

# Network Security and Monitoring

CCNA Routing and Switching

Connecting Networks v6.0



# Sections & Objectives

- 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.

- 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.

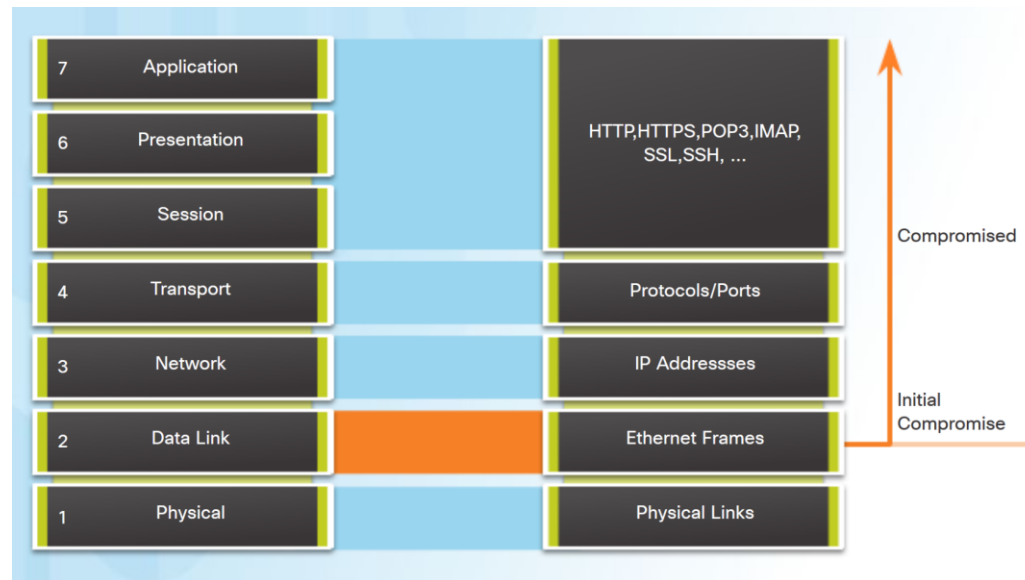
- Cisco Switch Port Analyzer (SPAN)

- Troubleshoot a network problem using SPAN.
  - Explain the features and characteristics of SPAN.
  - Configure local SPAN.
  - Troubleshoot suspicious LAN traffic using SPAN.

# LAN Security

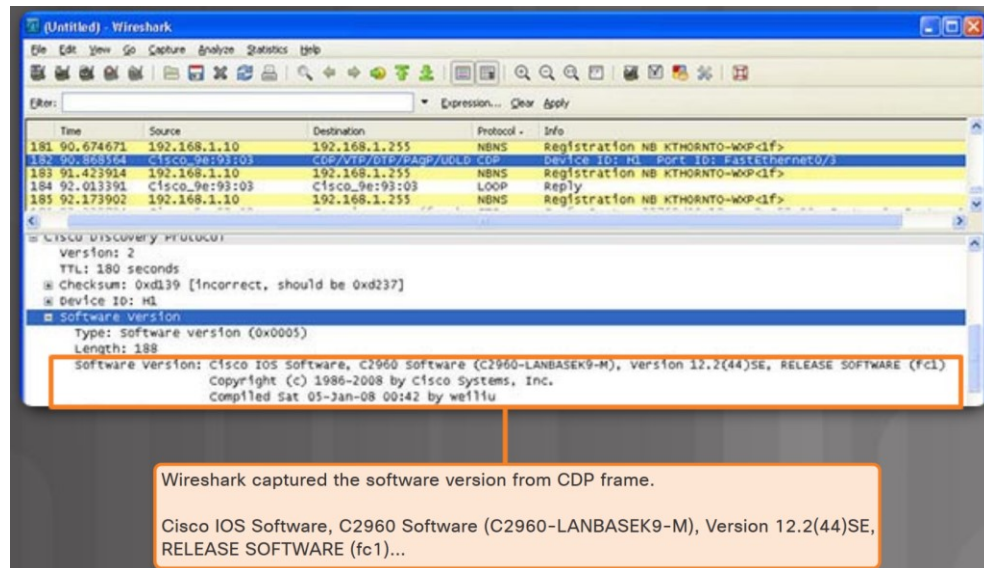
# Common LAN Attacks

- 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



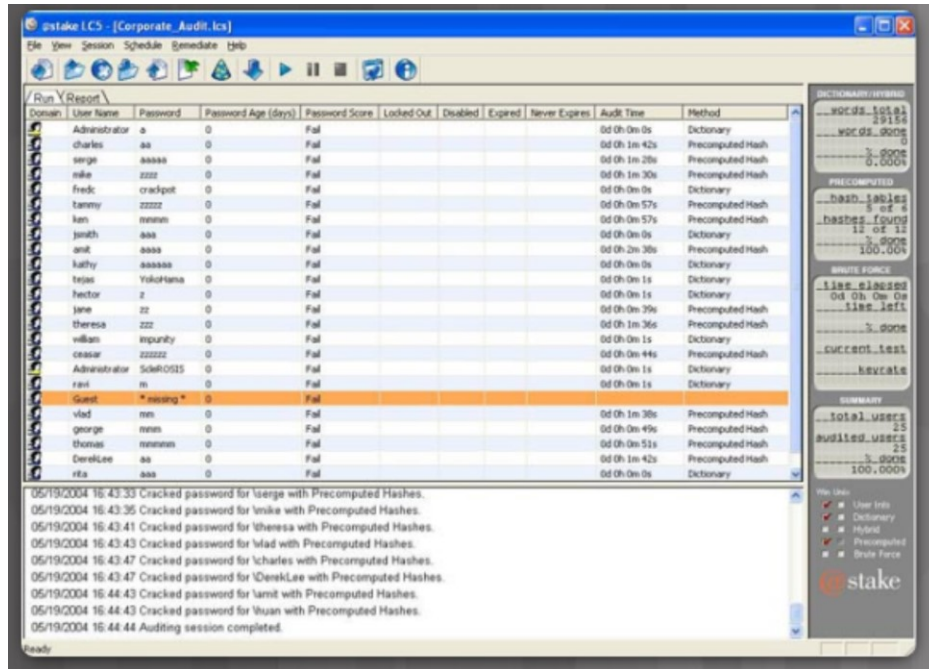
# CDP Reconnaissance Attack

- 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.



# LAN Security Attacks

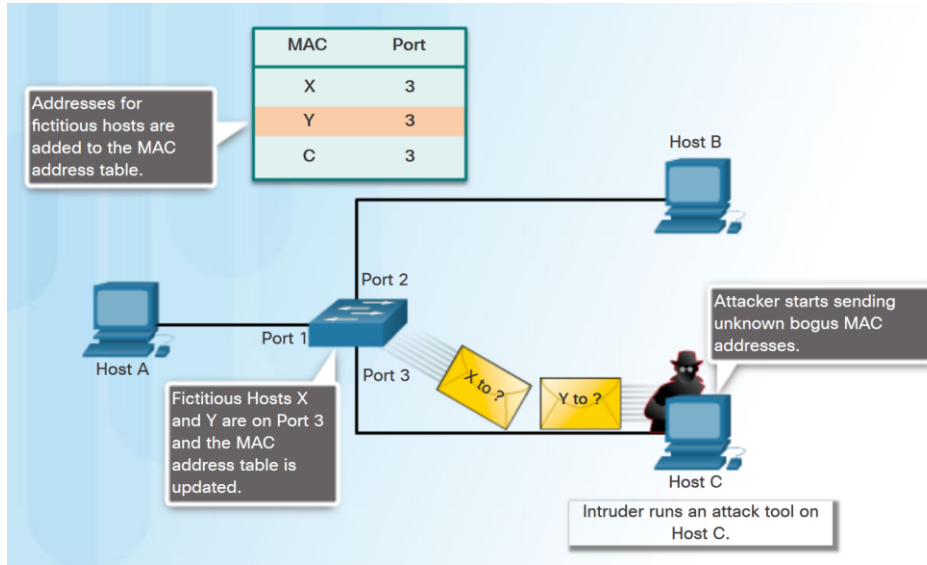
## Telnet Attacks



- 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 (*never Telnet unless no alternative*)
  - 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.

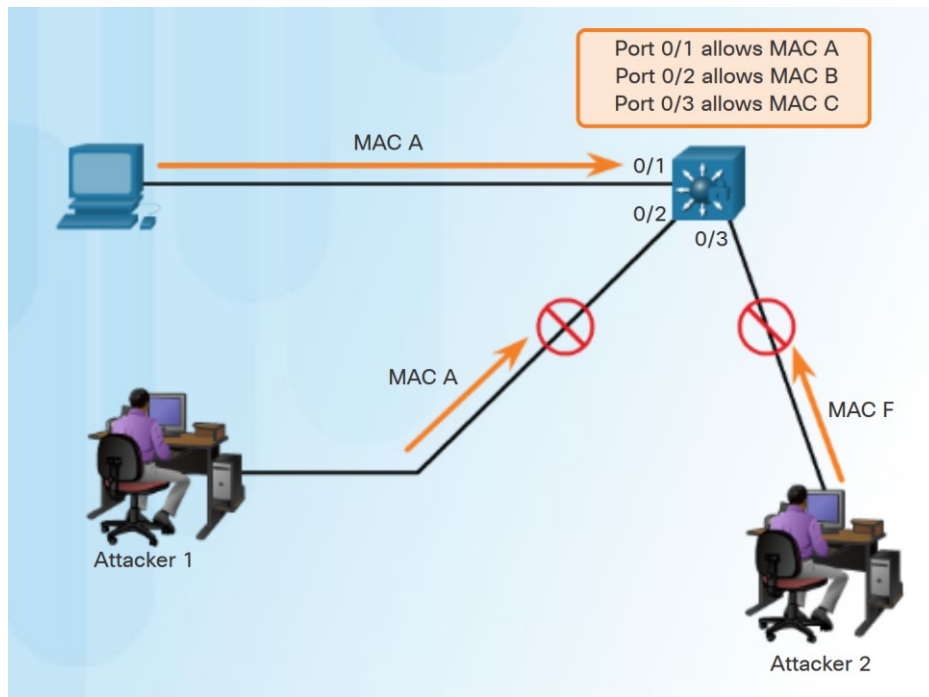
# LAN Security Attacks

## MAC Address Table Flooding Attack



- 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.

# Mitigate MAC Address Flooding Table Attacks



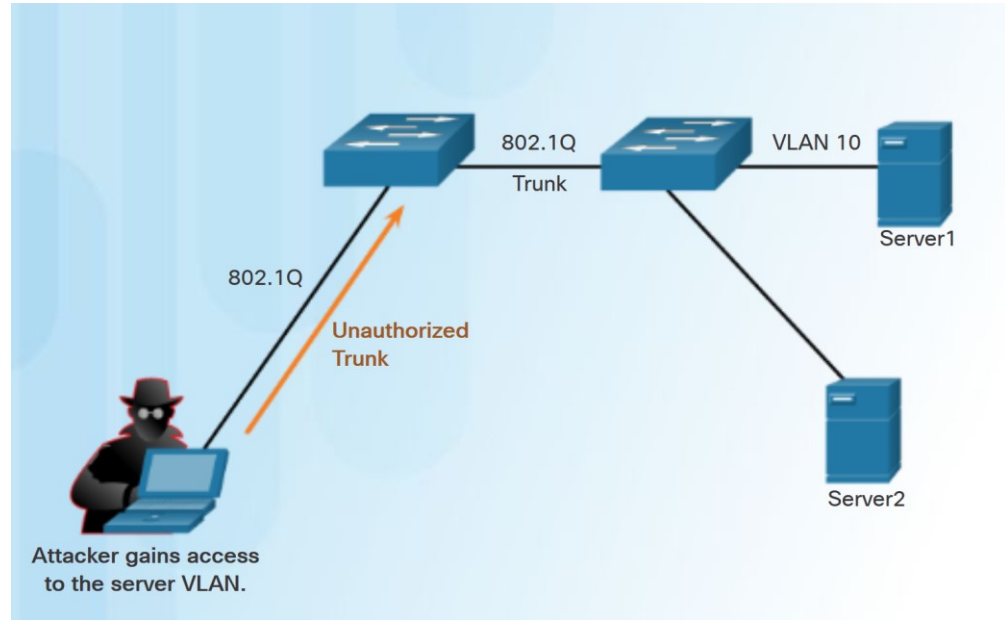
- Enable port security to prevent MAC table flooding attacks.
- Port security allows an administrator to do the following:
  - statically specify MAC addresses for a port.
  - permit the switch to dynamically learn a limited number of MAC addresses.
  - when the maximum number of MAC addresses is reached,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



# LAN Security Attacks

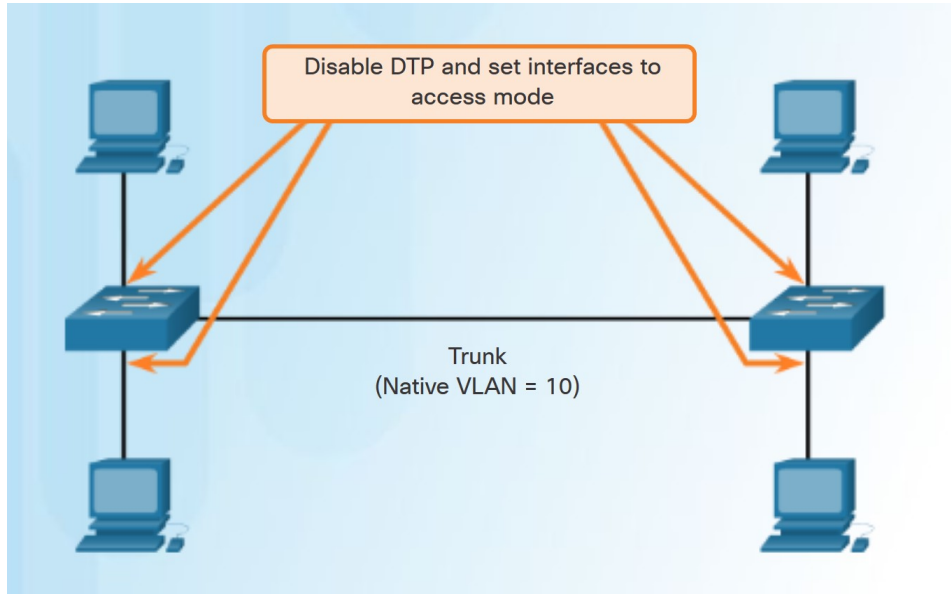
## VLAN Attacks

- 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.



# LAN Security Best Practices

## Mitigate VLAN Attacks

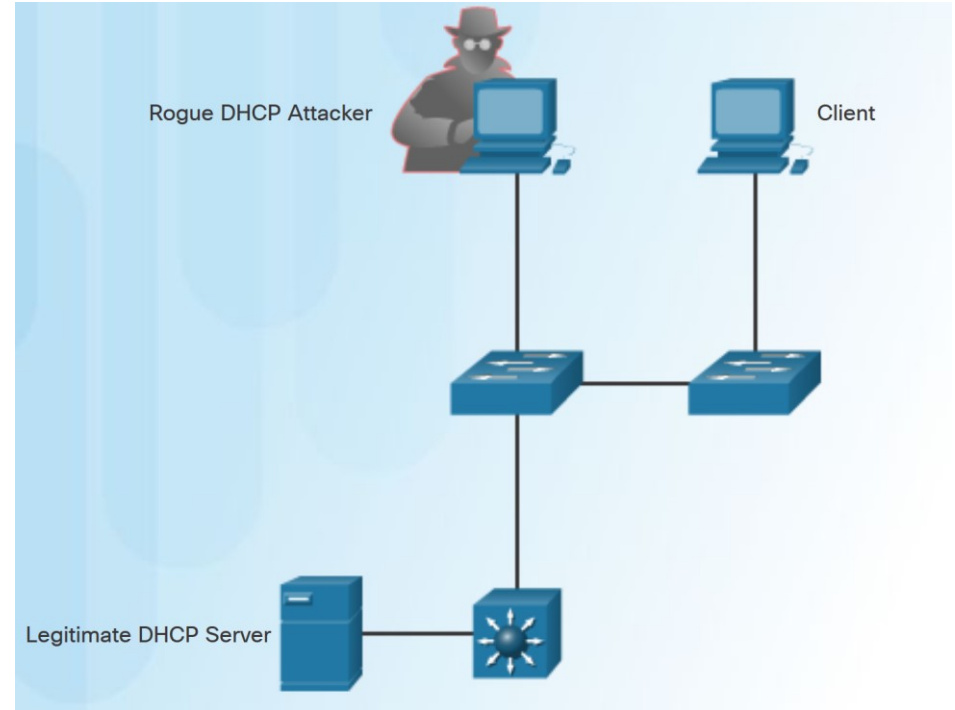


- To prevent basic VLAN attacks:
  - Disable DTP (auto trunking) negotiations on non-trunk ports and use **switchport mode access**.
  - Manually enable trunk links using **switchport mode trunk**.
  - Disable DTP (auto trunking) negotiations on trunking and non-trunking ports using **switchport nonegotiate**.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

# LAN Security Attacks

## DHCP Attacks

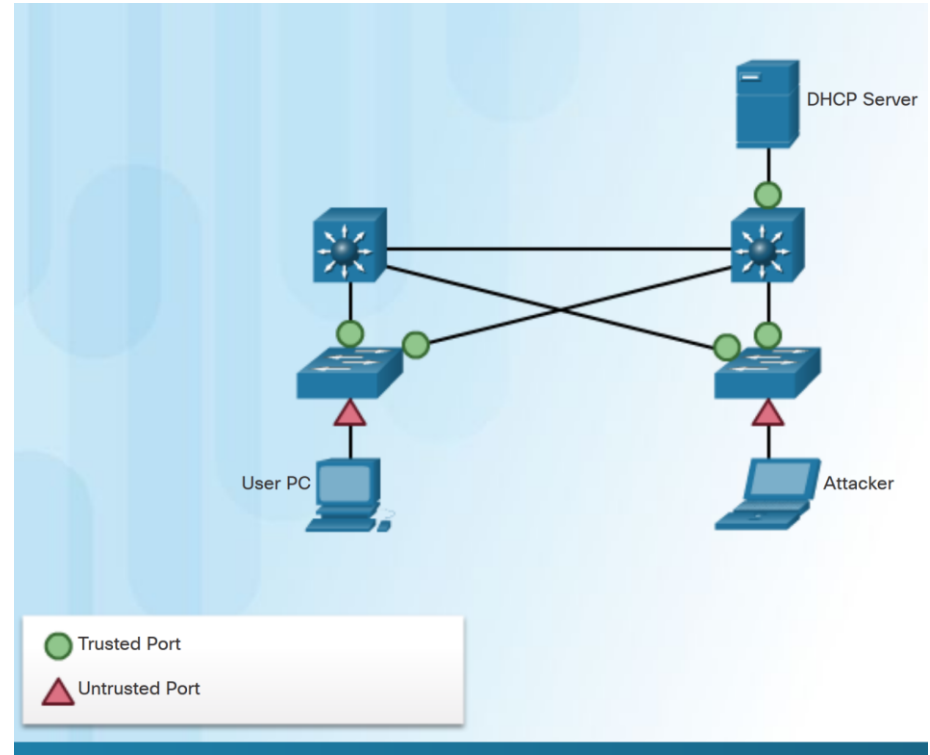
- **DHCP spoofing attack** - An attacker configures a fake DHCP server on the network to issue IP addresses to clients.
- **DHCP starvation attack** - An attacker floods the DHCP server with bogus DHCP requests and leases all of the available IP addresses. This results in a denial-of-service (DoS) attack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



# LAN Security Best Practices

## 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.

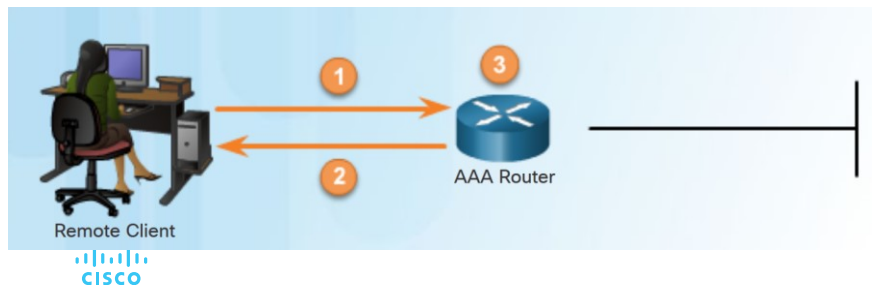


# Secure Administrative Access using AAA

- Authentication, authorisation and accounting (AAA)

- Local AAA Authentication

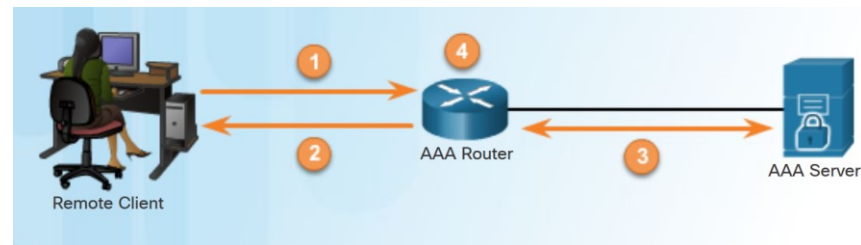
1. Client establishes a connection with the router.
2. AAA router prompts the user for username and password.
3. Router authenticates the username and password using the local database, and allows user access.



- Server-Based AAA Authentication

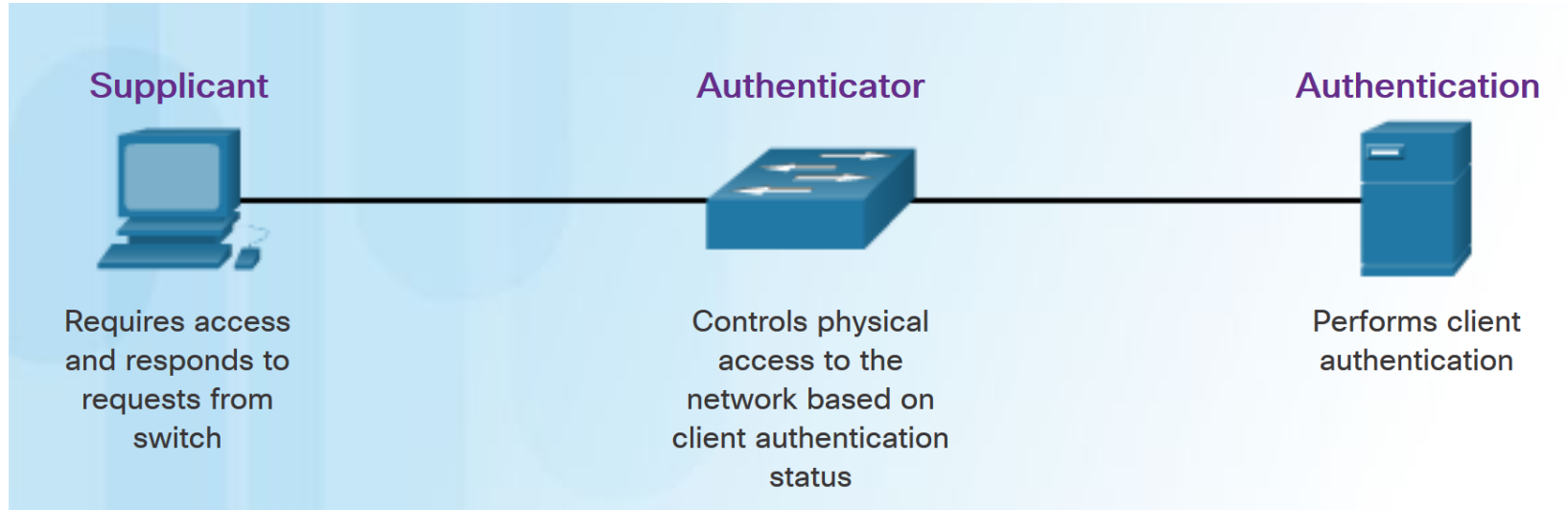
1. Client establishes a connection with the router.
2. AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a remote AAA server.

- 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

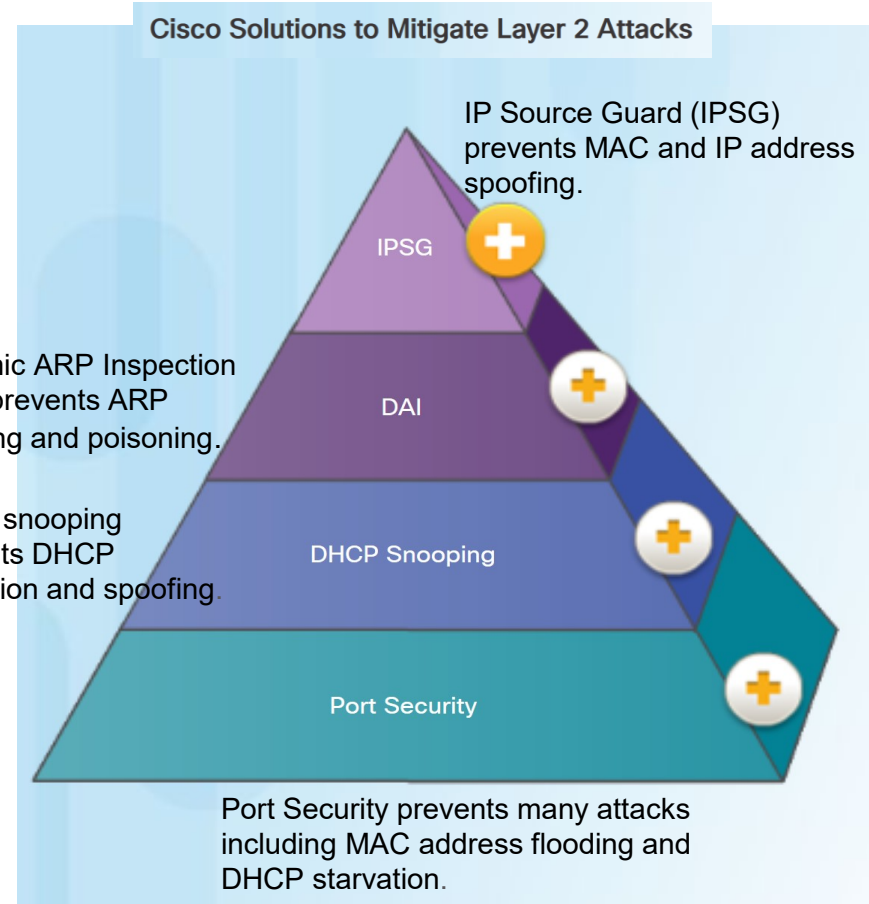
- IEEE 802.1X standard defines a port-based access control and authentication protocol.
  - Restricts unauthorized workstations from connecting to a LAN.
  - The authentication server authenticates each workstation connected to a switch port before making any services available.



# LAN Security Best Practices

## 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.

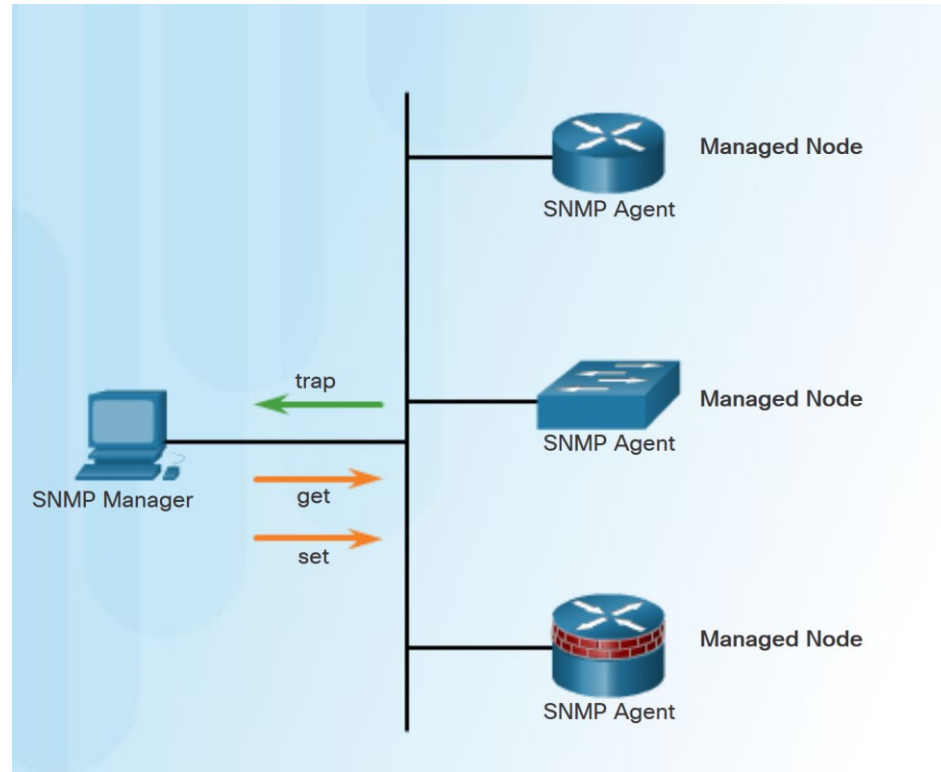


# SNMP



# 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.

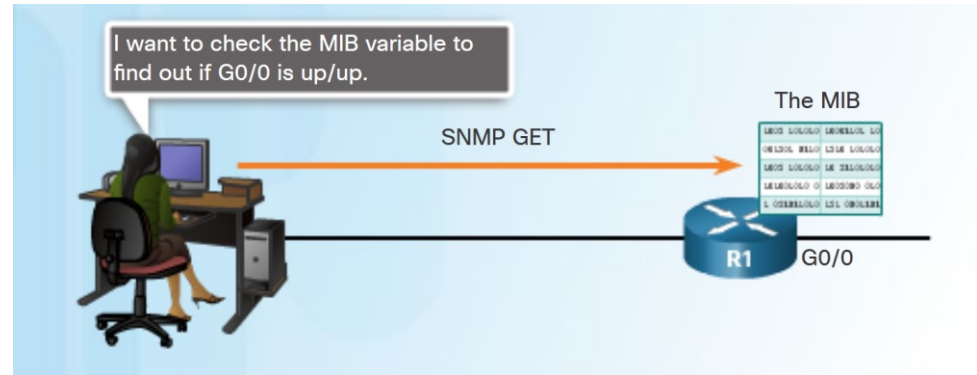


# SNMP Operation

## SNMP Operation

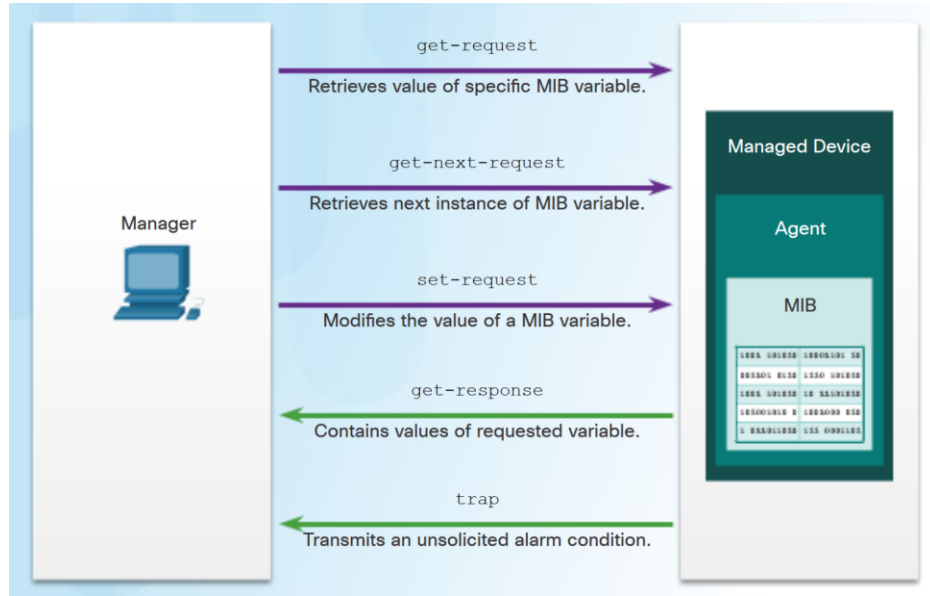
- SNMP agents that reside on managed devices collect and store information about the device.
- This information is stored by the agent locally in the MIB.
- SNMP manager then uses the SNMP agent to access information within the MIB.
- SNMP agent responds to SNMP manager requests as follows:
  - **Get an MIB variable** - The SNMP agent performs this in 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.



# SNMP Operation

## SNMP Agent Traps



- 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

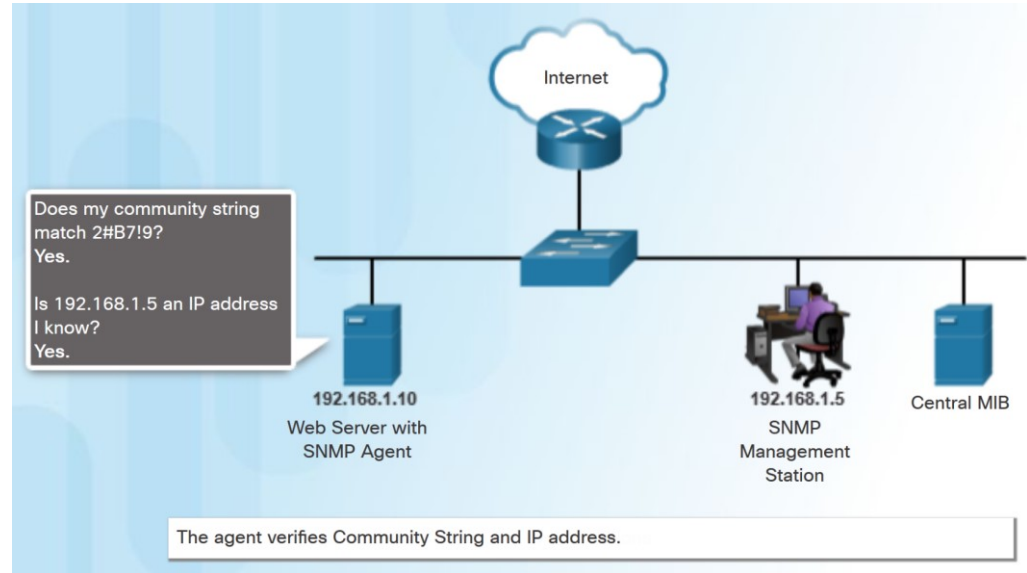
Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication (an 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: <ul style="list-style-type: none"><li>• DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.</li><li>• 3DES 168-bit encryption.</li><li>• AES 128-bit, 192-bit, or 256-bit encryption.</li></ul>

- 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

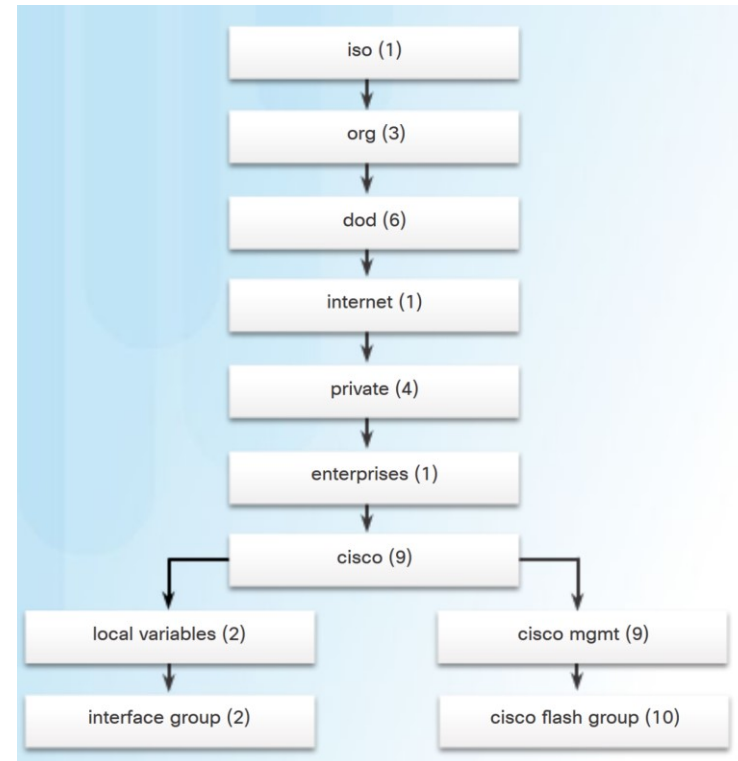
## Community Strings

- 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.



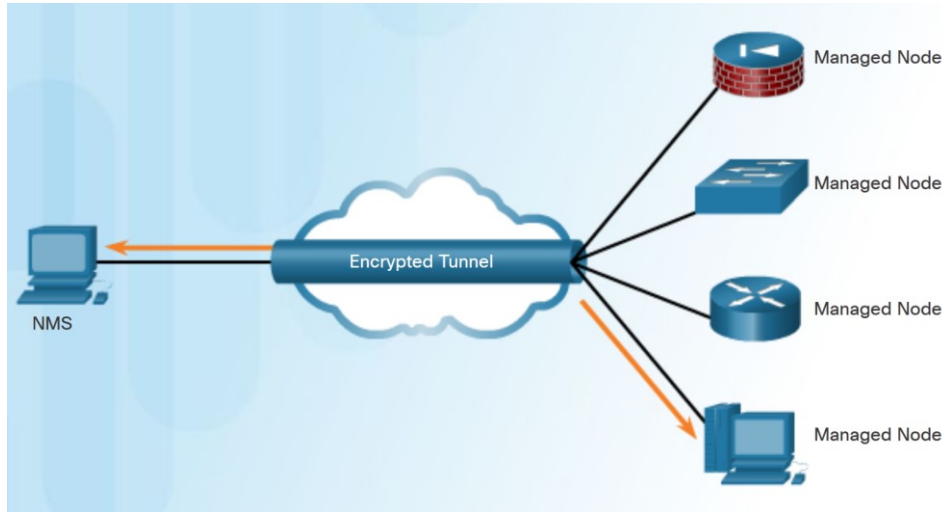
# Management Information Base Object ID

- 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.



# SNMP Operation

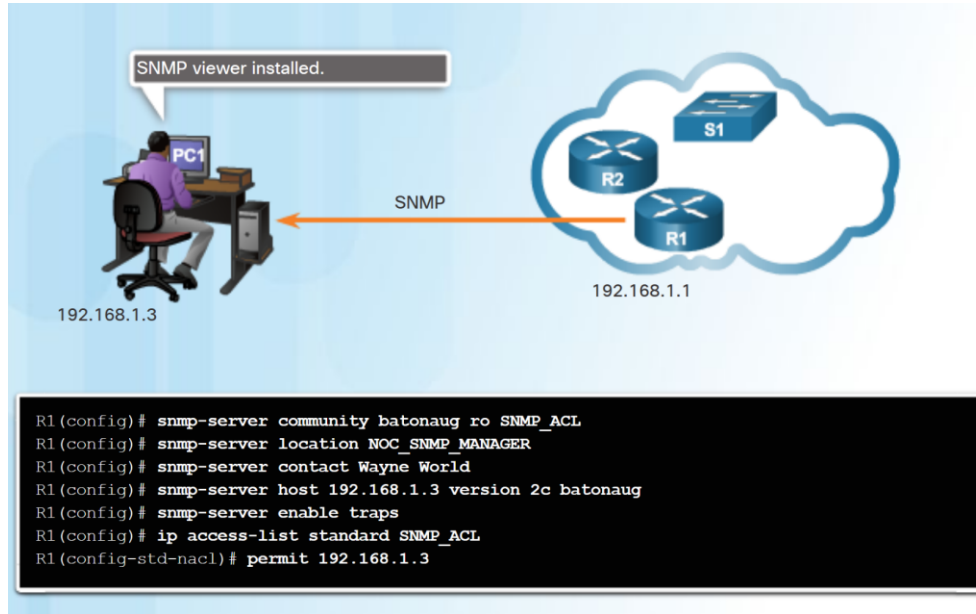
## SNMPv3



- 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.

# Configuring SNMP

## Steps for Configuring SNMP



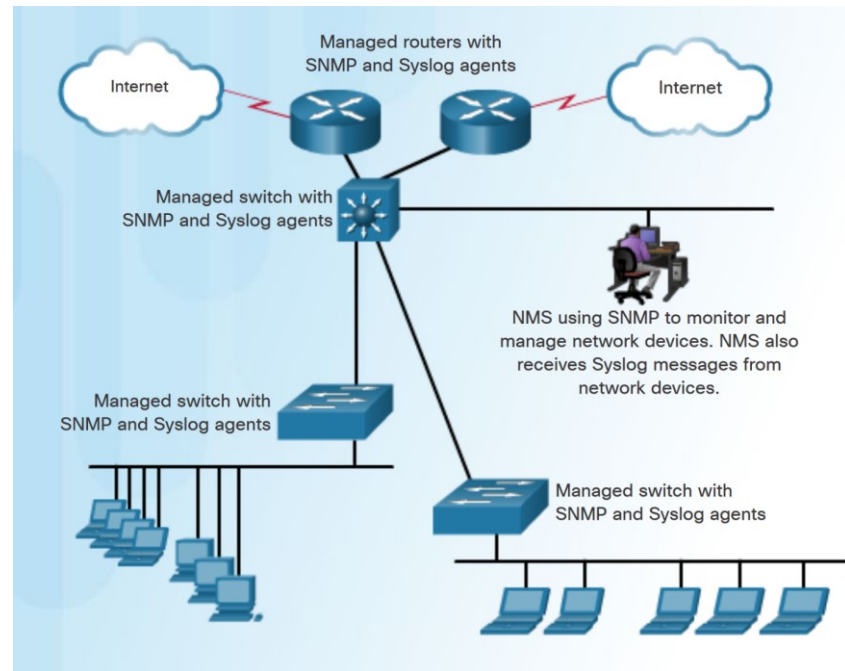
### Basic steps to configuring SNMP:

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**.



# 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.



# 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]
```

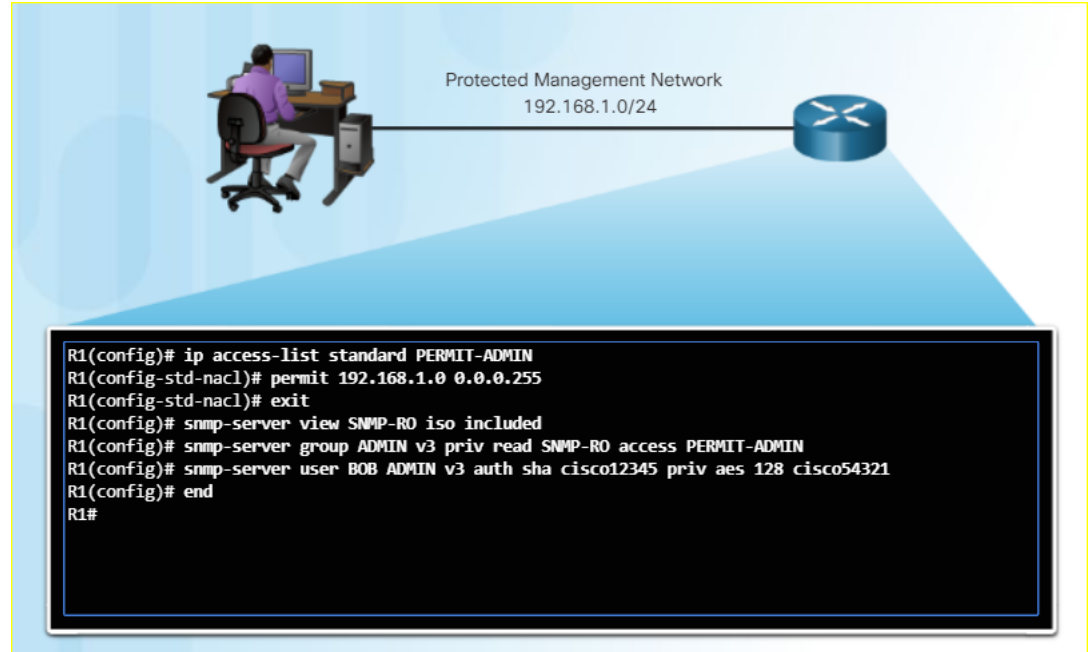
Step 4: Configure a user as a member of the SNMP group.

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

# Configuring SNMP

## 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.

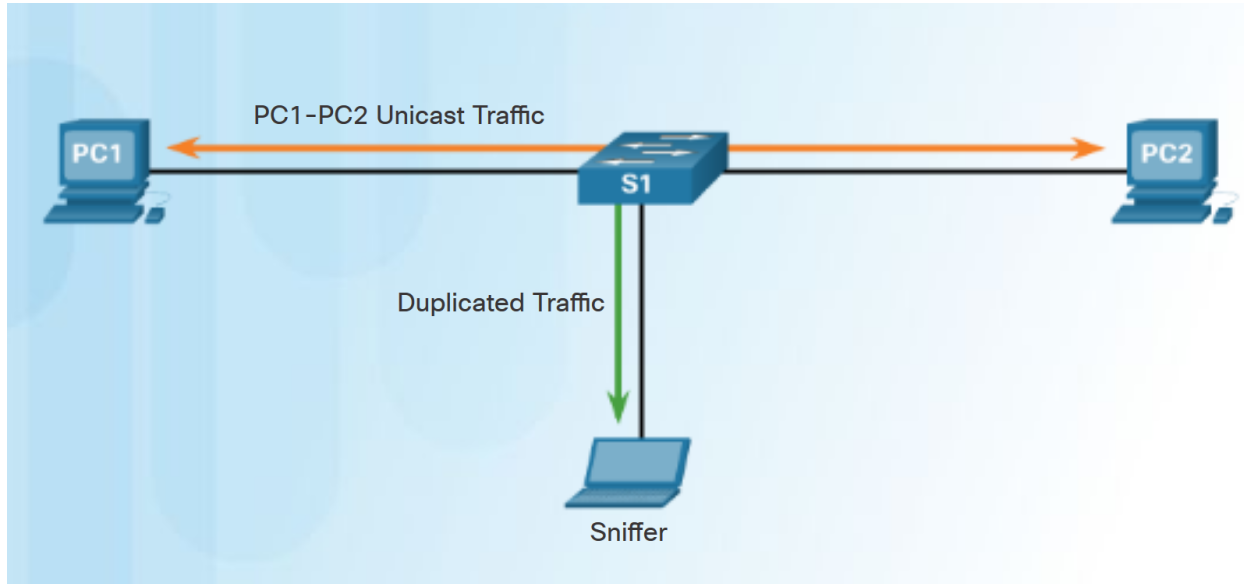


# Port Mirroring

## SPAN (Switched Port Analyzer)

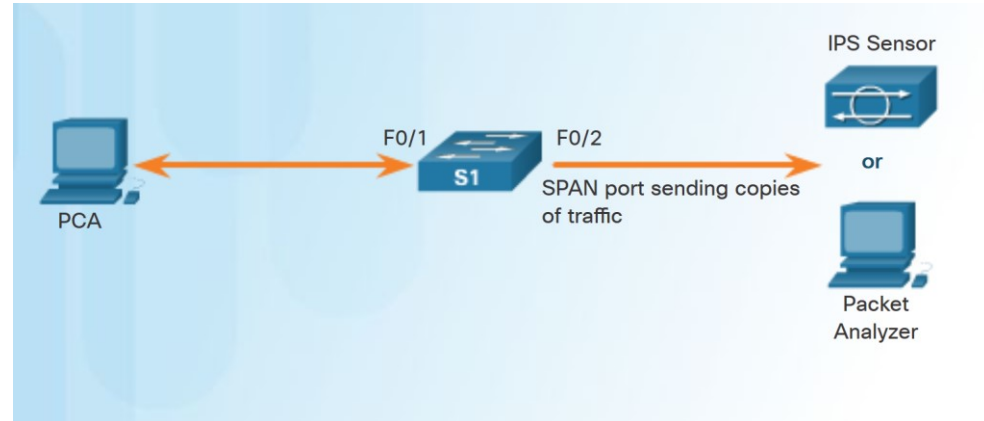
# Port Mirroring

- 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).

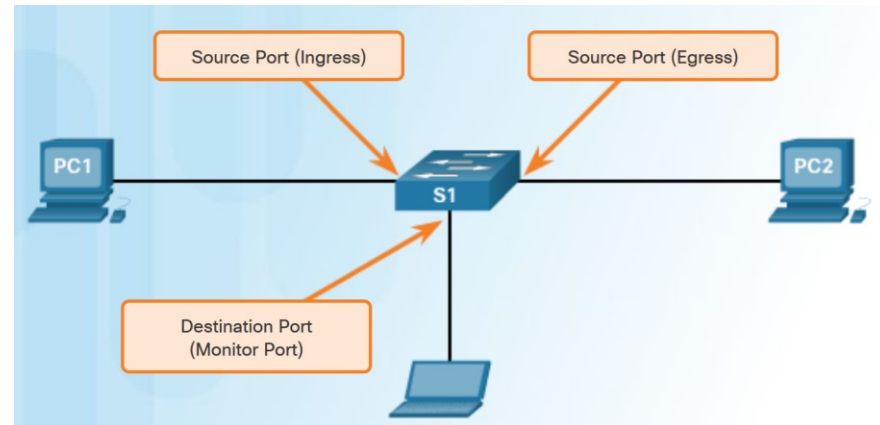


# SPAN Overview

## 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.

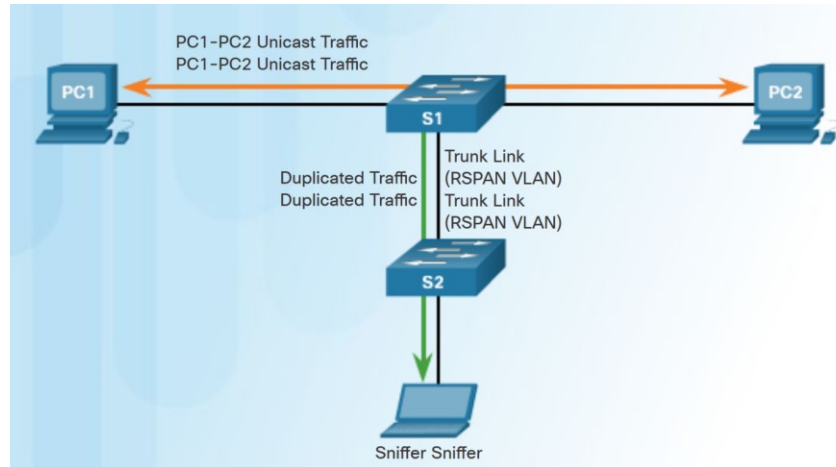
Term	Definition
Ingress traffic	This is traffic that enters the switch.
Egress traffic	This is traffic that leaves the switch.
Source (SPAN) port	This is a port that is monitored with use of the SPAN feature.
Destination (SPAN) port	This is a port that monitors source ports, usually where a packet analyzer, 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

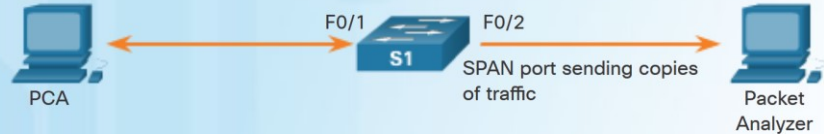
Term	Definition
RSPAN source session	This is the source port/VLAN to copy traffic from.
RSPAN destination session	This is the destination VLAN/port to send the traffic to.
RSPAN VLAN	<ul style="list-style-type: none"><li>A unique VLAN is required to transport the traffic from one switch to another.</li><li>The VLAN is configured with the <code>remote-span</code> vlan configuration command.</li><li>This VLAN must be defined on all switches in the path and must also be allowed on trunk ports between the source and destination.</li></ul>





# SPAN Configuration

## Configuring Local SPAN



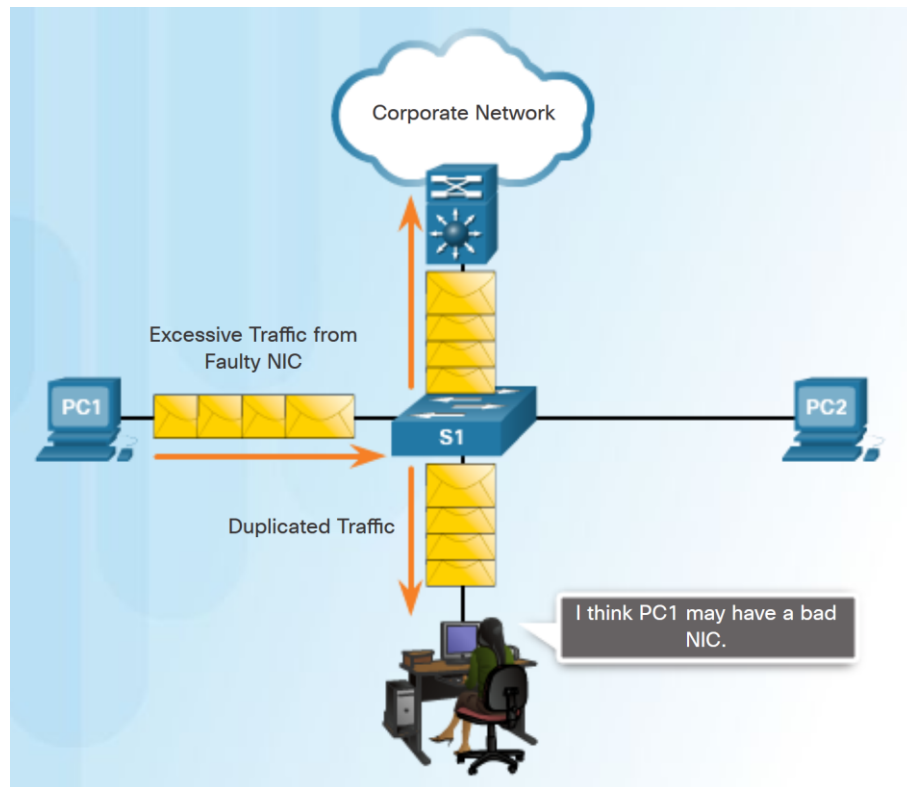
```
S1(config)# monitor session 1 source interface fastethernet 0/1
S1(config)# monitor session 1 destination interface fastethernet 0/2
```

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

- 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.
- 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.

# 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.



# 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.