Switching Security Features

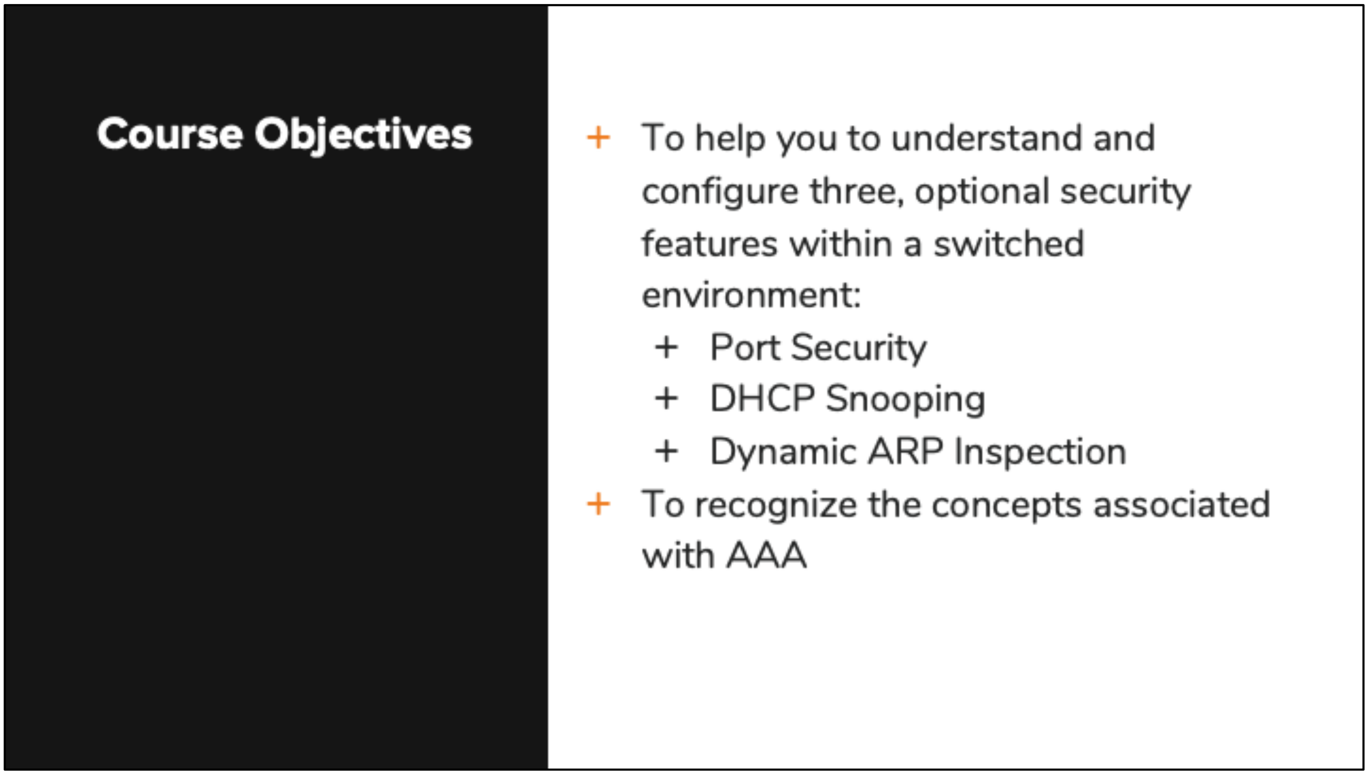
ine.com

Keith Bogart

CCIE #4923

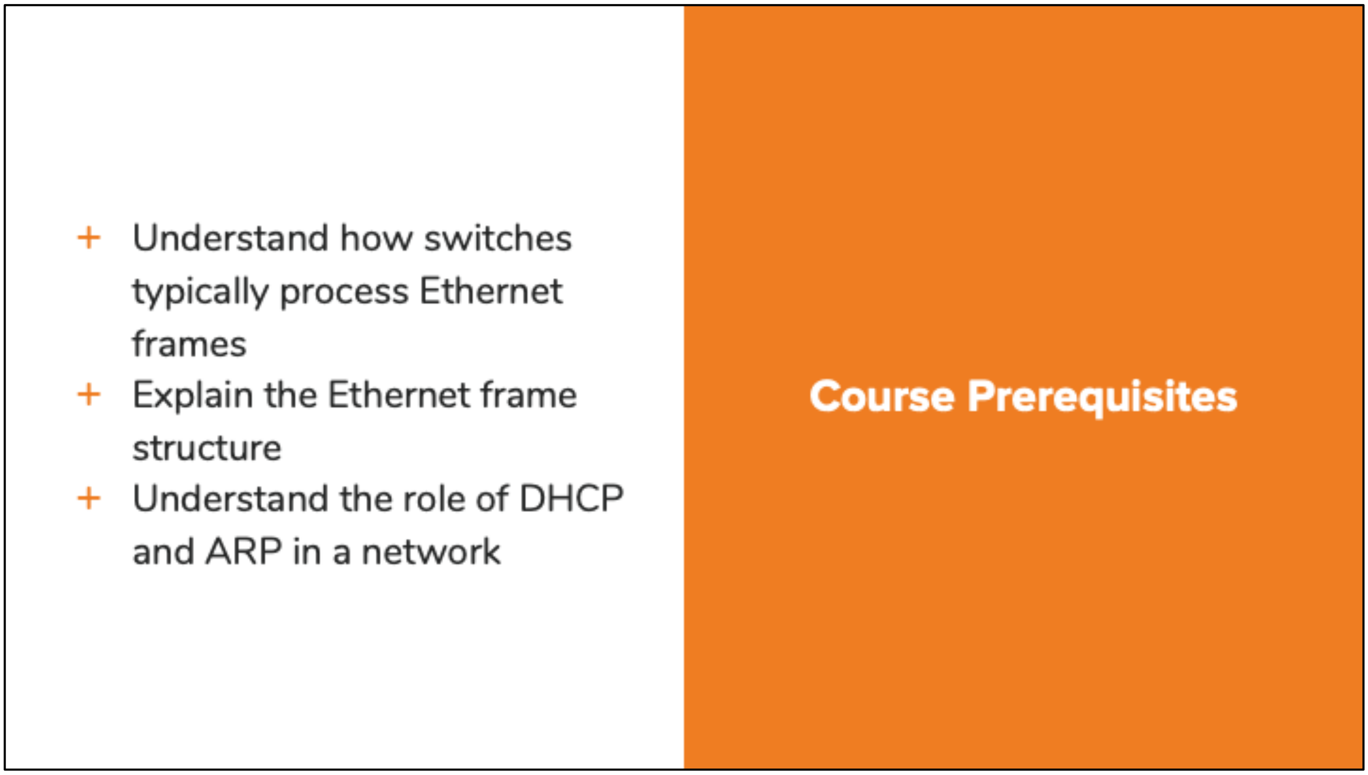
kbogart@ine.com
@keithbogart1
linkedin.com/in/keith-bogart-2a75042

CCIE Routing & Switching



Course Objectives

- To help you to understand and configure three, optional security features within a switched environment:
  - Port Security
  - DHCP Snooping
  - Dynamic ARP Inspection
- To recognize the concepts associated with AAA



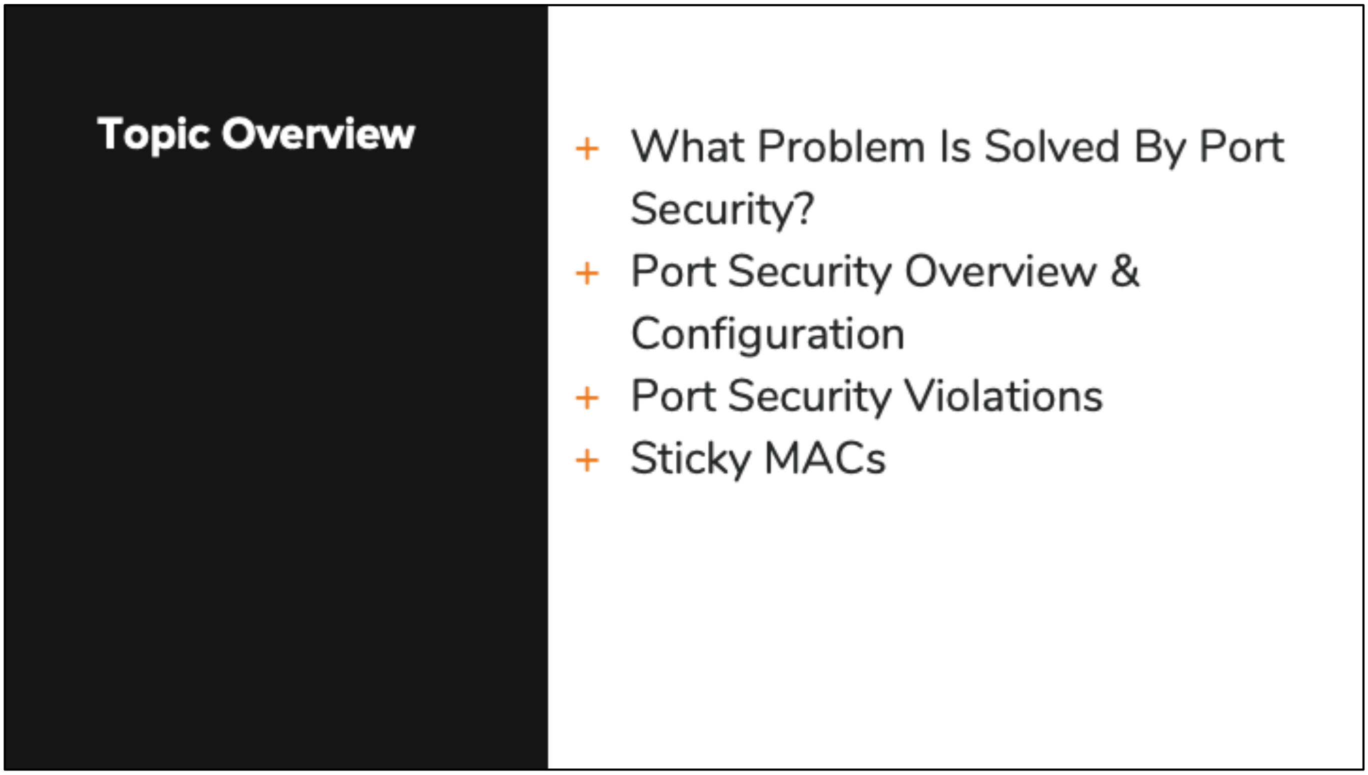
Course Prerequisites

- Understand how switches typically process Ethernet frames
- Explain the Ethernet frame structure
- Understand the role of DHCP and ARP in a network

INE

Port Security

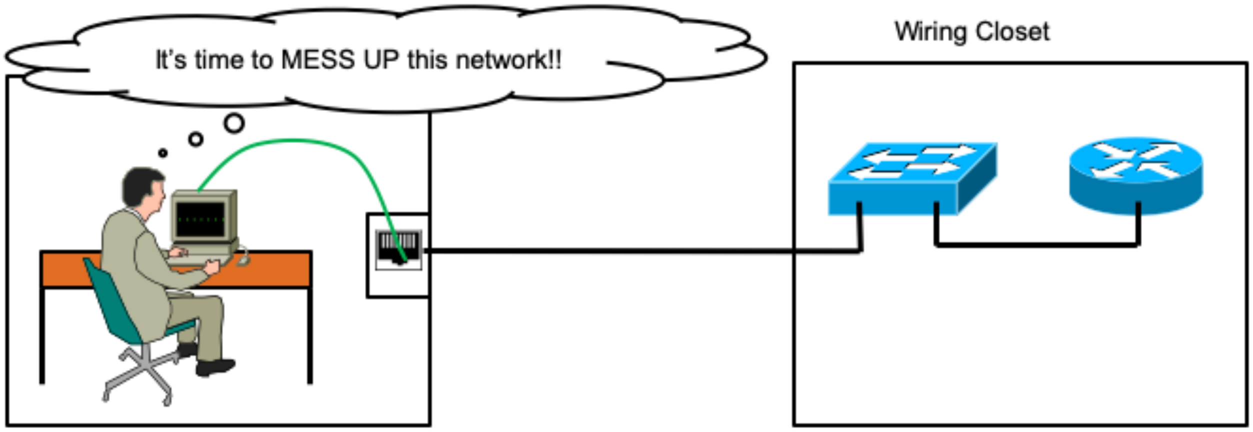
ine.com

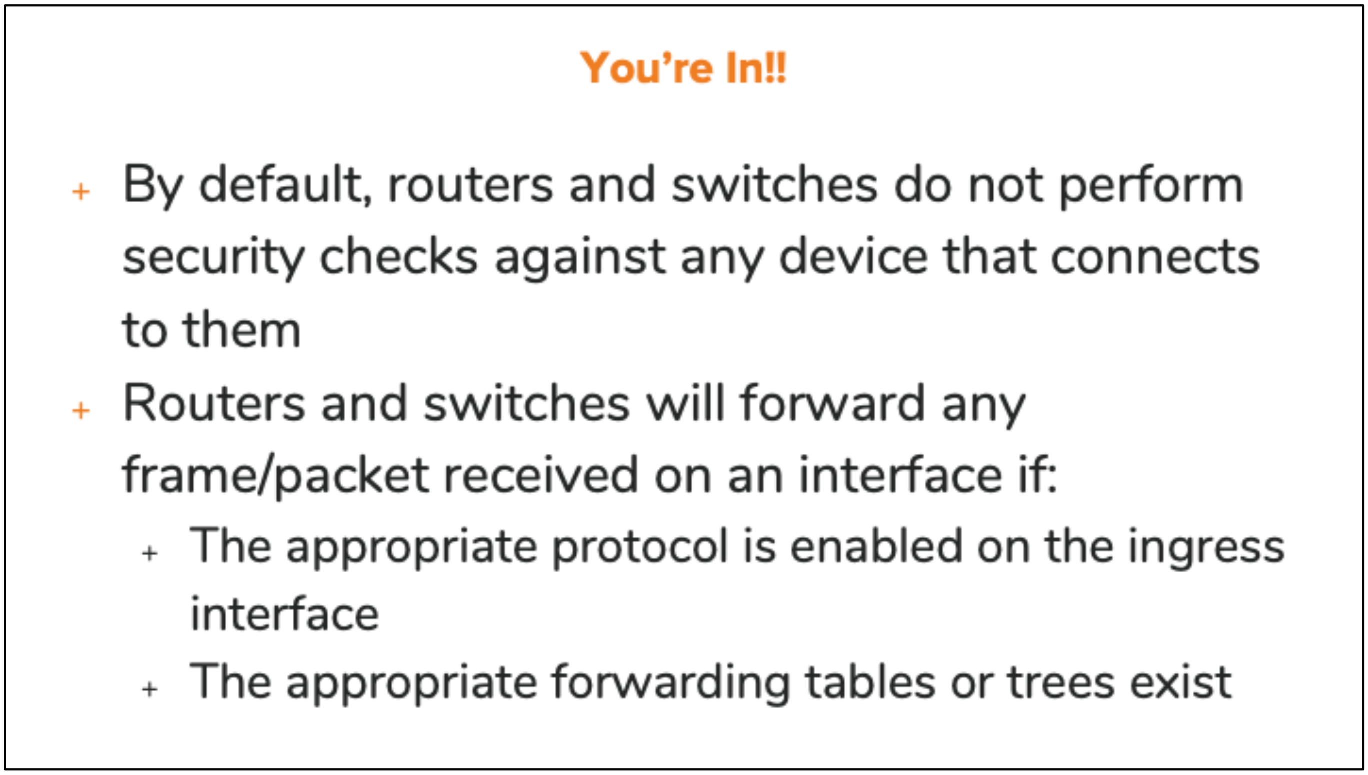


Topic Overview

- What Problem Is Solved By Port Security?
- Port Security Overview & Configuration
- Port Security Violations
- Sticky MACs

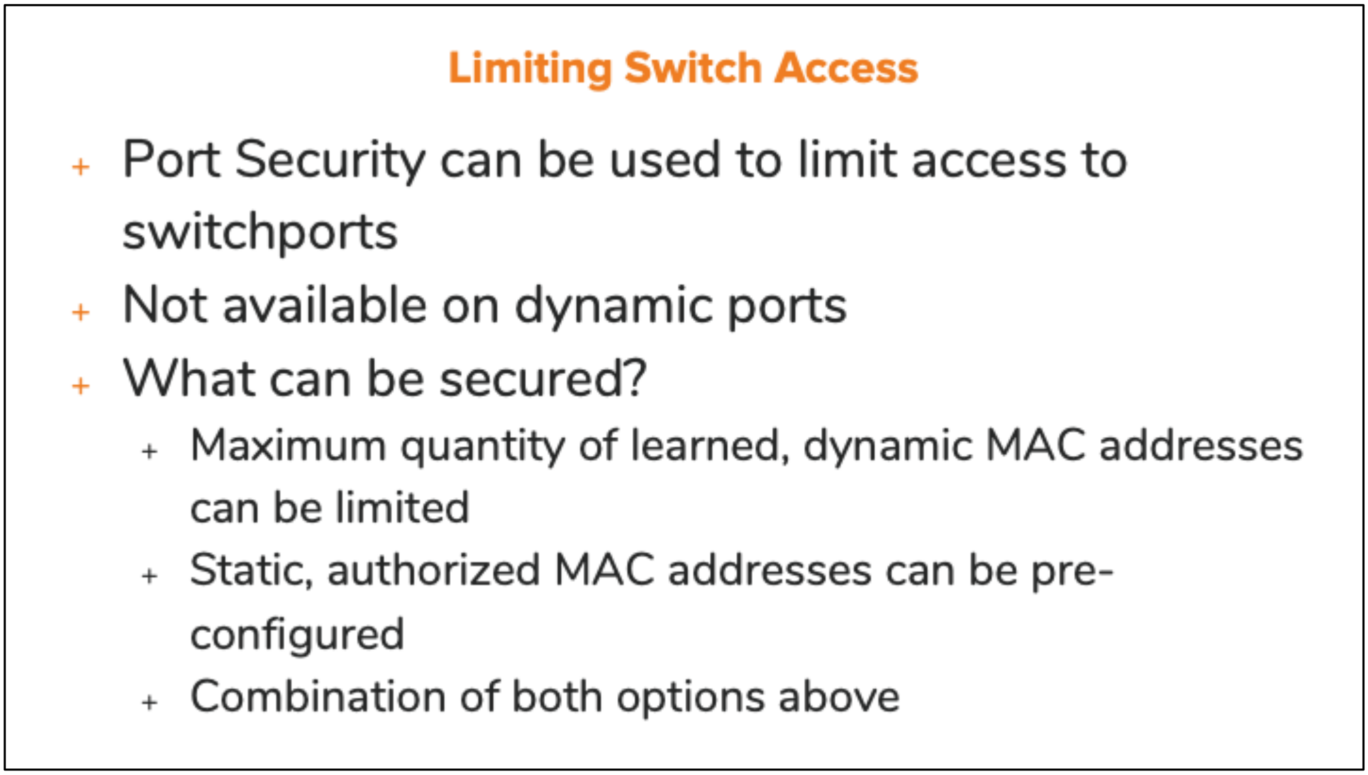
Anyone can connect to the network!





You’re In!!

- By default, routers and switches do not perform security checks against any device that connects to them
- Routers and switches will forward any frame/packet received on an interface if:
    - The appropriate protocol is enabled on the ingress interface
    - The appropriate forwarding tables or trees exist



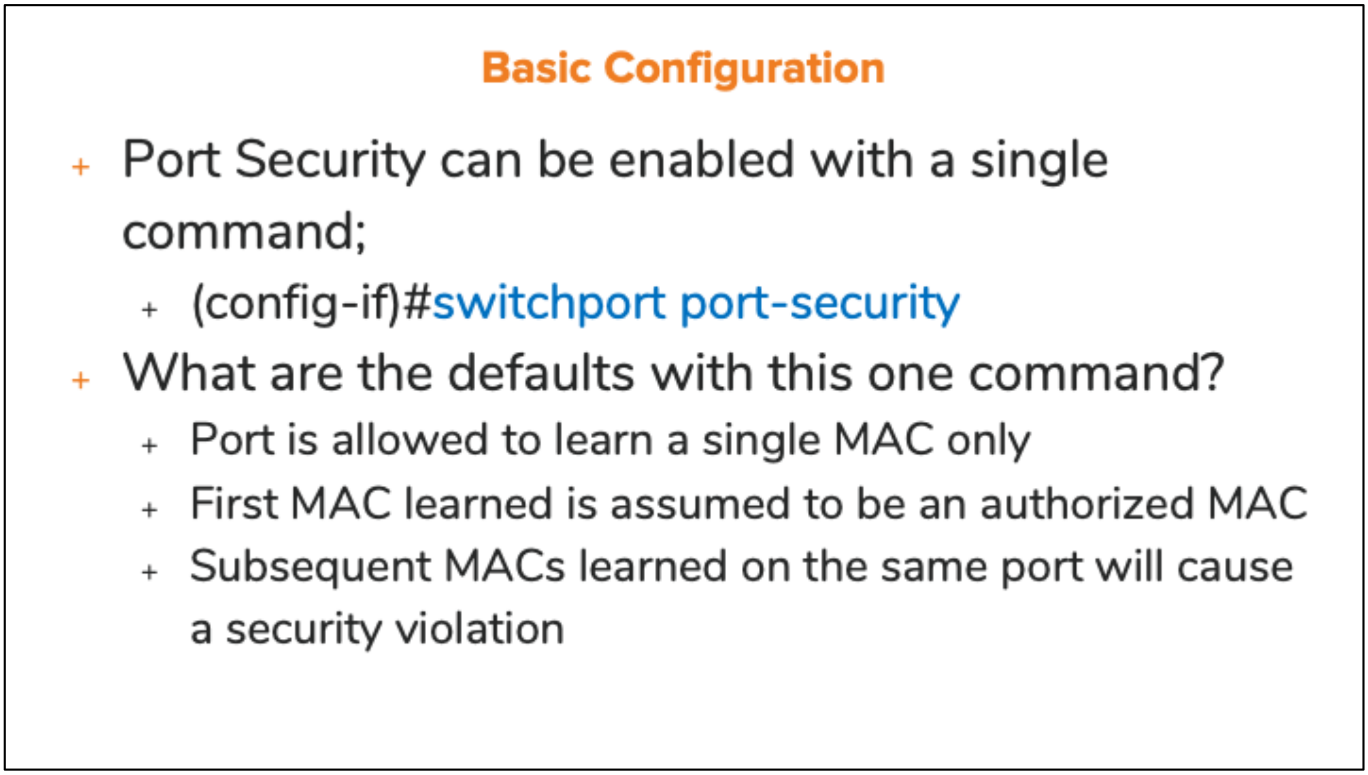
Limiting Switch Access

- Port Security can be used to limit access to switchports
- Not available on dynamic ports
- What can be secured?
  - Maximum quantity of learned, dynamic MAC addresses can be limited
  - Static, authorized MAC addresses can be pre-configured
  - Combination of both options above

Port Security will work on a trunk as long as DTP is not in-use.

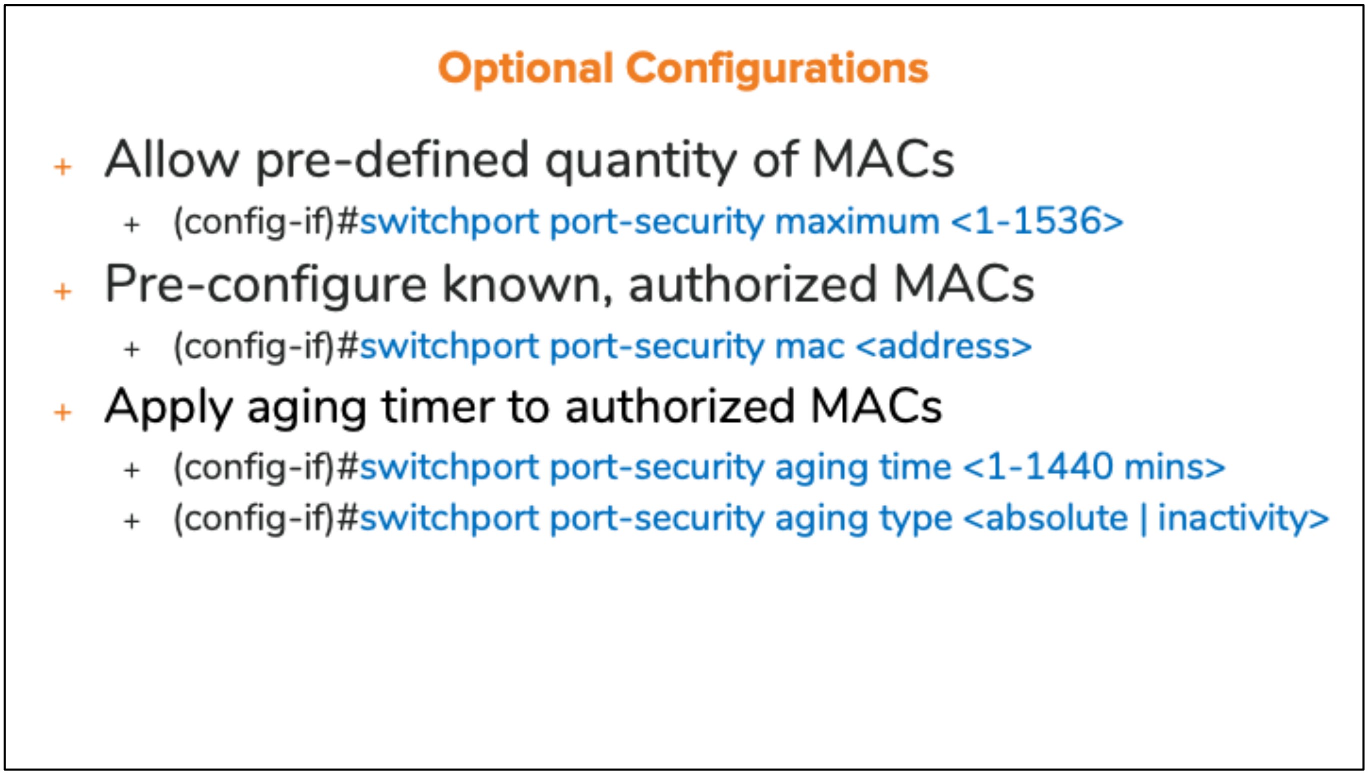
-

A secure port cannot be:
Destination port for SPAN
Port-channel
Private VLAN port



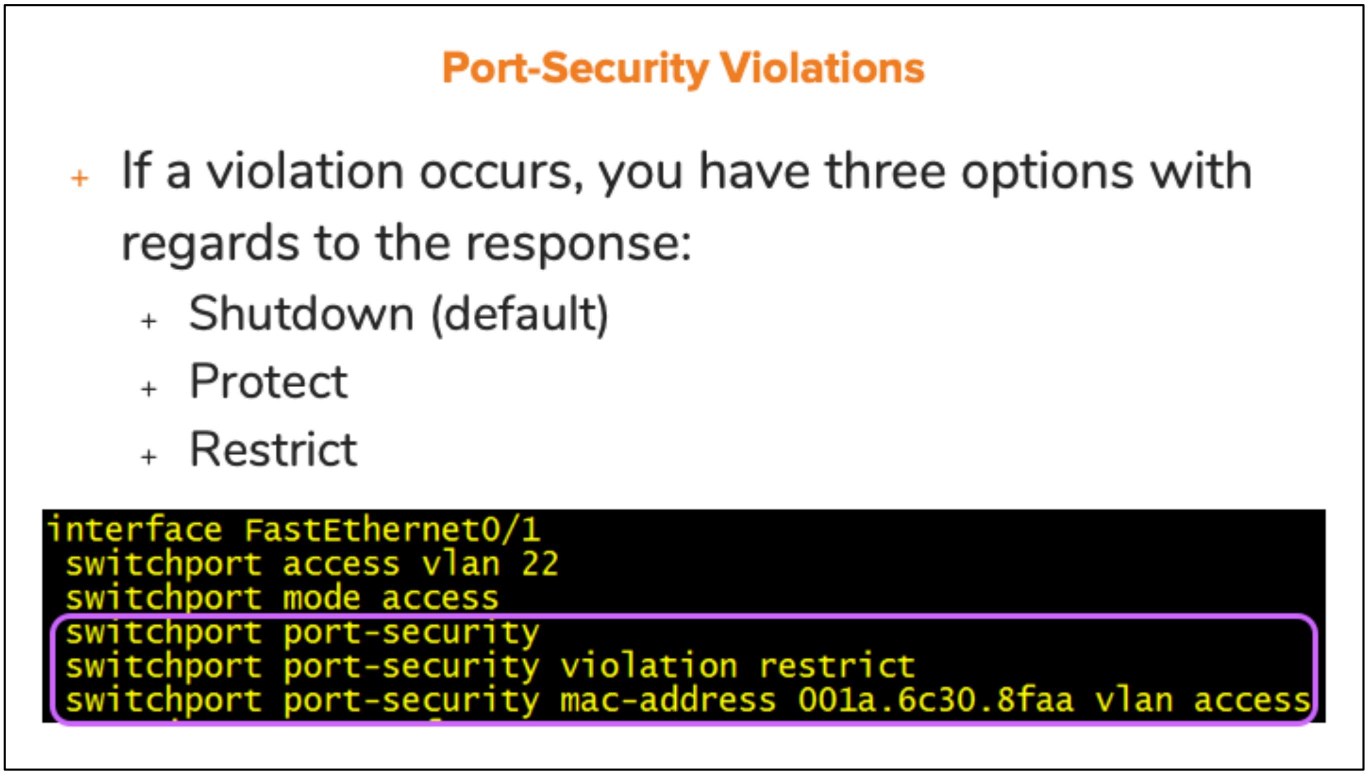
Basic Configuration

- Port Security can be enabled with a single command;
  - (config-if)#switchport port-security
- What are the defaults with this one command?
  - Port is allowed to learn a single MAC only
  - First MAC learned is assumed to be an authorized MAC
  - Subsequent MACs learned on the same port will cause a security violation



Optional Configurations

- Allow pre-defined quantity of MACs
  - (config-if)#switchport port-security maximum <1-1536>
- Pre-configure known, authorized MACs
  - (config-if)#switchport port-security mac <address>
- Apply aging timer to authorized MACs
  - (config-if)#switchport port-security aging time <1-1440 mins>
  - (config-if)#switchport port-security aging type <absolute | inactivity>



Port-Security Violations

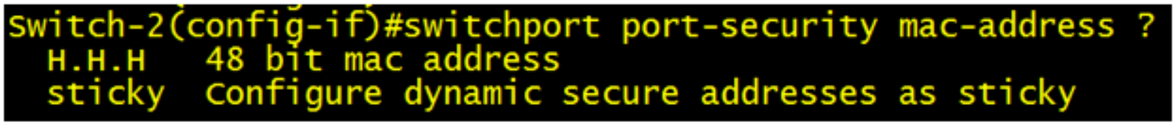
- If a violation occurs, you have three options with regards to the response:
  - Shutdown (default)
  - Protect
  - Restrict

```
interface FastEthernet0/1
 switchport access vlan 22
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 001a.6c30.8faa vlan access
```

Protect doesn’t give you syslogs or ANY indication that there has been a violation. ALL it does is silently discard the offending frames.

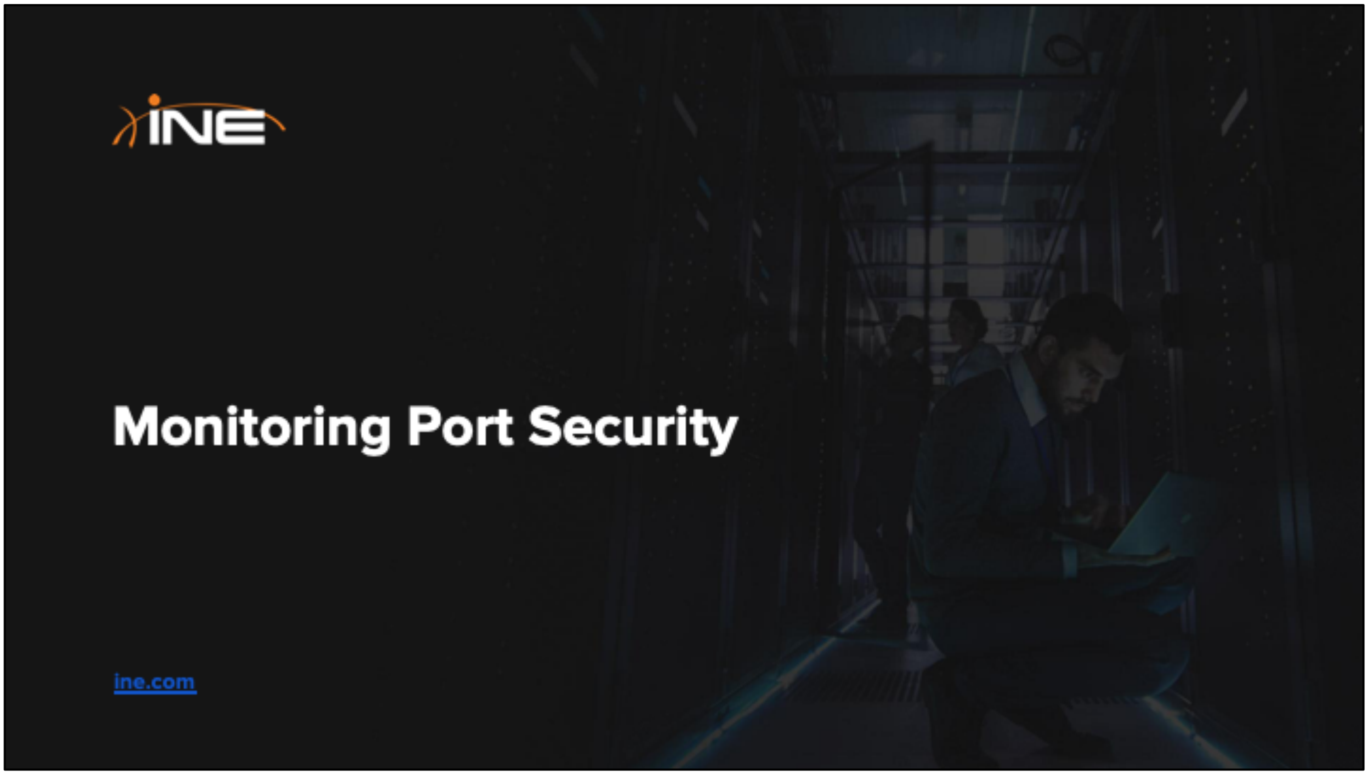
Sticky MACs

- Allows dynamic learning of allowed MAC addresses
- MACs learned become part of the Running-Config
- If saved (write memory) sticky MACs become static, authorized MACs upon a reload or powercycle



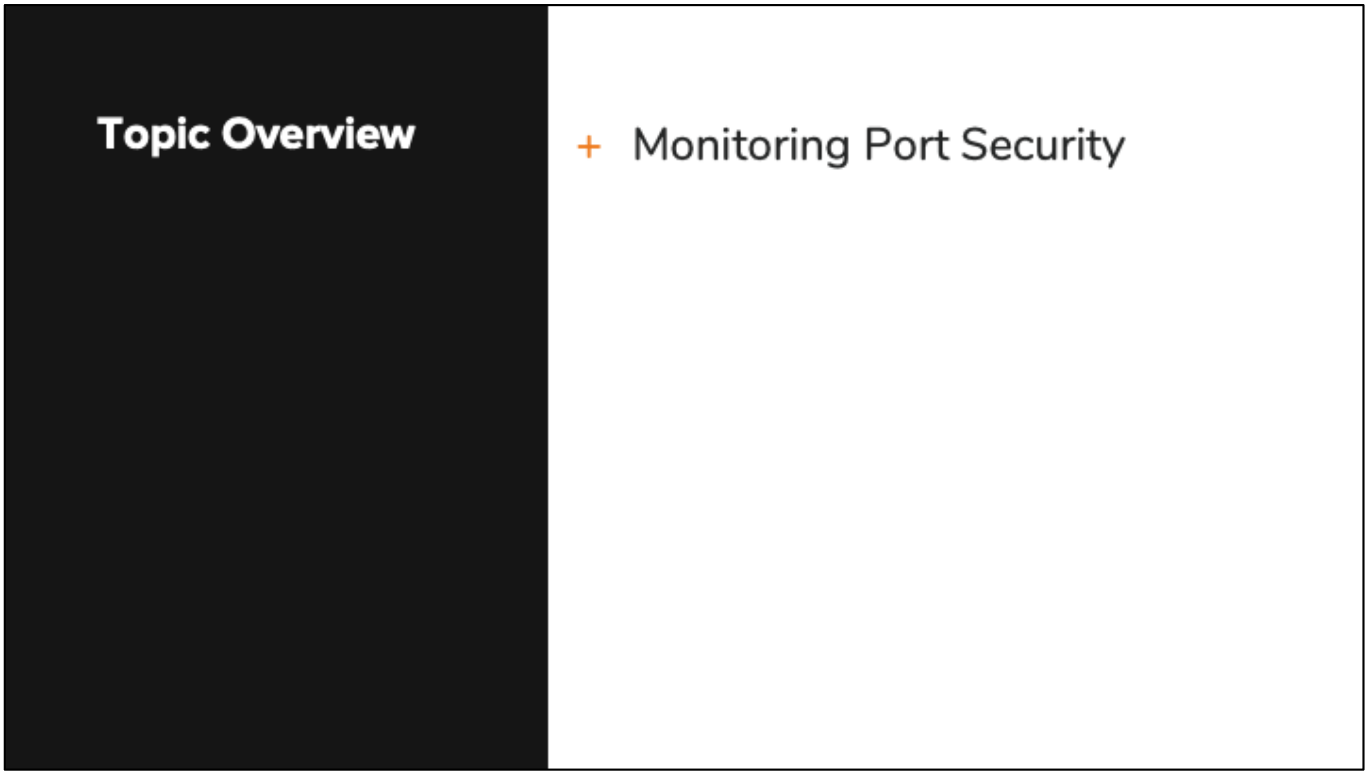
```
Switch-2(config-if)#switchport port-security mac-address ?
  H.H.H   48 bit mac address
  sticky  Configure dynamic secure addresses as sticky
```

Thanks for Watching!



Monitoring Port Security

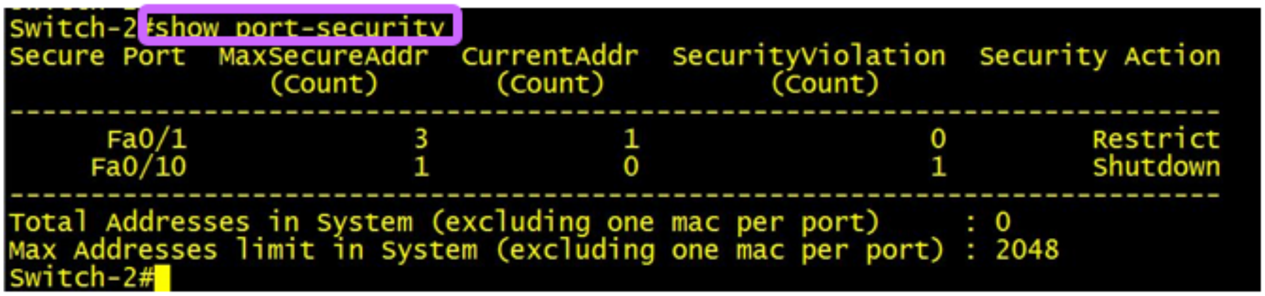
ine.com



Topic Overview

+ Monitoring Port Security

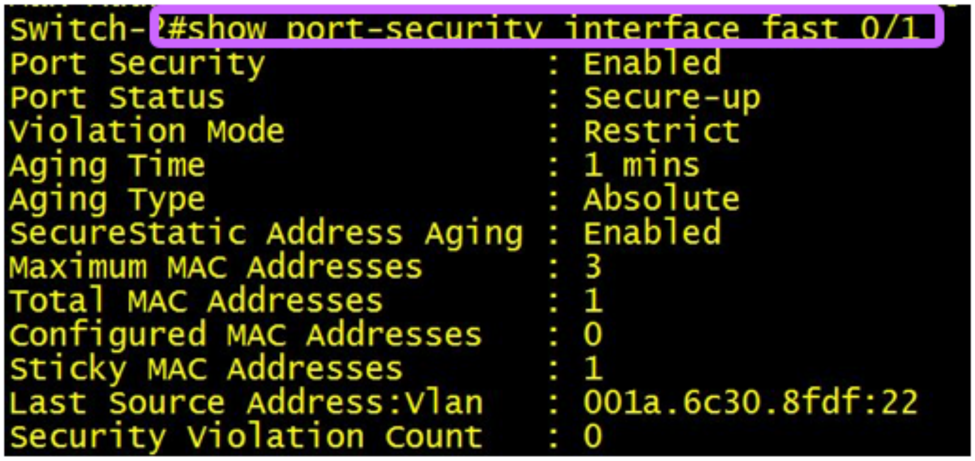
Monitoring Port Security



```
Switch-2#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)        (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/1              3            1                  0         Restrict
     Fa0/10              1            0                  1         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 2048
Switch-2#
```

The last line indicates that, of all the interfaces you have participating in this feature, you can have an aggregate total of 2048 secure (manually-configured) MAC addresses.

Monitoring Port Security



```
Switch-2#show port-security interface fast 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 1 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Enabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 001a.6c30.8fdf:22
Security Violation Count   : 0
```

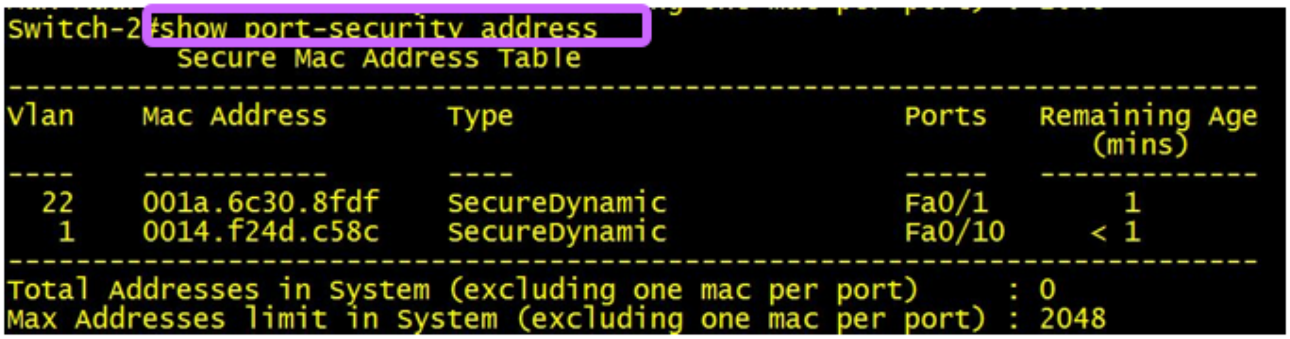
CCNA doesn’t expect you to know anything about Port-Security address aging.

-

When a MAC is “learned” and authorized via P-S it is entered as a “static” entry in CAM and so does NOT age.

P-S aging is a way of applying an aging timer to these types of MACs.

Monitoring Port Security

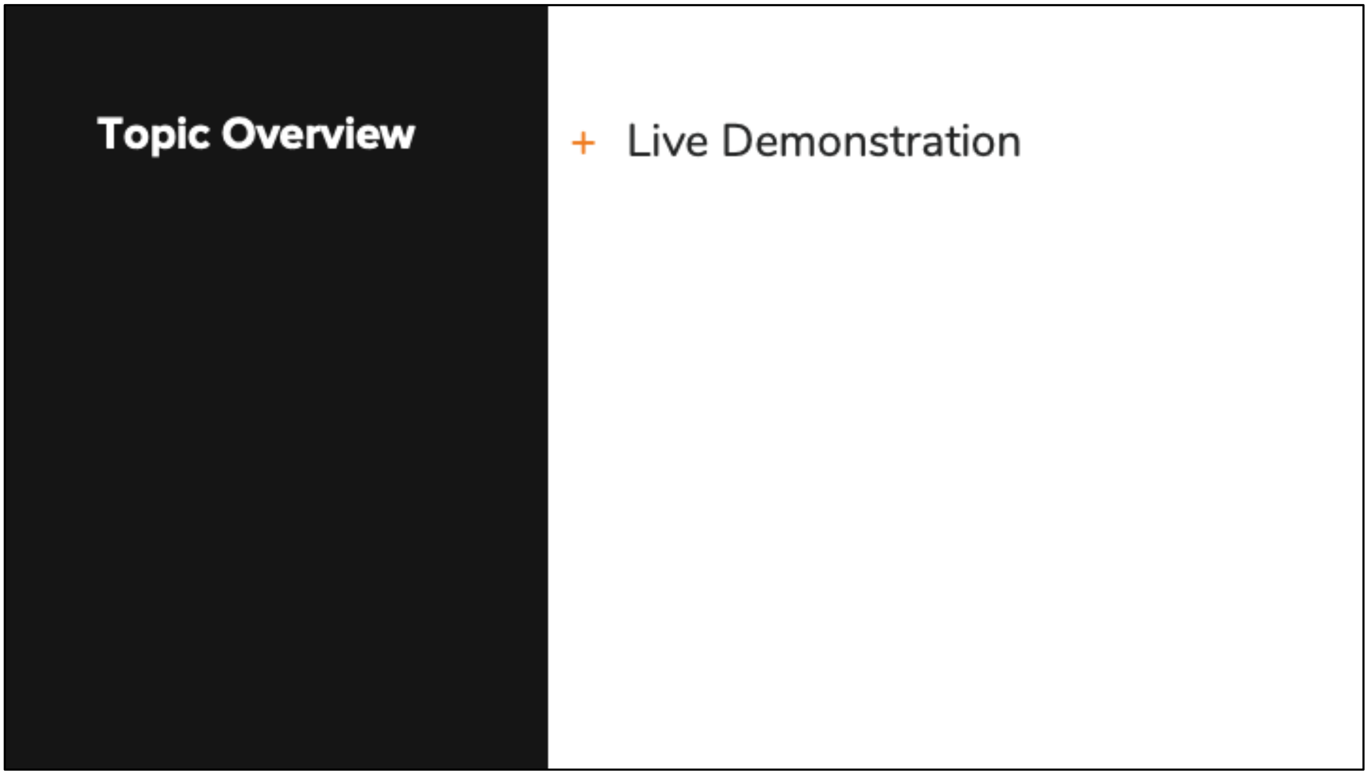


```
Switch-2#show port-security address
          Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
  22    001a.6c30.8fdf    SecureDynamic                 Fa0/1         1
   1    0014.f24d.c58c    SecureDynamic                 Fa0/10      < 1
-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 2048
```

Thanks for Watching!

Port Security Demonstration

ine.com



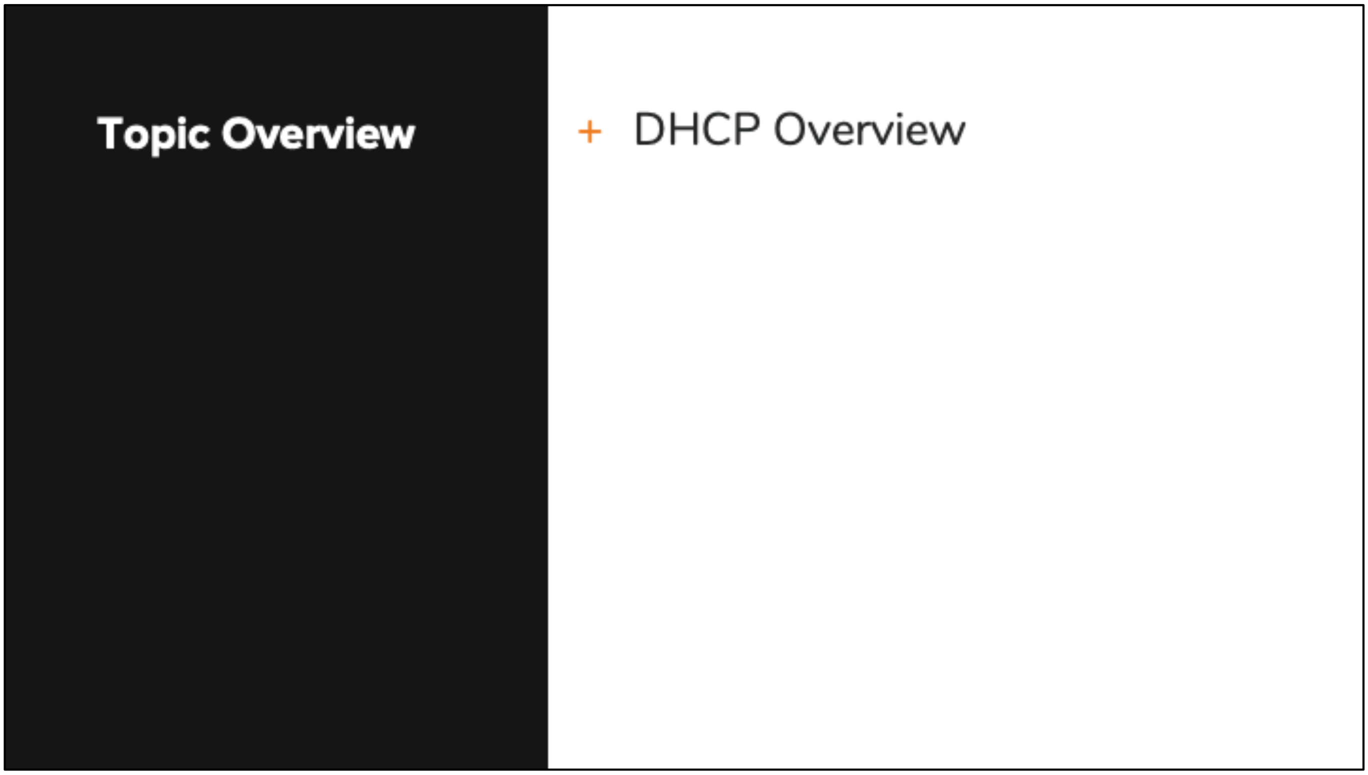
Topic Overview

- Live Demonstration

Thanks for Watching!

Overview Of DHCP Operations

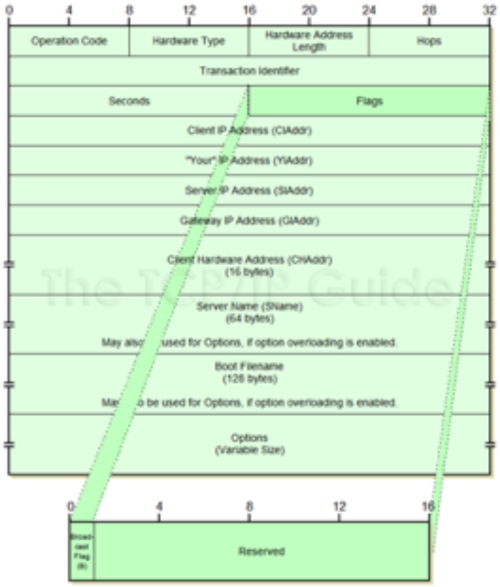
ine.com



Topic Overview

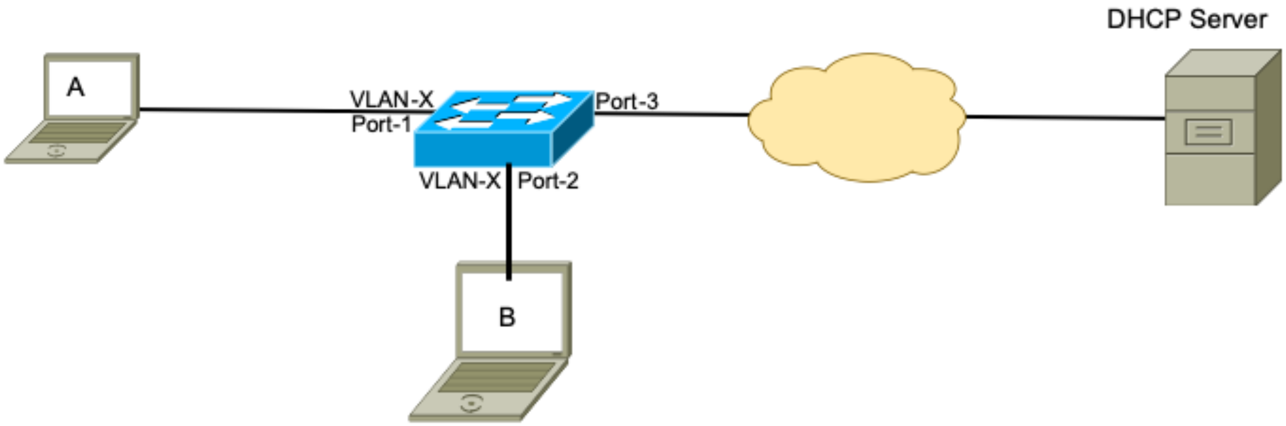
- DHCP Overview

DHCP Packet Format

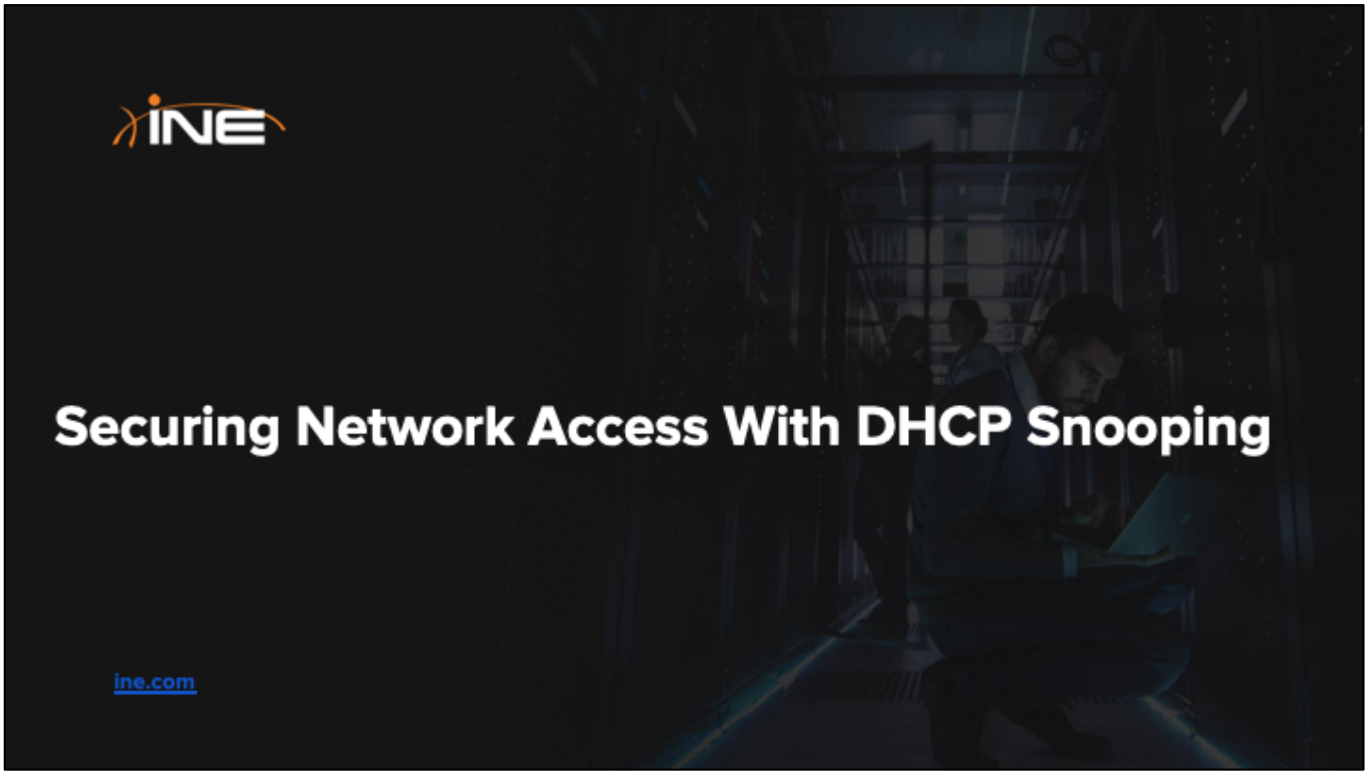

0
4
8
12
16
20
24
28
32
Operation Code
Hardware Type
Hardware Address Length
Hops
Transaction Identifier
Seconds
Flags
Client IP Address (CIAddr)
"Your" IP Address (YIAddr)
Server IP Address (SIAddr)
Gateway IP Address (GIAddr)
Client Hardware Address (CHAddr)
(16 bytes)
The TCP/IP Guide
Server Name (SName)
(64 bytes)
May also be used for Options, if option overloading is enabled.
Boot Filename
(128 bytes)
May also be used for Options, if option overloading is enabled.
Options
(Variable Size)
0
4
8
12
16
Broad-cast Flag (B)
Reserved

Graphic taken from TCP/IP Guide
-
http://www.tcpipguide.com/free/t_DHCPMessageFormat.htm
-
Emphasize the “GIAddr” and “Options” fields…both of which play a critical role in DHCP Snooping.

DHCP Operation



Thanks for Watching!

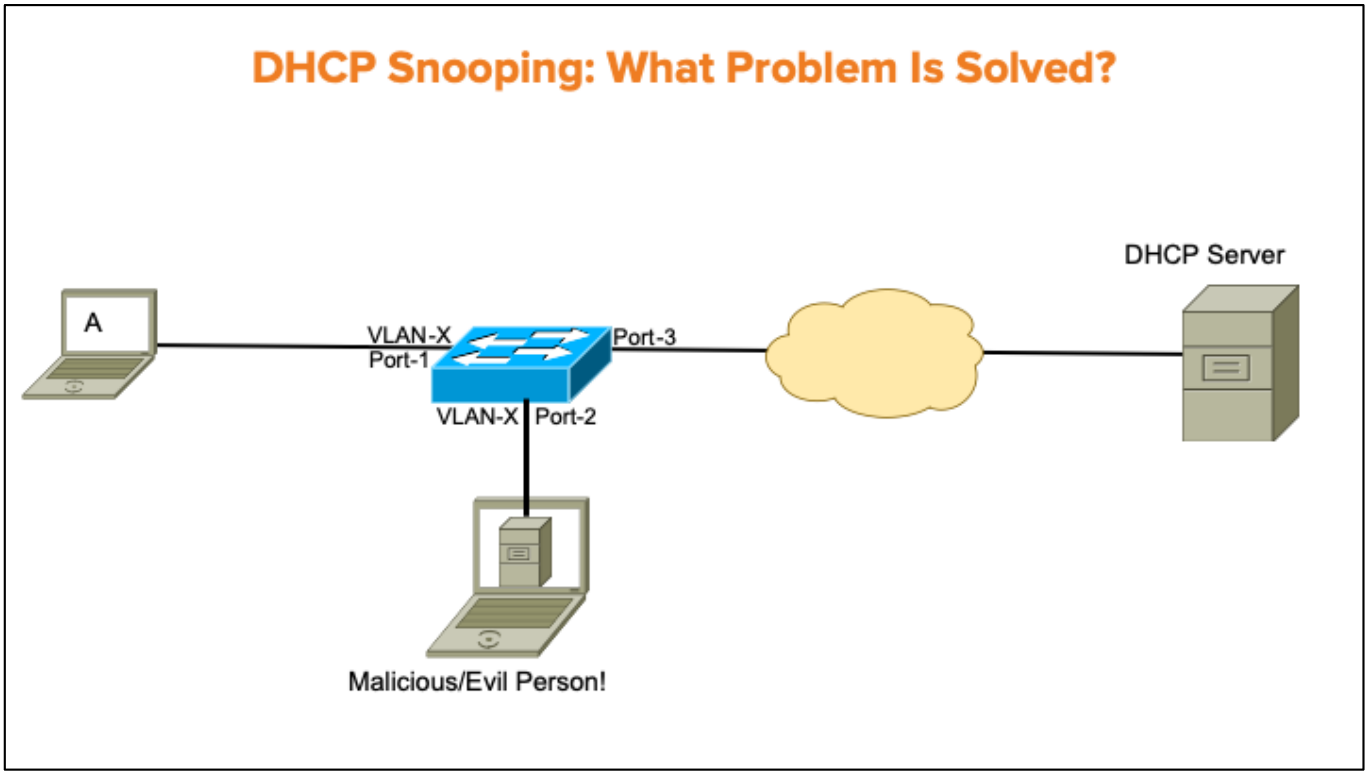


Securing Network Access With DHCP Snooping

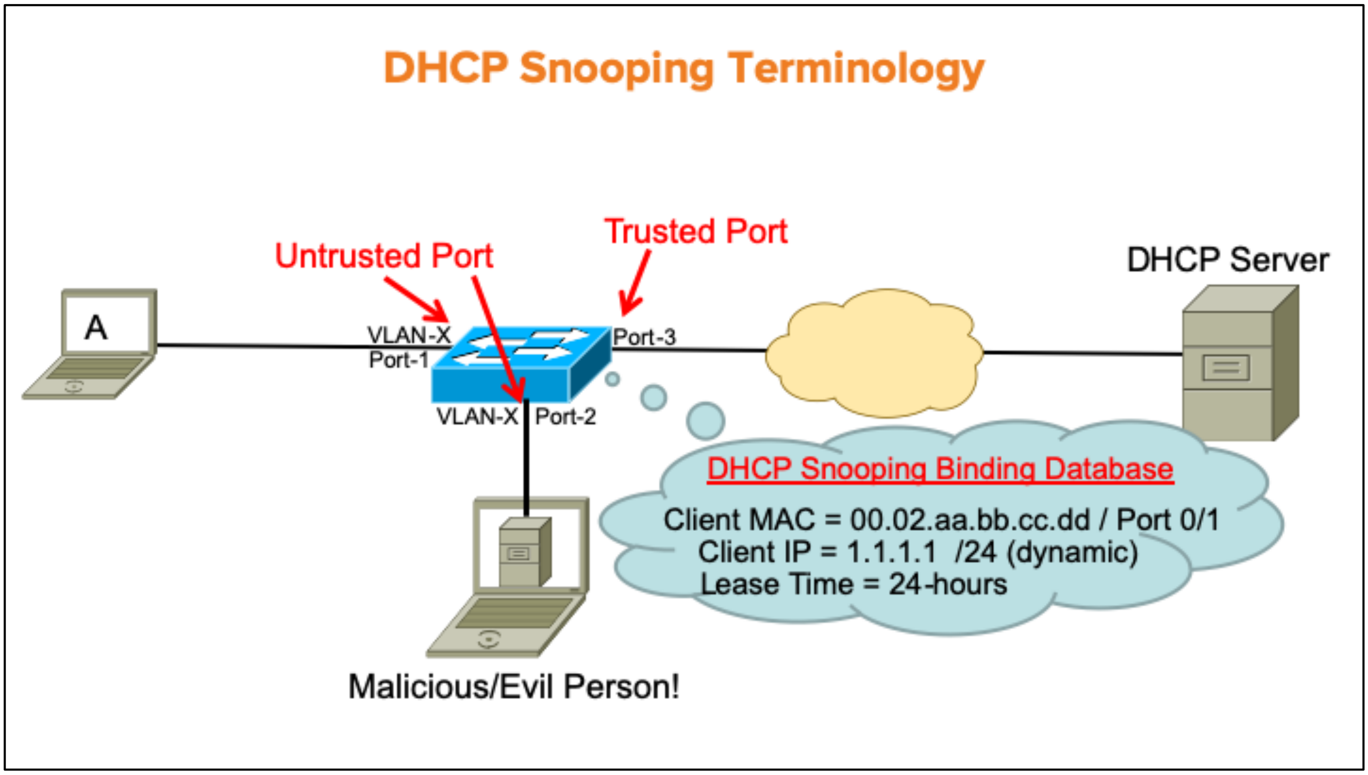
ine.com

Topic Overview

- What Problem Is Solved By DHCP Snooping?
- Terminology
- DHCP Snooping Operation



DHCP Snooping: What Problem Is Solved?



DHCP Snooping Terminology

DHCP Snooping Binding Database

Client MAC = 00.02.aa.bb.cc.dd / Port 0/1
Client IP = 1.1.1.1 /24 (dynamic)
Lease Time = 24-hours

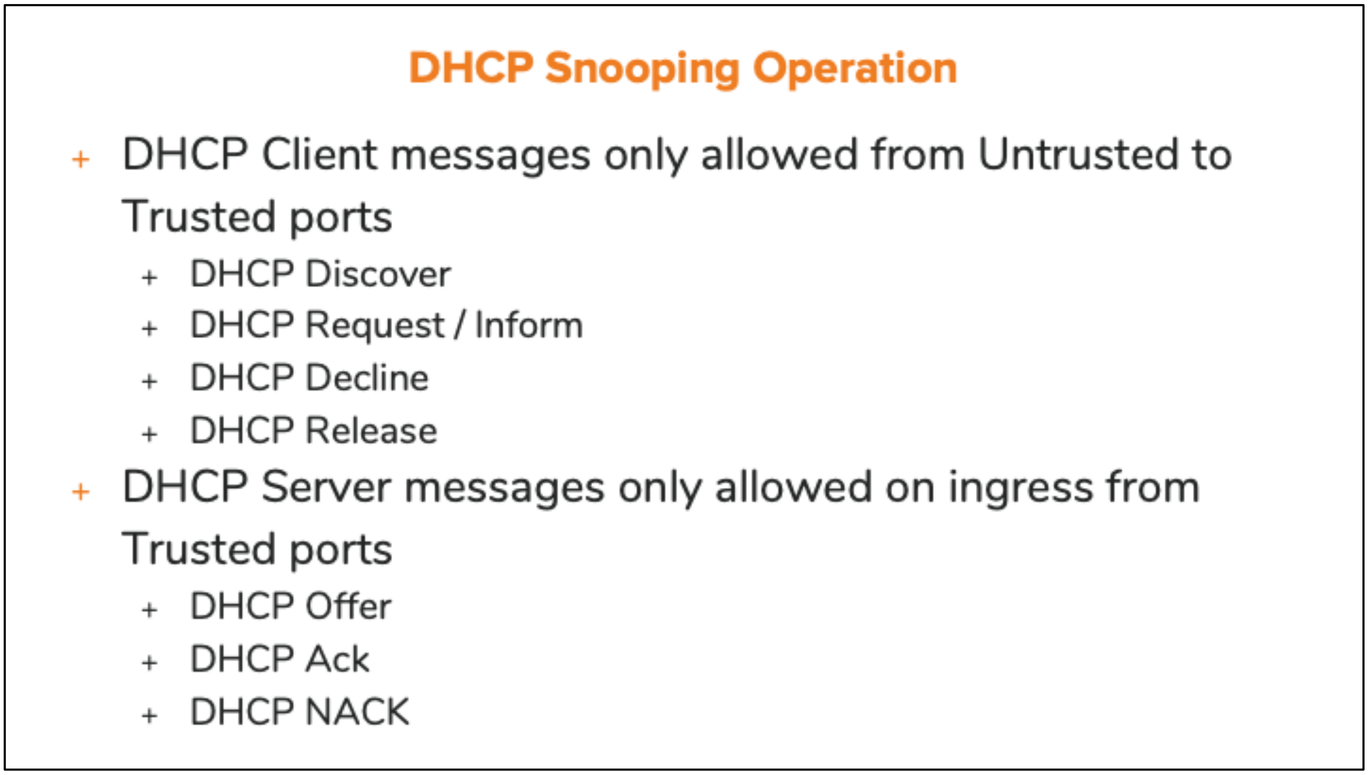
DHCP Binding Database only built based on information gleaned from UNTRUSTED interfaces.

-

Mention that Binding Database also used by many other features, (Dynamic ARP Inspection, IP Source Guard, etc).

-

No way to manually add entries to this table but other features that use this table have their own methods for adding static entries (for example, connected servers with static IP addresses).



DHCP Snooping Operation

- DHCP Client messages only allowed from Untrusted to Trusted ports
  - DHCP Discover
  - DHCP Request / Inform
  - DHCP Decline
  - DHCP Release
- DHCP Server messages only allowed on ingress from Trusted ports
  - DHCP Offer
  - DHCP Ack
  - DHCP NACK

DHCP Inform: Used by Client when it already has an address but would like to obtain other/additional information from DHCP Server.

-

This means that DHCP client messages won’t be seen by rogue DHCP servers on untrusted ports.

-

Feature should ONLY be enabled on access-layer switches because it drops any DHCP packet with a non-zero GIADDR field

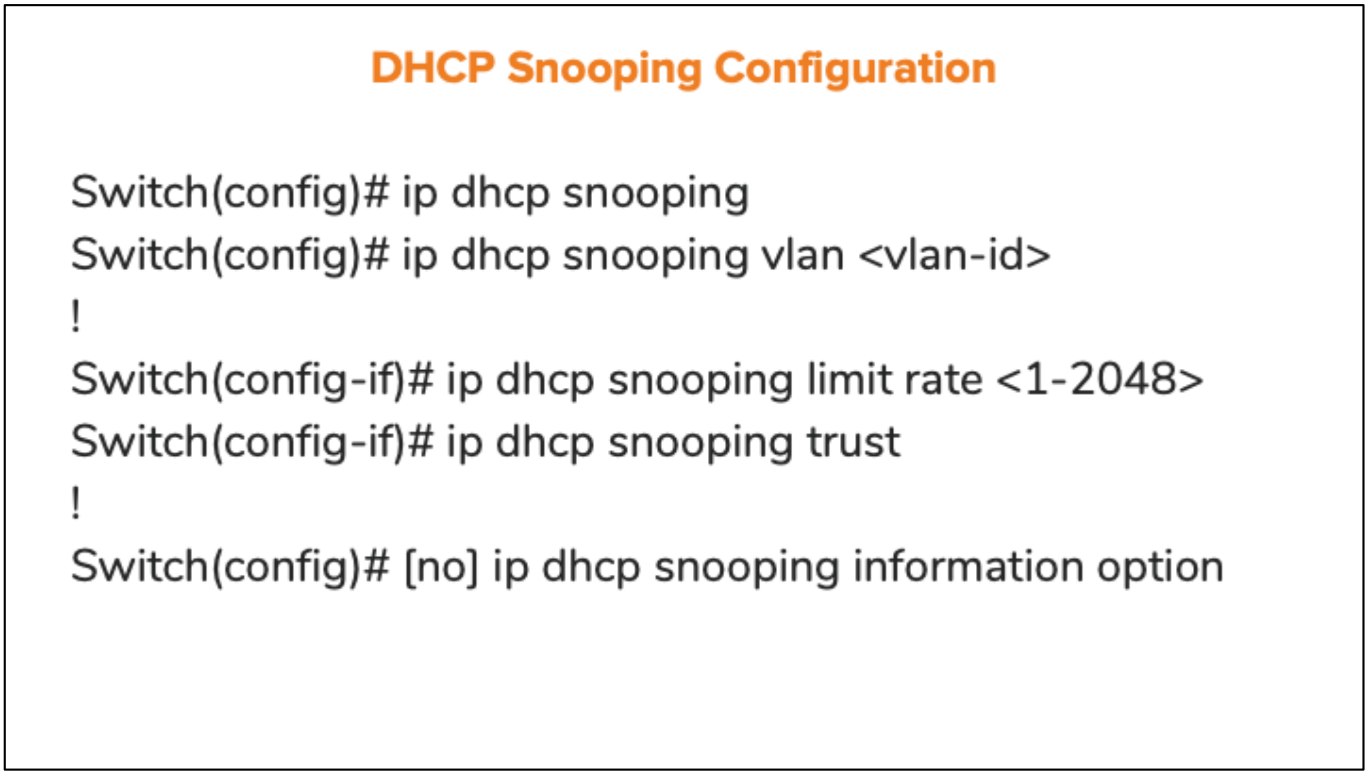
Thanks for Watching!

Configuring DHCP Snooping In Cisco IOS

ine.com

Topic Overview

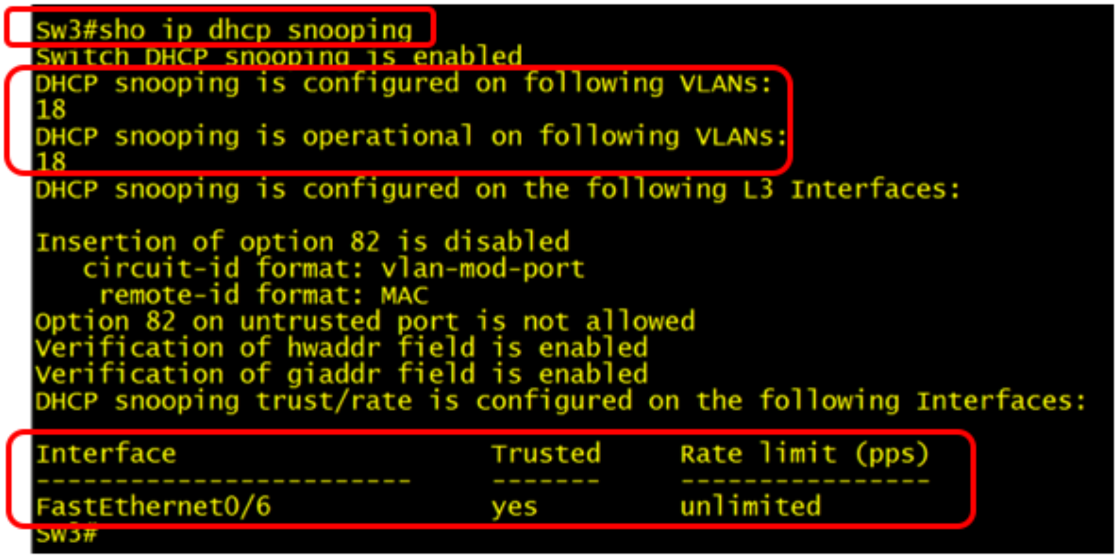
- DHCP Snooping Configuration
- DHCP Snooping Verification



DHCP Snooping Configuration

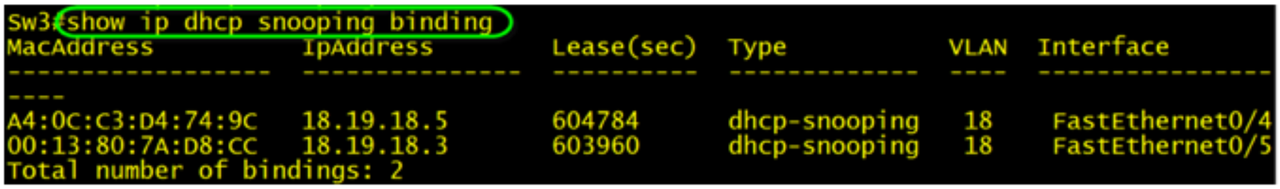
```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan <vlan-id>
!
Switch(config-if)# ip dhcp snooping limit rate <1-2048>
Switch(config-if)# ip dhcp snooping trust
!
Switch(config)# [no] ip dhcp snooping information option
```

DHCP Snooping Verification



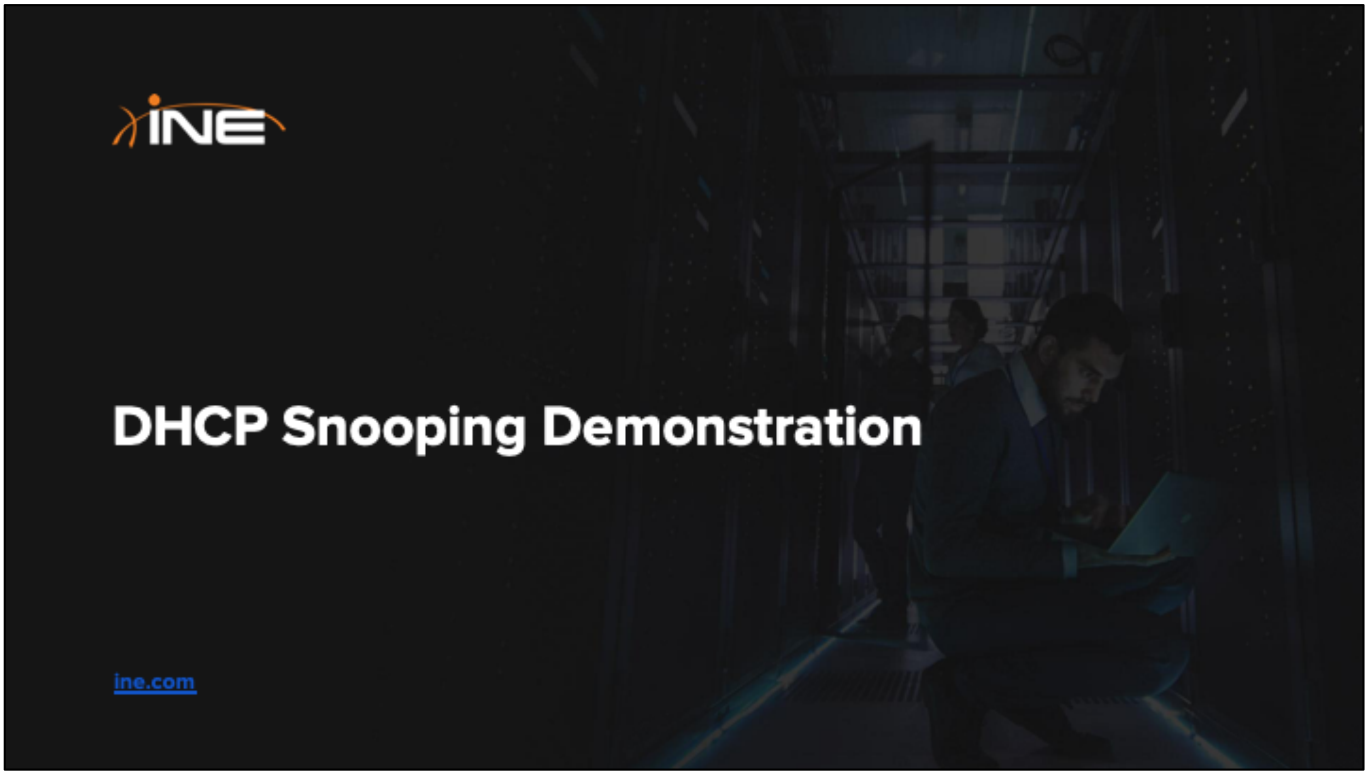
```
Sw3#sho ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
18
DHCP snooping is operational on following VLANs:
18
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/6              yes         unlimited
Sw3#
```

DHCP Snooping Monitoring



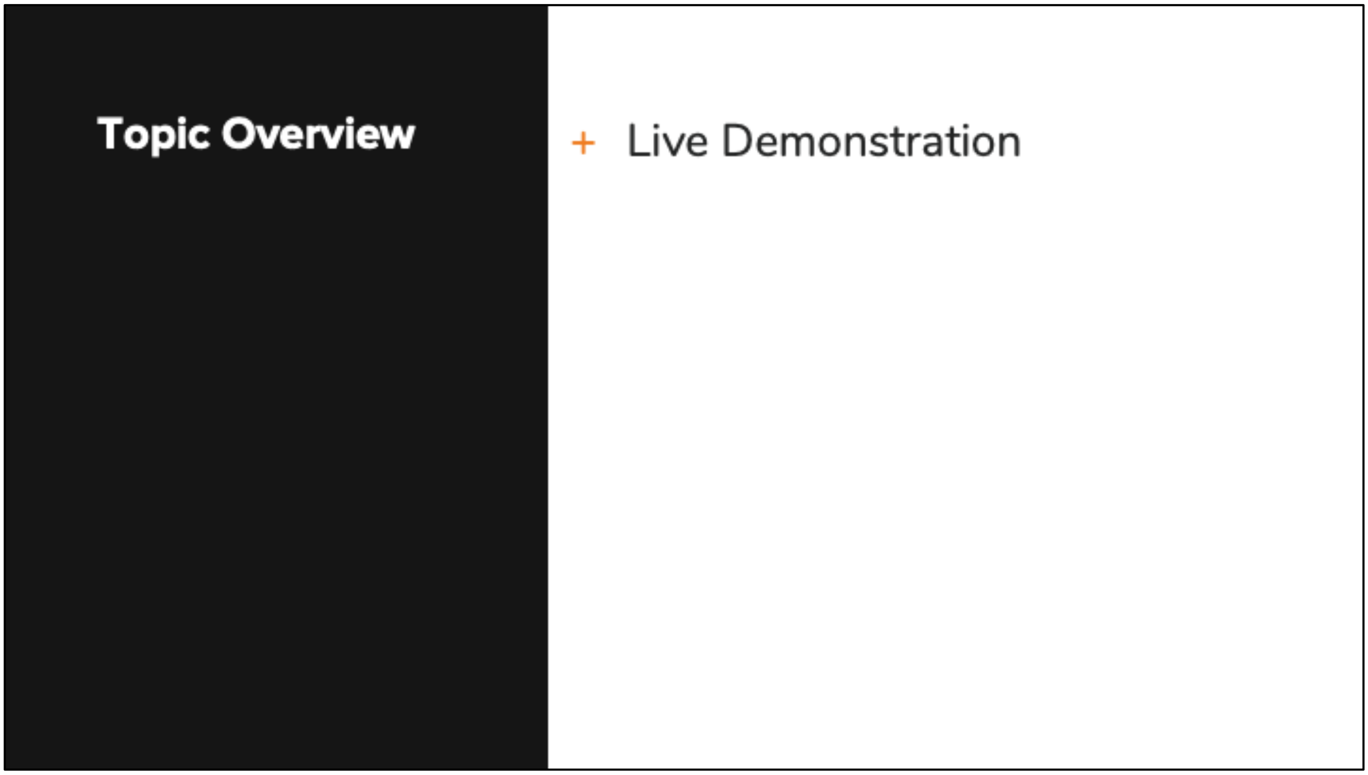
```
Sw3#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ----------------
----
A4:0C:C3:D4:74:9C   18.19.18.5       604784      dhcp-snooping   18    FastEthernet0/4
00:13:80:7A:D8:CC   18.19.18.3       603960      dhcp-snooping   18    FastEthernet0/5
Total number of bindings: 2
```

Thanks for Watching!



DHCP Snooping Demonstration

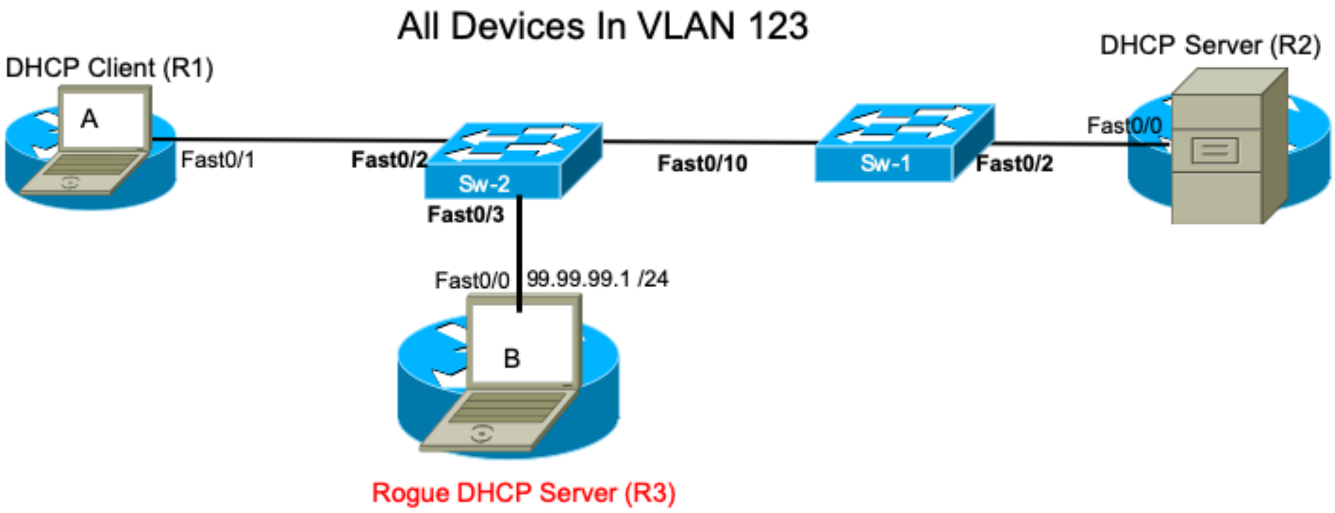
ine.com



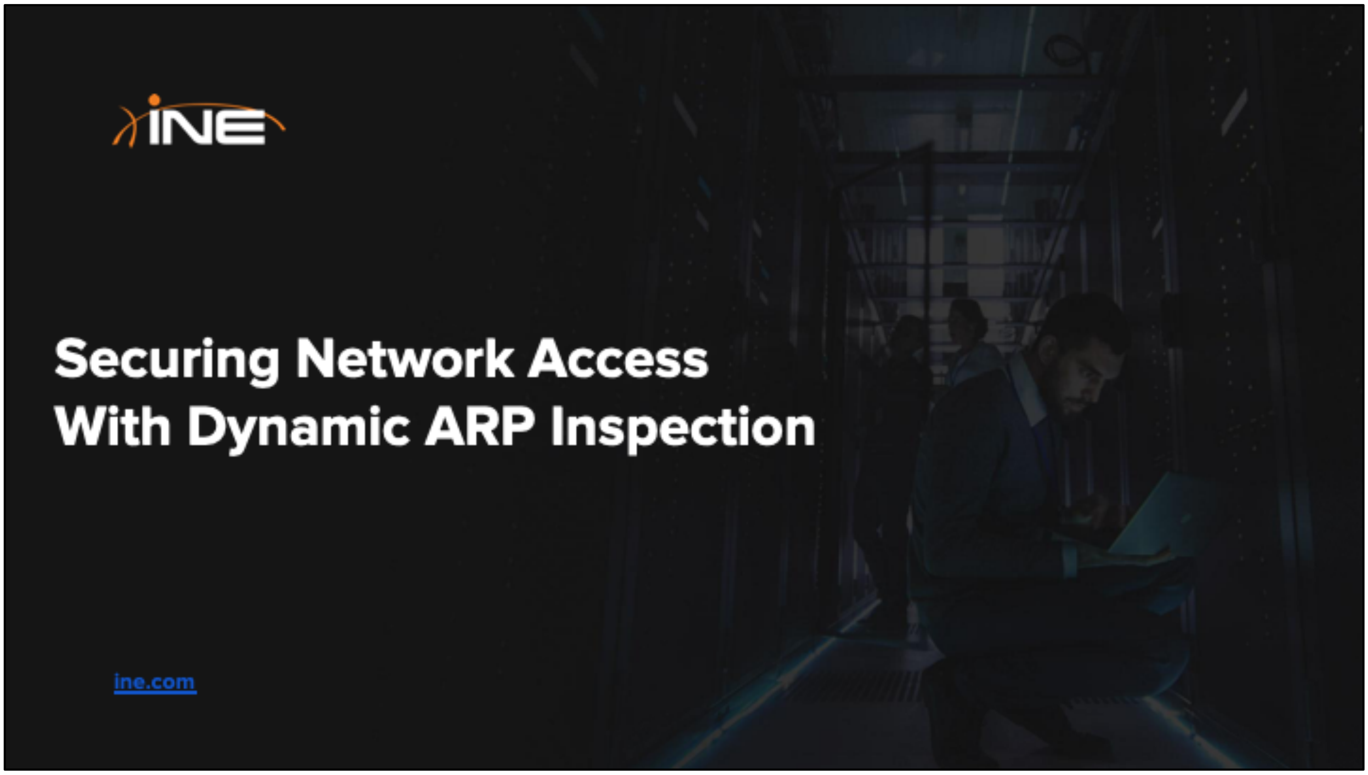
Topic Overview

- Live Demonstration

DHCP Demonstration Topology



Thanks for Watching!



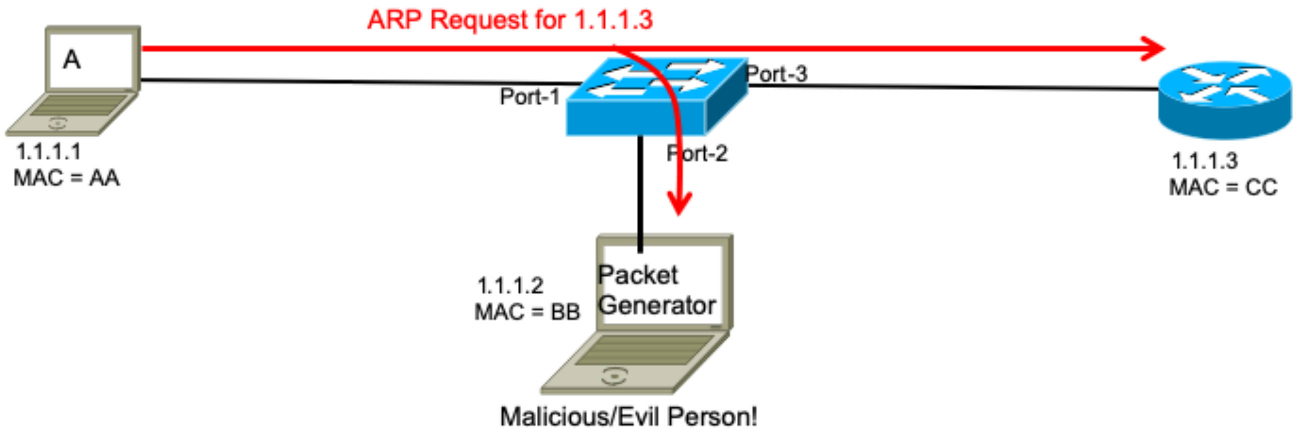
Securing Network Access With Dynamic ARP Inspection

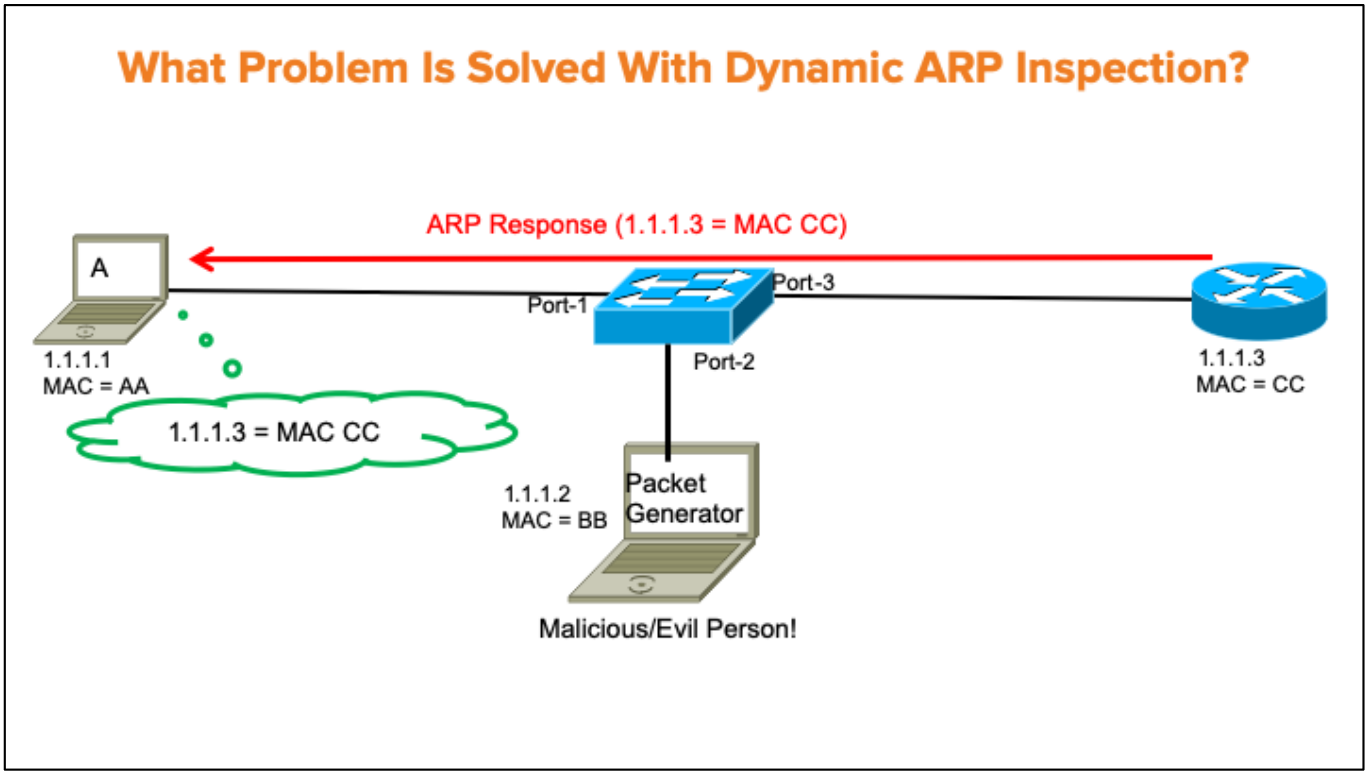
ine.com

Topic Overview

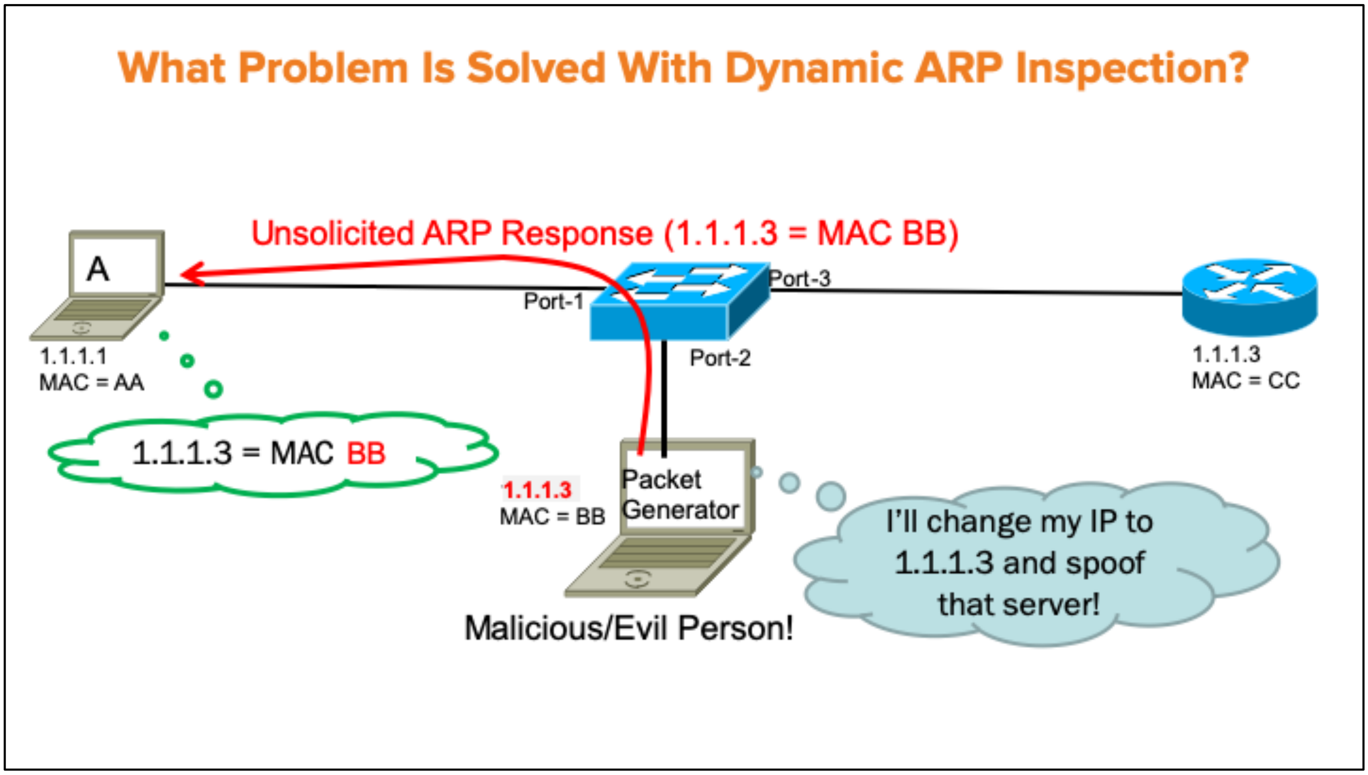
- What Problem Is Solved With Dynamic ARP Inspection?
- Overview Of Operation
- Terminology

What Problem Is Solved With Dynamic ARP Inspection?





What Problem Is Solved With Dynamic ARP Inspection?



What Problem Is Solved With Dynamic ARP Inspection?

Unsolicited ARP Response (1.1.1.3 = MAC BB)

A

1.1.1.1
MAC = AA

1.1.1.3 = MAC BB

Port-1

Port-2

Port-3

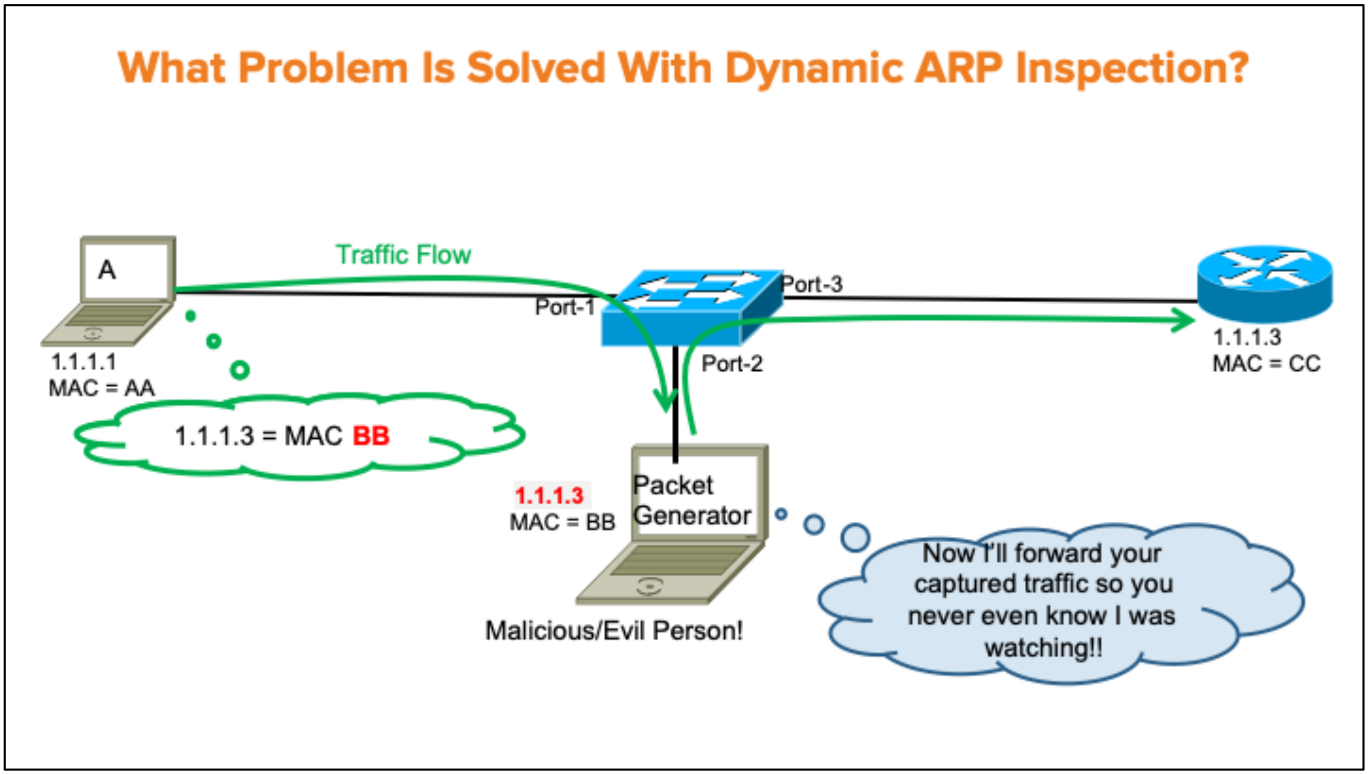
1.1.1.3
MAC = CC

1.1.1.3
MAC = BB

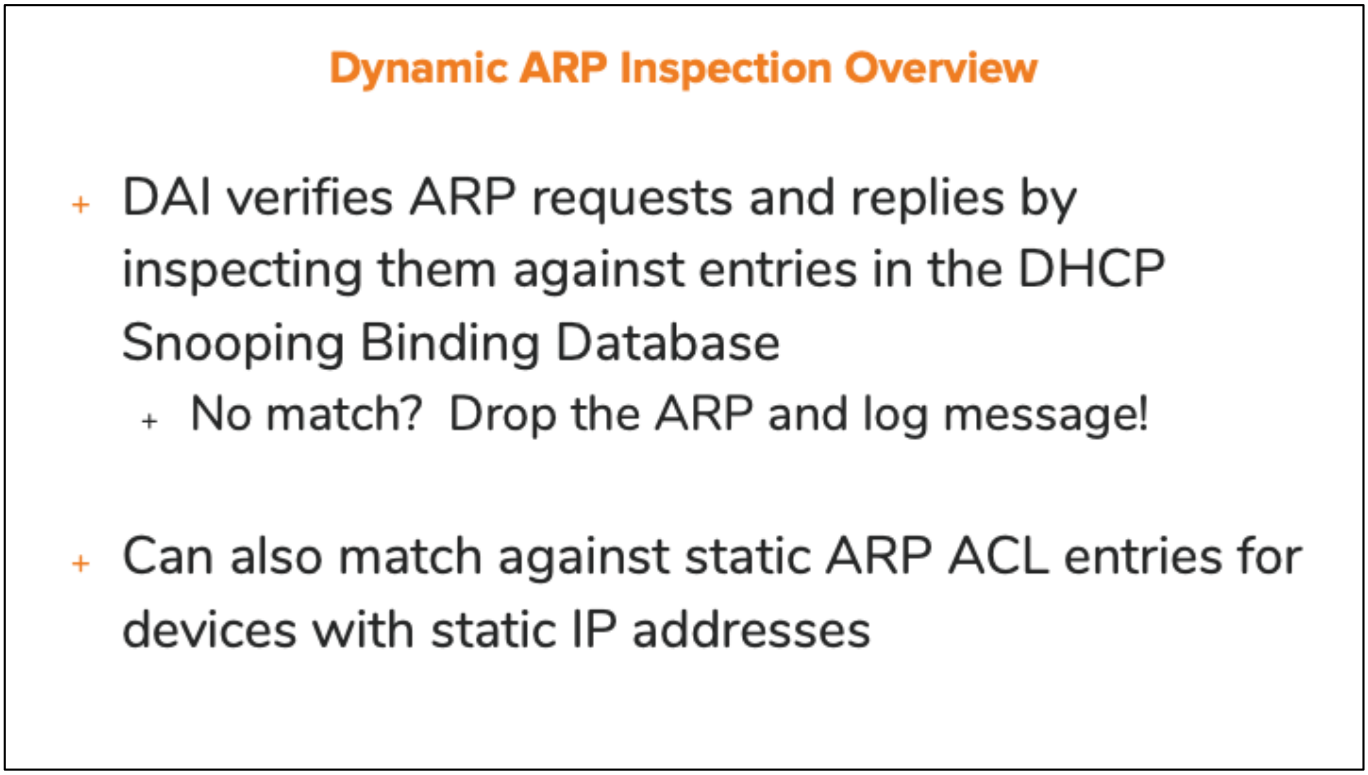
Packet
Generator

Malicious/Evil Person!

I'll change my IP to 1.1.1.3 and spoof that server!



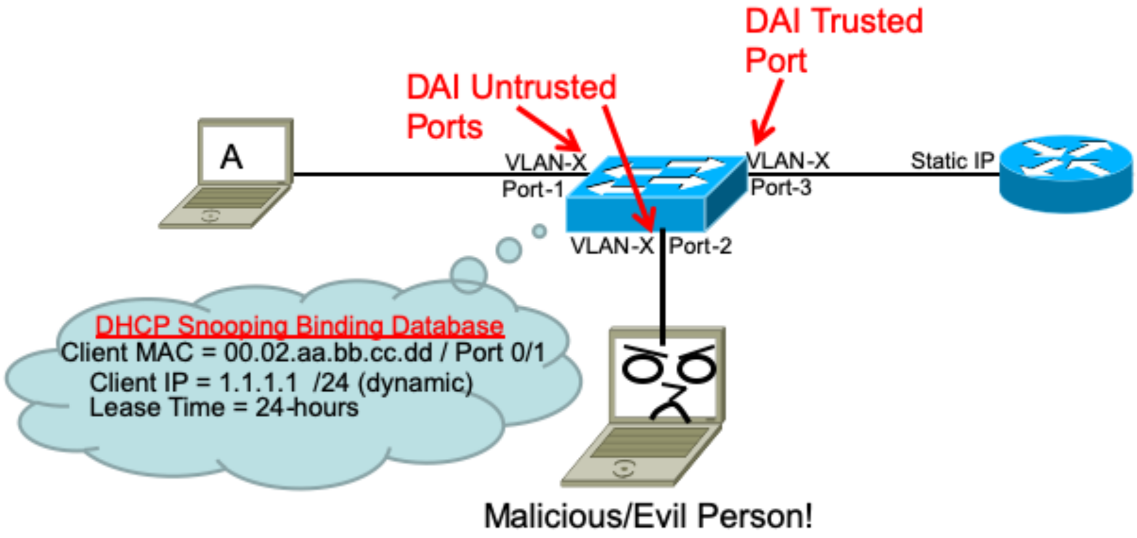
What Problem Is Solved With Dynamic ARP Inspection?



Dynamic ARP Inspection Overview

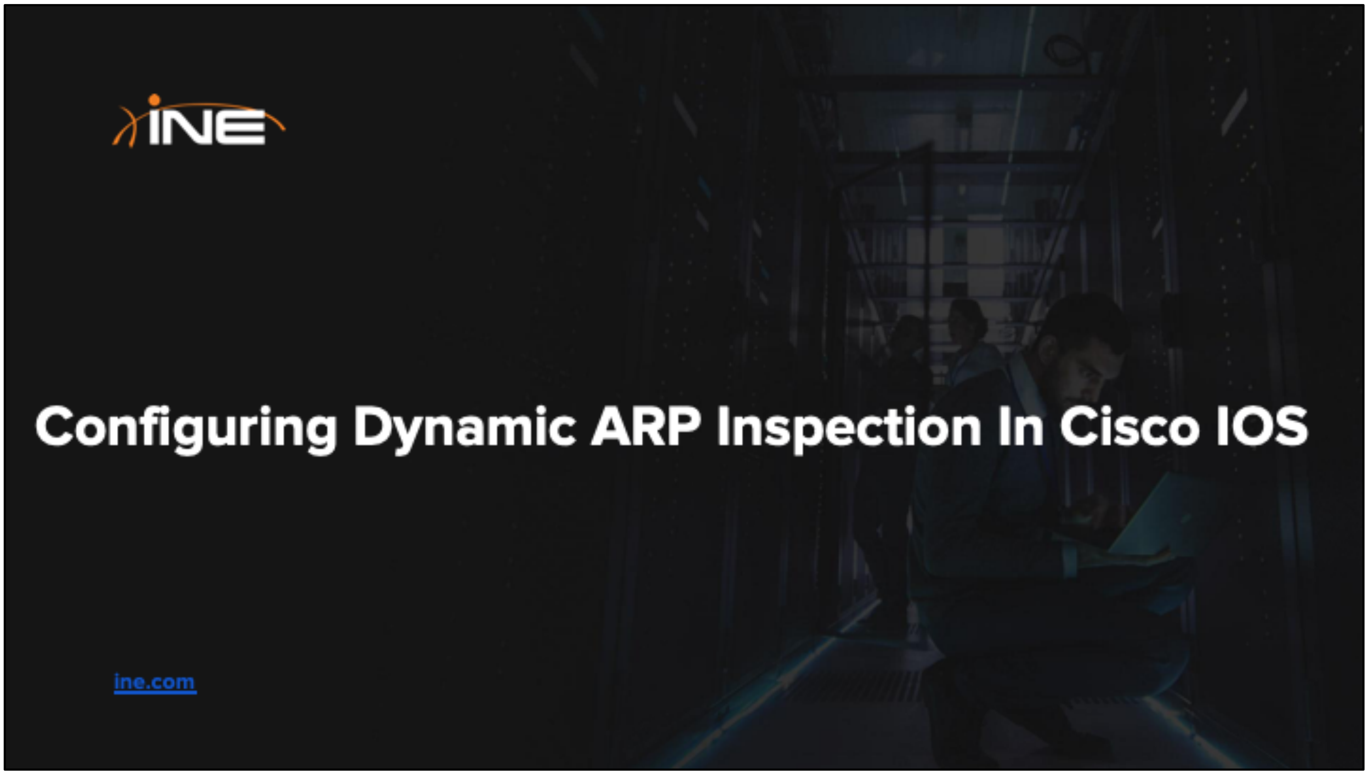
- DAI verifies ARP requests and replies by inspecting them against entries in the DHCP Snooping Binding Database
  - No match? Drop the ARP and log message!
- Can also match against static ARP ACL entries for devices with static IP addresses

DAI Terminology



DHCP Snooping Binding Database
Client MAC = 00.02.aa.bb.cc.dd / Port 0/1
Client IP = 1.1.1.1 /24 (dynamic)
Lease Time = 24-hours

Thanks for Watching!

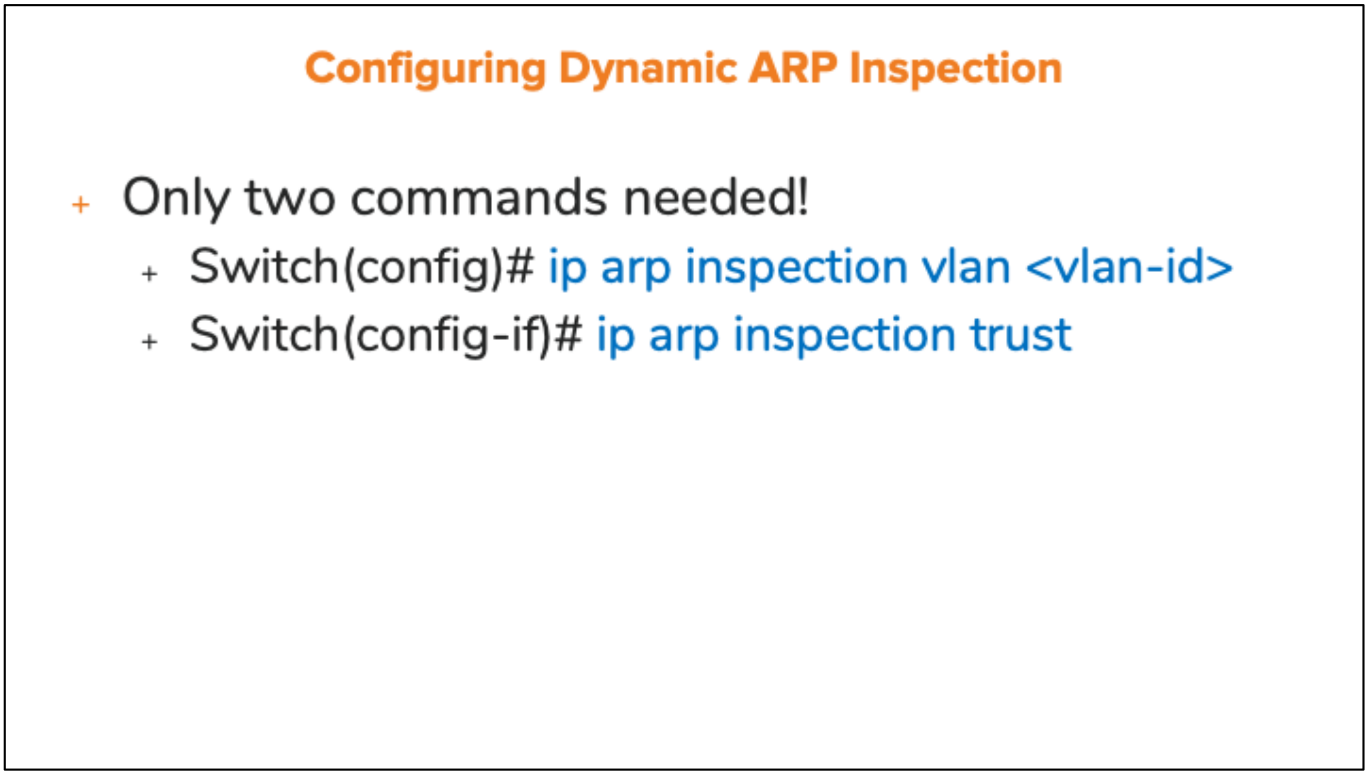


Configuring Dynamic ARP Inspection In Cisco IOS

ine.com

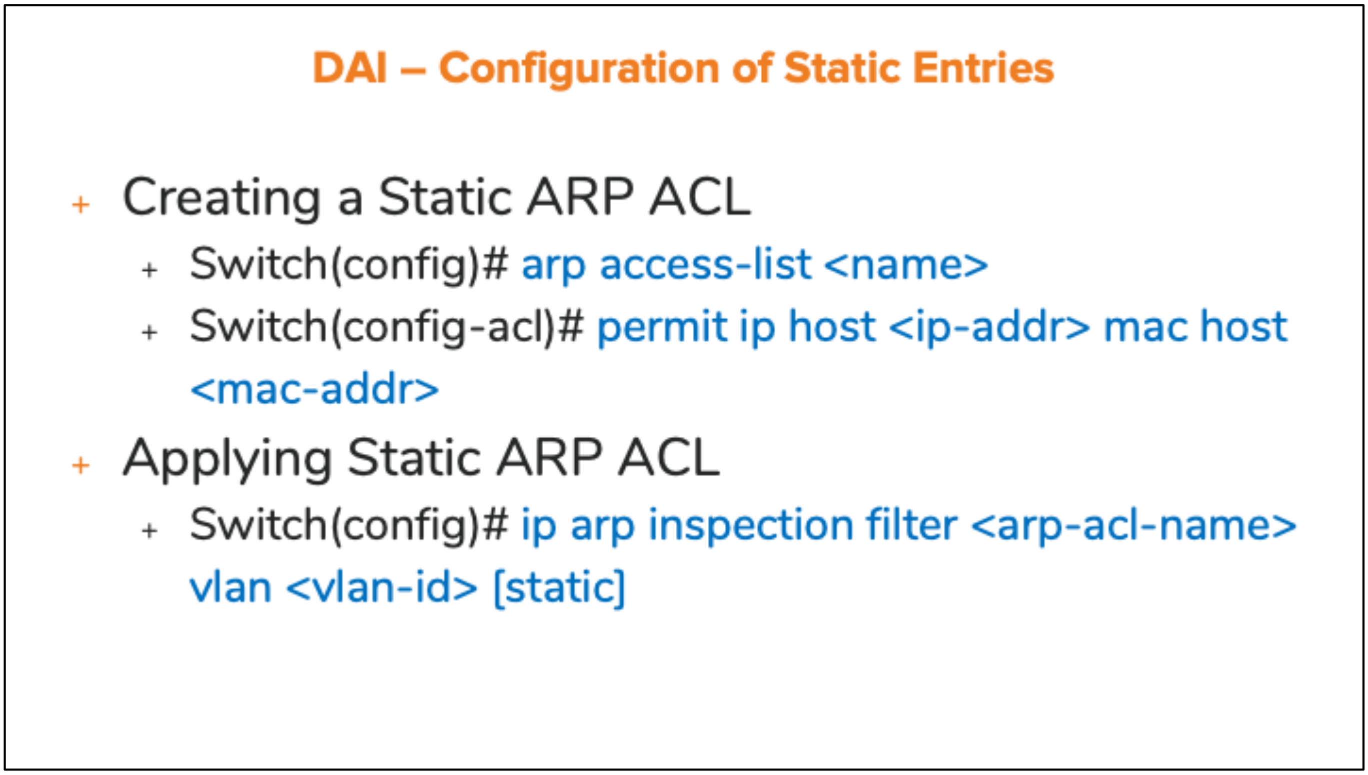
Topic Overview

- Configuration Of Dynamic ARP Inspection
- Incorporating DAI With Static IP Addresses
- What Gets Checked In The ARP Packet?
- Verification & Monitoring



Configuring Dynamic ARP Inspection

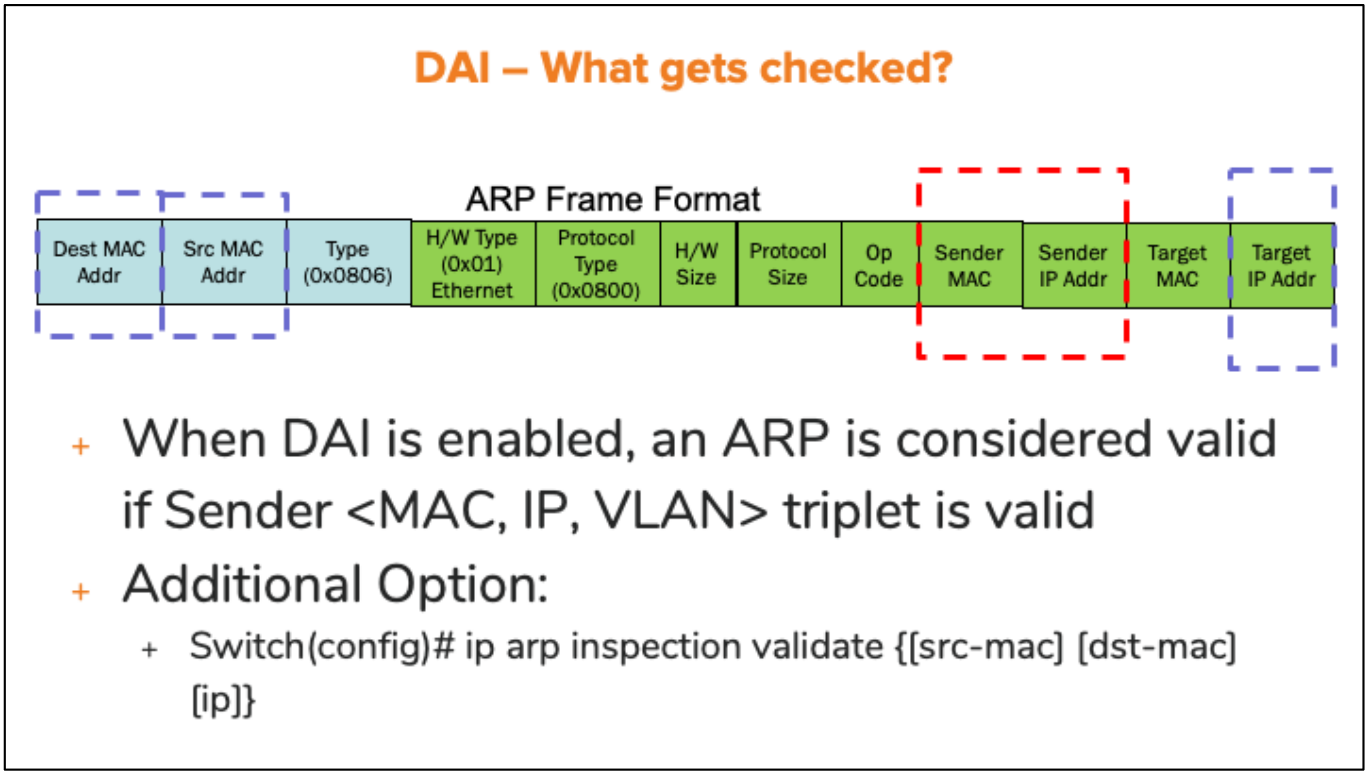
- Only two commands needed!
  - `Switch(config)# ip arp inspection vlan <vlan-id>`
  - `Switch(config-if)# ip arp inspection trust`



DAI – Configuration of Static Entries

- Creating a Static ARP ACL
  - Switch(config)# arp access-list <name>
  - Switch(config-acl)# permit ip host <ip-addr> mac host <mac-addr>
- Applying Static ARP ACL
  - Switch(config)# ip arp inspection filter <arp-acl-name> vlan <vlan-id> [static]

“static” keyword prevents checking of DHCP Snooping Binding table if ARP ACL doesn’t match (creates implicit “deny”)



DAI – What gets checked?

ARP Frame Format

Dest MAC Addr	Src MAC Addr	Type (0x0806)	H/W Type (0x01) Ethernet	Protocol Type (0x0800)	H/W Size	Protocol Size	Op Code	Sender MAC	Sender IP Addr	Target MAC	Target IP Addr

- When DAI is enabled, an ARP is considered valid if Sender <MAC, IP, VLAN> triplet is valid
- Additional Option:
  - Switch(config)# ip arp inspection validate {[src-mac] [dst-mac] [ip]}

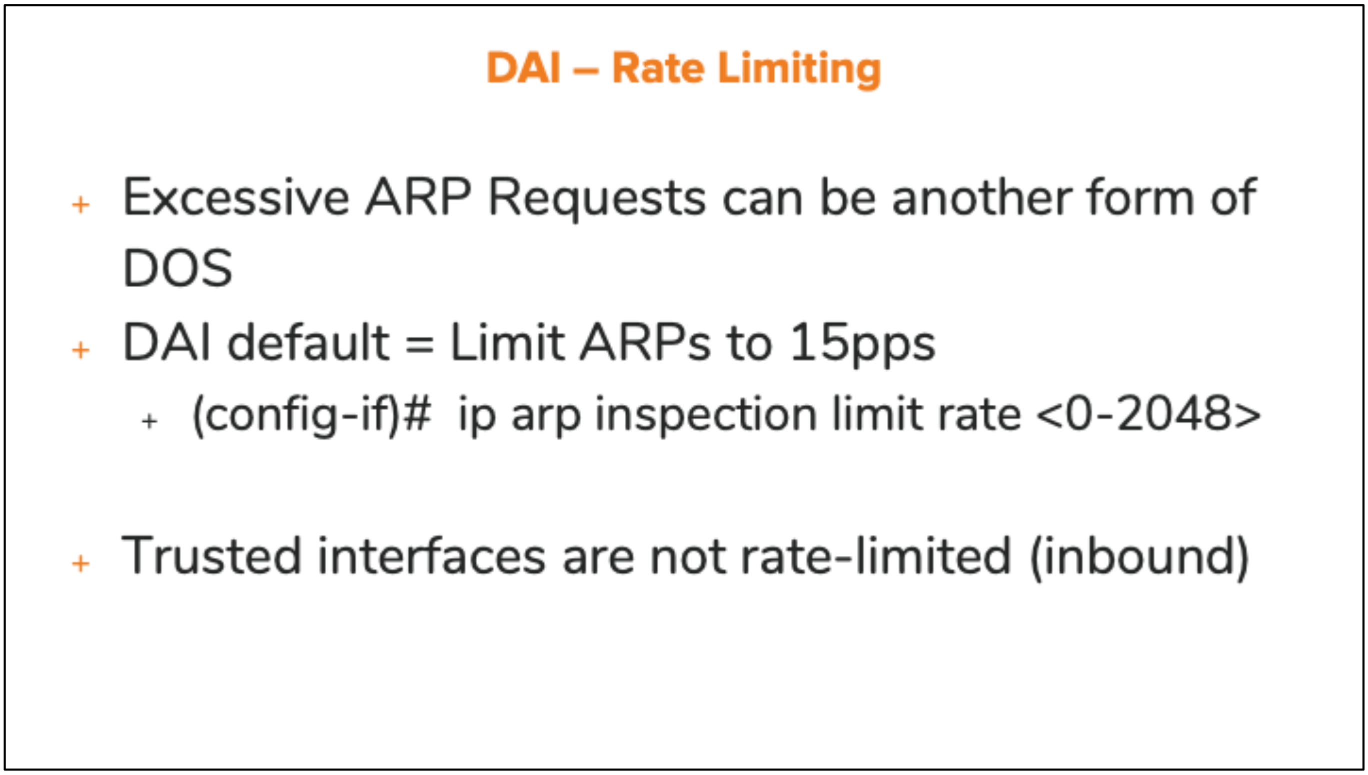
The “ip arp inspection validate” command is useful if you suspect that someone is crafting or forging ARP packets using a packet generator.

-

Src-Mac:(Optional) Enables validation of the source MAC address in the Ethernet header against the sender MAC address in the ARP body for ARP requests and responses. The devices classifies packets with different MAC addresses as invalid and drops them.

Dst-mac: (Optional) Enables validation of the destination MAC address in the Ethernet header against the target MAC address in the ARP body for ARP responses. The device classifies packets with different MAC addresses as invalid and drops them.

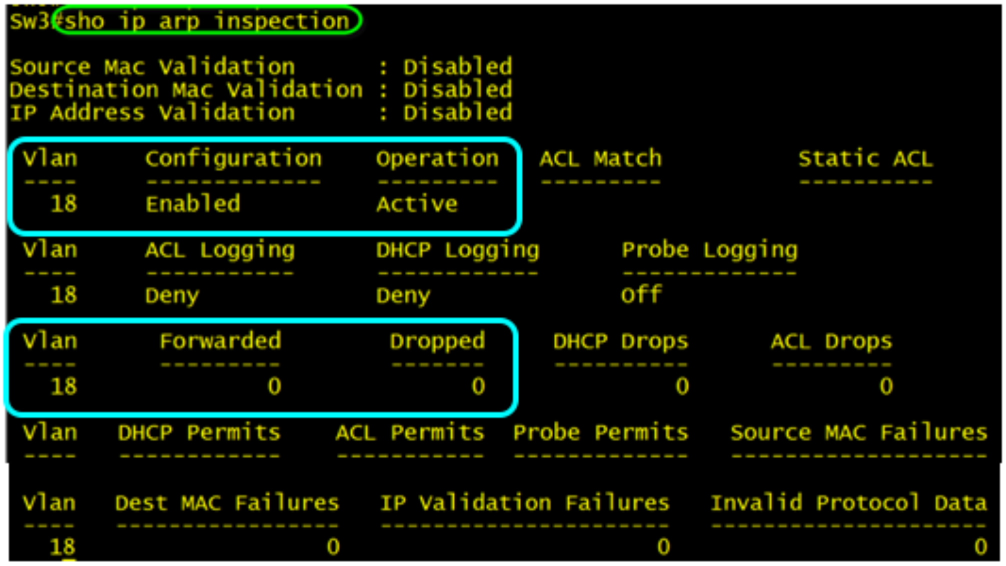
IP: (Optional) Enables validation of the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. The device checks the sender IP addresses in all ARP requests and responses and checks the target IP addresses only in ARP responses.



DAI – Rate Limiting

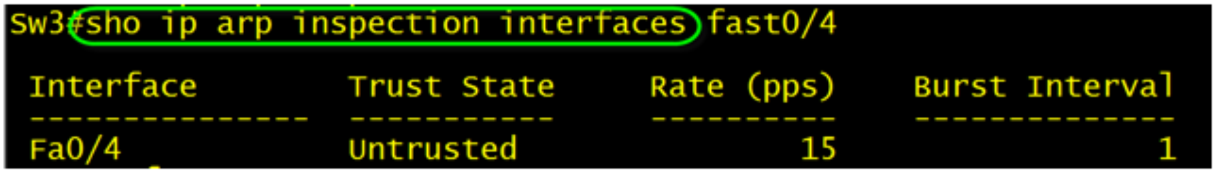
- Excessive ARP Requests can be another form of DOS
- DAI default = Limit ARPs to 15pps
  - (config-if)# ip arp inspection limit rate <0-2048>
- Trusted interfaces are not rate-limited (inbound)

Verifying Dynamic ARP Inspection



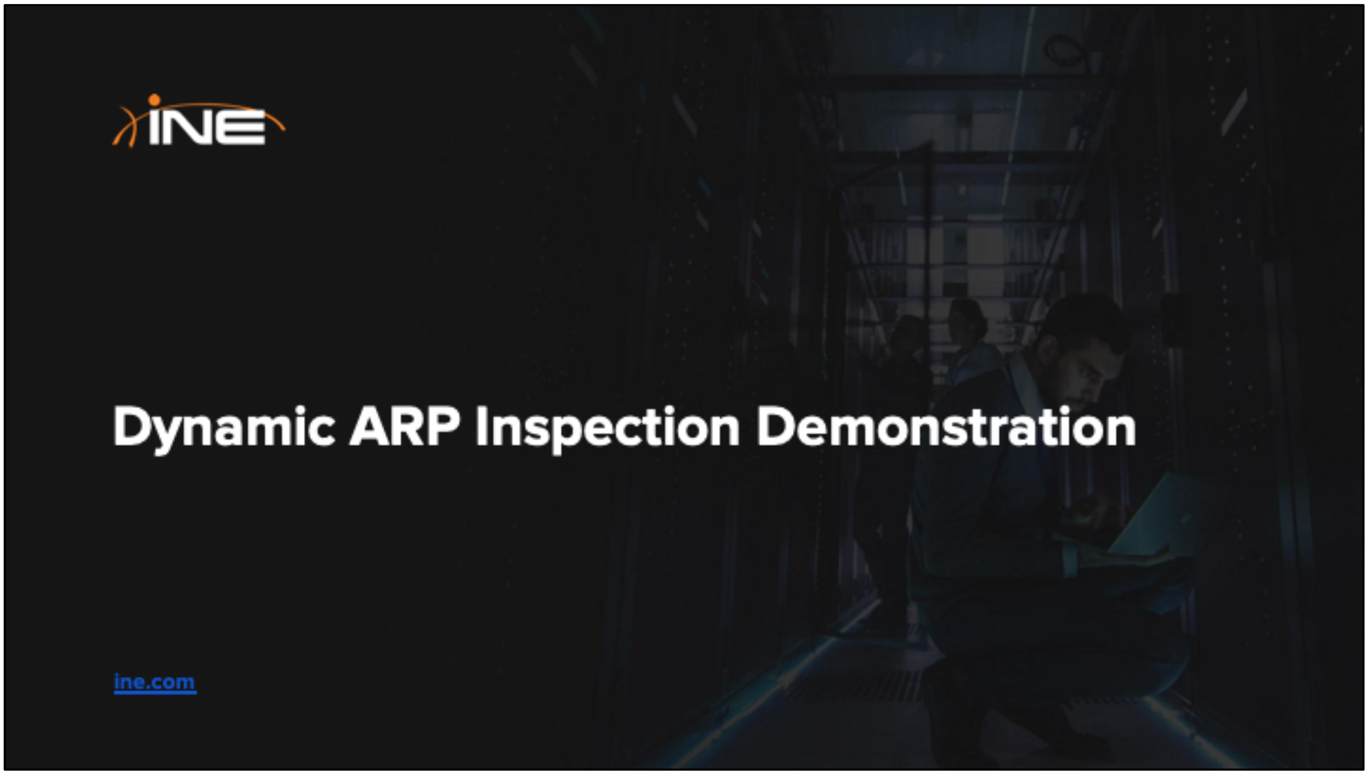
```
Sw3#sho ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   18     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
   18     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
   18              0              0              0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
   18                   0                        0                       0
```

Verifying Dynamic ARP Inspection



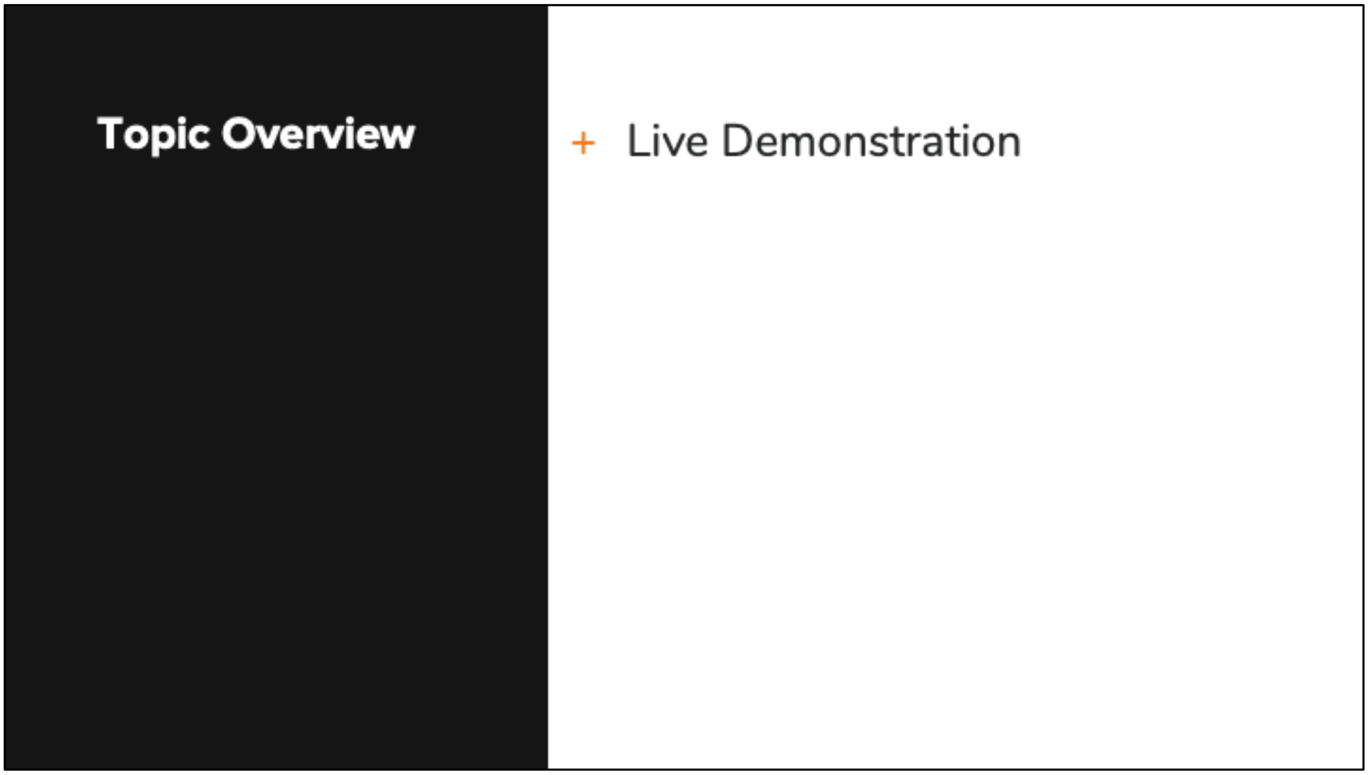
```
Sw3#sho ip arp inspection interfaces fast0/4

 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Fa0/4            Untrusted               15                 1
```

Thanks for Watching!



Dynamic ARP Inspection Demonstration

ine.com



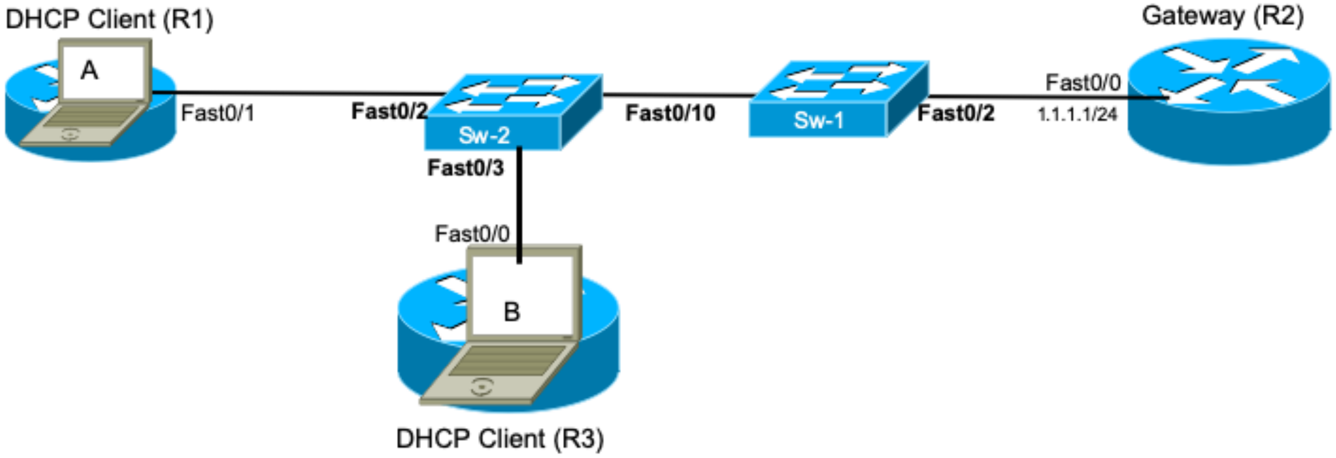
Topic Overview

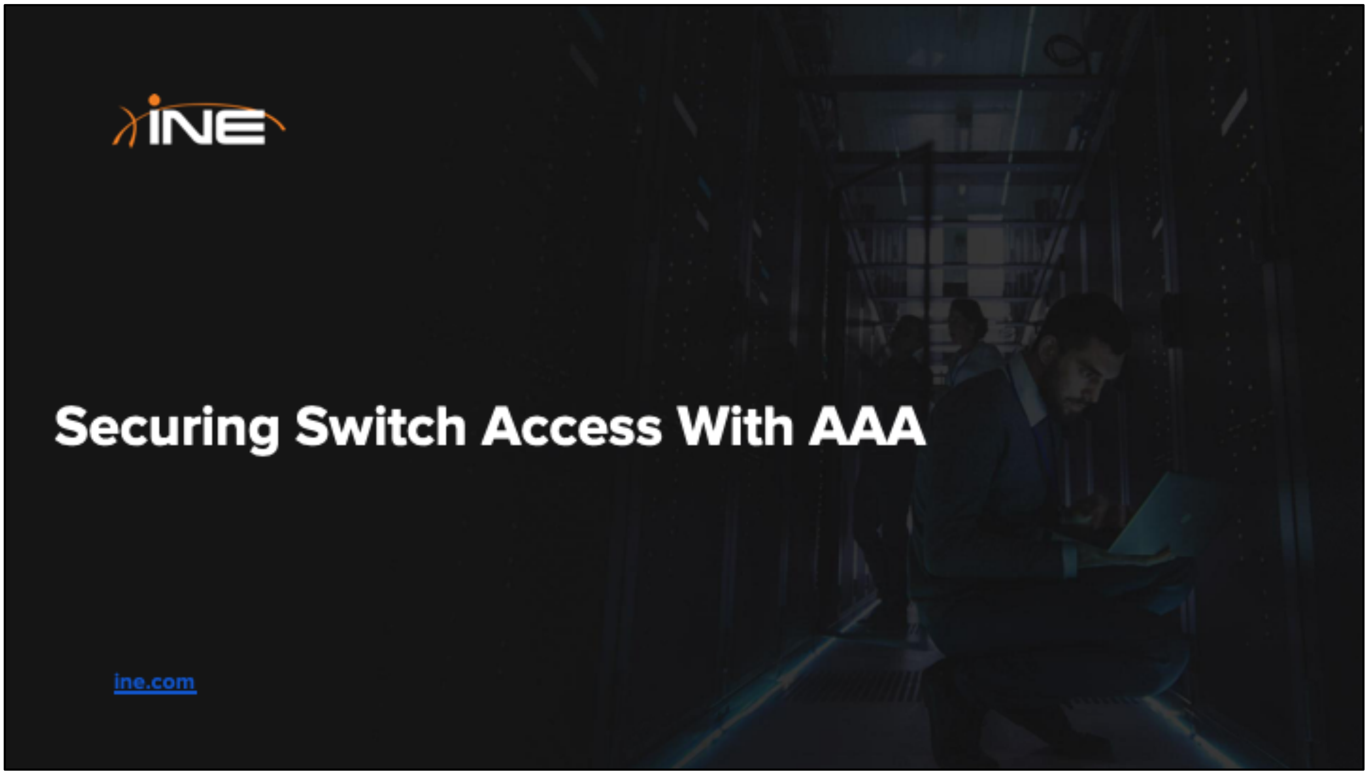
- Live Demonstration

Thanks for Watching!

DAI Demonstration Topology

All Devices In VLAN 123





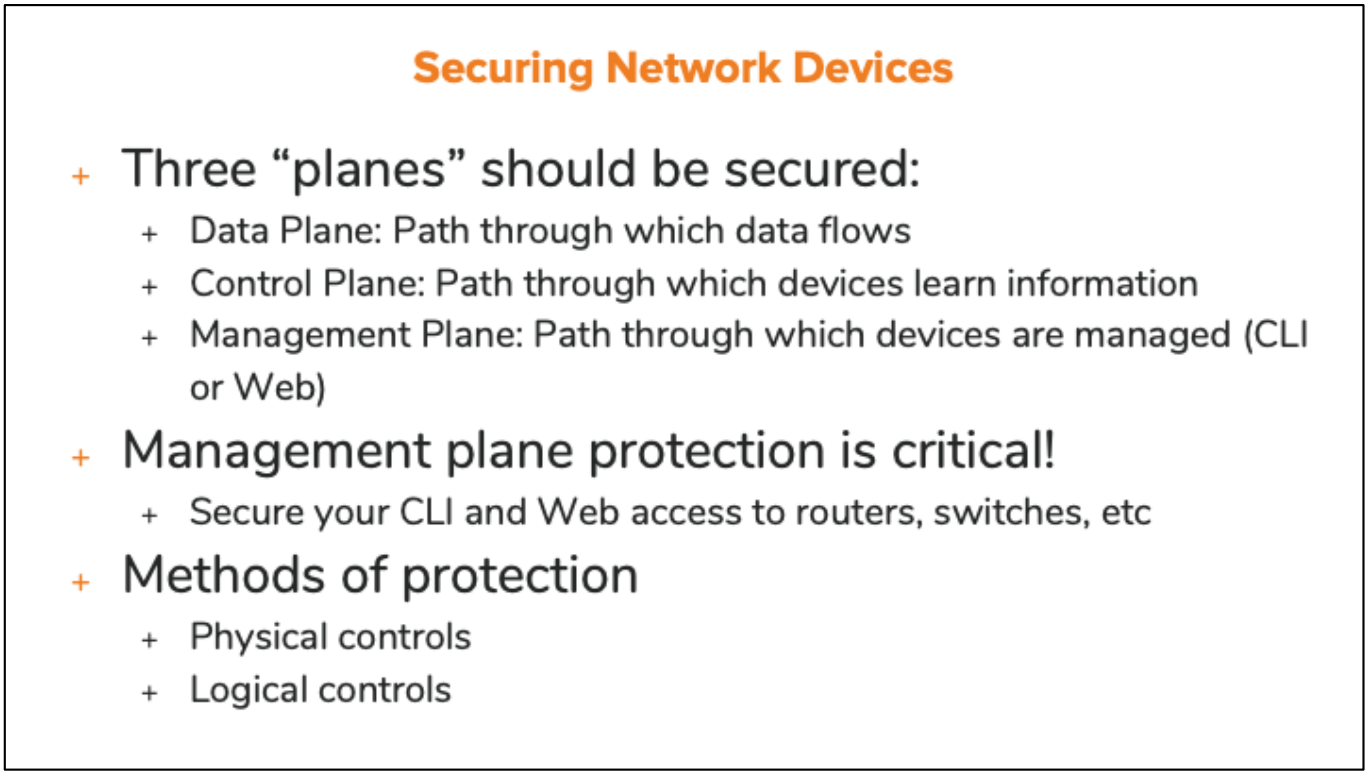
INE

Securing Switch Access With AAA

ine.com

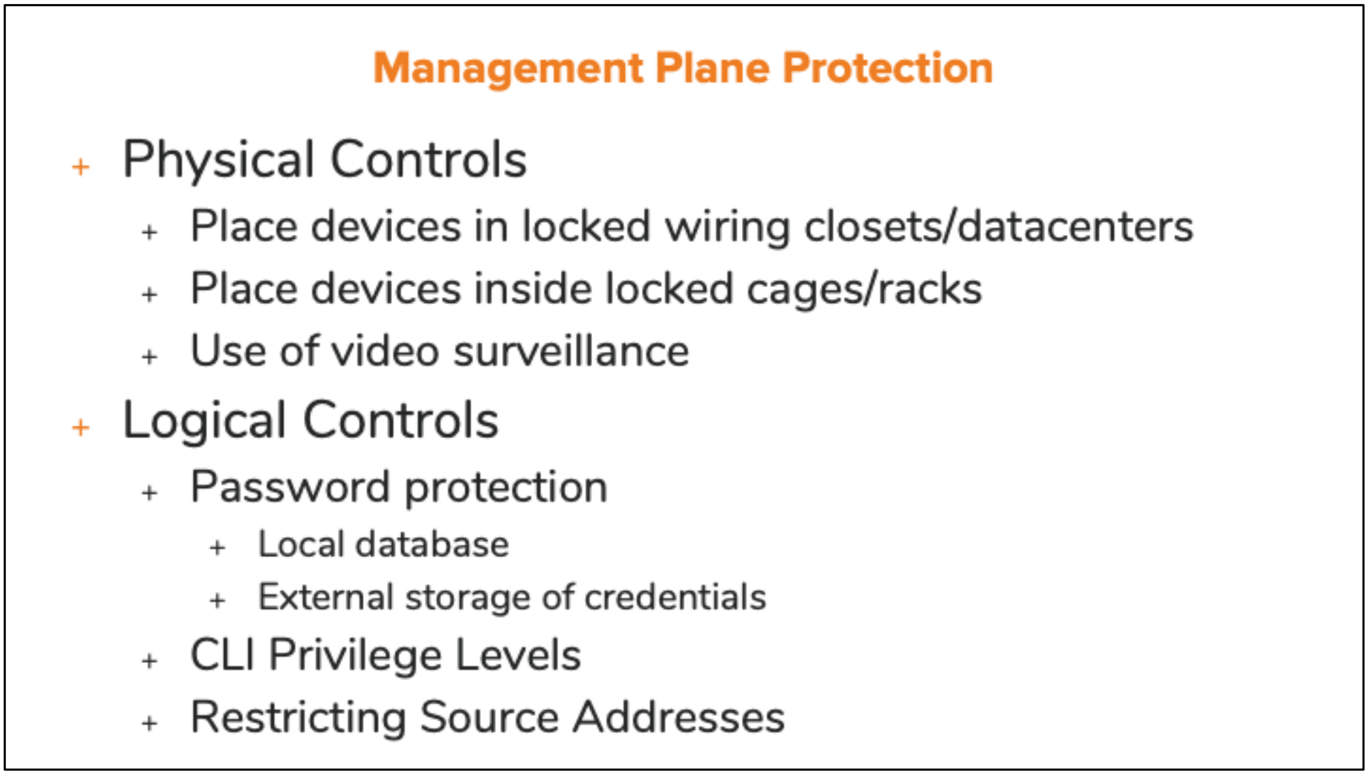
Topic Overview

- Securing Network Devices
- Management Plane Protection
- AAA Defined
- AAA Components
- Design Guidelines
- AAA Protocols
- Sample Configuration



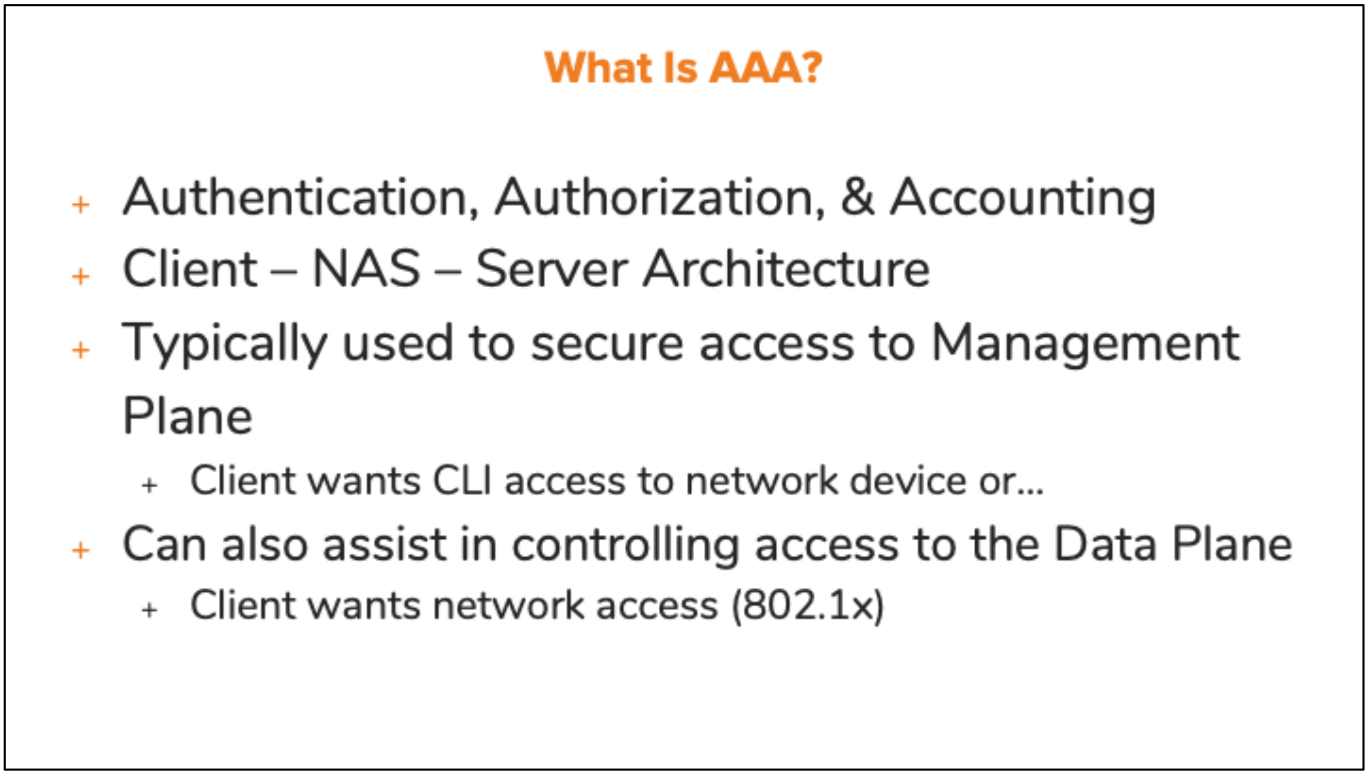
Securing Network Devices

- Three “planes” should be secured:
  - Data Plane: Path through which data flows
  - Control Plane: Path through which devices learn information
  - Management Plane: Path through which devices are managed (CLI or Web)
- Management plane protection is critical!
  - Secure your CLI and Web access to routers, switches, etc
- Methods of protection
  - Physical controls
  - Logical controls



Management Plane Protection

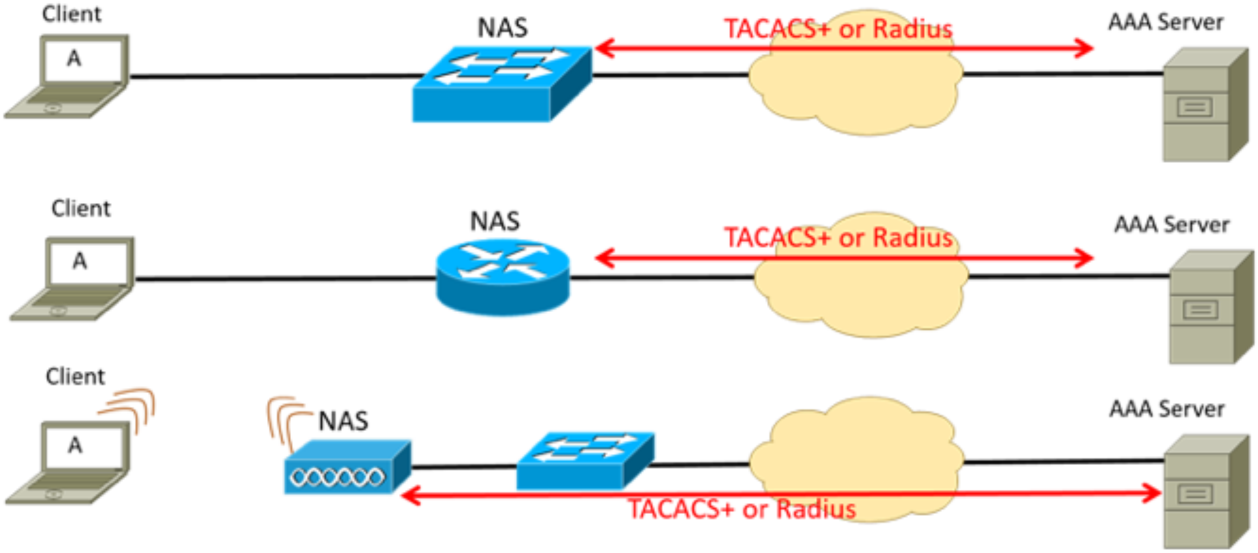
- Physical Controls
  - Place devices in locked wiring closets/datacenters
  - Place devices inside locked cages/racks
  - Use of video surveillance
- Logical Controls
  - Password protection
    - Local database
    - External storage of credentials
  - CLI Privilege Levels
  - Restricting Source Addresses

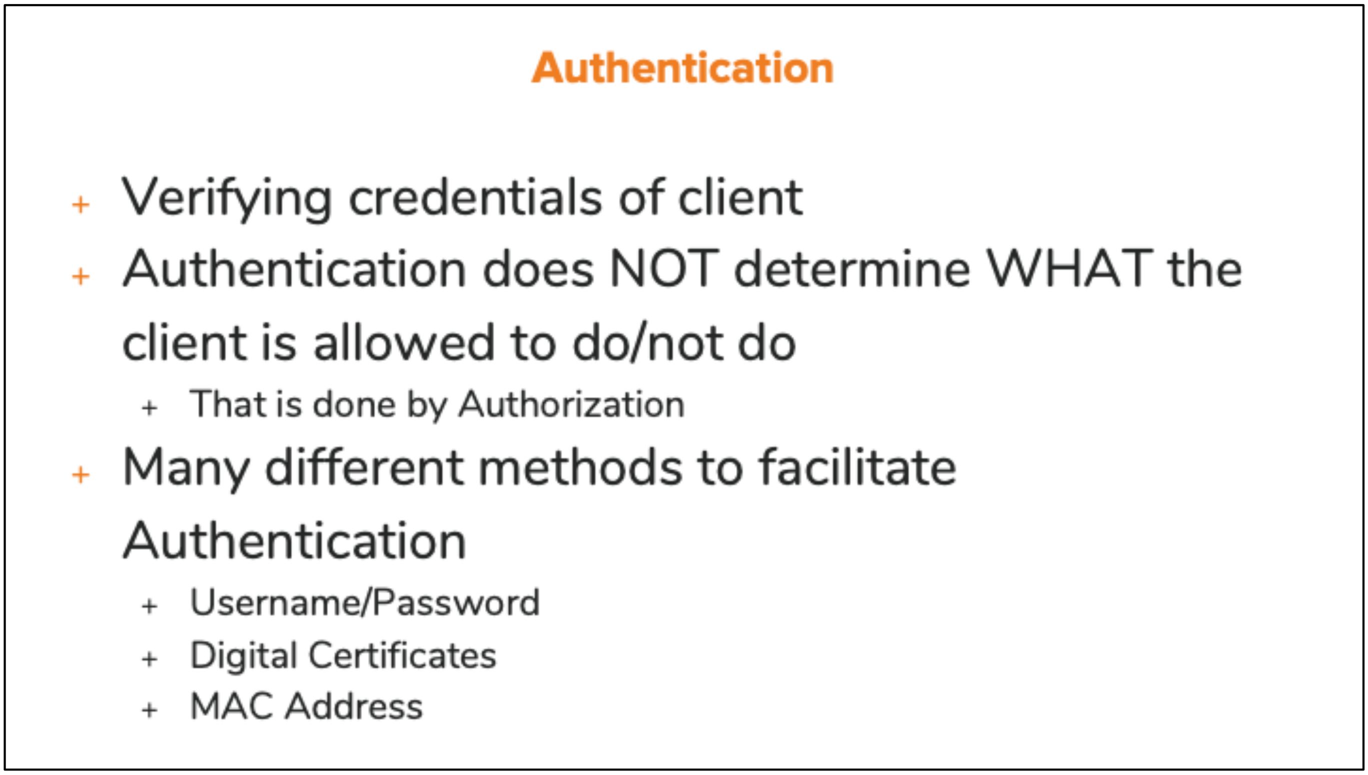


What Is AAA?

- Authentication, Authorization, & Accounting
- Client – NAS – Server Architecture
- Typically used to secure access to Management Plane
  - Client wants CLI access to network device or...
- Can also assist in controlling access to the Data Plane
  - Client wants network access (802.1x)

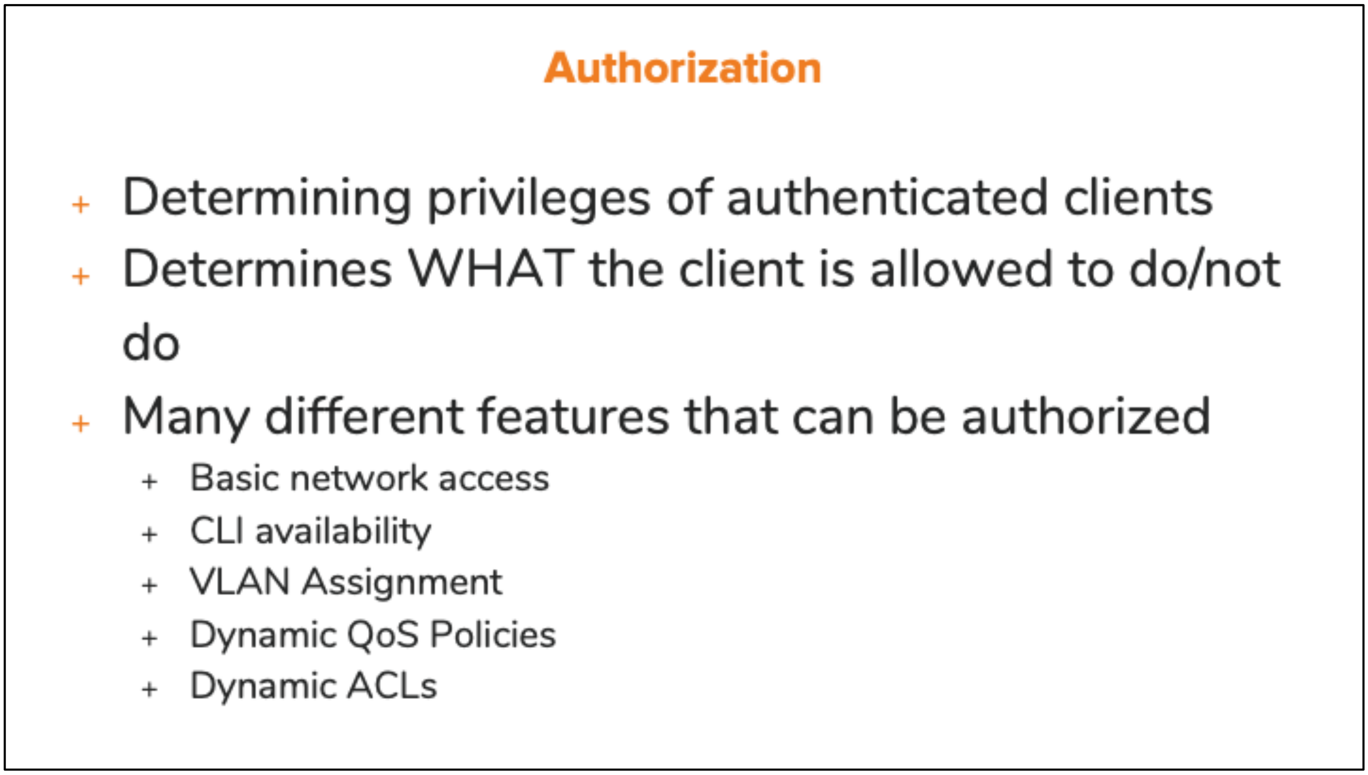
AAA Components





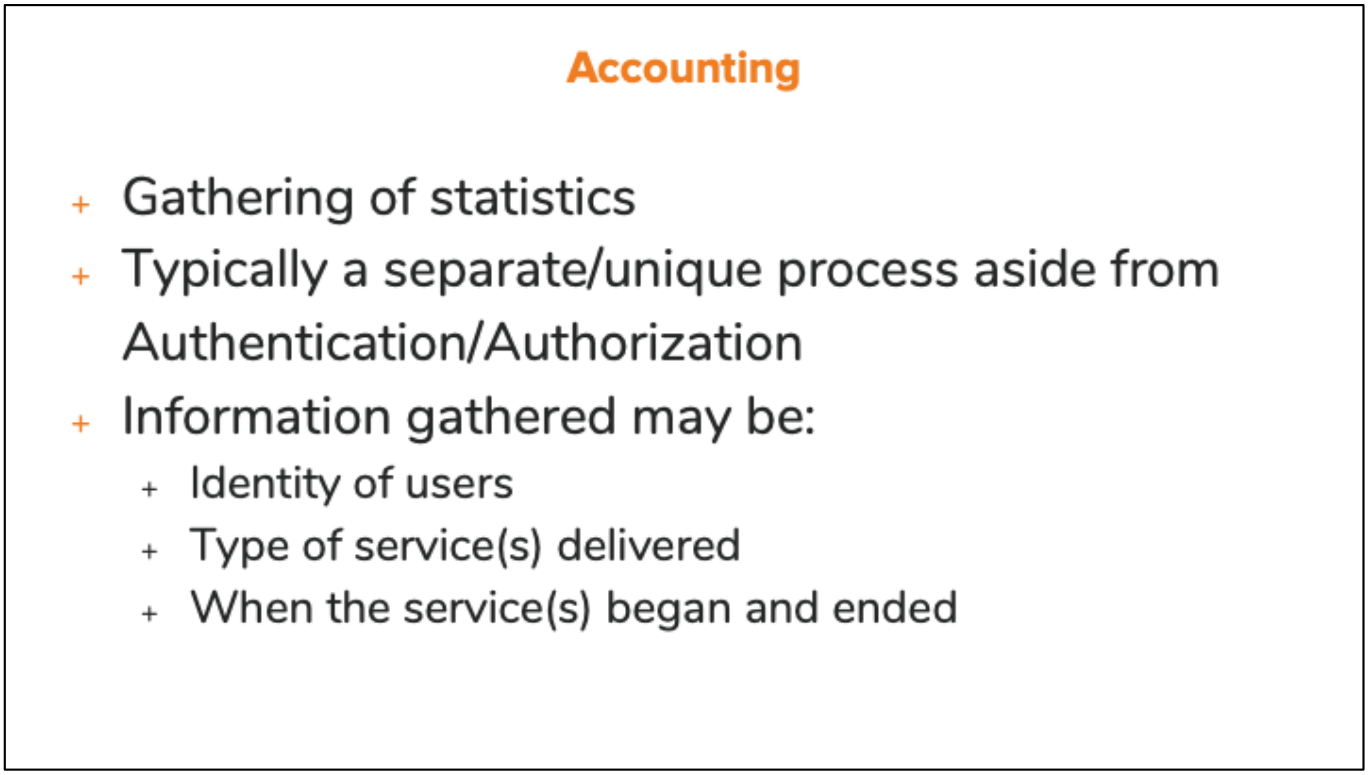
Authentication

- Verifying credentials of client
- Authentication does NOT determine WHAT the client is allowed to do/not do
  - That is done by Authorization
- Many different methods to facilitate Authentication
  - Username/Password
  - Digital Certificates
  - MAC Address



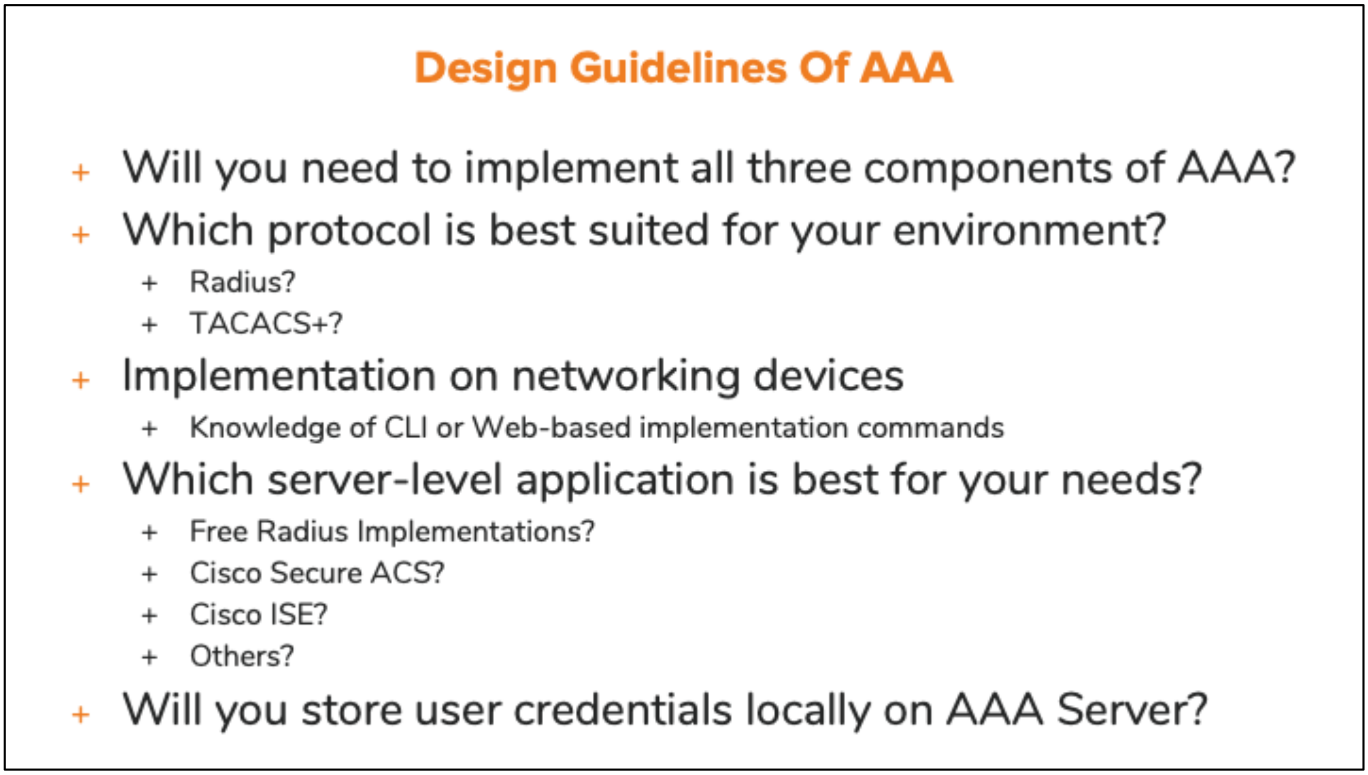
Authorization

- Determining privileges of authenticated clients
- Determines WHAT the client is allowed to do/not do
- Many different features that can be authorized
  - Basic network access
  - CLI availability
  - VLAN Assignment
  - Dynamic QoS Policies
  - Dynamic ACLs



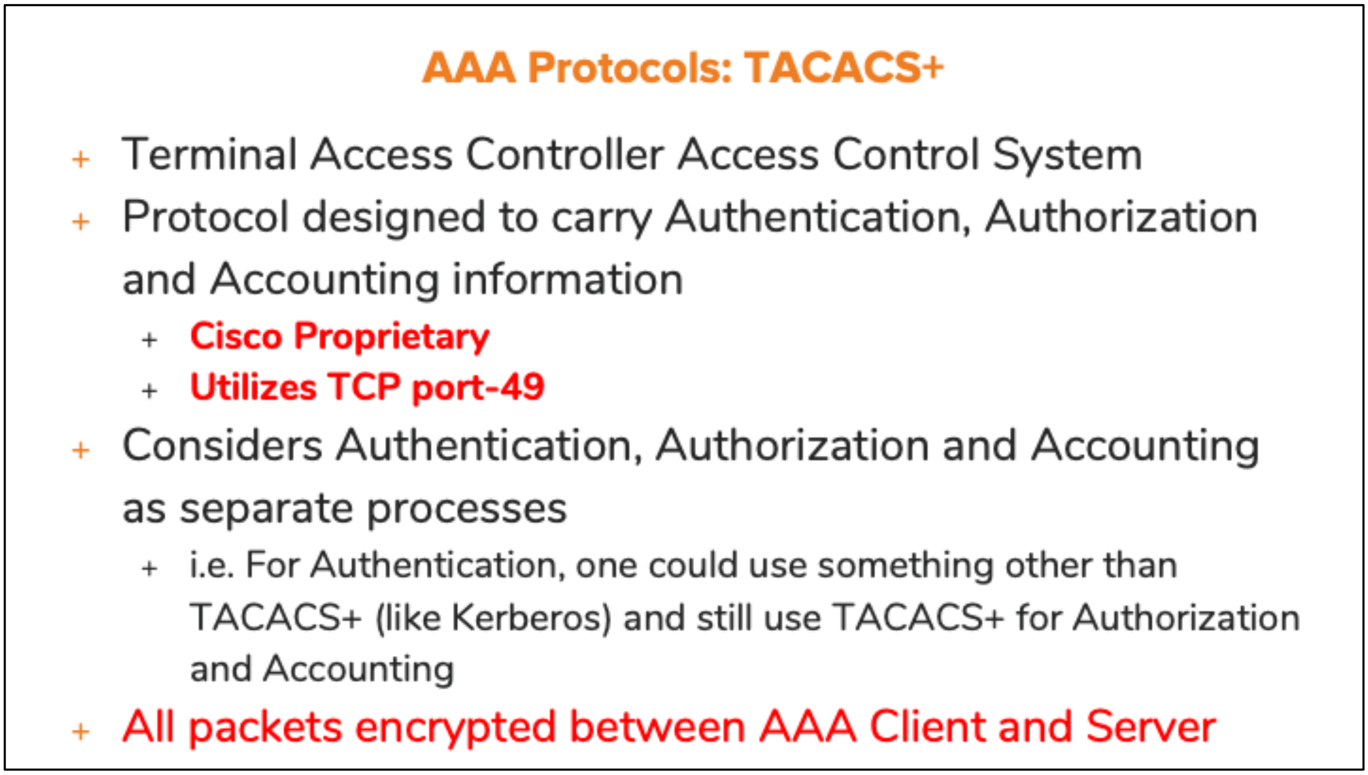
Accounting

- Gathering of statistics
- Typically a separate/unique process aside from Authentication/Authorization
- Information gathered may be:
  - Identity of users
  - Type of service(s) delivered
  - When the service(s) began and ended



Design Guidelines Of AAA

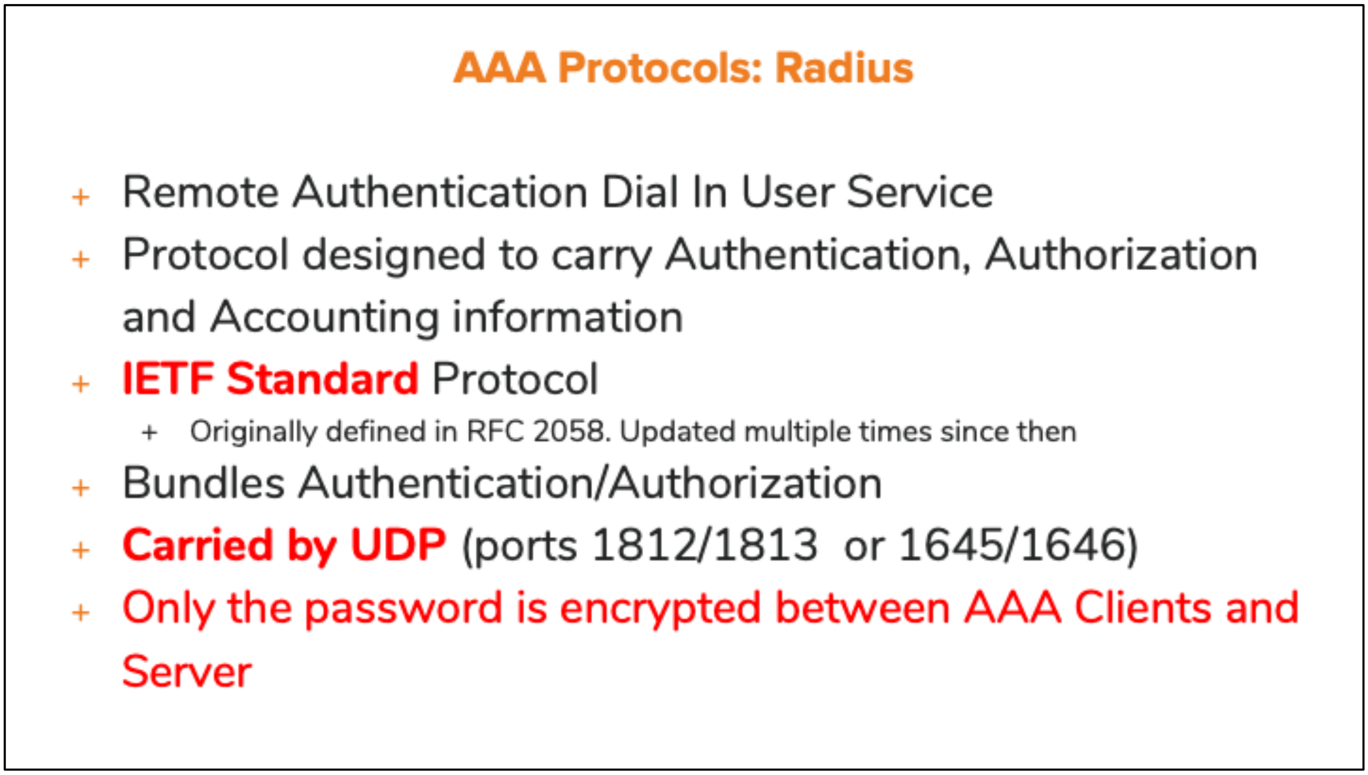
- Will you need to implement all three components of AAA?
- Which protocol is best suited for your environment?
  - Radius?
  - TACACS+?
- Implementation on networking devices
  - Knowledge of CLI or Web-based implementation commands
- Which server-level application is best for your needs?
  - Free Radius Implementations?
  - Cisco Secure ACS?
  - Cisco ISE?
  - Others?
- Will you store user credentials locally on AAA Server?



AAA Protocols: TACACS+

- Terminal Access Controller Access Control System
- Protocol designed to carry Authentication, Authorization and Accounting information
  - **Cisco Proprietary**
  - **Utilizes TCP port-49**
- Considers Authentication, Authorization and Accounting as separate processes
  - i.e. For Authentication, one could use something other than TACACS+ (like Kerberos) and still use TACACS+ for Authorization and Accounting
- All packets encrypted between AAA Client and Server

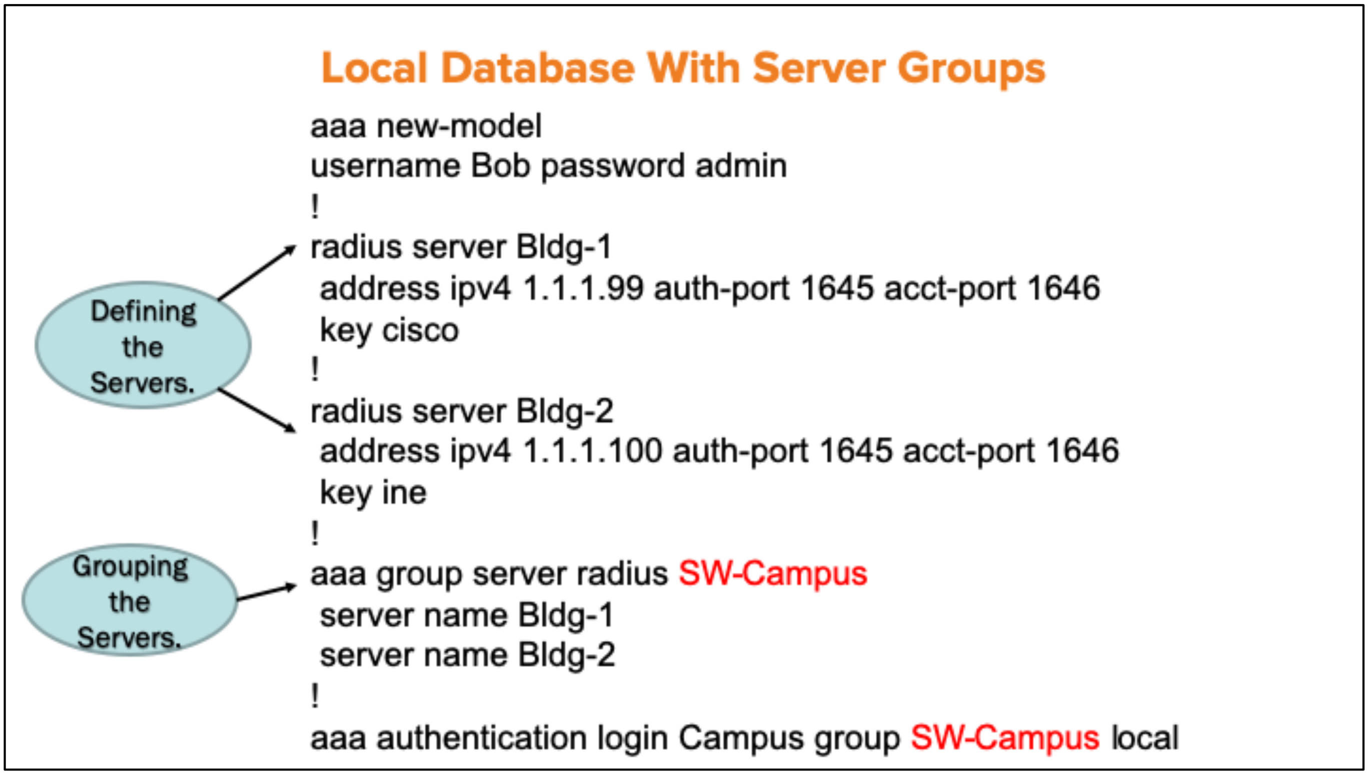
TACACS really designed to control which specific IOS commands a Network Admin is allowed access to.



AAA Protocols: Radius

- Remote Authentication Dial In User Service
- Protocol designed to carry Authentication, Authorization and Accounting information
- **IETF Standard** Protocol
  - Originally defined in RFC 2058. Updated multiple times since then
- Bundles Authentication/Authorization
- **Carried by UDP** (ports 1812/1813 or 1645/1646)
- Only the password is encrypted between AAA Clients and Server

Carried by UDP port 1812 (Authentication) and 1813 (Accounting)
…
Originally was UDP 1645 (Authentication) and 1646 (Accounting).
-
Original intent behind radius was to protect the Data Plane. Dialup users had to pass Radius Authentication/Authorization before being granted access to the Data Plane. Although it CAN protect the Management Plane…that is not its forte nor original purpose.
-
Generally acknowledged as providing more detailed and comprehensive Accounting support than



Local Database With Server Groups

Defining the Servers.

Grouping the Servers.

```
aaa new-model
username Bob password admin
!
radius server Bldg-1
 address ipv4 1.1.1.99 auth-port 1645 acct-port 1646
 key cisco
!
radius server Bldg-2
 address ipv4 1.1.1.100 auth-port 1645 acct-port 1646
 key ine
!
aaa group server radius SW-Campus
 server name Bldg-1
 server name Bldg-2
!
aaa authentication login Campus group SW-Campus local
```

In this configuration we’ve created a named-method list called, “Campus” that calls on all the Radius servers in the group called, “SW-Campus”.

Thanks for Watching!