Chapter 5: Network Security and Monitoring

CCNA Routing and Switching

Connecting Networks v6.0

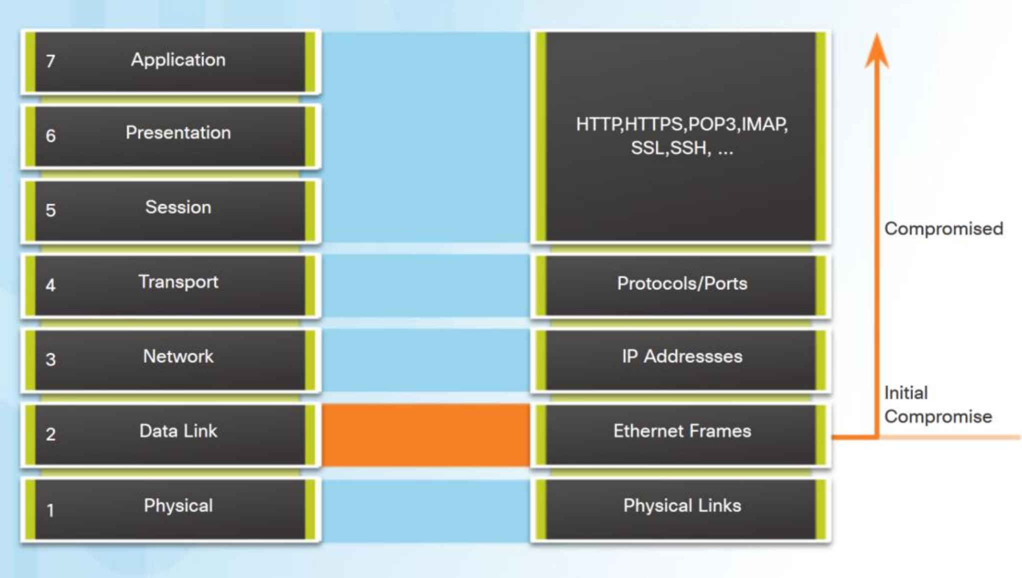
Chapter 5 - Sections & Objectives

- 5.1 LAN Security
- Explain how to mitigate common LAN security attacks.
  - Describe common LAN security attacks.
  - Explain how to use security best practices to mitigate LAN attacks.
- 5.2 SNMP
  - Configure SNMP to monitor network operations in a small to medium-sized business network.
    - Explain how SNMP operates.
    - Configure SNMP to compile network performance data.
- 5.3 Cisco Switch Port Analyzer (SPAN)
  - Troubleshoot a network problem using SPAN.
    - Explain the features and characteristics of SPAN.
    - Configure local SPAN.
    - Troubleshoot suspicious LAN traffic using SPAN.

5.1 LAN Security

Common LAN Attacks

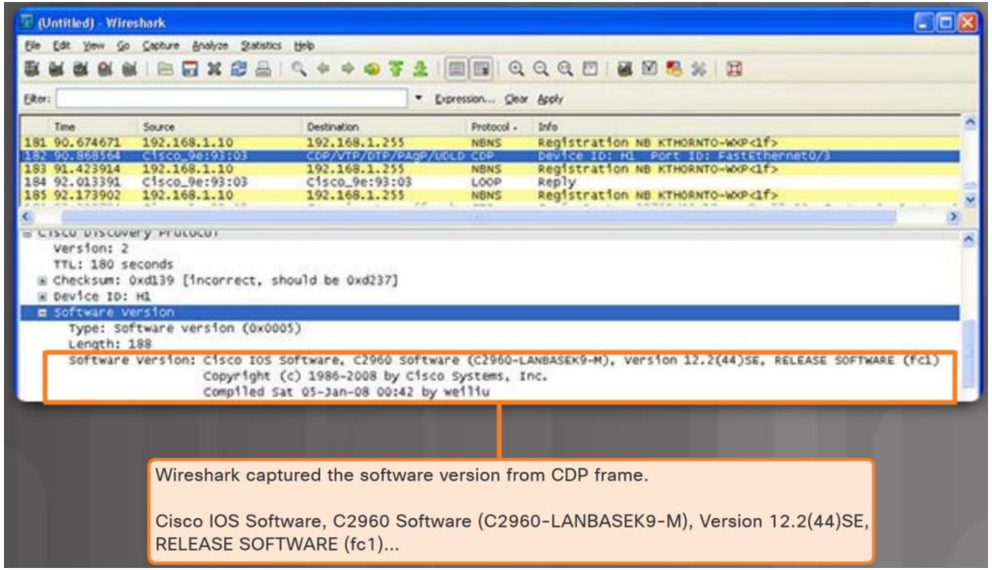
- Common security solutions using routers, firewalls, Intrusion Prevention System (IPSs), and VPN devices protect Layer 3 up through Layer 7.
- Layer 2 must also be protected.
- Common Layer 2 attacks include:
  - CDP Reconnaissance Attack
  - Telnet Attacks
  - MAC Address Table Flooding Attack
  - VLAN Attacks
  - DHCP Attacks



LAN Security Attacks

CDP Reconnaissance Attack

- The Cisco Discovery Protocol (CDP) is a proprietary Layer 2 link discovery protocol, enabled by default.
- CDP can automatically discover other CDP-enabled devices.
- CDP information can be used by an attacker.
- Use the **no cdp run** global configuration command to disable CDP globally.
- Use the **no cdp enable** interface configuration command to disable CDP on a port.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
    Time       Source           Destination           Protocol  Info
181 90.674671  192.168.1.10     192.168.1.255         NBNS      Registration NB KTHORNTO-WXP<1f>
182 90.868564  Cisco_9e:93:03   CDP/VTP/DTP/PAgP/UDLD CDP       Device ID: H1  Port ID: FastEthernet0/3
183 91.423914  192.168.1.10     192.168.1.255         NBNS      Registration NB KTHORNTO-WXP<1f>
184 92.013391  Cisco_9e:93:03   Cisco_9e:93:03        LOOP      Reply
185 92.173902  192.168.1.10     192.168.1.255         NBNS      Registration NB KTHORNTO-WXP<1f>
```

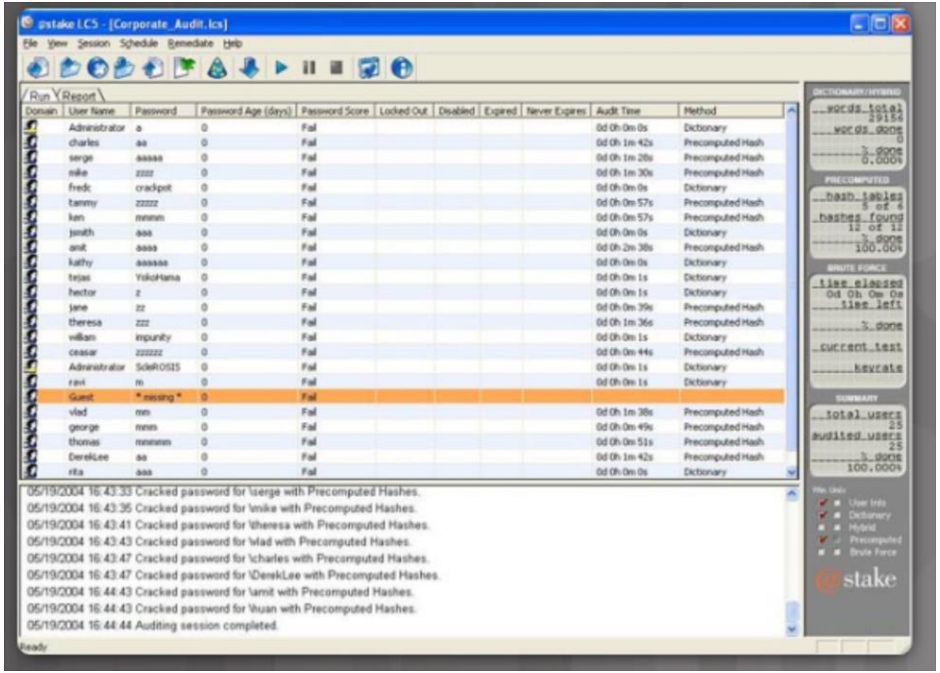
```
⊟ Cisco Discovery Protocol
    Version: 2
    TTL: 180 seconds
  ⊞ Checksum: 0xd139 [incorrect, should be 0xd237]
  ⊞ Device ID: H1
  ⊟ Software Version
      Type: Software version (0x0005)
      Length: 188
      Software Version: Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE, RELEASE SOFTWARE (fc1)
                        Copyright (c) 1986-2008 by Cisco Systems, Inc.
                        Compiled Sat 05-Jan-08 00:42 by weiliu
```

Wireshark captured the software version from CDP frame.

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE, RELEASE SOFTWARE (fc1)...

LAN Security Attacks

Telnet Attacks


@stake LC5 - [Corporate_Audit.lcs]
File View Session Schedule Remediate Help
Run
Report

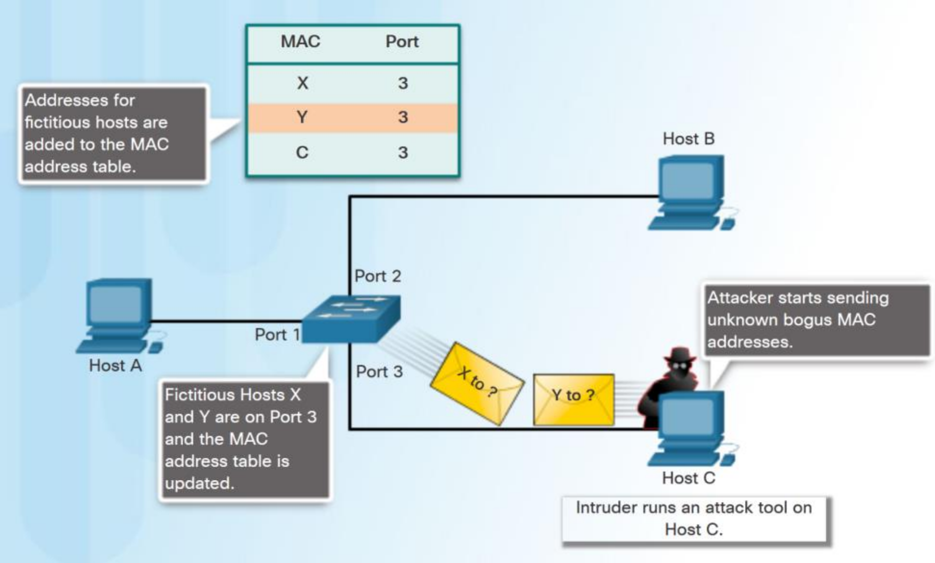
Domain	User Name	Password	Password Age (days)	Password Score	Locked Out	Disabled	Expired	Never Expires	Audit Time	Method
	Administrator	a	0	Fail					0d 0h 0m 0s	Dictionary
	charles	aa	0	Fail					0d 0h 1m 42s	Precomputed Hash
	serge	aaaaa	0	Fail					0d 0h 1m 20s	Precomputed Hash
	mike	zzzz	0	Fail					0d 0h 1m 30s	Precomputed Hash
	fredc	crackpot	0	Fail					0d 0h 0m 0s	Dictionary
	tammy	zzzzz	0	Fail					0d 0h 0m 57s	Precomputed Hash
	ken	mmmm	0	Fail					0d 0h 0m 57s	Precomputed Hash
	jsmith	aaa	0	Fail					0d 0h 0m 0s	Dictionary
	amit	aaaa	0	Fail					0d 0h 2m 38s	Precomputed Hash
	kathy	aaaaaa	0	Fail					0d 0h 0m 0s	Dictionary
	tejas	YokoHama	0	Fail					0d 0h 0m 1s	Dictionary
	hector	z	0	Fail					0d 0h 0m 1s	Dictionary
	jane	zz	0	Fail					0d 0h 0m 39s	Precomputed Hash
	theresa	zzz	0	Fail					0d 0h 1m 36s	Precomputed Hash
	william	impunity	0	Fail					0d 0h 0m 1s	Dictionary
	ceasar	zzzzzz	0	Fail					0d 0h 0m 44s	Precomputed Hash
	Administrator	ScleROSIS	0	Fail					0d 0h 0m 1s	Dictionary
	ravi	m	0	Fail					0d 0h 0m 1s	Dictionary
	Guest	* missing *	0	Fail						
	vlad	mm	0	Fail					0d 0h 1m 38s	Precomputed Hash
	george	mmm	0	Fail					0d 0h 0m 49s	Precomputed Hash
	thomas	mmmmm	0	Fail					0d 0h 0m 51s	Precomputed Hash
	DerekLee	aa	0	Fail					0d 0h 1m 42s	Precomputed Hash
	rita	aaa	0	Fail					0d 0h 0m 0s	Dictionary

```
05/19/2004 16:43:33 Cracked password for \serge with Precomputed Hashes.
05/19/2004 16:43:35 Cracked password for \mike with Precomputed Hashes.
05/19/2004 16:43:41 Cracked password for \theresa with Precomputed Hashes.
05/19/2004 16:43:43 Cracked password for \vlad with Precomputed Hashes.
05/19/2004 16:43:47 Cracked password for \charles with Precomputed Hashes.
05/19/2004 16:43:47 Cracked password for \DerekLee with Precomputed Hashes.
05/19/2004 16:44:43 Cracked password for \amit with Precomputed Hashes.
05/19/2004 16:44:43 Cracked password for \huan with Precomputed Hashes.
05/19/2004 16:44:44 Auditing session completed.
```

```
DICTIONARY/HYBRID
words total      29156
words done           0
% done          0.000%
PRECOMPUTED
hash tables     5 of 6
hashes found  12 of 12
% done        100.000%
BRUTE FORCE
time elapsed  0d 0h 0m 0s
time left
% done
current test
keyrate
SUMMARY
total users         25
audited users       25
% done        100.000%
```

- There are two types of Telnet attacks:
  - **Brute Force Password Attack** - trial-and-error method used to obtain the administrative password.
  - **Telnet DoS Attack** - Attacker continuously requests Telnet connections in an attempt to render the Telnet service unavailable.
- To mitigate these attacks:
  - Use SSH
  - Use strong passwords that are changed frequently.
  - Limit access to the vty lines using an access control list (ACL)
  - Use AAA with either TACACS+ or RADIUS protocols.

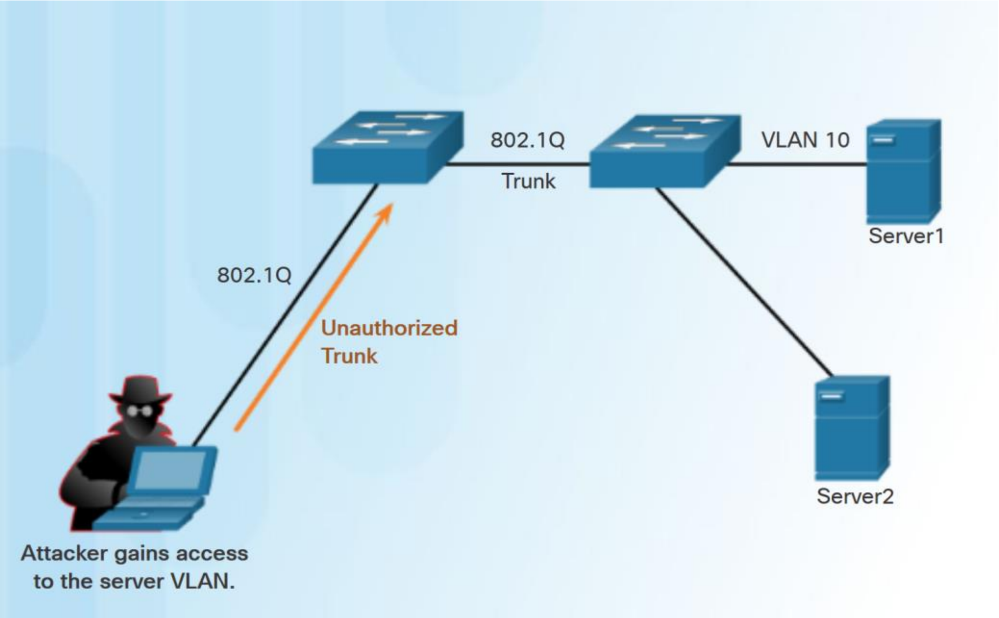
MAC Address Table Flooding Attack


Addresses for fictitious hosts are added to the MAC address table.
MAC
Port
X
3
Y
3
C
3
Host B
Port 2
Host A
Port 1
Port 3
X to ?
Y to ?
Attacker starts sending unknown bogus MAC addresses.
Fictitious Hosts X and Y are on Port 3 and the MAC address table is updated.
Host C
Intruder runs an attack tool on Host C.

- Common LAN switch attack is the MAC address table flooding attack.
  - An attacker sends fake source MAC addresses until the switch MAC address table is full and the switch is overwhelmed.
  - Switch is then in fail-open mode and broadcasts all frames, allowing the attacker to capture those frames.
- Configure port security to mitigate these attacks.

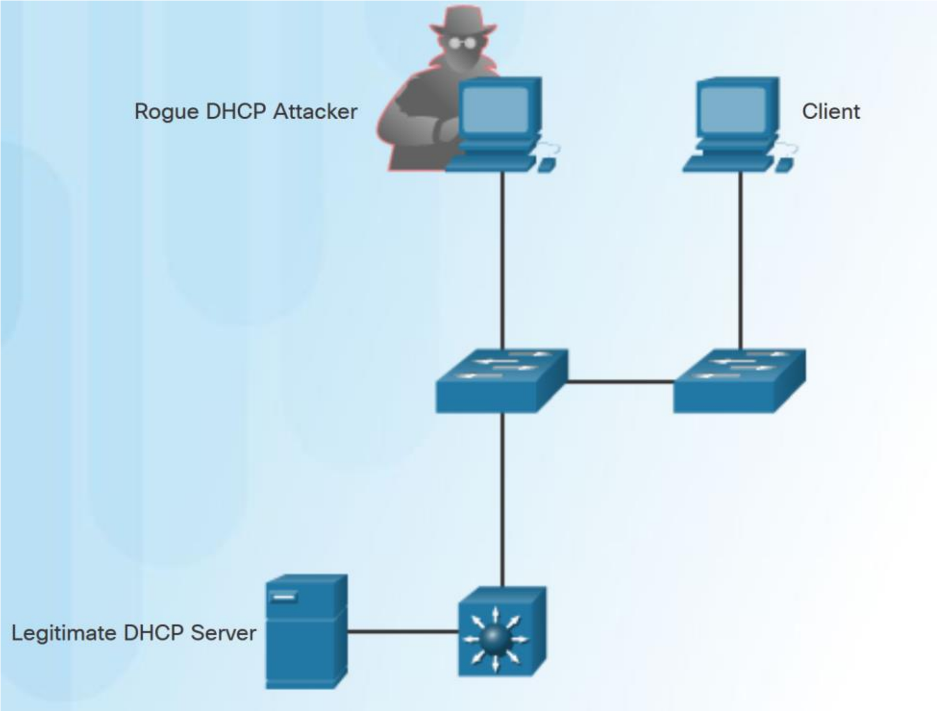
VLAN Attacks

- Switch spoofing attack - an example of a VLAN attack.
  - Attacker can gain VLAN access by configuring a host to spoof a switch and use the 802.1Q trunking protocol and DTP to trunk with the connecting switch.
- Methods to mitigate VLAN attacks:
  - Explicitly configure access links.
  - Disable auto trunking.
  - Manually enable trunk links.
  - Disable unused ports, make them access ports, and assign to a black hole VLAN.
  - Change the default native VLAN.
  - Implement port security.



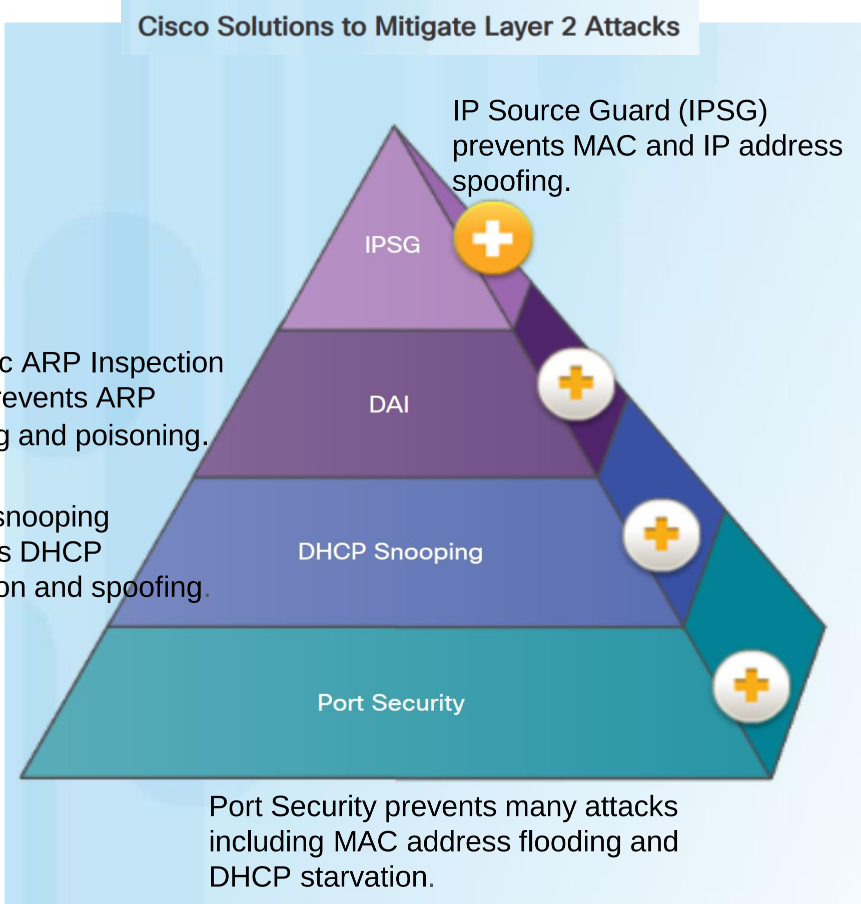
DHCP Attacks

- **DHCP spoofing attack** - An attacker configures a fake DHCP server on the network to issue IP addresses to clients.
- **DHCP starvation attack** - An attacker floods the DHCP server with bogus DHCP requests and leases all of the available IP addresses. This results in a denial-of-service (DoS) attack as new clients cannot obtain an IP address.
- Methods to mitigate DHCP attacks:
  - Configure DHCP snooping
  - Configure port security



Secure the LAN

- Strategies to help secure Layer 2 of a network:
  - Always use secure variants of protocols such as SSH, SCP, and SSL.
  - Use strong passwords and change often.
  - Enable CDP on select ports only.
  - Secure Telnet access.
  - Use a dedicated management VLAN
  - Use ACLs to filter unwanted access.



IP Source Guard (IPSG) prevents MAC and IP address spoofing.

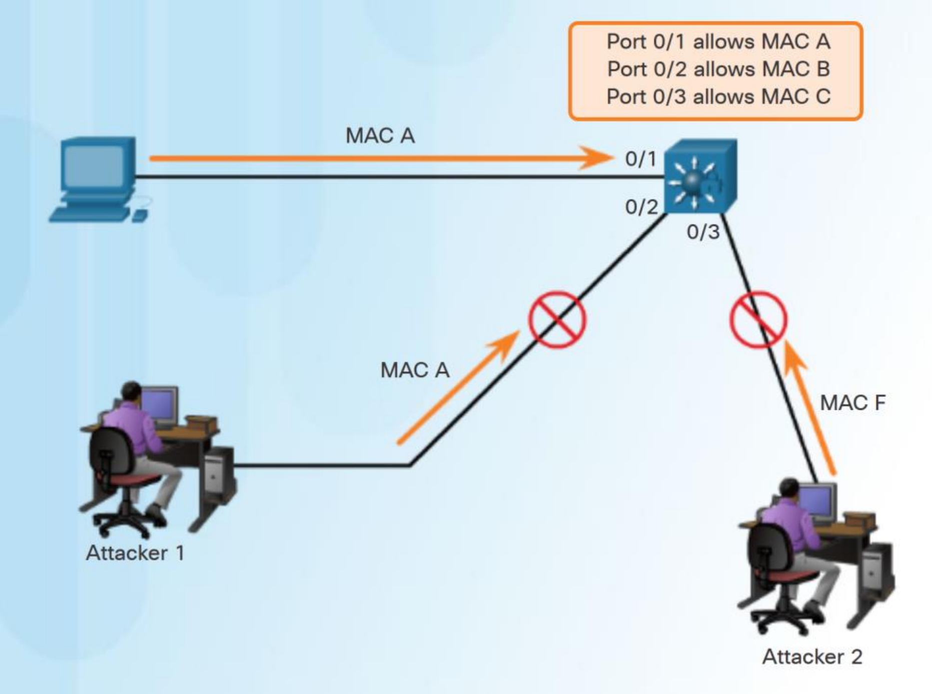
Dynamic ARP Inspection (DAI) prevents ARP spoofing and poisoning.

DHCP snooping prevents DHCP starvation and spoofing.

Port Security prevents many attacks including MAC address flooding and DHCP starvation.

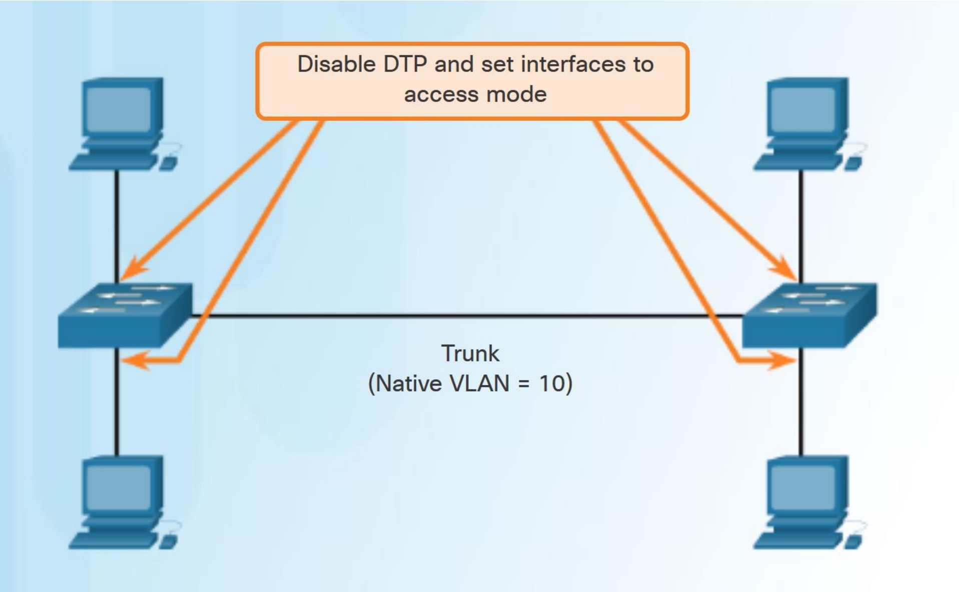
LAN Security Best Practices

Mitigate MAC Address Flooding Table Attacks



- Enable port security to prevent MAC table flooding attacks.
- Port security allows an administrator to do the following:
  - statically specify MAC addresses for a port.
  - permit the switch to dynamically learn a limited number of MAC addresses.
  - when the maximum number of MAC addresses is reached, any additional attempts to connect by unknown MAC addresses will generate a security violation.

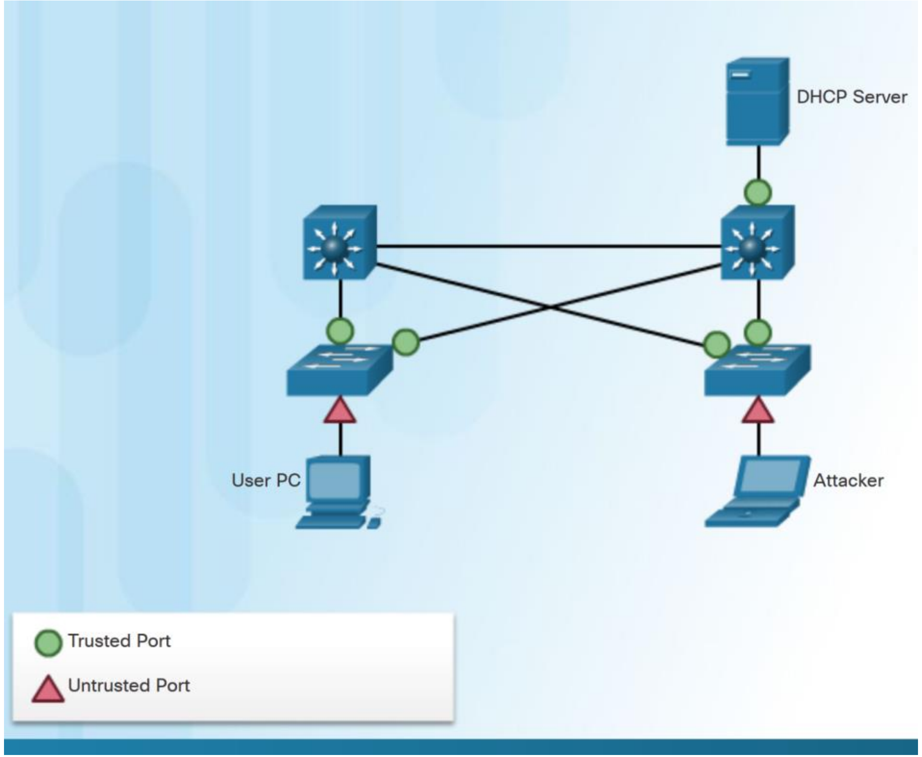
Mitigate VLAN Attacks



- To prevent basic VLAN attacks:
  - Disable DTP (auto trunking) negotiations on non-trunk ports and use **switchport mode access.**
  - Manually enable trunk links using **switchport mode trunk.**
  - Disable DTP (auto trunking) negotiations on trunking and non-trunking ports using **switchport nonegotiate.**
  - Change the native VLAN from VLAN 1.
  - Disable unused ports and assign them to an unused VLAN.

Mitigate DHCP Attacks

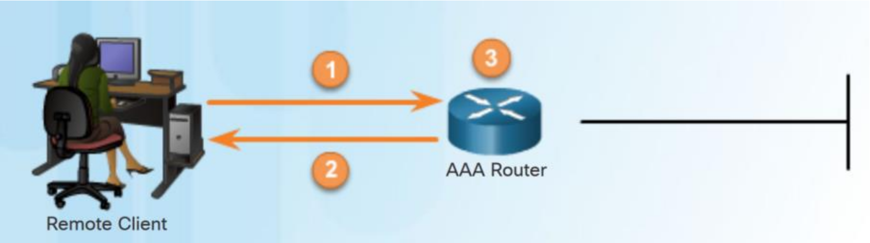
- To prevent DHCP attacks use DHCP snooping.
- With DHCP snooping enabled on an interface, the switch will deny packets containing:
  - Unauthorized DHCP server messages coming from an untrusted port.
  - Unauthorized DHCP client messages not adhering to the DHCP Snooping Binding Database or rate limits.
- DHCP snooping recognizes two types of ports:
  - **Trusted DHCP ports** - Only ports connecting to upstream DHCP servers should be trusted.
  - **Untrusted ports** - These ports connect to hosts that should not be providing DHCP server messages.



Secure Administrative Access using AAA

- Local AAA Authentication

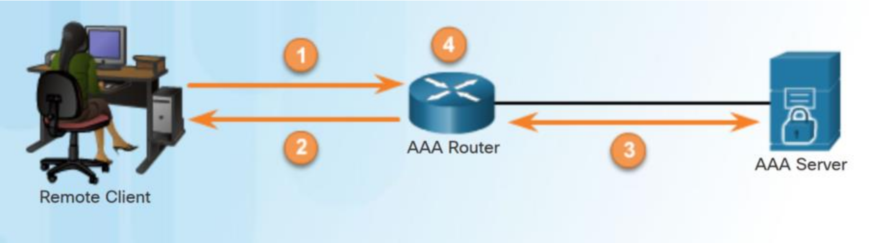
  1. Client establishes a connection with the router.
  2. AAA router prompts the user for username and password.
  3. Router authenticates the username and password using the local database, and allows user access.



- Server-Based AAA Authentication

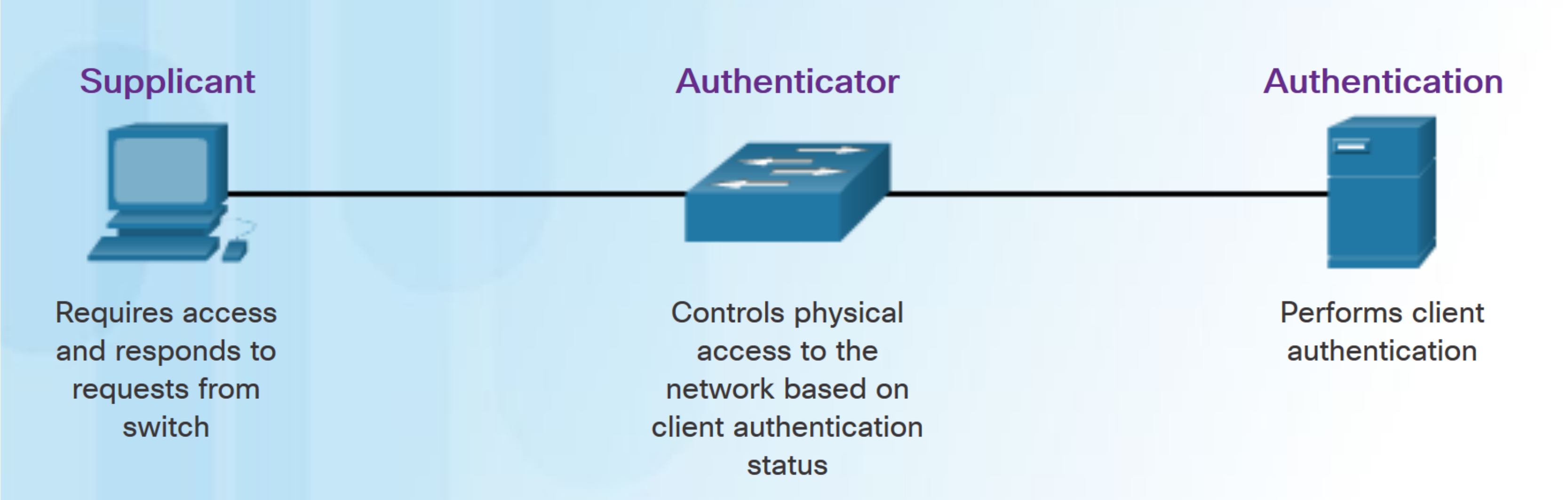
  1. Client establishes a connection with the router.
  2. AAA router prompts the user for a username and password.
  3. The router authenticates the username and password using a remote AAA server.

- The AAA router uses Terminal Access Controller Access Control System (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) protocol to communicate with the AAA server.



Secure Device Access using 802.1X

- IEEE 802.1X standard defines a port-based access control and authentication protocol.
  - Restricts unauthorized workstations from connecting to a LAN.
  - The authentication server authenticates each workstation connected to a switch port before making any services available.

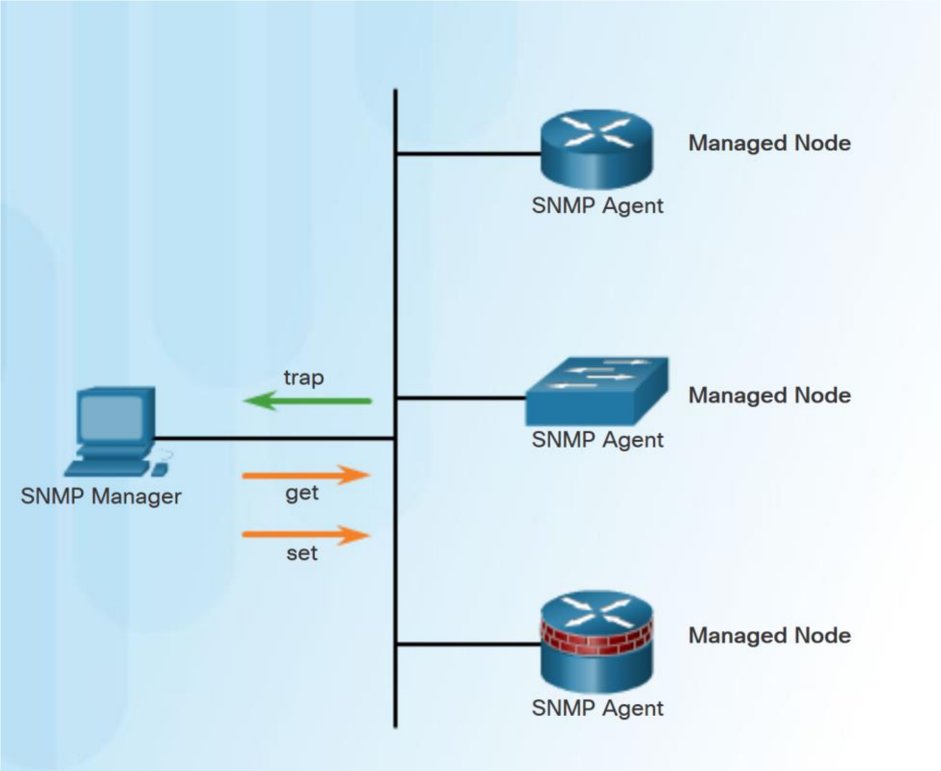

Supplicant
Requires access and responds to requests from switch
Authenticator
Controls physical access to the network based on client authentication status
Authentication
Performs client authentication

5.2 SNMP

SNMP Operation

Introduction to SNMP

- Simple Network Management Protocol (SNMP) enables network administrators to monitor and manage network nodes.
- The SNMP system consists of three elements:
  - **SNMP manager-** collects information from an SNMP agent using the “get” action. Changes configurations on an agent using the “set” action.
  - **SNMP agents** (managed node)
  - **Management Information Base (MIB)-** stores data and operational statistics about the managed device.



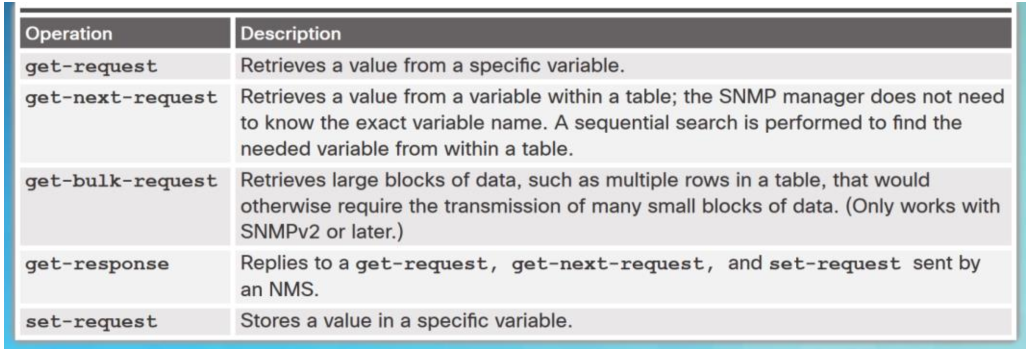
SNMP Operation

- SNMP agents that reside on managed devices collect and store information about the device.

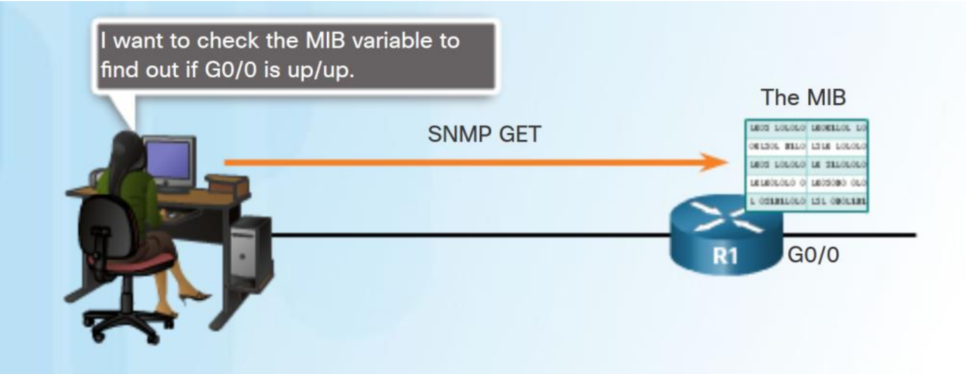
- This information is stored by the agent locally in the MIB.

- SNMP manager then uses the SNMP agent to access information within the MIB.

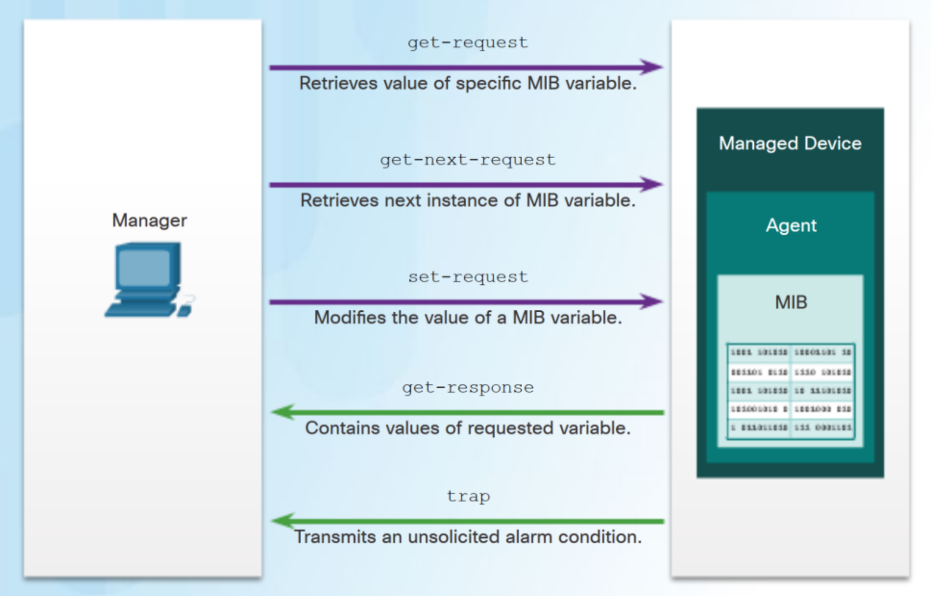
- SNMP agent responds to SNMP manager requests as follows:
  - **Get an MIB variable** - The SNMP agent performs this n response to a GetRequest-PDU from the network manager.
  - **Set an MIB variable** - The SNMP agent performs this in response to a SetRequest-PDU from the network manager.



Operation	Description
`get-request`	Retrieves a value from a specific variable.
`get-next-request`	Retrieves a value from a variable within a table; the SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
`get-bulk-request`	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (Only works with SNMPv2 or later.)
`get-response`	Replies to a `get-request`, `get-next-request`, and `set-request` sent by an NMS.
`set-request`	Stores a value in a specific variable.


I want to check the MIB variable to find out if G0/0 is up/up.
SNMP GET
The MIB
R1
G0/0

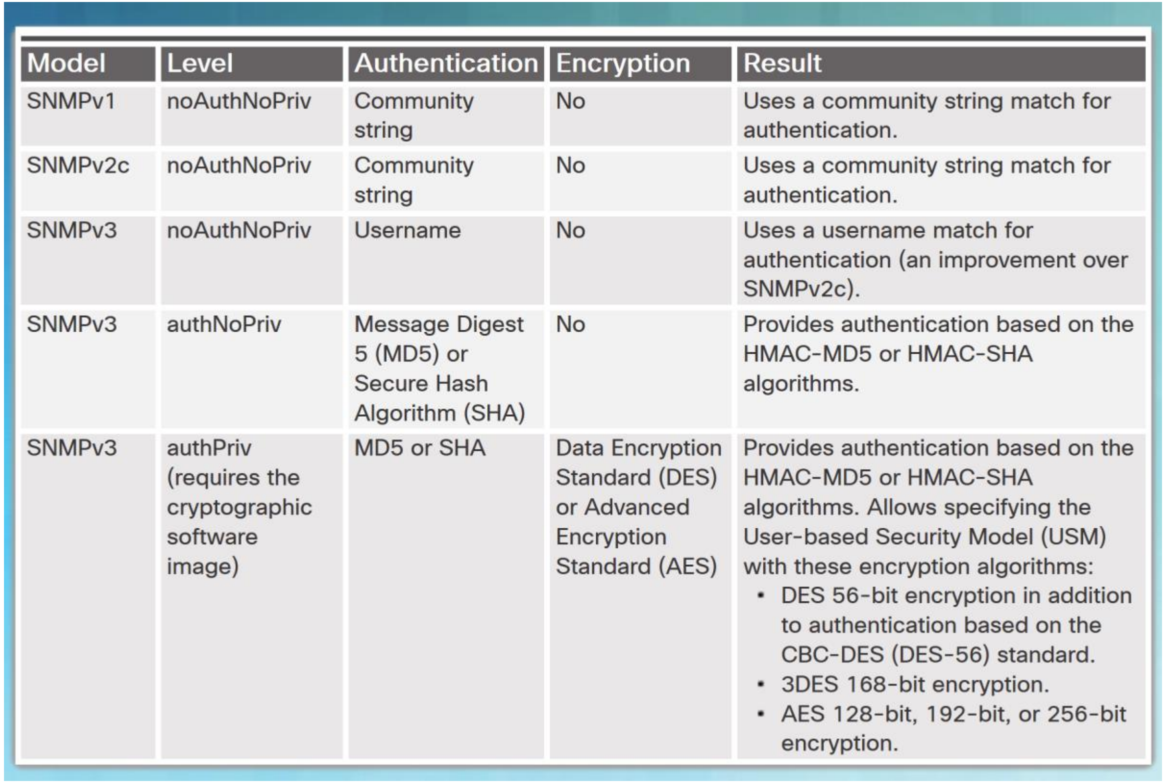
SNMP Agent Traps


Manager
get-request
Retrieves value of specific MIB variable.
get-next-request
Retrieves next instance of MIB variable.
set-request
Modifies the value of a MIB variable.
get-response
Contains values of requested variable.
trap
Transmits an unsolicited alarm condition.
Managed Device
Agent
MIB

- An Network Management System (NMS) periodically polls the SNMP agents using the get request.
- Using this process, SNMP can collect information to monitor traffic loads and to verify device configurations of managed devices.
- SNMP agents to generate and send traps to inform the NMS immediately of certain events.
  - Traps are unsolicited messages alerting the SNMP manager to a condition or event such as improper user authentication or link status.

SNMP Operation

SNMP Versions



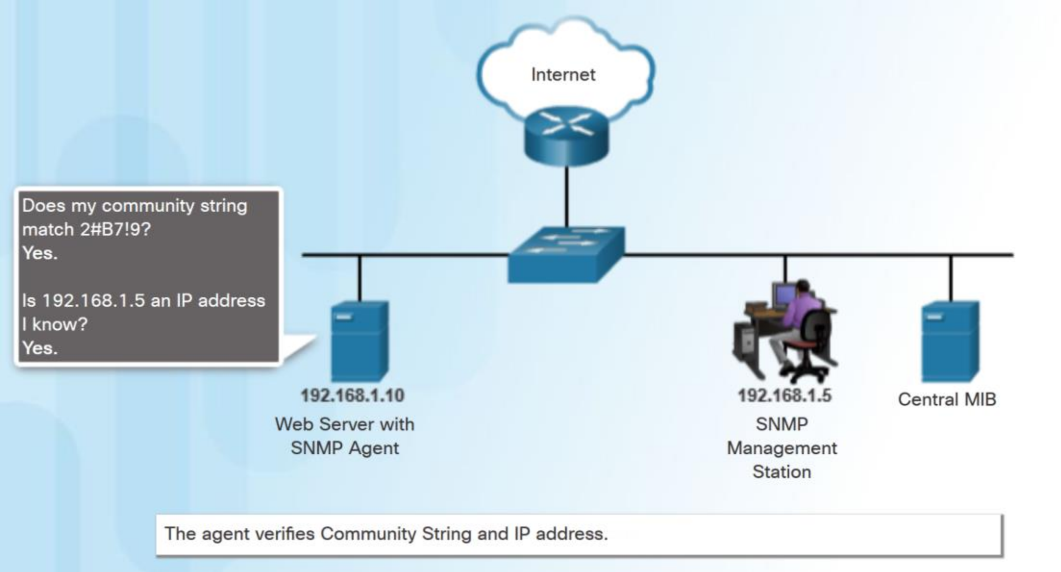
Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication (an improvement over SNMPv2c).
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv (requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: • DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. • 3DES 168-bit encryption. • AES 128-bit, 192-bit, or 256-bit encryption.

- All versions use SNMP managers, agents, and MIBs, this course focuses on versions 2c and 3.
- A network administrator must configure the SNMP agent to use the SNMP version supported by the management station.

SNMP Operation

Community Strings

- SNMPv1 and SNMPv2c use community strings that control access to the MIB.
- Two types of community strings:
  - **Read-only (ro)** - Provides access to the MIB variables, but no changes can be made.
  - **Read-write (rw**) - Provides read and write access to all objects in the MIB.



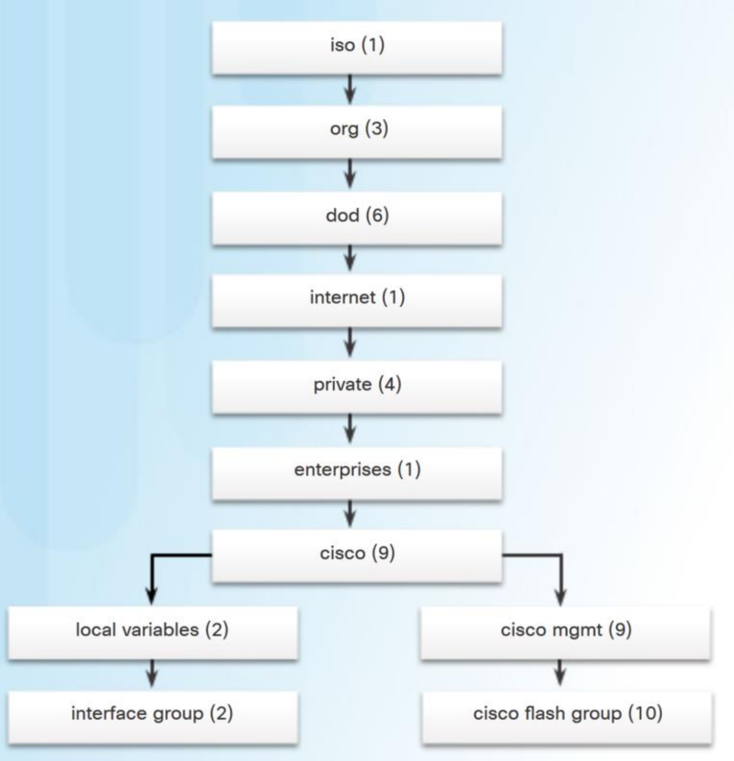
Does my community string match 2#B7!9?
Yes.

Is 192.168.1.5 an IP address I know?
Yes.

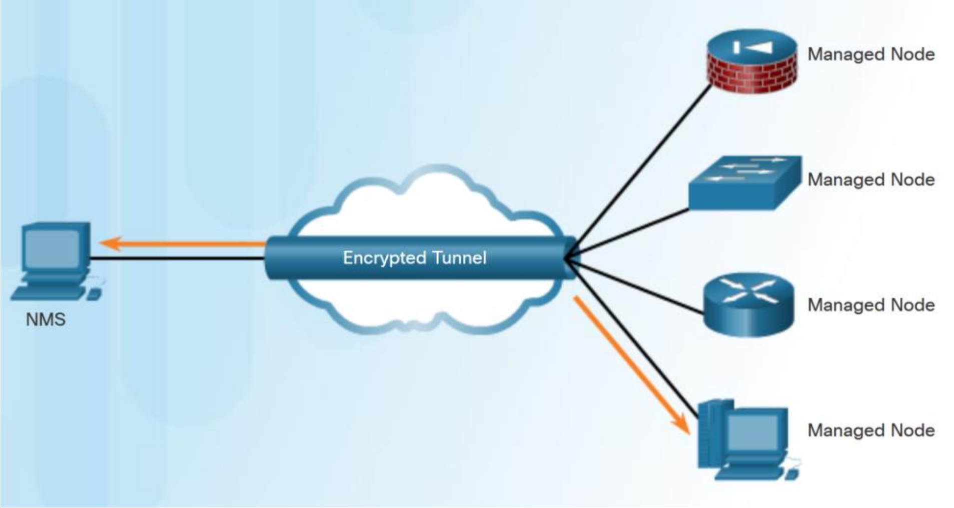
The agent verifies Community String and IP address.

Management Information Base Object ID

- The MIB defines each variable as an object ID (OID).
  - OIDs uniquely identify managed objects.
  - OIDs are organized based on RFC standards into a hierarchy or tree.
- Most devices implement RFC defined common public variables.
  - Vendors such as Cisco can define private branches on the tree to accommodate their own variables.
- CPU is one of the key resources, it should be measured continuously.
  - An SNMP graphing tool can periodically poll SNMP agents, and graph the values.
  - The data is retrieved via the snmpget utility.

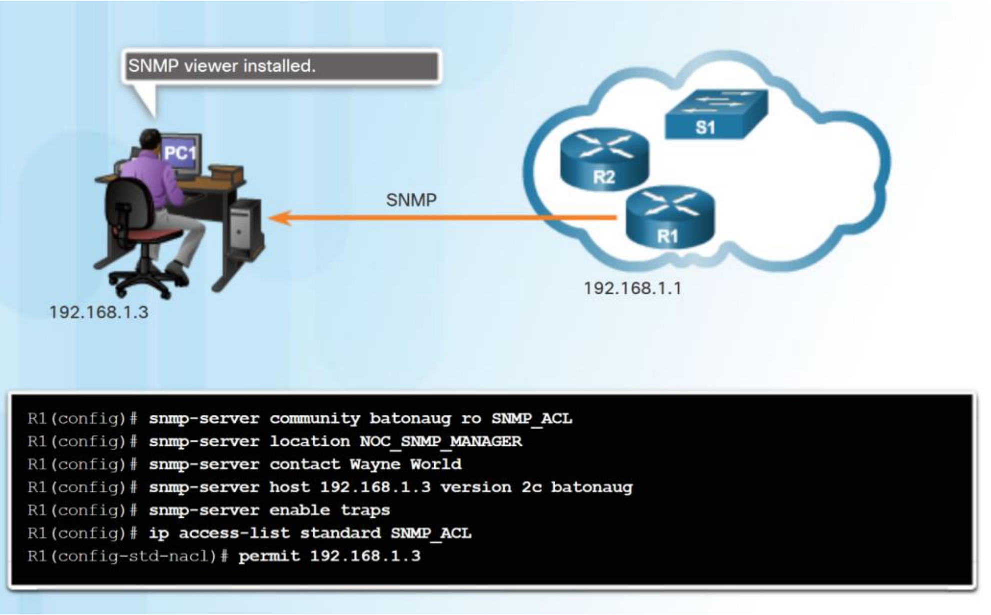


SNMPv3



- SNMPv3 authenticates and encrypts packets over the network to provide secure access to devices.
- SNMPv3 provides three security features:
  - **Message integrity and authentication** - Transmissions from the SNMP manager to agents (managed nodes) can be authenticated.
  - **Encryption** - SNMPv3 messages may be encrypted to ensure privacy.
  - **Access control** - Restricts SNMP managers to certain actions on specific portions of data.

Steps for Configuring SNMP

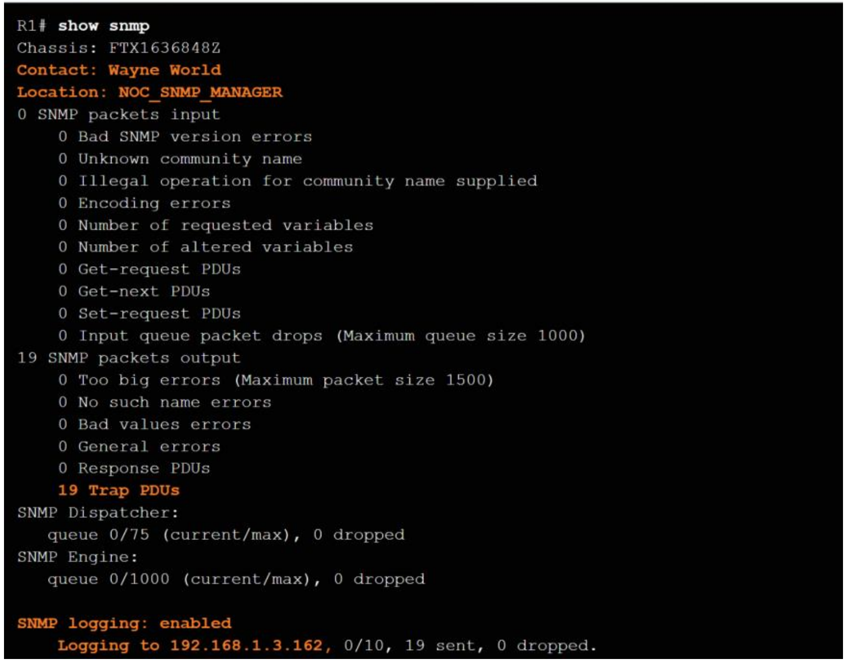


```
R1(config)# snmp-server community batonaug ro SNMP_ACL
R1(config)# snmp-server location NOC_SNMP_MANAGER
R1(config)# snmp-server contact Wayne World
R1(config)# snmp-server host 192.168.1.3 version 2c batonaug
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.1.3
```

- Basic steps to configuring SNMP:

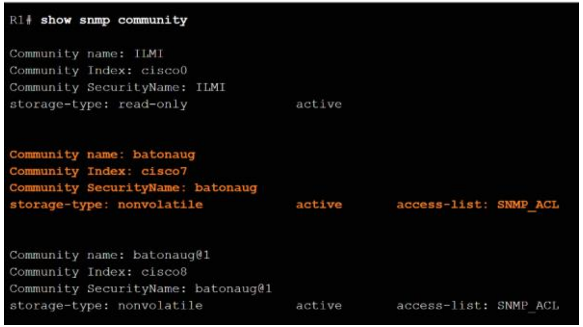
1. Configure the community string and access level using **snmp-server community** *string* **ro | rw** command.
2. (Optional) Document the location of the device using the **snmp-server location** *text* command.
3. (Optional) Document the system contact using the **snmp-server contact** *text* command.
4. (Optional)Use an ACL to restrict SNMP access to NMS hosts (SNMP managers). Reference the ACL using **snmp-server community** *string access-list-number-or-name.*

Verifying SNMP Configuration



```
R1# show snmp
Chassis: FTX1636848Z
Contact: Wayne World
Location: NOC_SNMP_MANAGER
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
19 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    19 Trap PDUs
SNMP Dispatcher:
   queue 0/75 (current/max), 0 dropped
SNMP Engine:
   queue 0/1000 (current/max), 0 dropped

SNMP logging: enabled
    Logging to 192.168.1.3.162, 0/10, 19 sent, 0 dropped.
```

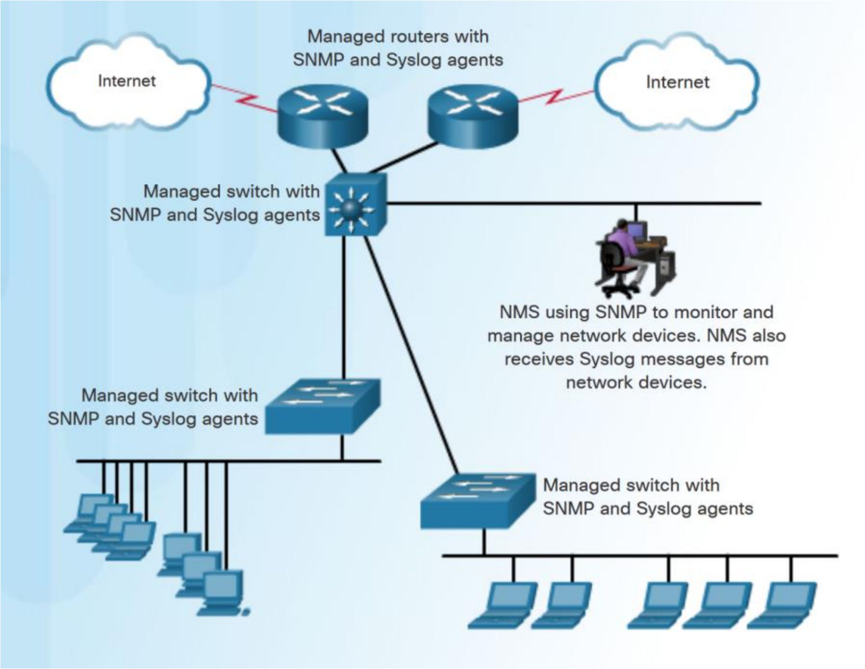
- Kiwi Syslog Server is one of several solutions that display SNMP output.
- The SNMP traps are sent to the SNMP manager and displayed on the syslog server.
- To verify the SNMP configuration use the **show snmp** command.
- Use the **show snmp community** command to show SNMP community string and ACL information.



```
R1# show snmp community

Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only            active


Community name: batonaug
Community Index: cisco7
Community SecurityName: batonaug
storage-type: nonvolatile          active       access-list: SNMP_ACL


Community name: batonaug@1
Community Index: cisco8
Community SecurityName: batonaug@1
storage-type: nonvolatile          active       access-list: SNMP_ACL
```

SNMP Best Practices

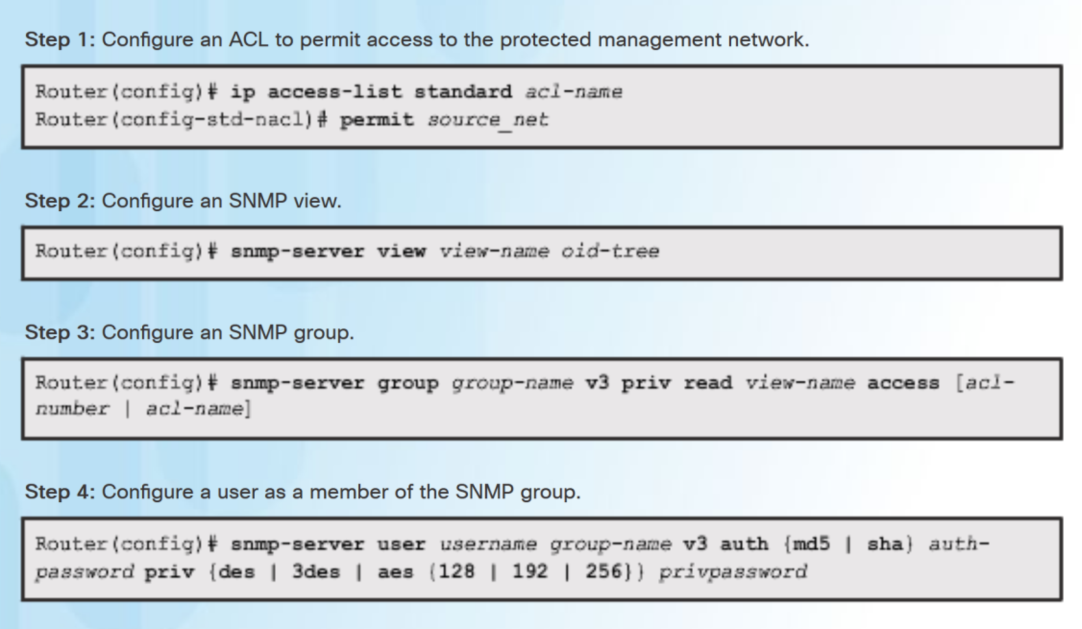
- SNMP can create security vulnerabilities.
- For SNMPv1 and SNMPv2c - community strings should be strong and changed frequently.
- ACLs should be used to prevent SNMP messages from going beyond the required devices and to limit access to monitored devices.
- SNMPv3 is recommended because it provides security authentication and encryption.
  - The **snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} command creates a new SNMP group on the device.
  - The **snmp-server user** *username groupname* command is used to add a new user to the group.


Internet
Managed routers with SNMP and Syslog agents
Internet
Managed switch with SNMP and Syslog agents
NMS using SNMP to monitor and manage network devices. NMS also receives Syslog messages from network devices.
Managed switch with SNMP and Syslog agents
Managed switch with SNMP and Syslog agents

Steps for Configuring SNMPv3

- Steps to configure SNMPv3:

1. Configure a standard ACL that will permit access for authorized SNMP managers.
2. Configure an SNMP view to identify which OIDs the SNMB manager will be able to read.
3. Configure the SNMP group and features including name, version, type of authentication and encryption, associates view to the group, read or write, filter with ACL.
4. Configure a user with features including username, associates with group, version, authentication type, encryption type and password.



Step 1: Configure an ACL to permit access to the protected management network.

```
Router(config)# ip access-list standard acl-name
Router(config-std-nacl)# permit source_net
```

Step 2: Configure an SNMP view.

```
Router(config)# snmp-server view view-name oid-tree
```

Step 3: Configure an SNMP group.

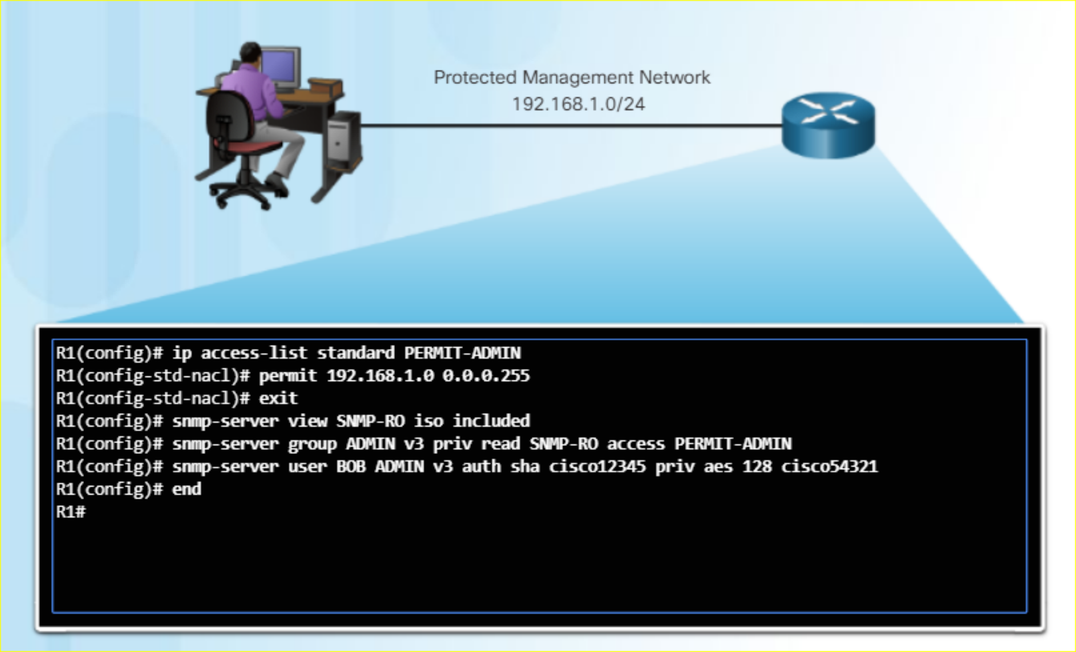
```
Router(config)# snmp-server group group-name v3 priv read view-name access [acl-
number | acl-name]
```

Step 4: Configure a user as a member of the SNMP group.

```
Router(config)# snmp-server user username group-name v3 auth {md5 | sha} auth-
password priv {des | 3des | aes {128 | 192 | 256}} privpassword
```

SNMPv3 Configuration

- The example configures a standard ACL named PERMIT-ADMIN. It is configured to permit only the 192.168.1.0/24 network. All hosts attached to this network will be allowed to access the SNMP agent running on R1.
- An SNMP view is named SNMP-RO and is configured to include the entire ISO tree from the MIB.

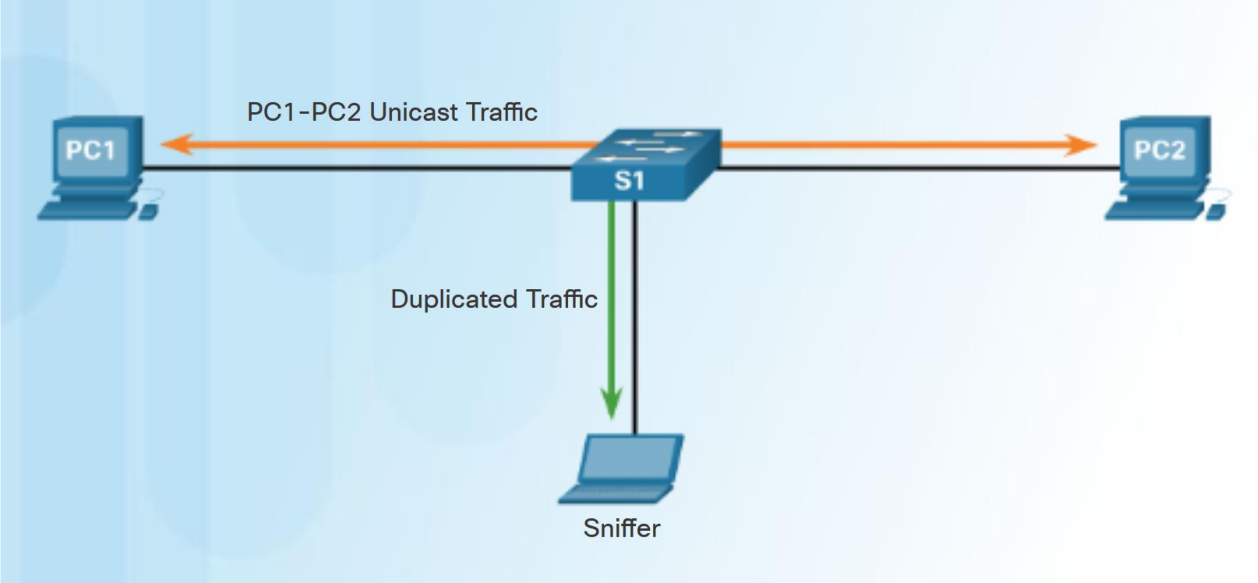


```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)# snmp-server view SNMP-RO iso included
R1(config)# snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
R1(config)# snmp-server user BOB ADMIN v3 auth sha cisco12345 priv aes 128 cisco54321
R1(config)# end
R1#
```

5.3 Cisco Switch Port Analyzer

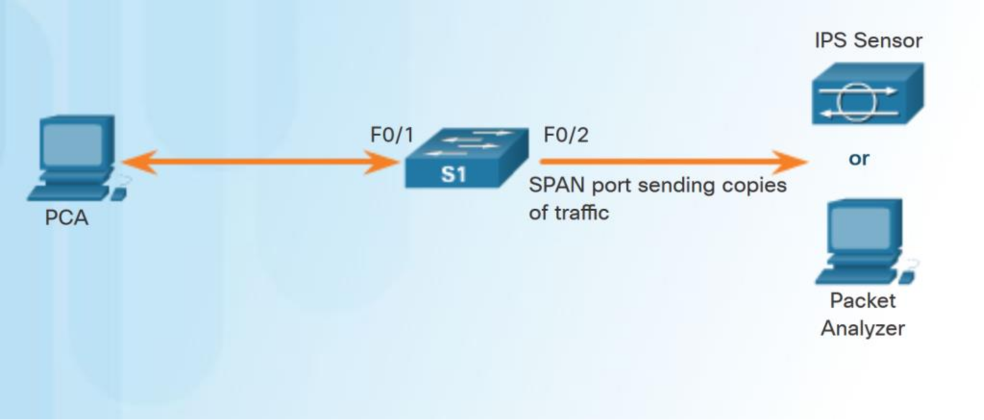
Port Mirroring

- Port mirroring allows a switch to copy and send Ethernet frames from specific ports to the destination port connected to a packet analyzer.



Analyzing Suspicious Traffic

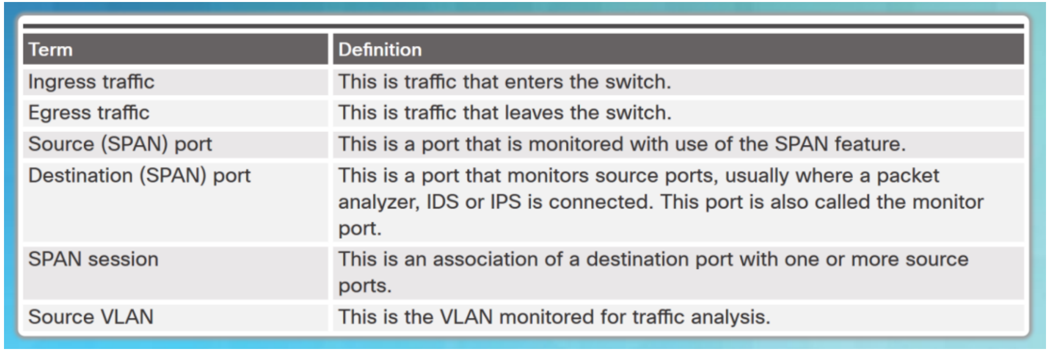
- SPAN is a type of port mirroring that allows administrators or devices to collect and analyze traffic.
- SPAN is commonly implemented to deliver traffic to specialized devices including:
  - Packet analyzers – Using software such as Wireshark to capture and analyze traffic for troubleshooting purposes.
  - Intrusion Prevention Systems (IPSs) – IPSs are focused on the security aspect of traffic and are implemented to detect network attacks as they happen.
- SPAN can be implemented as either Local SPAN or Remote SPAN (RSPAN).



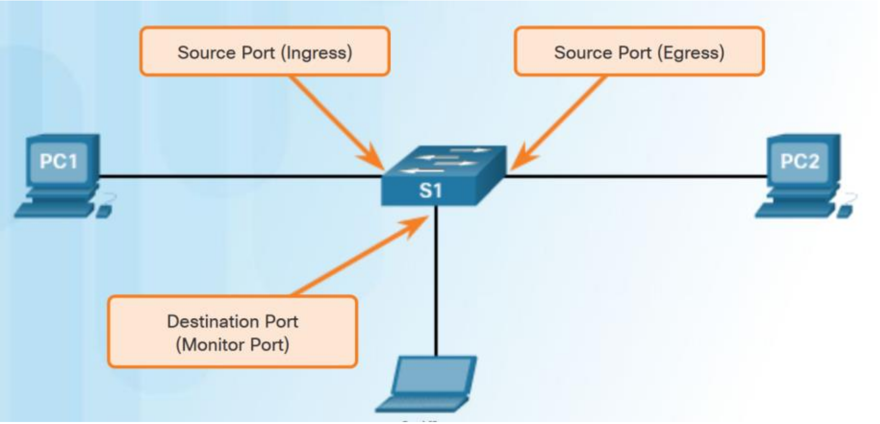
SPAN Overview

Local SPAN

- Local SPAN is when traffic on a switch is mirrored to another port on that switch.
- A SPAN session is the association between source ports (or VLANs) and a destination port.
- Three important things to consider when configuring SPAN:
    - The destination port cannot be a source port, and the source port cannot be a destination port.
    - The number of destination ports is platform-dependent.
    - The destination port is no longer a normal switch port. Only monitored traffic passes through that port.

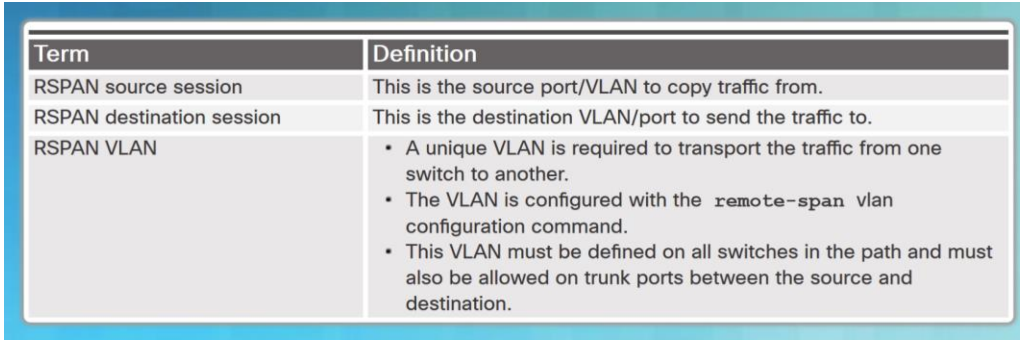


Term	Definition
Ingress traffic	This is traffic that enters the switch.
Egress traffic	This is traffic that leaves the switch.
Source (SPAN) port	This is a port that is monitored with use of the SPAN feature.
Destination (SPAN) port	This is a port that monitors source ports, usually where a packet analyzer, IDS or IPS is connected. This port is also called the monitor port.
SPAN session	This is an association of a destination port with one or more source ports.
Source VLAN	This is the VLAN monitored for traffic analysis.

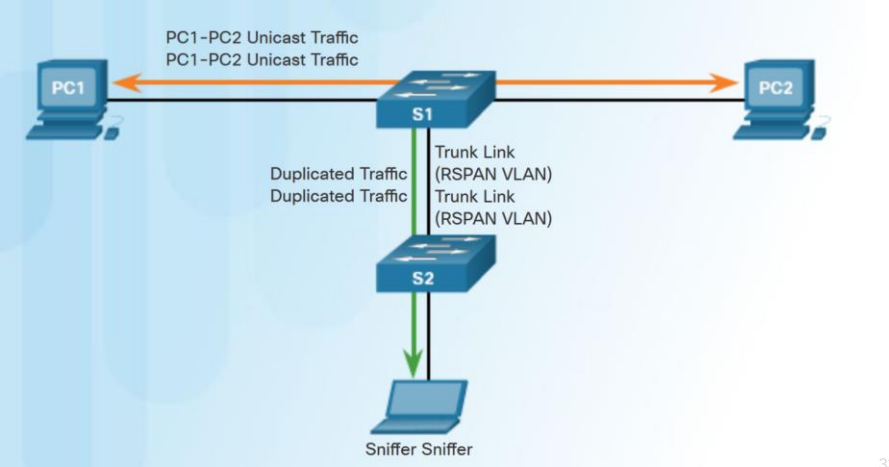


Remote SPAN

- Remote SPAN (RSPAN) allows source and destination ports to be in different switches.
- RSPAN uses two sessions.
  - One session is used as the source and one session is used to copy or receive the traffic from a VLAN.
  - The traffic for each RSPAN session is carried over trunk links in a user-specified RSPAN VLAN

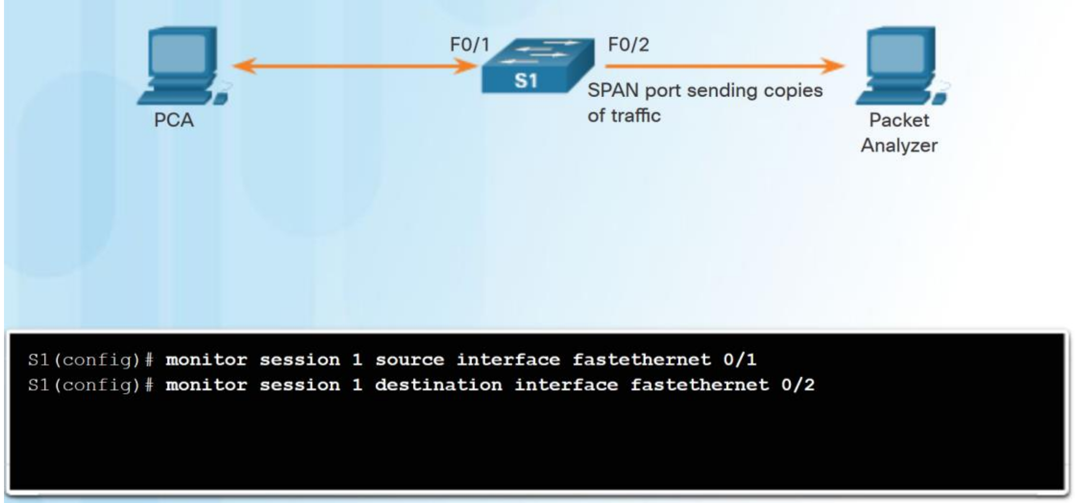


Term	Definition
RSPAN source session	This is the source port/VLAN to copy traffic from.
RSPAN destination session	This is the destination VLAN/port to send the traffic to.
RSPAN VLAN	• A unique VLAN is required to transport the traffic from one switch to another. • The VLAN is configured with the `remote-span` vlan configuration command. • This VLAN must be defined on all switches in the path and must also be allowed on trunk ports between the source and destination.



SPAN Configuration

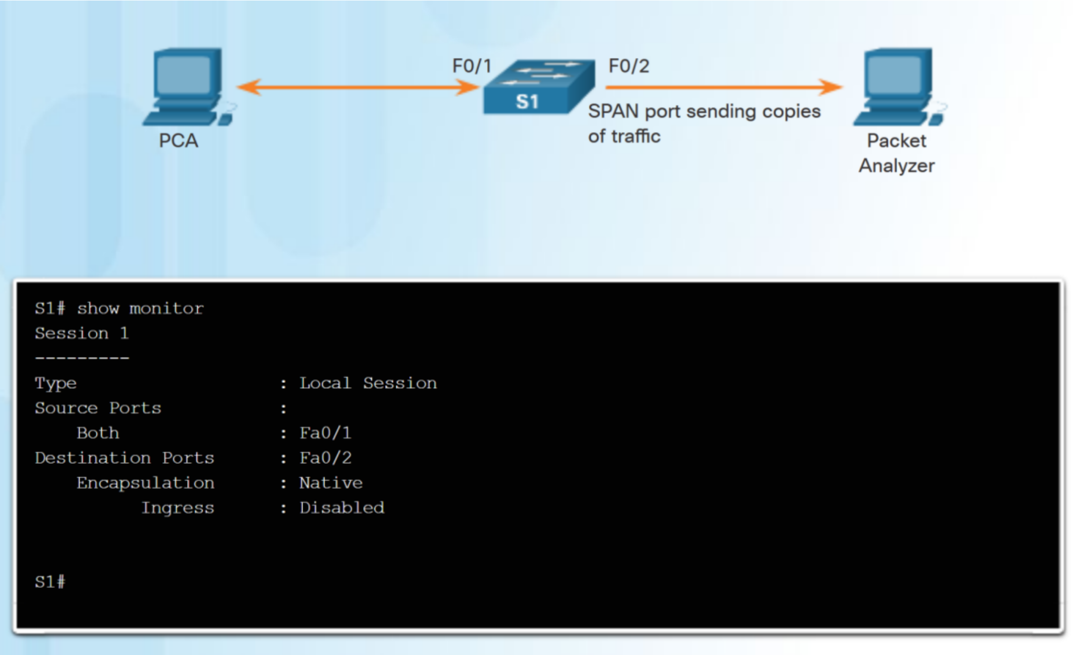
Configuring Local SPAN



```
S1(config)# monitor session 1 source interface fastethernet 0/1
S1(config)# monitor session 1 destination interface fastethernet 0/2
```

- A session number is used to identify a local SPAN session.
- Use **monitor session** command to associate a source port and a destination port with a SPAN session.
- A separate monitor session command is used for each session.
- A VLAN can be specified instead of a physical port.

Verifying Local SPAN



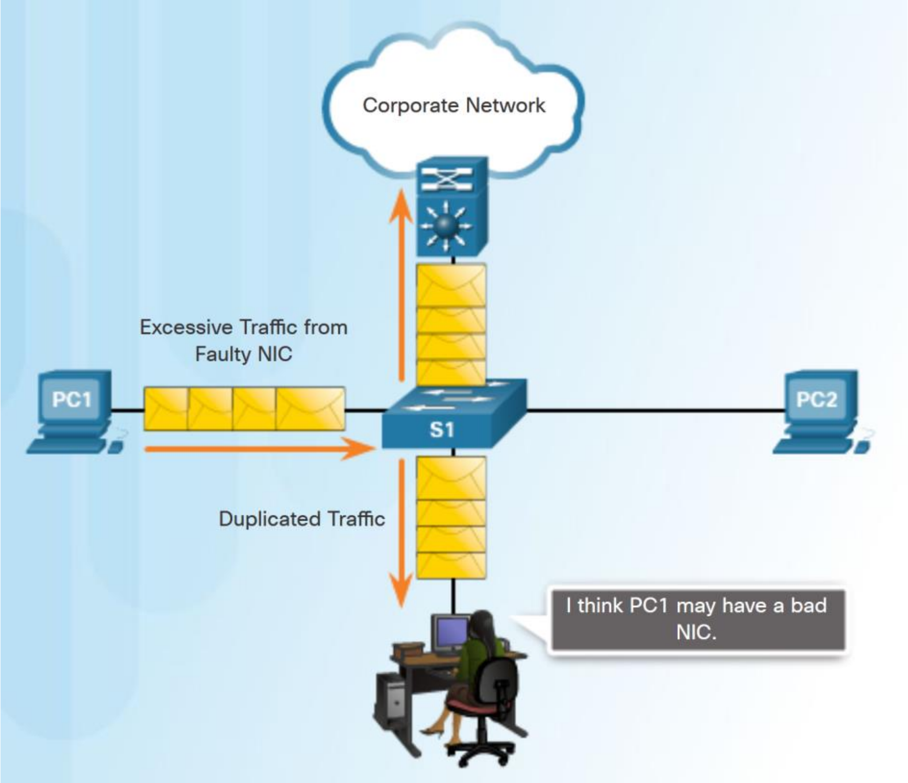
```
S1# show monitor
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Fa0/1
Destination Ports      : Fa0/2
    Encapsulation      : Native
          Ingress      : Disabled


S1#
```

- Use the **show monitor** command to verify the SPAN session. It displays the type of the session, the source ports for each traffic direction, and the destination port.

SPAN as a Troubleshooting Tool

Troubleshooting with SPAN Overview

- SPAN allows administrators to troubleshoot network issues.
  - To investigate a slow network application, a network administrator can use SPAN to duplicate and redirect traffic to a packet analyzer such as Wireshark.
  - Older systems with faulty NICs can also cause issues. If SPAN is enabled a network technician can detect and isolate the end device causing the problem.


Corporate Network
Excessive Traffic from Faulty NIC
PC1
S1
PC2
Duplicated Traffic
I think PC1 may have a bad NIC.

5.4 Chapter Summary

Conclusion

Chapter 5: Network Security and Monitoring

- Explain how to mitigate common LAN security attacks.
- Configure SNMP to monitor network operations in a small to medium-sized business network.
- Troubleshoot a network problem using SPAN.

cisco