Chapter 5: Network Security and Monitoring

Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 5

- 5.1 LAN Security
- 5.2 Syslog and NTP
- 5.3 SNMP
- 5.4 NetFlow
- 5.5 Cisco Switch Port Analyzer (SPAN)

5.1 LAN Security

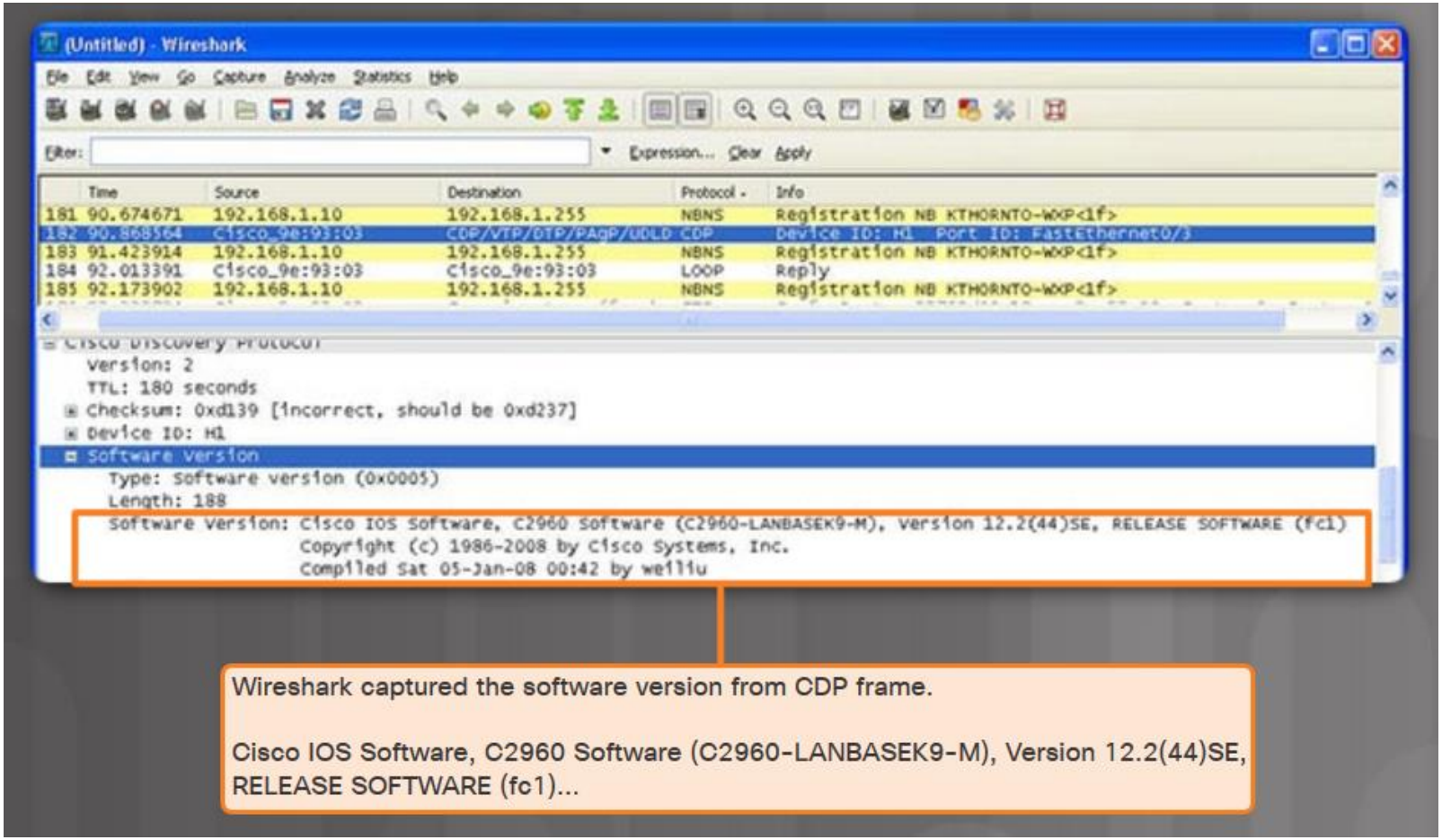
Cisco | Networking Academy®
Mind Wide Open™

L2 Security

- CDP Reconnaissance Attacks
- Telnet Attacks
- MAC Address Table Flooding Attacks
- VLAN Attacks
- DHCP Attacks
- L2 Device Access Control

CDP Reconnaissance Attacks

- CDP automatically discover other CDP-enabled devices.
- CDP data: IP address, IOS version, platform, capabilities.
- CDP uses unencrypted broadcast communication.



Telnet Attacks

- Attacking administration access to a switch or router.
- Insecure communication with unencrypted password.

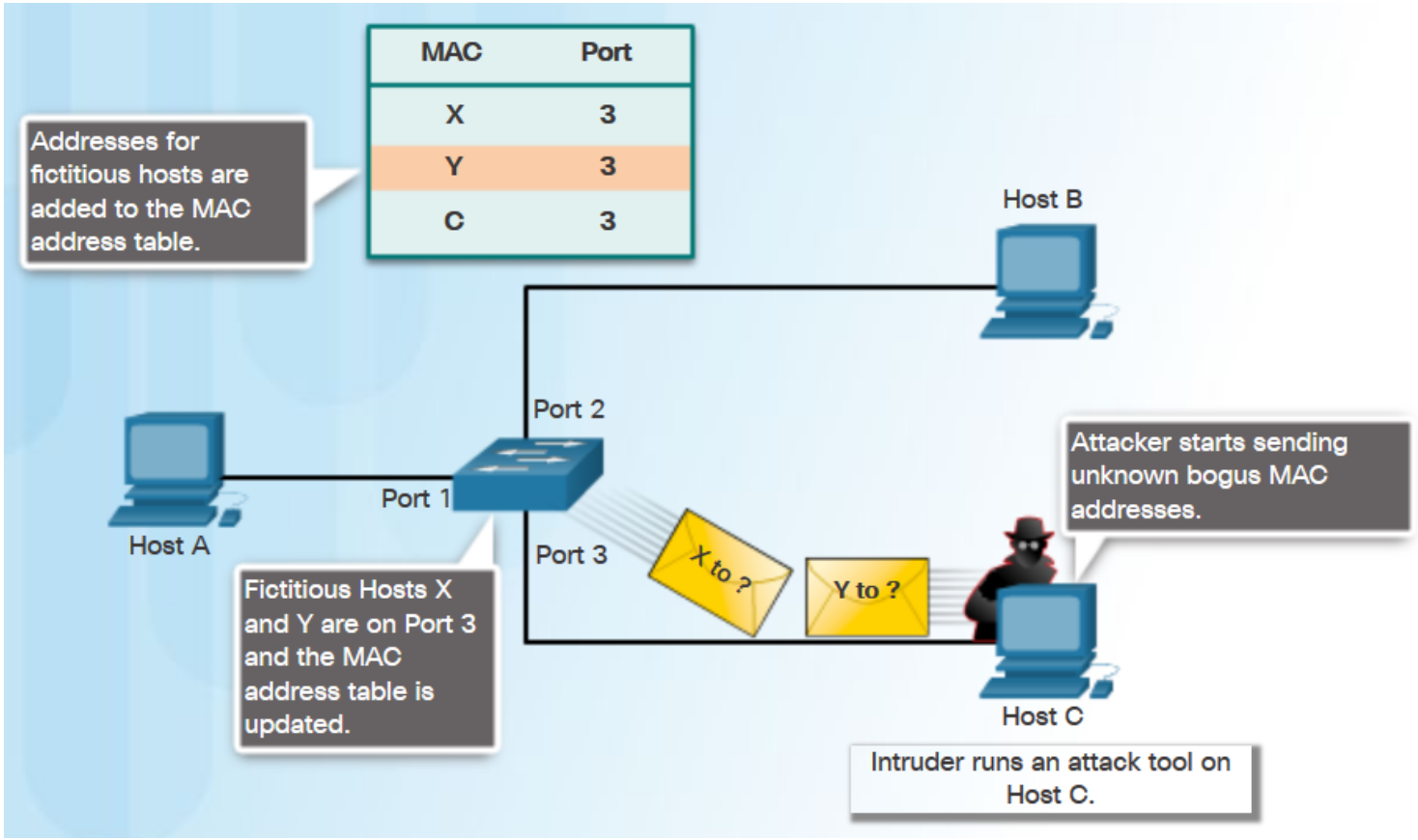
1. Brute force password attack: generating passwords
2. Telnet DoS attack: prevents Telnet process to accept legitimate connections

Mitigation

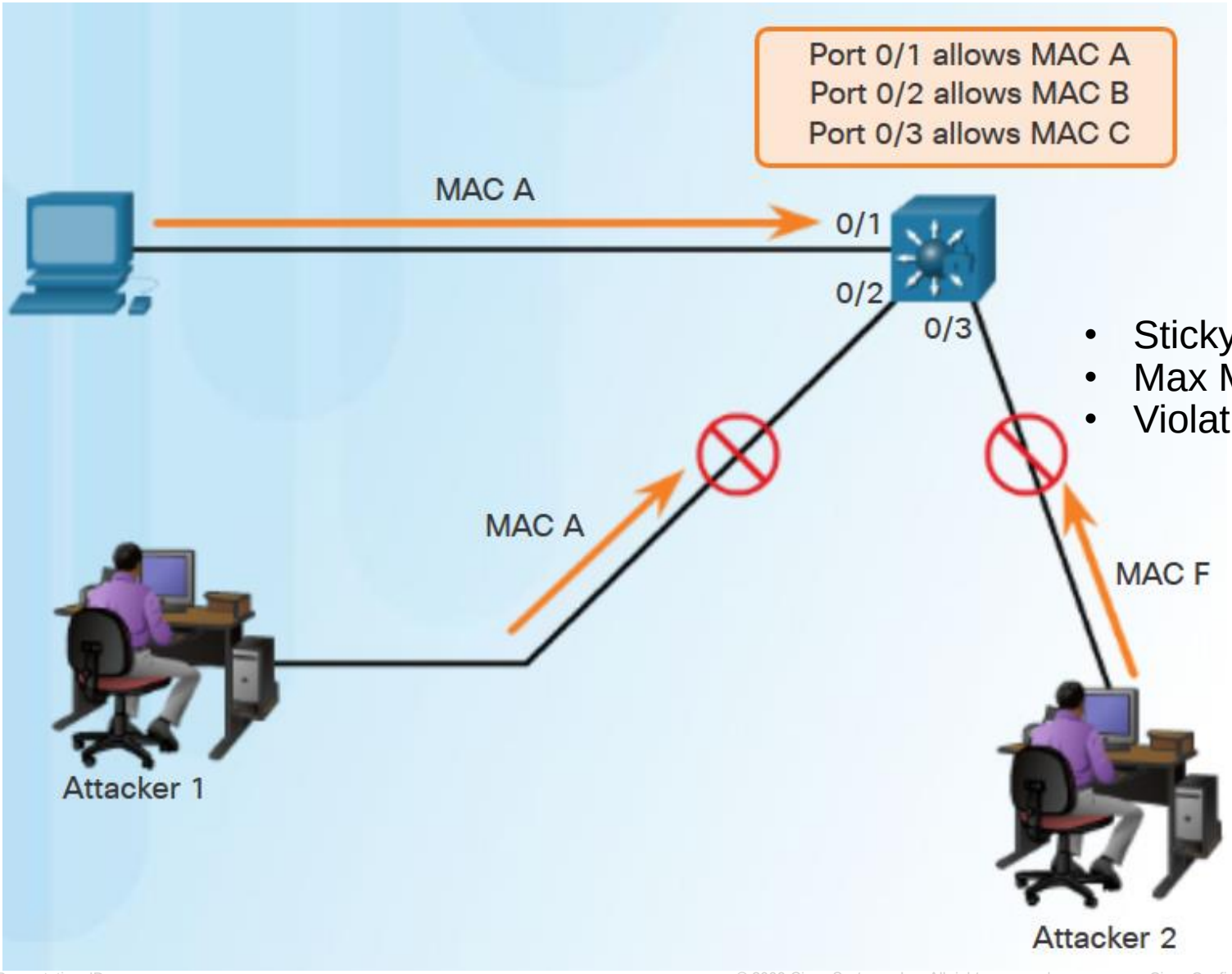
- Use SSH
- Filter VTY access using ACL
- Use strong password
- Apply AAA authentication

MAC Address Table Flooding Attacks (CAM Table Overflow)

- An attacker sends frames with spoofed source MAC address
- A switch assigns MAC addresses to the port in the CAM table
- If MAC table is full, no more addresses can be inserted and the switch broadcasts every.

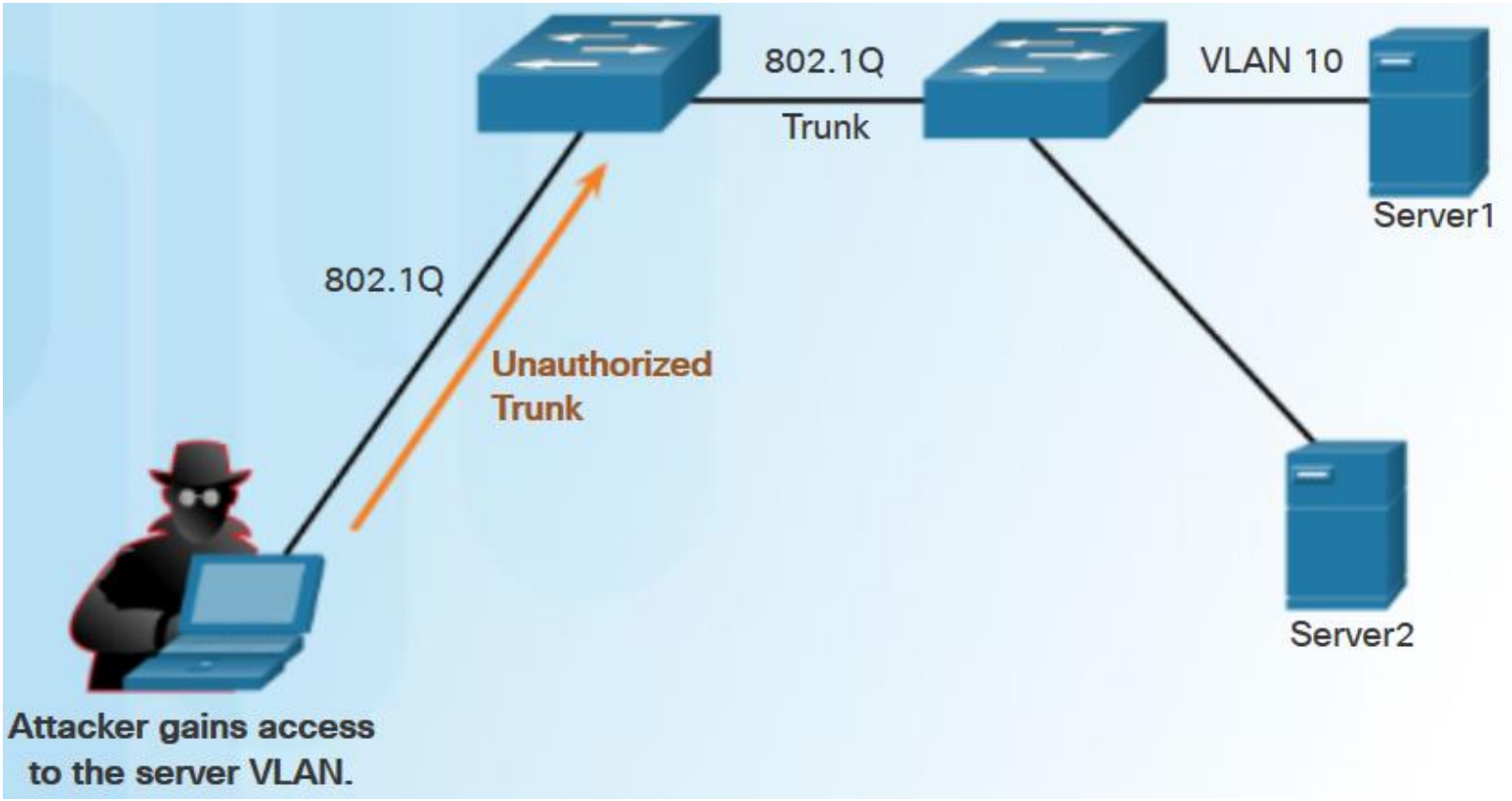


Mitigating CAM Overflow using Port Security

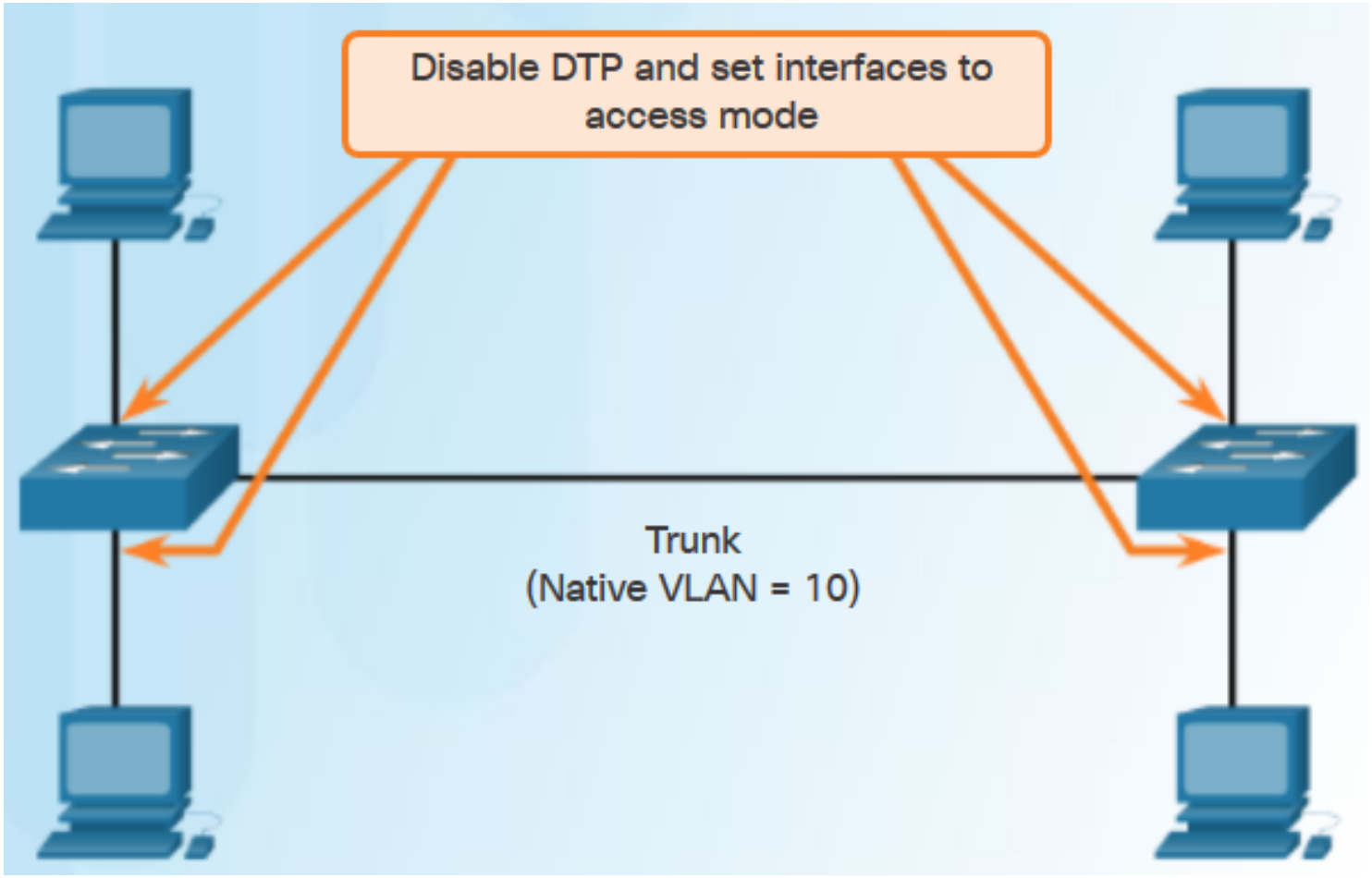


- Sticky address
- Max MAC addresses
- Violation policy

- VLAN Attacks (VLAN spoofing)
  - An attacker pretends to be a switch.
  - He imposes 802.1Q trunk using DTP communication.
  - When successful, a trunk between a switch and a host is established.
  - Attacker can access all VLANs.



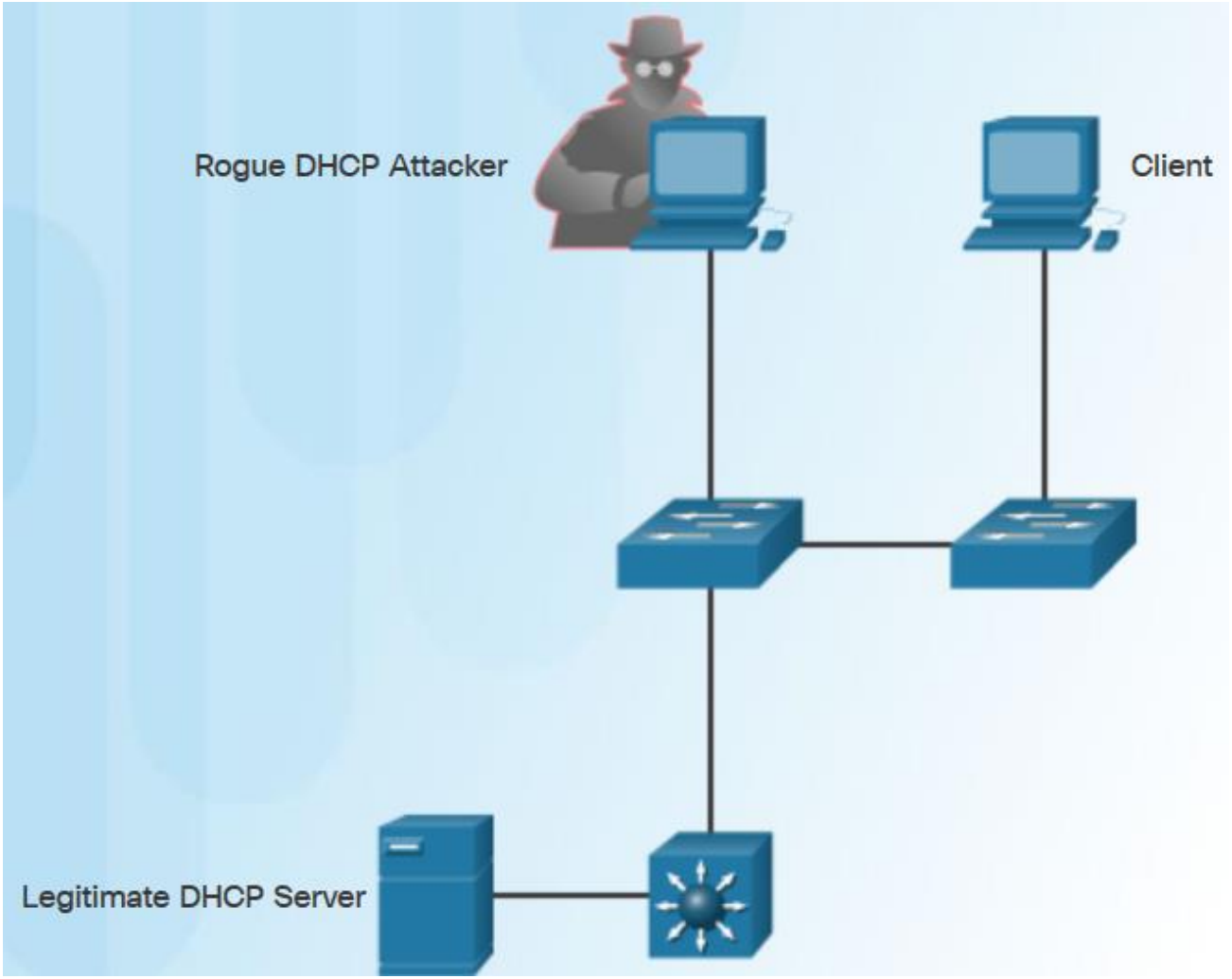
Mitigating VLAN attacks



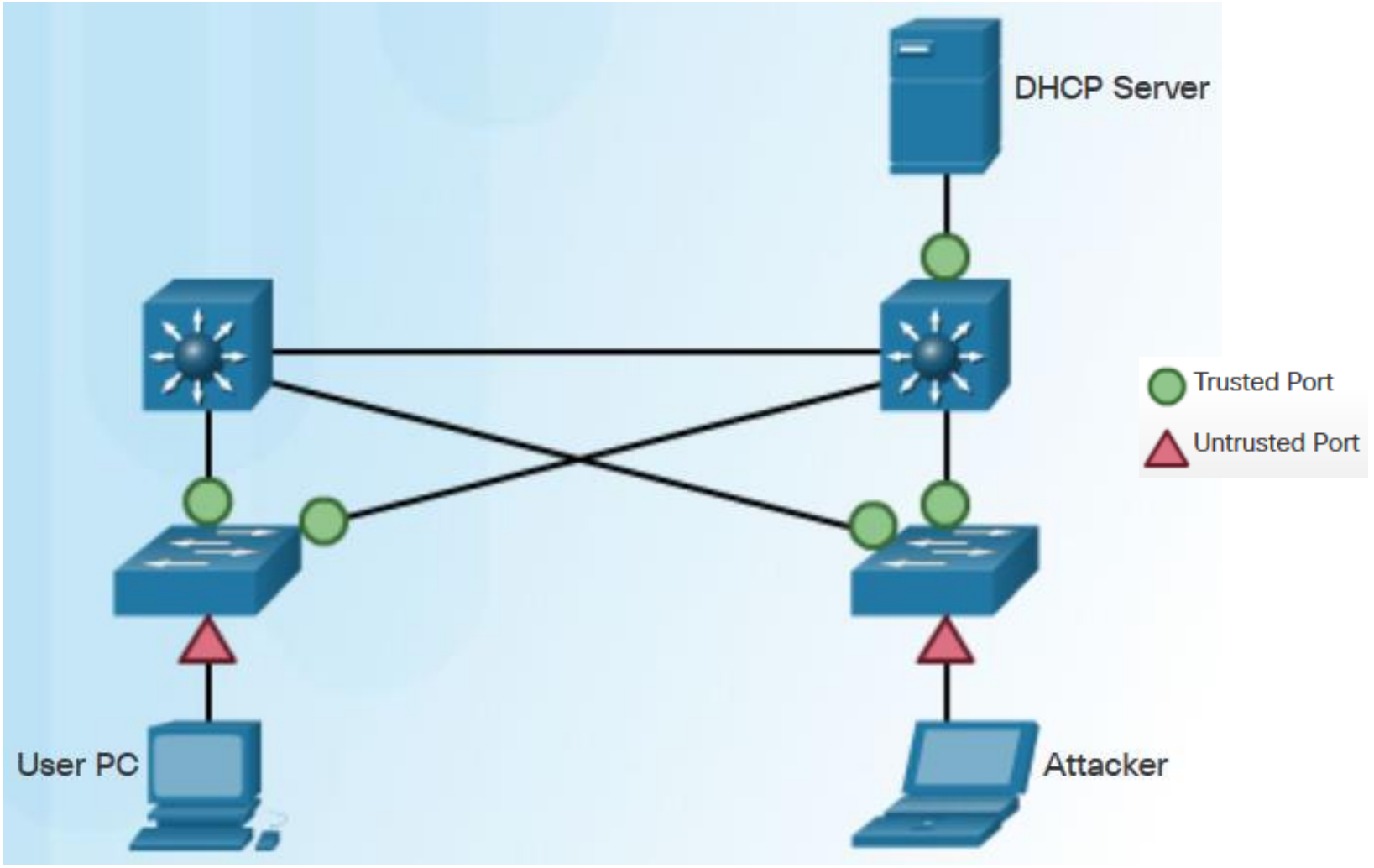
- Explicitly configure access links
- Disable DTP auto trunking using `switchport non-negotiate`
- Manually enable trunk links
- Set the native VLAN to others than 1
- Disable unused port and assign them to a black-hole VLAN.

DHCP Attacks

- DHCP spoofing attack – using a roque DHCP server
- DHCP starvation attack – an attacker leases all available IP addresses

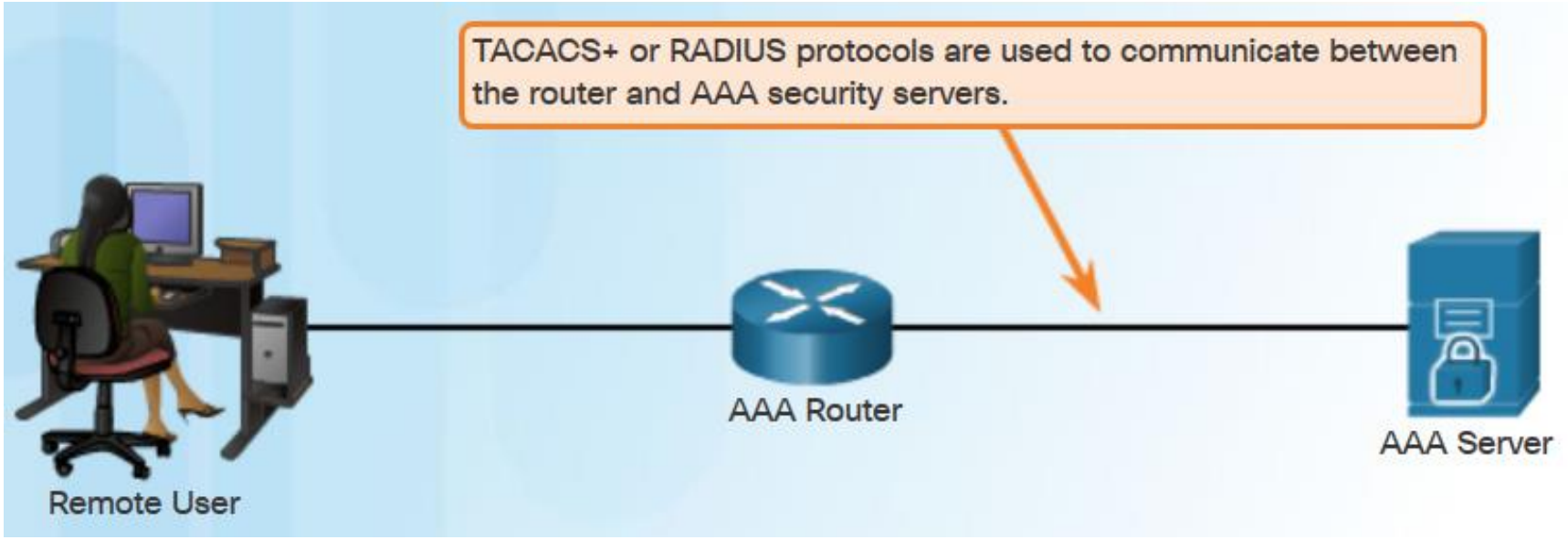


Mitigating DHCP attacks using DHCP snooping



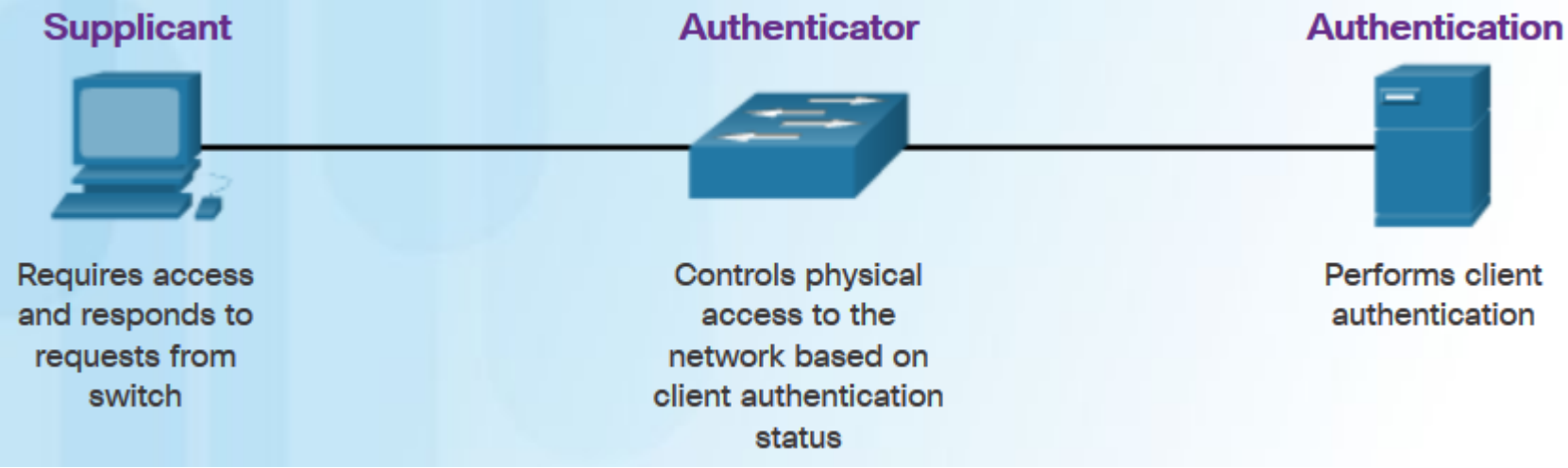
- Enable DHCP snooping on a interface or a VLAN
- Define trusted ports to upstream DPHC servers (explicitly configured)
- Define untrusted ports to hosts (default)

User Access Control on L2 using AAA



- AAA Framework: Authentication, Authorization, Accounting
- Router/switch authenticates a user via username and password.
- Implementing AAA in Cisco devices:
  1. Local AAA Authentication: local user database
  2. Server-based AAA Authentication: central Radius/TACACS+ database

Port Based Authentication



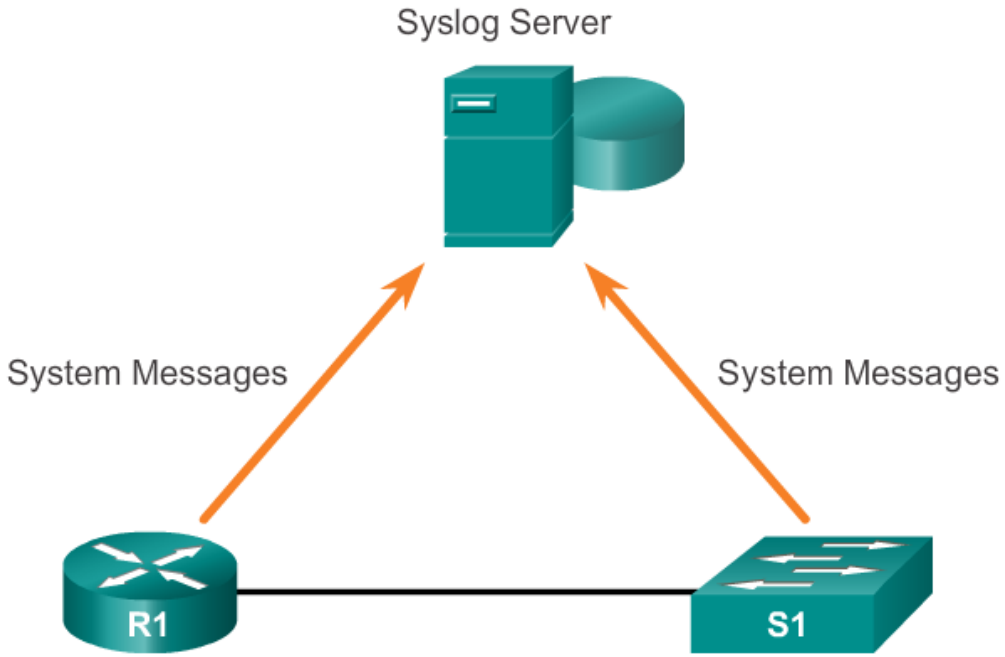
- Configure 802.1x port-based authentication
- Client software provides authentication with the switch or AP
- Switch (Authentication) uses local database or contact authentication server (Radius, TACACS+)

5.2 Syslog and NTP

Cisco | Networking Academy®
Mind Wide Open™

Introduction to Syslog

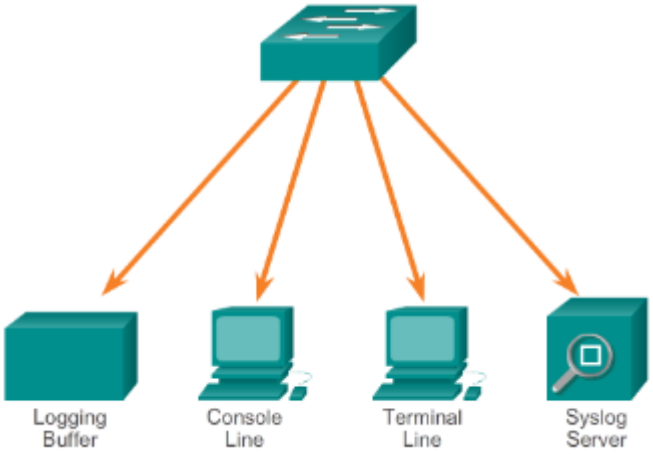
- Protocol for logging computers and network device messages (RFC 5424)
- Supported by routers, switches, application servers, firewalls, etc.
- System messages sent across the network to syslog servers:
  - Gather logging information for monitoring and troubleshooting
  - Select the type of logging information that is captures



Syslog Operation

Syslog destinations

- Logging buffer
- Console line
- Terminal line
- Syslog server



Syslog message format

- Severity levels 0-7

Severity Name	Severity Level	Explanation
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

- Message format

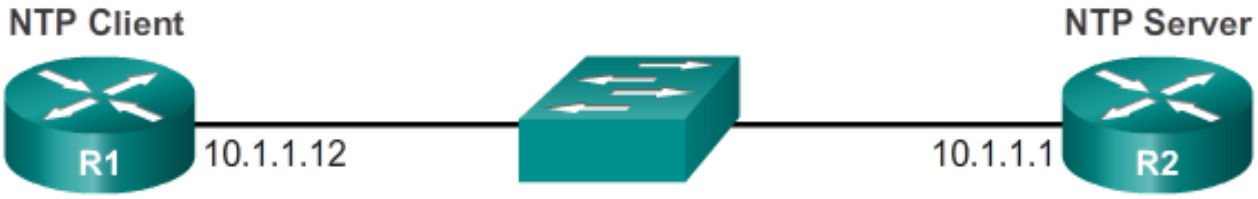
seq no: timestamp: %facility-severity-MNEMONIC:description

Field	Explanation
seq no	Stamps log messages with a sequence number only if the **`service sequence-numbers`** global configuration command is configured.
timestamp	Date and time of the message or event, which appears only if the **`service timestamps`** global configuration command is configured.
facility	The facility to which the message refers.
severity	Single-digit code from 0 to 7 that is the severity of the message.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

Service Timestamp

- Log messages can be time-stamped.
- Timestamps are set using `(conf)#service timestamp log datetime`
- The clock can be configured manually or automatically using NTP.

Configuring Network Time Protocol (NTP)

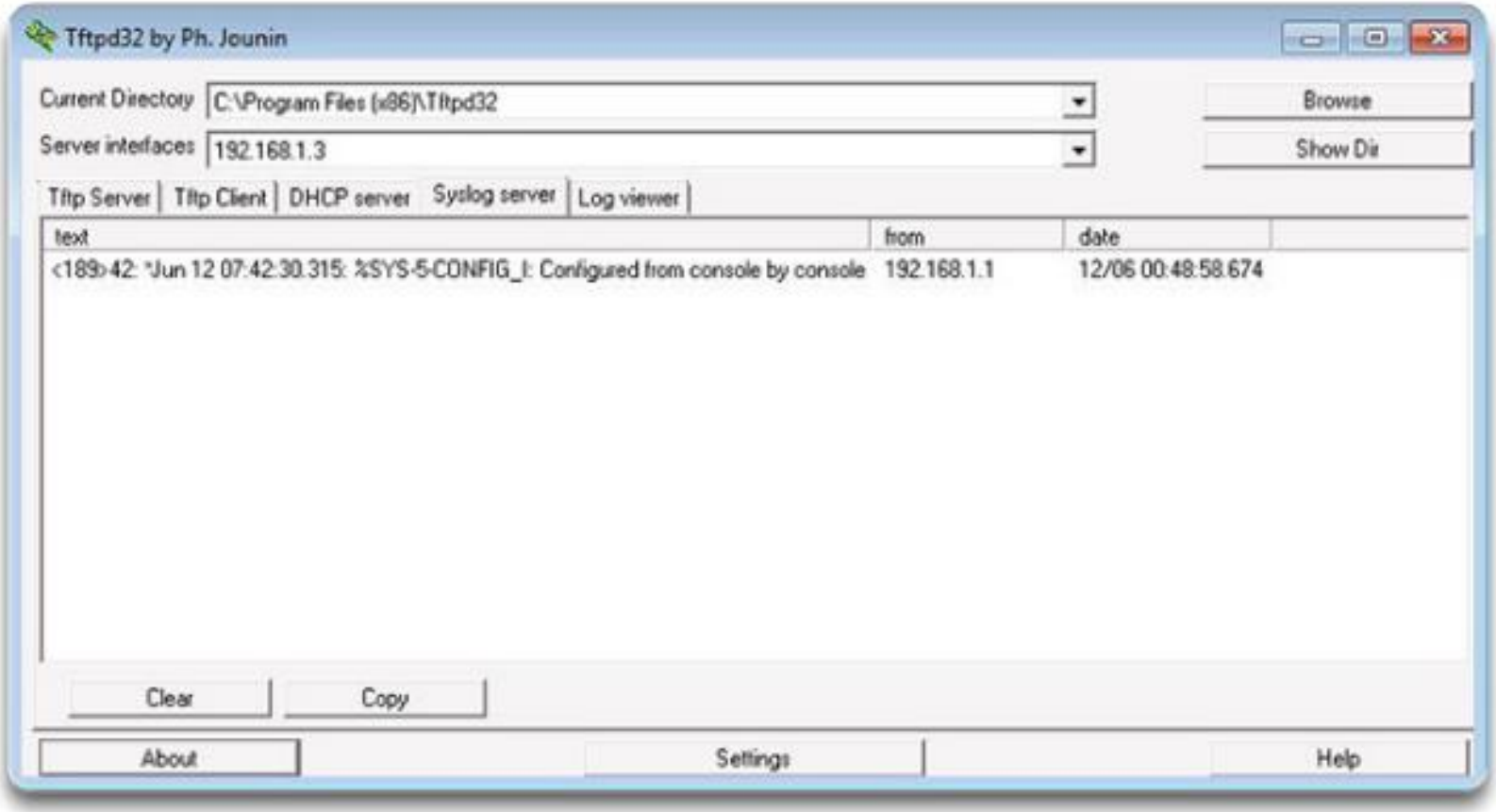



```
R2(config)# ntp master 1
```

```
R1(config)# ntp server 10.1.1.1
```

Syslog Server

- Provides a relatively user-friendly interface for viewing syslog output.
- Parses the output and displays the messages
- Network administrators can easily navigate the large amount of data.



Router and Switch Commands for Syslog Clients

```
R1(config)# logging 192.168.1.3
R1(config)# logging trap 4
R1(config)# logging source-interface g0/0
R1(config)# interface loopback 0
R1(config-if)#
*Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:06:03.902: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:06:03.902: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to
host 192.168.1.3 port 514 started - CLI initiated
R1(config-if)# shutdown
R1(config-if)#
*Jun 12 22:06:49.642: %LINK-5-CHANGED: Interface Loopback0,
changed state to administratively down
*Jun 12 22:06:50.642: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to down
R1(config-if)# no shutdown
R1(config-if)#
*Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:09:19.210: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
R1(config-if)#
```

Syslog Configuration

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0
flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

    Console logging: level debugging, 32 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 32 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 34 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (8192 bytes):

*Jan  2 00:00:02.527: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User
```

Default Logging Service Settings

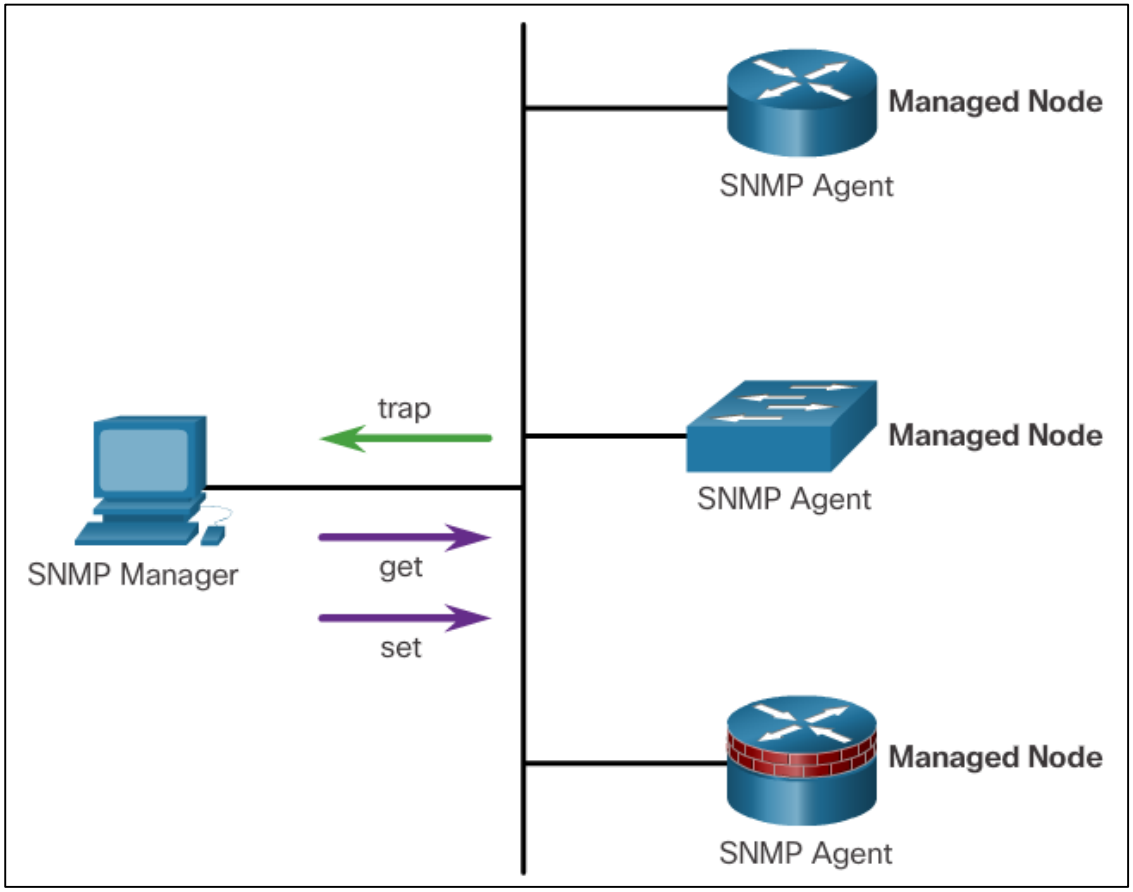
Verifying Syslog

```
R1# show logging | include changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface Serial0/0/1,
changed state to up
*Jun 12 17:46:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/1, changed state to up
*Jun 12 17:46:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/0/1, changed state to up
*Jun 12 20:28:43.427: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
*Jun 12 20:28:44.427: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
*Jun 12 22:04:11.862: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:06:03.902: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:09:19.210: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:35:55.926: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:35:56.926: %LINEPROTO-5-UPDOWN: Line protocol on
```

5.3 SNMP

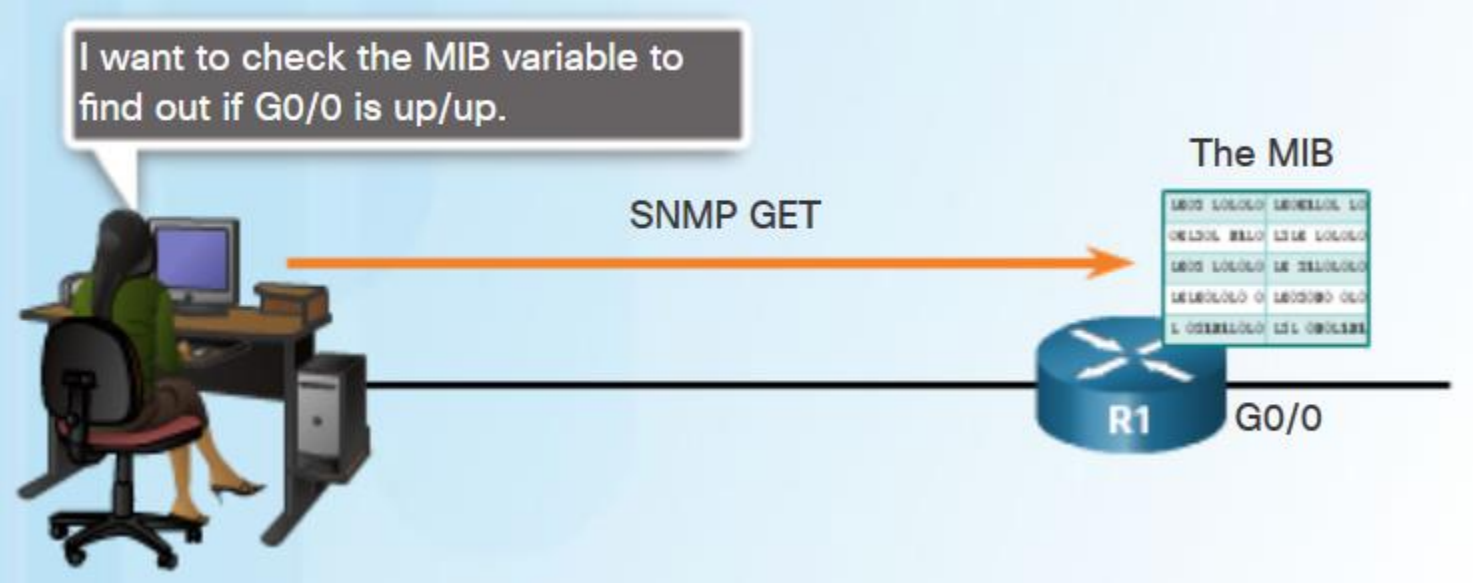
Cisco | Networking Academy®
Mind Wide Open™

Simple Network Management Protocol (SNMP)



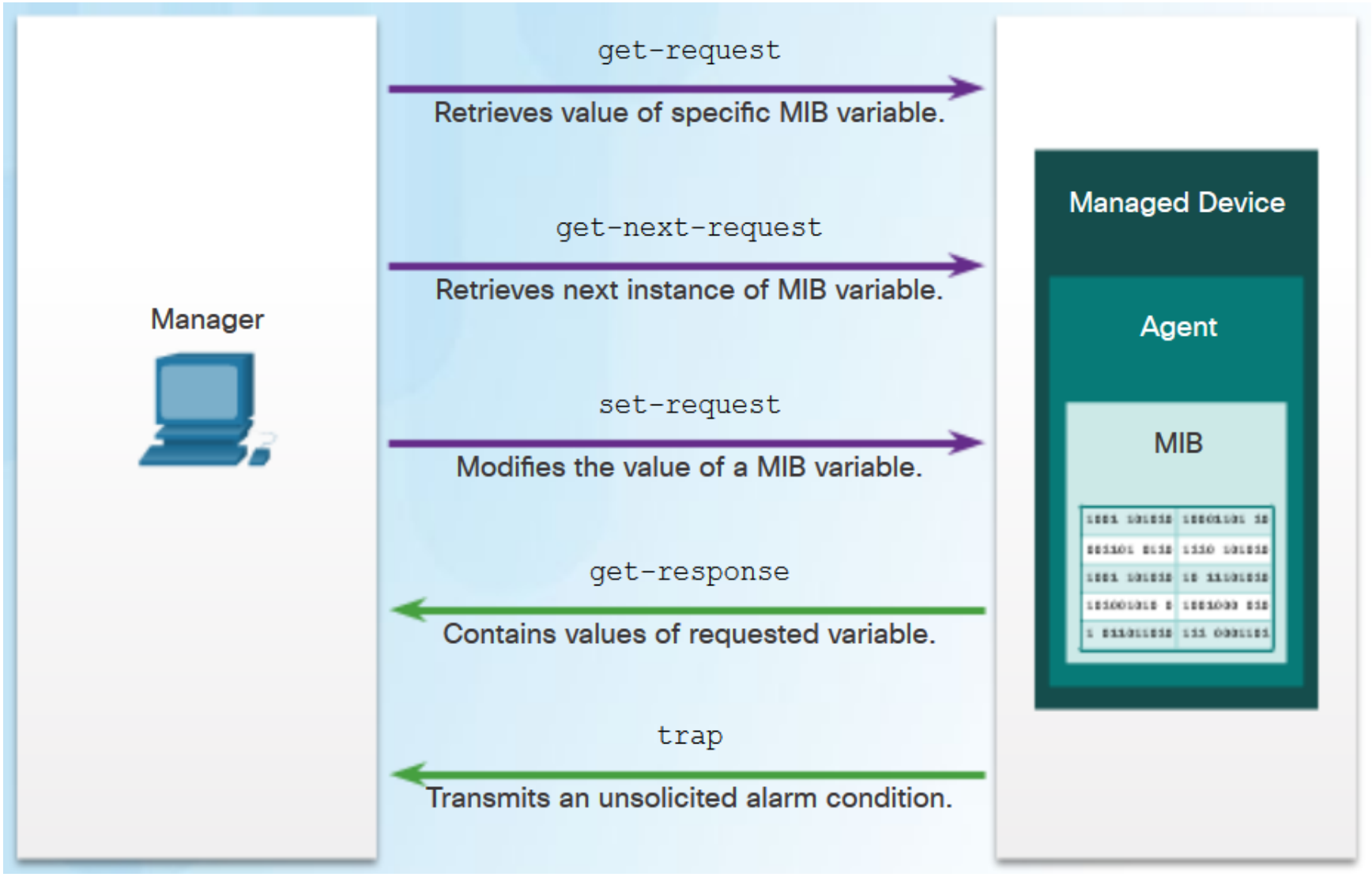
- SNMP allows administrators to monitor devices on an IP network.
- SNMP Elements: Manager, Agent, MIB
- SNMP Operation: Trap, Get, Set

Simple Network Management Protocol (SNMP)



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.

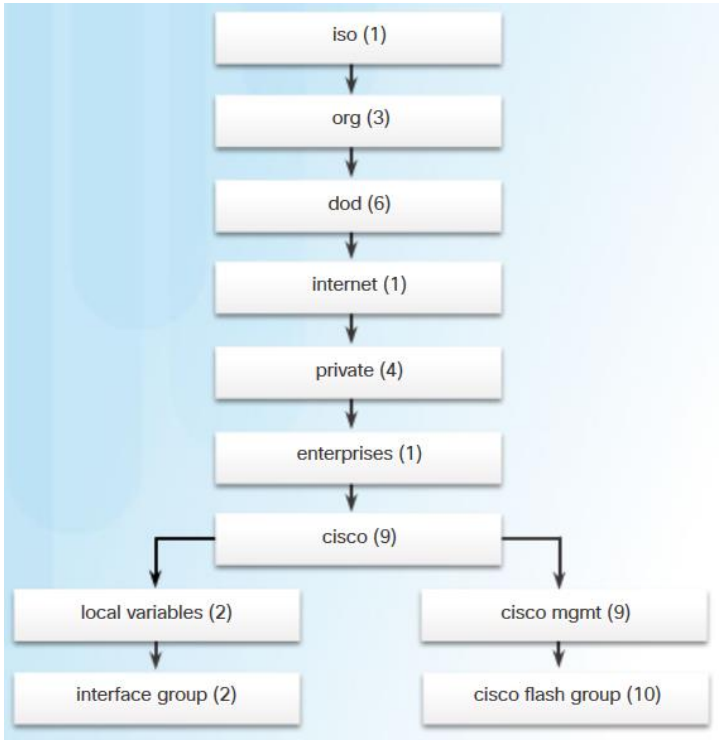
Simple Network Management Protocol (SNMP)



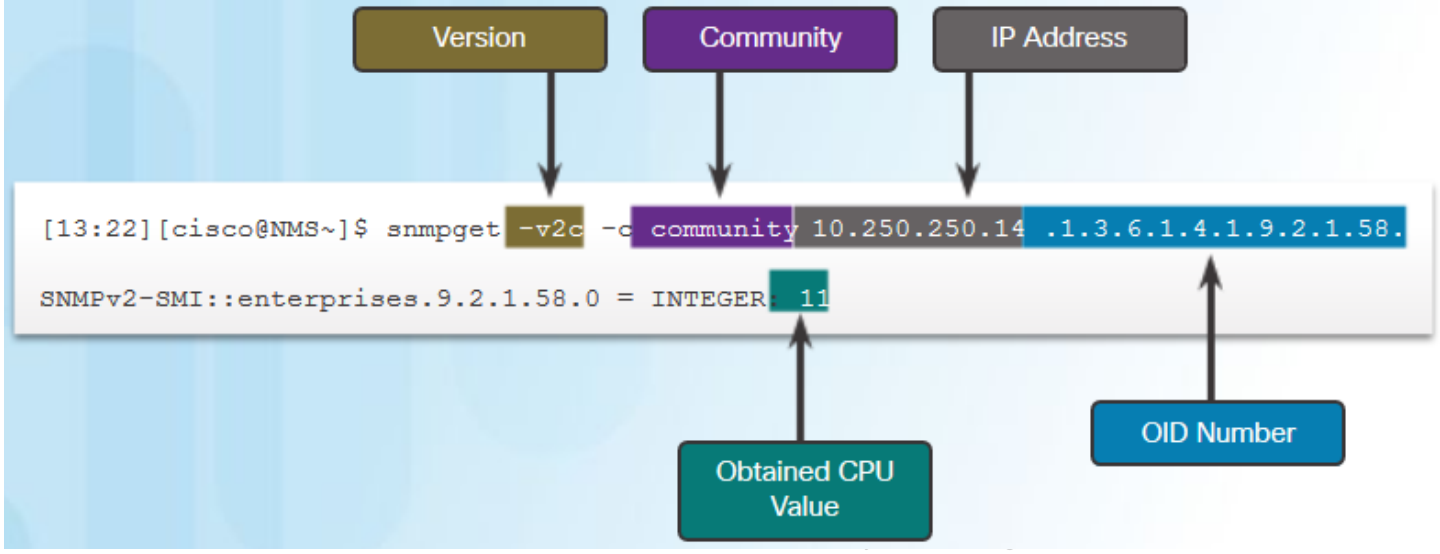
SNMP Versions and Security

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.

SNMP MIB



SNMP Object Navigator



Configuring SNMP

1. (Required) Configure the community string and access level

```
snmp-server community string ro | rw
```

2. (Optional) Set the location of the device

```
snmp-server location text
```

3. (Optional) Set the system contact

```
snmp-server contact text
```

4. (Optional) Restrict SNMP access to by an ACL

```
snmp-server community string access-list-number
```

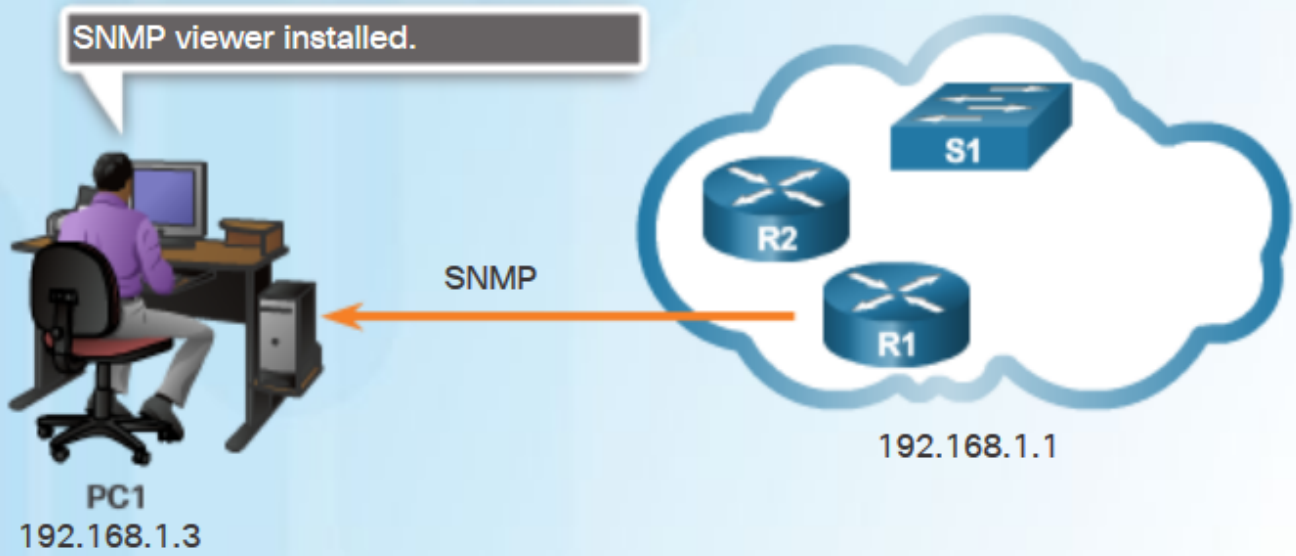
5. (Optional) Specify the recipient of the SNMP trap operations

```
snmp-server host host-id [version {1 | 2c | 3 [auth |
noauth | priv]}] community-string
```

6. (Optional) Enable traps on an SNMP agent

```
snmp-server enable traps notification-types
```

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
```

Verifying SNMP Configuration

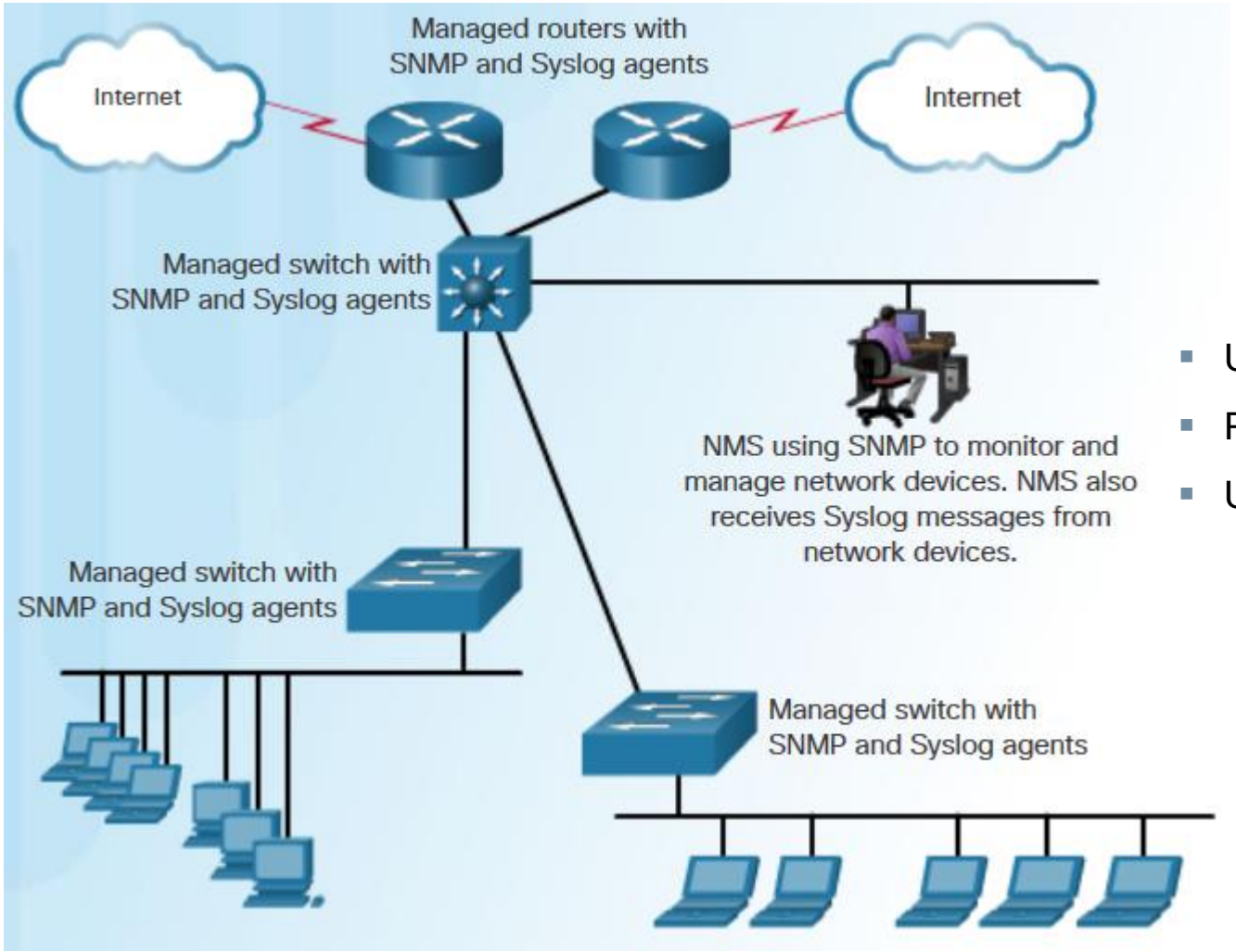
```
R1# show snmp
Chassis: FTX1636848Z
Contact: Wayne World
Location: NOC_SNMP_MANAGER
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered 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.
```

show snmp

```
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
```

show snmp community

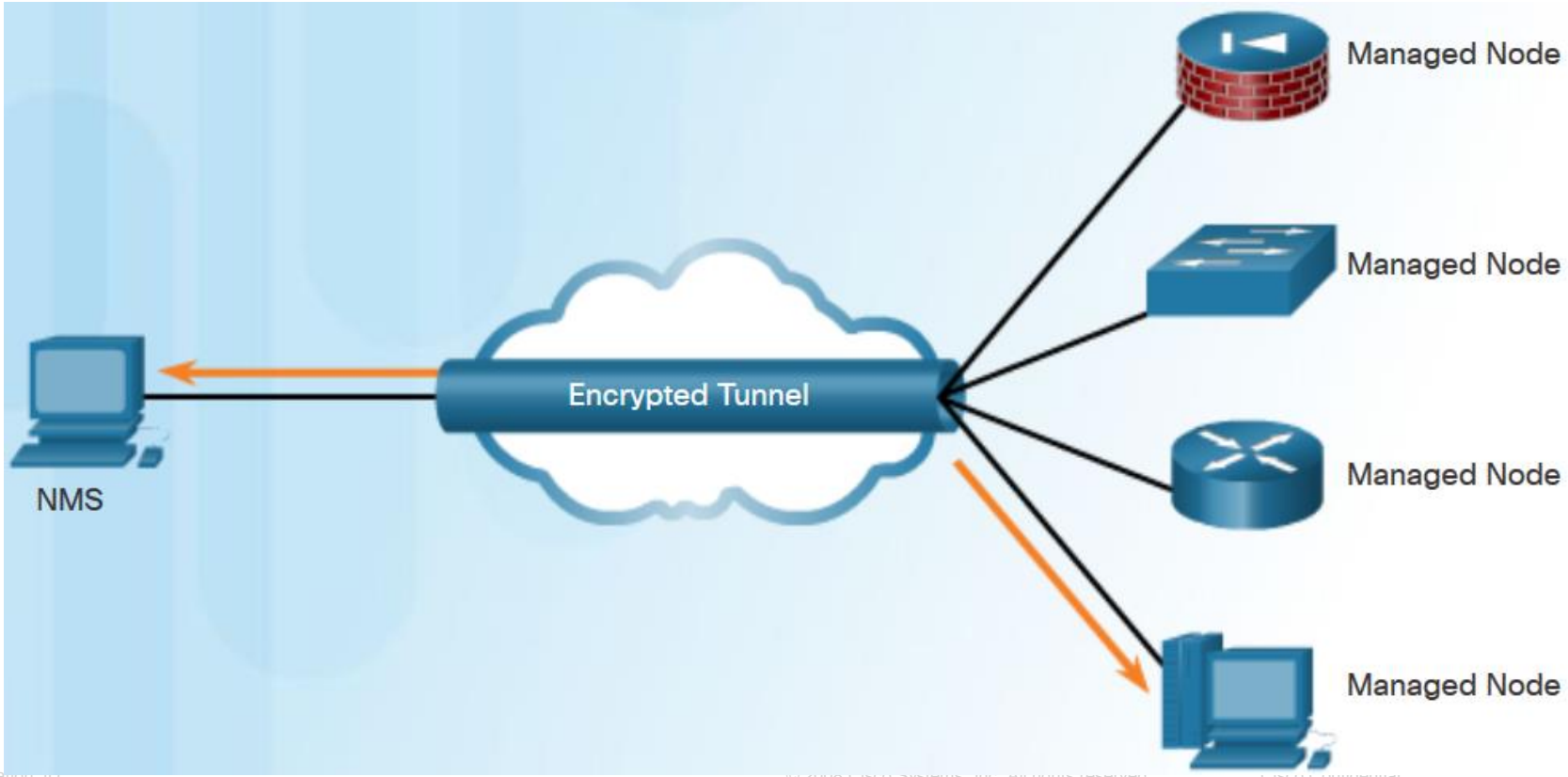
SNMP Best Practices



- Use read-only communities
- Restrict access using ACLs
- Use SNMPv3

SNMPv3

- Message Encryption and Authentication
  1. Message integrity and authentication
  2. Encryption
  3. Access control



Configuring SNMPv3

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
```

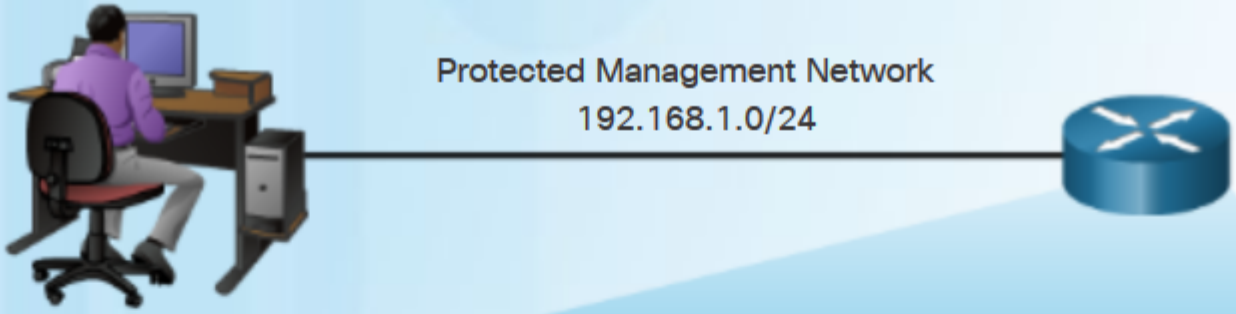
Step 3: Configure an SNMP group.

```
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 SNMPv3



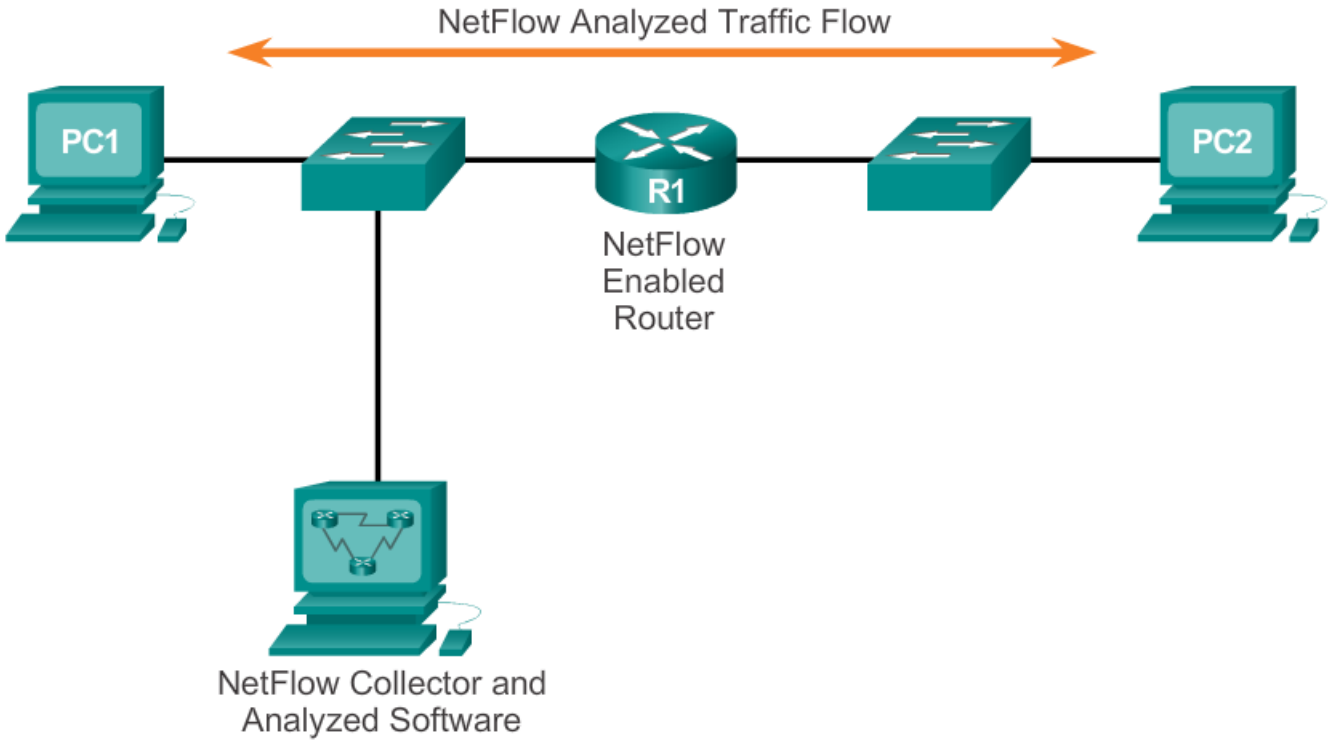

```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)# snmp-server view SNMP-RO iso included
R1(config)# snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
R1(config)# snmp-server user BOB ADMIN v3 auth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

5.4 NetFlow

Cisco | Networking Academy®
Mind Wide Open™

Introduction to NetFlow

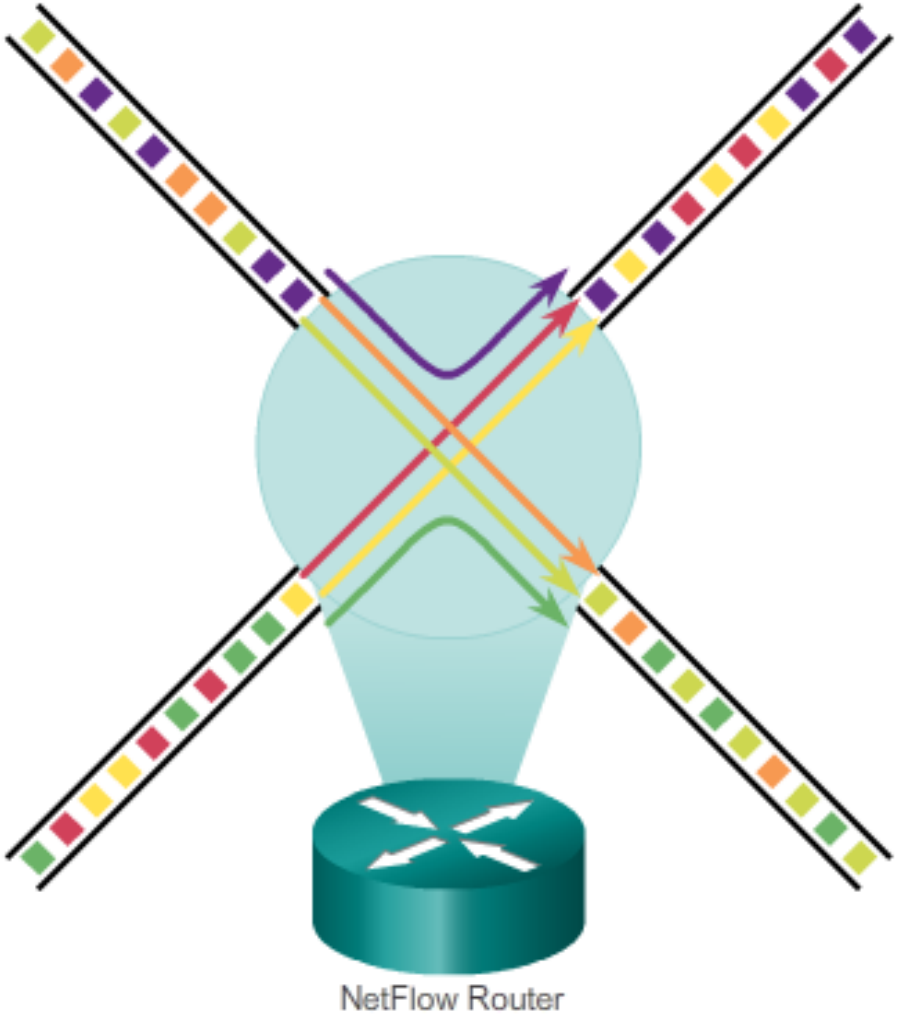
- Monitoring system to collect statistics on packets flowing through a device.
- Defined by RFC 3954 (NetFlow version 9)
- Architecture
  - NetFlow Exporter (NetFlow Enabled Router, NetFlow Probe)
  - NetFlow Collector and Analyzed software
  - NetFlow Protocol



Network Flows

The flow is a set of packets having the same combination of seven key fields.

- Source and destination IP address
- Source and destination port number
- Layer 3 protocol type
- Type of service (ToS) marking
- Input logical interface



NetFlow Configuration

1. Configure NetFlow data capture from ingress and egress interface

```
(conf-if)# ip flow ingress
(conf-if)# ip flow egress
```

2. Configure NetFlow data export

```
(conf)# ip flow-export destination ip-address {udp-port}
```

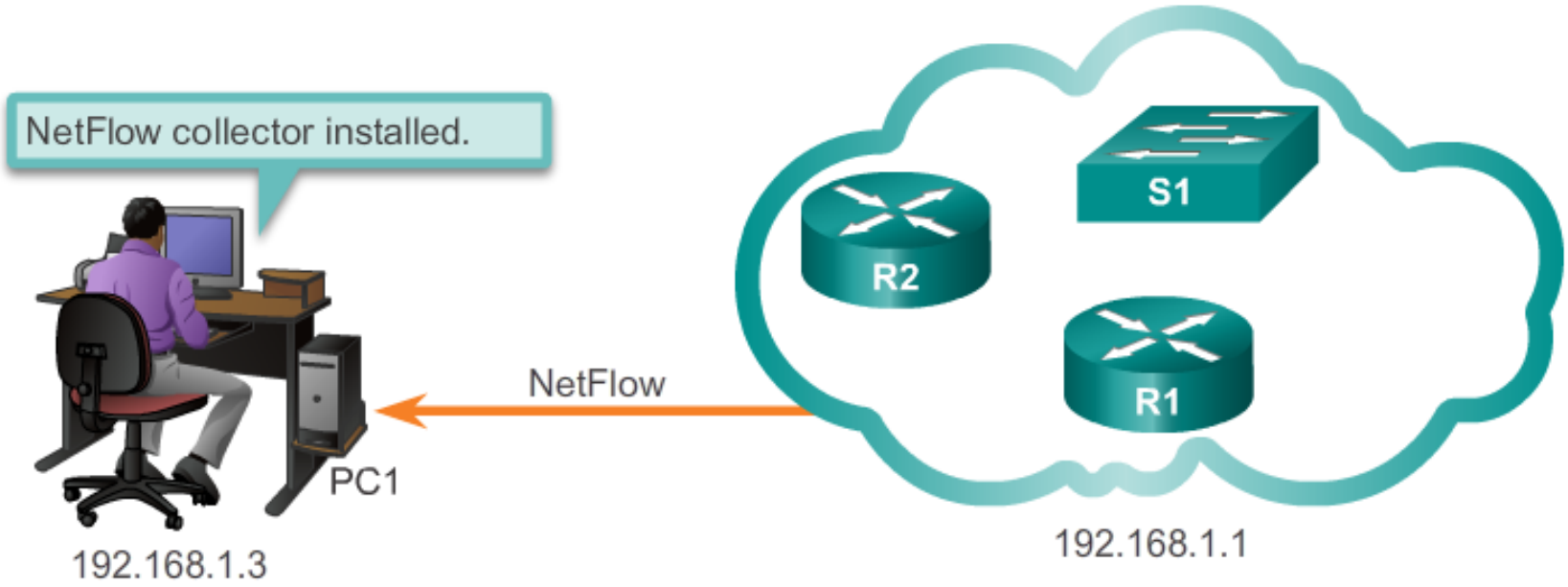
3. (Optional) Configure NetFlow version (1, 5, 7, 8, 9)

```
(conf)# ip flow-export version version
```

4. (Optional) Define source interface as the source of packets sent to a collector

```
(conf)# ip flow-export source typenumber
```

NetFlow Configuration




```
R1(config)# interface GigabitEthernet 0/1
R1(config-if)# ip flow ingress
R1(config-if)# ip flow egress
R1(config-if)# exit
R1(config)# ip flow-export destination 192.168.1.3 2055
R1(config)# ip flow-export version 5
```

Verifying NetFlow

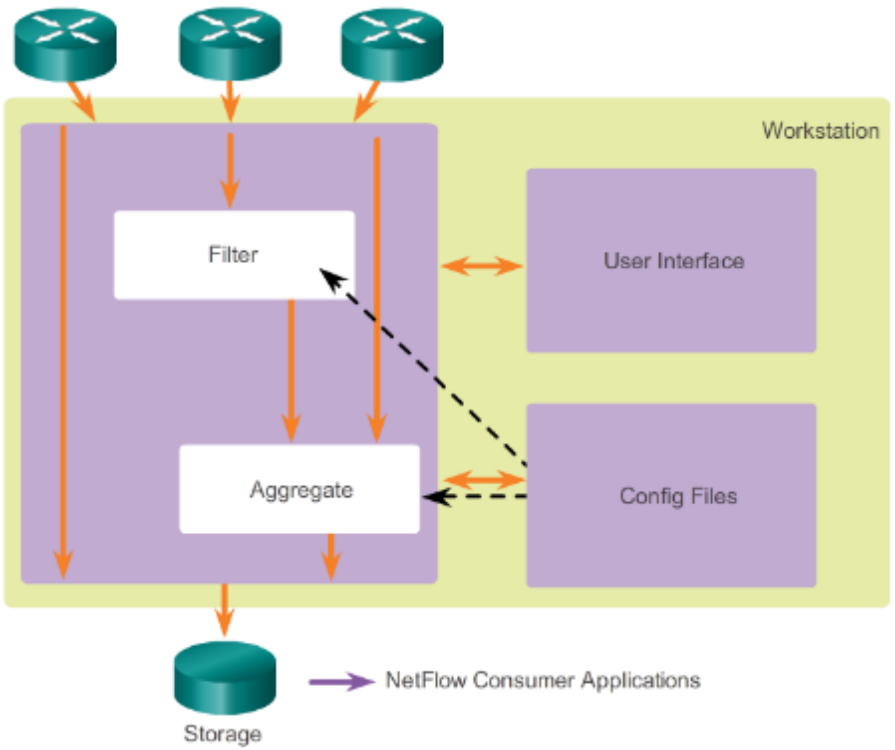
```
R1# show ip cache flow
IP packet size distribution (178617 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .002 .080 .008 .005 .001 .000 .001 .001 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .895 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  5 active, 4091 inactive, 1573 added
  18467 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  5 active, 1019 inactive, 1569 added, 1569 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol       Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------       Flows     /Sec    /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet         3      0.0        3    50      0.0       1.0      15.0
TCP-WWW          245      0.0        6    93      0.0       0.3       2.4
TCP-other        529      0.0       27    57      0.2       0.7       6.2
UDP-other        328      0.0        6   107      0.0       2.4      15.3
ICMP             711      0.0      226  1261      2.4       0.2      15.4
Total:          1816      0.0       98  1137      2.7       0.8      11.0

SrcIf         SrcIPaddress    DstIf      DstIPaddress    Pr SrcP DstP  Pkts
G0/1          192.168.1.3     Local      192.168.1.1     06 100B 01BB     1
G0/1          192.168.1.3     Local      192.168.1.1     01 0000 0303     1
G0/1          192.168.1.3     Local      192.168.1.1     01 0000 0800     1
```

```
R1# show ip flow interface
GigabitEthernet0/1
  ip flow ingress
  ip flow egress
```

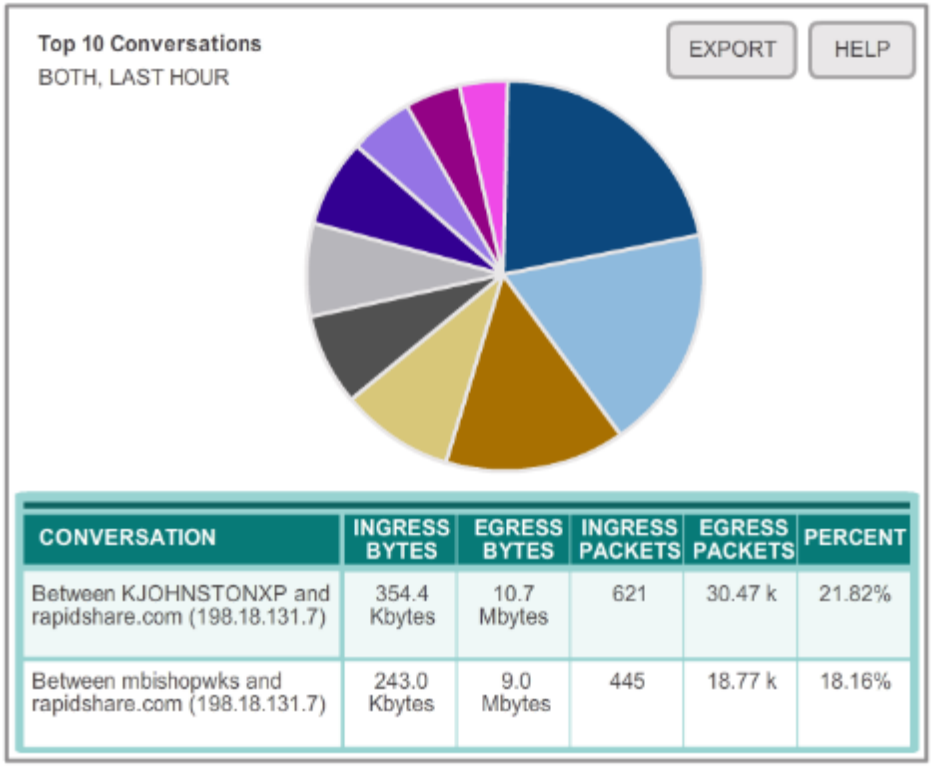
```
R1# show ip flow export
Flow export v5 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.1.3 (2055)
  Version 5 flow records
  1764 flows exported in 532 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

NetFlow Collector

NetFlow Collector Functions



NetFlow Collector Top Talkers



CONVERSATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
Between KJOHNSTONXP and rapidshare.com (198.18.131.7)	354.4 Kbytes	10.7 Mbytes	621	30.47 k	21.82%
Between mbishopwks and rapidshare.com (198.18.131.7)	243.0 Kbytes	9.0 Mbytes	445	18.77 k	18.16%

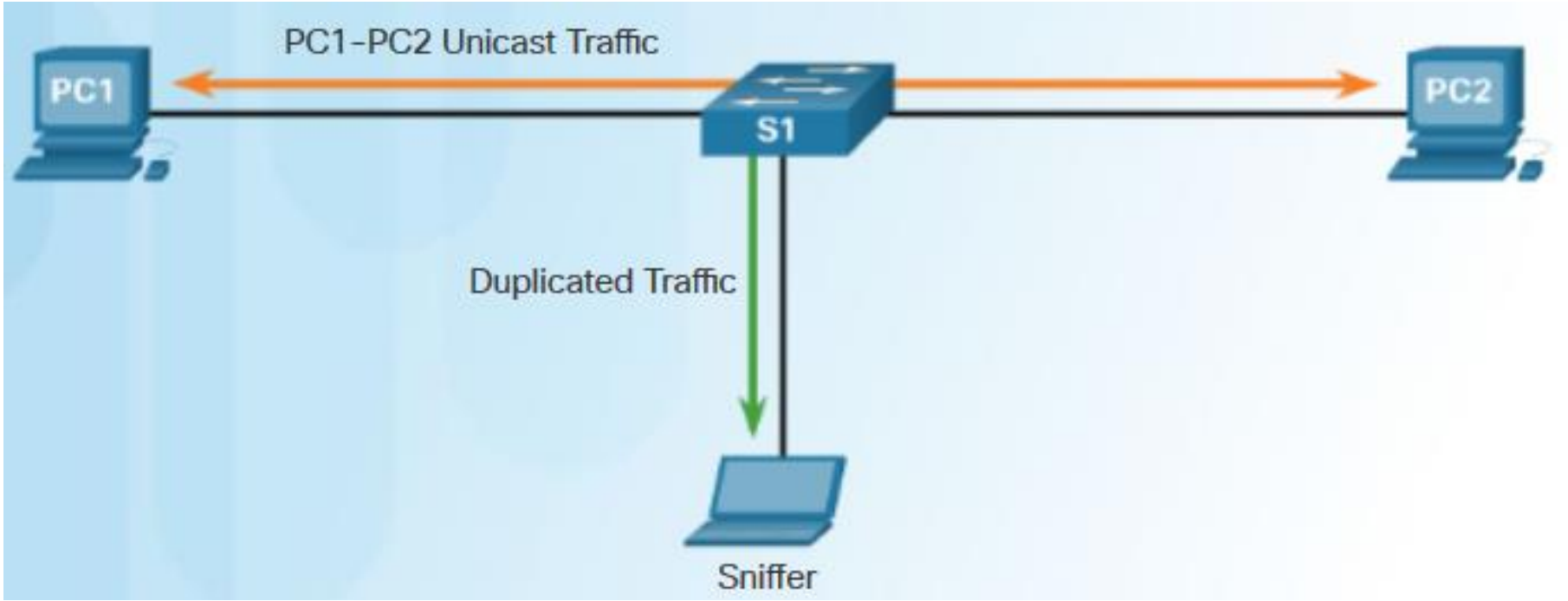
5.5 Switch Port Analyzer

Cisco | Networking Academy®
Mind Wide Open™

Cisco Switch Port Analyzer (SPAN)

Port mirroring

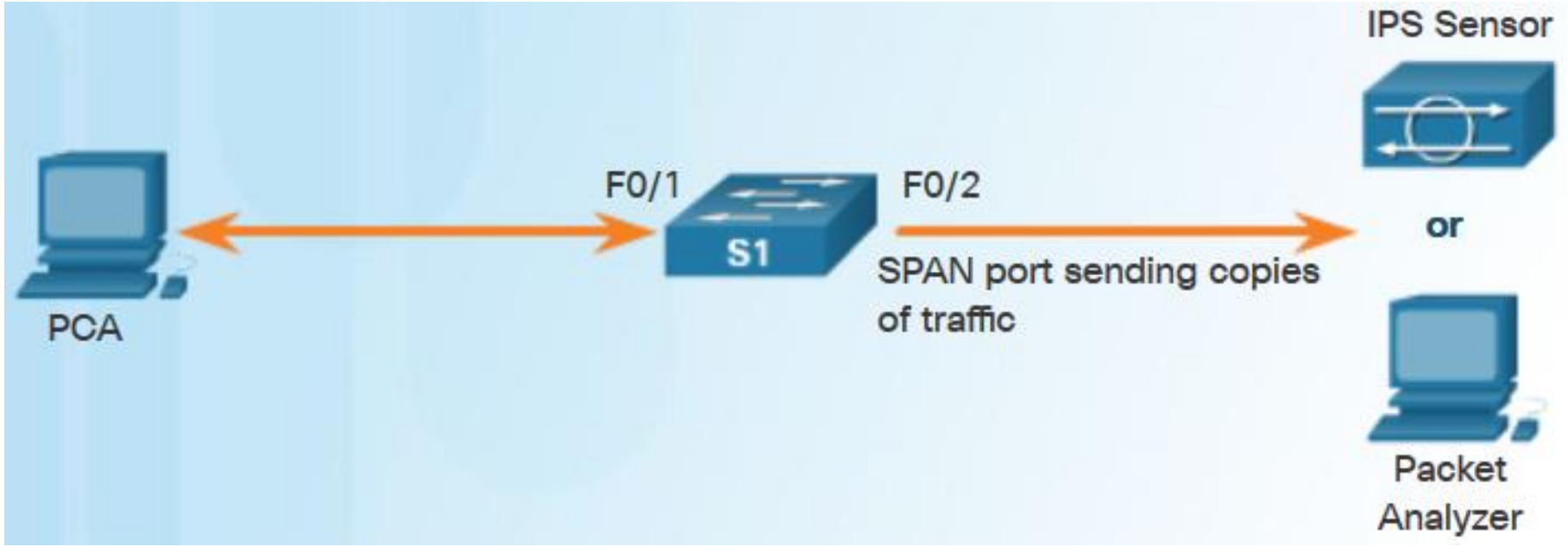
- The port mirroring feature allows a switch to copy and send Ethernet frames from specific ports to the destination port connected to a packet analyzer.
- The original frame is still forwarded in the usual manner.



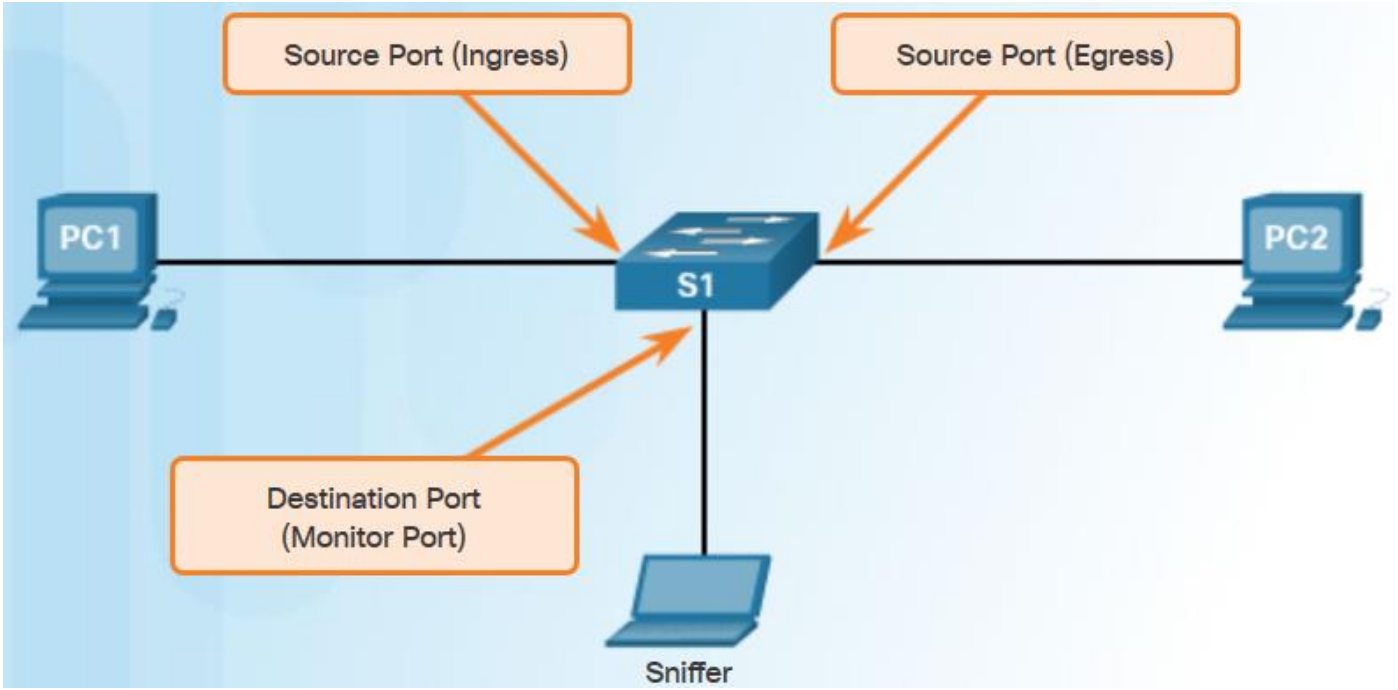
Cisco Switch Port Analyzer (SPAN)

Analyzing Suspicious Traffic

- Packet analyzers
- Intrusion Prevention Systems (IPSs)

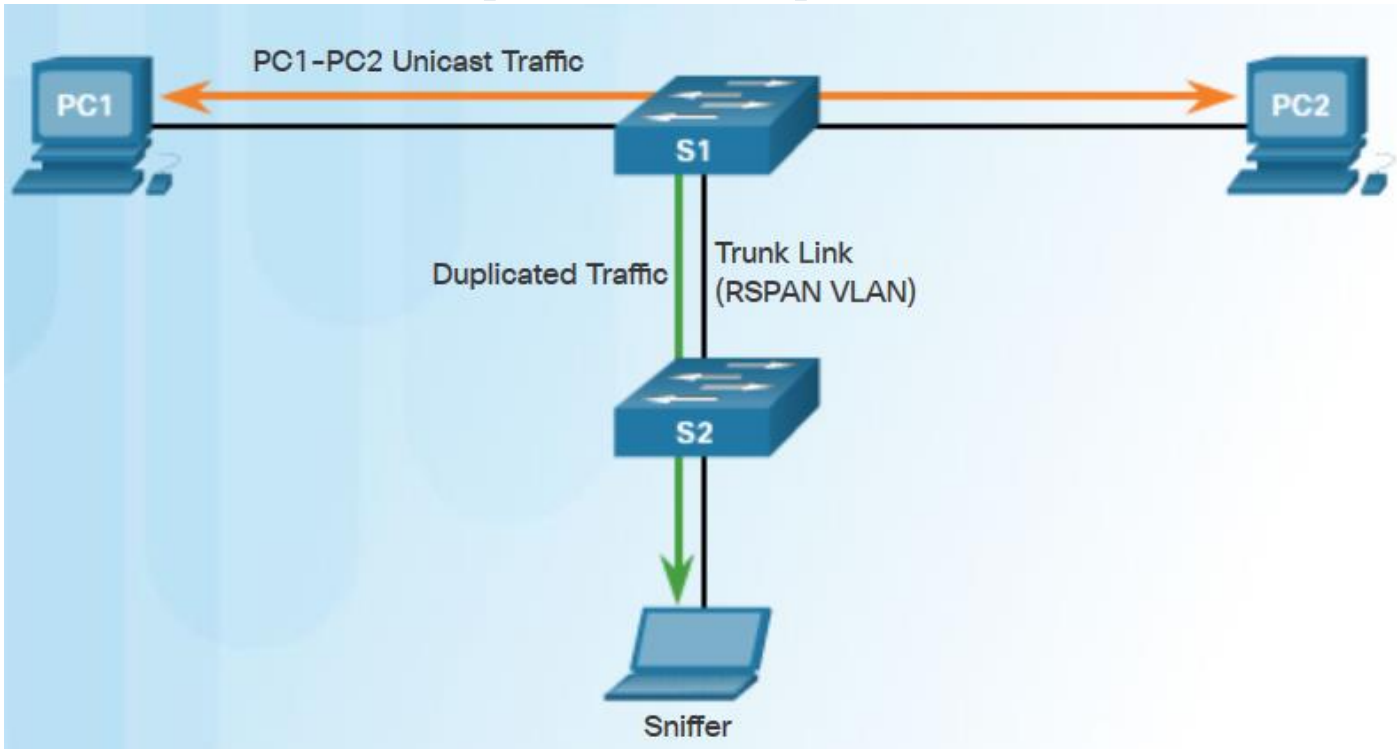


Local SPAN



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 (RSPAN)



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

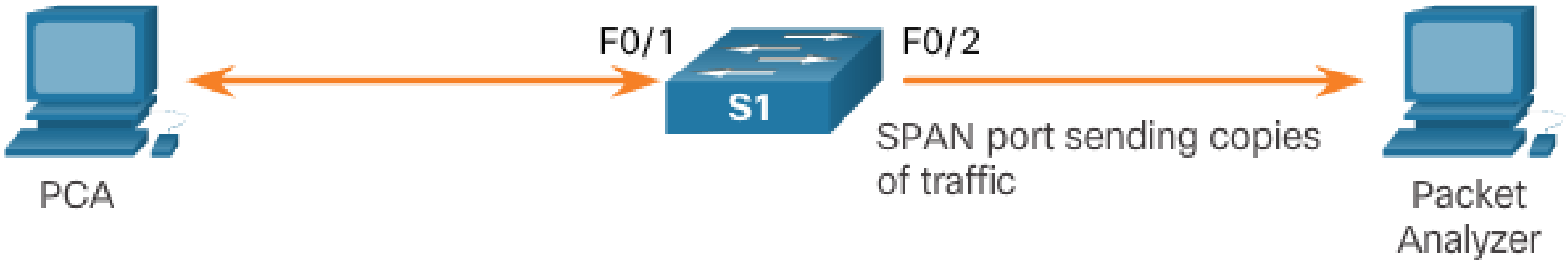
- Use **monitor session** global configuration command

Associate a SPAN session with a source port

```
Switch(config)# monitor session number source [ interface interface | vlan vlan ]
```

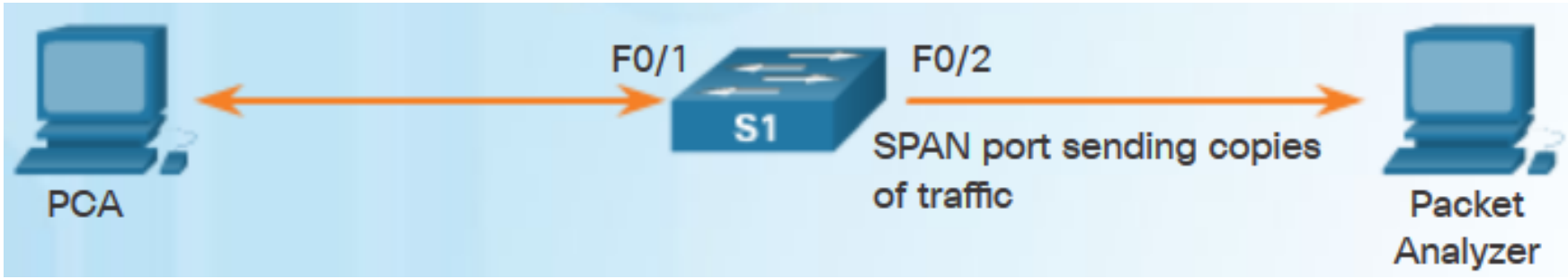
Associate a SPAN session with a destination port

```
Switch(config)# monitor session number destination [ interface interface | vlan vlan ]
```




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

SPAN Verification




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


S1#
```