**Infrastructure Security**

Revision de Vlans, trunking, STP

**Best practices for securing your switches**

* avoid using VLAN 1 anywhere, because it is a default
* configure access ports as access ports so that users cannot negotiate a trunk and disable DTP (Do not allow negotiation)
* limit the number of MAC addresses learned on a given port with the port security feature
* select an unused vlans and use that for the native Vlan for all your trunk (do not use this native vlan for any of your enabled access port)
* control Spanning tree to stop users or unknown devices from manipulating spanning tree. you can do this by using the BPDU Guard and Root Guard features.
* Turn off CDP on port facing untrusted or unknown networks that do not require CDP for anything positive
* on a new switch, shut down all ports and assign them to a vlan that is not used for anything. Then bring up the ports and assign correct vlan as the ports are allocated and needed

**Layer 2 Security Toolkit:** BPDU Guard, Root guard, Port security, DHCP snooping, Dynamic ARP inspection, IP Source Guard, 802.1X, storm control, ACL

**Storm Control:** limits the amount of broadcast or multicast traffic flowing through the switch

**BPDU Guard:**

Applied to port that should only be access ports to end stations. It could prevent manipulation of your current STP topology. If a bpdu is seen inbound on port you enable BPDU guard, the port is disable

**Root Guard**

When your switch is connected to other switches that you do not manage you can configure root guard on the local port to prevent your local switch from learning about a new root switch. This help in preventing with your existing STP topology

**Port security:**

* limits the number of MAC addresses to be learned on an access switch ports.
* It protects against malicious applications that may be sending thousands of frames into the network with a different bogus (faux) MAC address for each frame. That attacker tries to exhaust the limits of the dynamic MAC address table on the switch, which cause the switch to forward all frames to all ports within a Vlans so that the attacker can begin to sniff all packets. This is referred to as a CAM table overflow attack
* Port security also prevent the client from depleting DHCP server resources, which could have been done by sending thousands of DHCP request, each using a different source MAC address

**Port Security violation modes** (refer to ccna, déjà vu et compris)

**CDP/LLDP** : déjà vu ccna

**DCHP Snooping**

Features :

* validates DHCP messages received from untrusted sources and filters out invalid messages
* rate-limits DHCP traffic from trusted and untrusted sources
* builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses

**Dynamic ARP Inspection (déjà vu)**

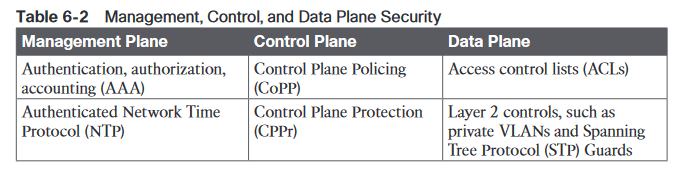
**S**ecurity feature that validates ARP packets in a network. DAI intercepts, logs and discard ARP packets with invalid IP-to-MAC address bindings. DAI determines the validity of an ARP packets based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database.

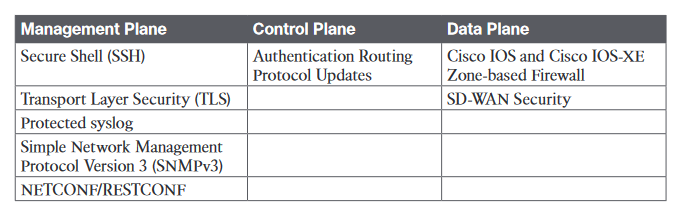
Use to avoids Arp cache poisoning (main in the middle attack)

**Network Foundation Protection**

* is design to assist you to **logically** group functions that occur on the network and then focus on specific security measures you can take with each of these functions
* **NFP framework** is broken down into three basic planes
* **Management plane**: include the protocols and traffic that an administrator uses between his workstation and the router or switch itself (like ssh)
* **Control plane**: includes protocols and traffic that the network devices use on their own without direct interaction from an administrator (like routing protocol)
* **Data plane**: include traffic is being forwarded through the network

**Security measures to protect each plane**





**Understanding and securing the management plane**

**Best practice**

* Enforce password policy (maximum number of logins attempts and minimum password length), strong password
* implement role-based access control (RBAC). By creating a group that has specific rights and then placing users in that group, you can more easily manage and allocate administrators
* Use AAA services (such as cisco ISE). With AAA a network router or switch can interact with a centralized server before allowing any access..., require administrators to authenticate using usernames and passwords.
* Login Password Retry Lockout feature allows system administrators to lock out a local AAA user account after a configured number of unsuccessful attempts by the user to log
* keep accurate time across all network devices using secure NTP
* use SNMPv3 (it is encrypted and authenticated version
* control which Ip address are allowed to initiate management sessions with network device
* secure syslog (encrypt syslog data)
* disabled any unnecessary services, especially those that use UDP to avoids Dos attacks
* use encrypted management protocols such as SSH, HTTPS,

**Securing control plane :**

* using COPP/CPPr you can specify which types of management traffic are acceptable at which level
* Routing protocol authentication is another best practice for securing the control plane

**Securing the data plane**

* implement ACL that deny traffic that is not allowed

**Password recommendations**

* minimum eight characters for password, mix of any alphanumeric character, uppercase and lowercase characters, and symbols, and spaces
* Multifactor authentication and Duo

**Role Based Access Control**

The concept of RBAC is to create a set of permissions or limited access and assign that set of permissions to users or groups. Those permissions are used by individuals for their given roles such as a role of administrator, a role of help desk person, and so on.

Ways to implement RBAC: **creating custom levels and creating parser views**

**Custom Privilege Levels**

User mode = privilege level 1

Privilege mode = privilege level 15 (user can issue all the commands that are attached to or associated with level 15 and below.

Nearly all the configuration commands and the commands that get us into configuration mode, are associated by default with privilege level 15

Creating custom privilege levels: (between levels 2 and 14) is to give subset of commands that are normally associated with privilege level 15 to the individual who either logs in as this custom level

**Limiting the administrator by assigning a View**

Custom privilege levels are tedious, we can use a parser view and associate it with a subset of commands

**Encrypted management Protocols**: SSH, HTTPS provides confidentiality for the packets and you should use them for security

**Logging files**

* Administrators should, on a regular basic, analyze logs, especially from network devices
* Logging information can provide insight into the nature of an attack, can be used for troubleshooting purposes, can provide event correlation information

Logging informations destinations :

* **Console**
* **vty lines**
* **Buffer**: in router memory for detailed analysis. But when the router is rebooted messages are lost
* **SNMP server**: A router or switch can generate log messages in the form of SNMP traps and them to an SNMP manager (server)
* **Syslog server** (it is a popular choice): we can store a large volume of logs, easily configuration

**Syslog level (voir ccna)**

**Understanding NTP (ccna)**

* NTP uses UDP port 123 and allows network devices to synchronize their time to a trusted time server.
* NTP version 3 supports cryptographic authentication between NTP devices

Protecting cisco IOS, Cisco IOS-XE, Cisco IOS-XR, and Cisco NX-OS Files

**Cisco Operating system**

* for enterprise routers is Cisco IOS-XE
* Service provider routers: Cisco IOS-XR
* Data center infrastructure devices : NX-OS
* To protect a router from accidental or malicious tampering of the IOS or startup configuration we can copy the router IOS image and startup conf files and maintains them at all times

Review IPv6 (voir resumé ccna) (addresses types, configuring routing)

**Best Practices common to both IPv4 and IPv6**

* Physical security:
* Device hardening: disable services that are not in use and features and interfaces that are not in use
* Routing protocol security: use authentication with routing protocols
* Use AAA
* Have and update a security policy

**Threats common to both ipv4 and ipv6**

* Application layer attacks, main-in-the-middle attacks, unauthorized access, DOS, sniffing or eavesdropping etc.

**Risks with IPv6**

* **Neighbor Discovery Protocol (NDP):** clients discover router using NDP. A rogue router can be pretend to be a legitimate router and send incorrect information to the clients about network (default gateway, others parameters). (man in the middle attack) The router now has opportunity to see all packets from the hosts that are being sent to remote networks
* **Neighbor cache resource starvation**
* **DHCPv6:** a rogue router could manipulate the client into using incorrect DHCP-learned information. This could cause a man in the middle attack
* **Autoconfiguration, dual stacks, bugs in code**

**IPv6 Best Practices**

* **Filter bogus addresses, nonlocal multicast addresses,**
* **drop routing header type 0 packets** (may contain many intermediate next hops and if followed an attacker could control the path of a packet through a network.
* **Use manual tunnels rather than automatic tunnels**
* **Protect against rogue IPv6 rogue devices:** 
  + **Ipv6 first hop security binding table**: this table is used to validate that the IPv6 neighbors are legitimate
  + **Ipv6 device tracking**: provides the ipv6 neighbor table with the ability to immediately reflect changes when an IPv6 host becomes inactive
  + **IPV6 port-based access-list support**: similar to ipv4 acl
  + **IPv6 RA Guard: provides** the capability to bock or reject rogue RA Guard messages that arrive at the network switch platform
  + **Ipv6 ND Inspection**: analyzes neighbor discovery messages to build a trusted binding table database, and IPv6 neighbor discovery that do not conform are dropped
  + **Secure Neighbor Discovery in IPv6 (SeND)**: this feature defines a set of new ND options, and two new ND messages, Certification Path Solicitation (CPS) and Certification Path Answer (CPA), to help mitigate the effects of the ND spoofing and redirection