command)
- + MAC address filtering could be enforced as well
 - + Requires port-security enabled on interface
 - + Additional parameter ip verify source port-security
- + Static IP to MAC mapping on a VLAN
 - + **ip source binding** (global command)





Switch Security

Private VLANs



In This Section

- + Private VLANs
- + Private VLANs & VTPv3

Private VLANs

- + Allows for layer 2 isolation between ports within the same VLAN
 - + Expansion of protected port feature
 - + Allows isolation across multiple switches
- + Allows for additional granular control within the same VLAN
 - + Requires “sub-VLAN” within the “main” VLAN

Private VLANs (cont.)

- + Private VLANs use “sub-VLANs” within the primary VLAN for the layer 2 isolation
 - + Main VLAN is known as “Primary” VLAN
 - + Sub-VLAN is known as “Secondary” VLAN
- + There are two types of Secondary VLANs
 - + Community
 - + Isolated

Private VLANs Port Types

- + Two type of ports
- + Promiscuous ports
 - + Connects to router
- + Host ports
 - + Connects to end hosts
 - + Either isolated or community ports

Private VLANs VLAN Types

- + Primary VLAN
 - + Carries traffic from Promiscuous to Host ports
- + Isolated VLAN
 - + Carries traffic from Host ports to Promiscuous port
- + Community VLAN
 - + Carries traffic between Community host ports and to the Promiscuous port

Private VLANs & VTPv3

- + VTPv1 & v2 cannot advertise extended VLANs
 - + Private VLANs are Extended VLANs
 - + Implies that Private VLAN config must be manually synced
- + VTPv3 fixes this
 - + Private & Extended VLANs can be advertised





Device Security

Router Security Features



In This Section

- + Standard ACLs
- + Extended ACLs
- + IPv6 ACLs
- + Time Based ACLs
- + Unicast Reverse Path Forwarding (URPF)

Access-Lists

- + Standard Access-Lists match on...
 - + Source IP address
- + Extended Access-Lists match on...
 - + IP protocol number
 - + Source address/Destination address
 - + Protocol options
 - + TCP / UDP ports (eq, neq, lt, gt, range)
 - + ICMP Type Code
 - + TCP state (established keyword)
 - + Packet markings (DSCP/IPP)
 - + Non-initial fragments (fragments keyword)

Access List Logging

- + Log message can be generated on ACL match
 - + log vs. log-input
 - + Generated as syslog level “informational”
 - + Causes packets to be process switched
- + ACL Logging rate-limiting
 - + **ip access-list logging interval**
 - + **ip access-list log-update threshold**
 - + **logging rate-limit**
- + ACL Syslog Correlation Tags
 - + **log [cookie]**
 - + **ip access-list logging hash-generation**

IPv4 ACL Applications

- + Traffic Filtering
 - + ip access-group
- + Traffic Classification
 - + match access-group
- + Route Filtering
 - + distribute-list or route-map
- + VTY line/username access-control
 - + access-class in/out

IPv6 ACL Applications

- + Traffic Filtering
 - + `ipv6 traffic-filter`
- + VTY line/username access-control
 - + `ipv6 access-class`

Time Based ACLs

- + Used to activate ACL entry based on clock
- + Defined as time-range [name]
 - + Absolute
 - + At one specific time period
 - + Periodic
 - + At one or more recurring time periods
- + Potential Applications
 - + Time based traffic filter
 - + Time based QoS

URPF

- + Unicast Reverse Path Forwarding (URPF)
 - + Used to simplify bogon/martian filters
 - + Ingress traffic has source checked against CEF table
 - + Packets without a correct reverse route are dropped
- + Can be both strict and loose
 - + Strict means reverse route must be via ingress interface
 - + Loose means reverse route can be via any interface





Device Security

IPv6 First Hop Security



What is First Hop Security (FHS)?

- + First Hop
 - + Network segment between end hosts and their default gateway
 - + i.e. the Access Layer
- + Security
 - + Prevent against internal threats at the access layer
 - + E.g. a Man-in-the-Middle (MiM) attack

Why is IPv6 FHS Needed?

- + Both IPv4 and IPv6 suffer from insecure control plane protocols in the access layer
- + For IPv4...
 - + ARP
 - + DHCP
- + For IPv6...
 - + ICMPv6 Neighbor Discovery (ND)
 - + Duplicate Address Detection (DAD)
 - + Stateless Address AutoConfiguration (SLAAC)
 - + DHCPv6

How ICMPv6 ND Works

- + ICMPv6 ND/NDP replaces IPv4 ARP
- + IPv4 ARP uses 2 messages: Request & Reply
- + ICMPv6 ND uses 4 messages:
 - + NS – Neighbor Solicitation
 - + Ask for information about neighbor
 - + NA – Neighbor Advertisement
 - + Advertise yourself to other neighbors
 - + RS – Router Solicitation
 - + Ask for information about local routers
 - + RA – Router Advertisement
 - + Advertise yourself as an active router

ICMPv6 ND Workflow for New Hosts

- + When an end host wants to join the IPv6 LAN...
- + Choose a link-local address
 - + FE80::/10 + EUI-64
- + Check if link-local address is unique
 - + Send NS for link-local solicited node multicast
 - + FF02:0:0:0:0:1:FF00::/104 + 24 low-order bits
 - + If no reply address is unique
- Announce yourself as a live host
 - Send NA to all hosts multicast FF02::1

ICMPv6 ND Workflow (cont.)

- + Discover the routers
 - + Send RS to all routers multicast FF02::2
- + Router replies with RA
 - + Contains the router's IPv6 address and MAC, along with prefix information for SLAAC
- + Host chooses a global prefix for SLAAC
 - + RA Prefix + EUI-64
 - + Perform DAD again for the global prefix
 - + If unique, send NA for global prefix

Potential Attacks in the First Hop Segment

- + Spoof the router
 - + Send gratuitous RA to announce yourself as the router
 - + Result is MiM or a basic DoS attack
- + Spoof the DHCPv6 server
 - + Respond with bogus offer
 - + Result is basic DoS attack or MiM if combined with RA spoofing
- + Poison the router's ND cache
 - + Send gratuitous NA messages with other people's addresses
 - + Result is MiM or a basic DoS attack
- + Overload the router's ND cache
 - + Send packets to entire /64 range
 - + Result is router's CPU is DoSed trying to send lots of NS messages

IPv6 RA Guard

- + Hosts dynamically discover the default gateway based on NDP RA messages (ICMPv6)
- + Prevents router spoofing on the segment
- + Prevents prefix spoofing on the segment
- + Policy can be applied at VLAN or port level

DHCPv6 Guard

- + DHCPv6 does not assign default-router as in IPv4
- + Default router is learned through SLAAC from RA messages
- + Similar in scope with IPv4 DHCP Snooping
- + Prevents DHCPv6 server spoofing
- + Policy can be applied at VLAN or port level

IPv6 Snooping

- + IPv6-to-MAC resolution achieved through NDP NS/NA messages (ICMPv6)
 - + Similar in scope with IPv4 DAI
- + Inspects DHCPv6 and NDP messages
 - + Performs neighbor binding table through IPv6 neighbor tracking
 - + Prevents host spoofing on the segment
 - + Optionally enables basic RA Guard and DHCPv6 Guard
 - + Optionally can inspect data packets to perform neighbor binding
- + Manual bindings are possible for strict control
- + Policy can be applied at the VLAN or port level

IPv6 Source-Guard

- + Similar in scope to IPv4 Source Guard
 - + Relies on IPv6 Snooping to create the IPv6 neighbor binding table
 - + Creates automatic IPv6 PACL to filter sources based on neighbor binding table

IPv6 Secure Neighbor Discovery (SeND)

- + An extension to NDP to secure and authenticate these messages
 - + Requires PKI infrastructure and routers enrolled (certificates issued)
 - + Hosts do not need to be enrolled but need to trust the PKI chain
- + RA and RS messages are authenticated between hosts and routers
 - + Routers are authorized to send RA messages for specific prefixes based on IPv6 Extension certificate field

