Chapter 5: Network Security and Monitoring

Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved.

Chapter 5 - Sections & Objectives

- 5.1 LAN Security
  - Explain how to mitigate common LAN security.
- 5.2 SNMP
  - Configure SNMP to monitor network operations in a small to medium-sized business network.
- 5.3 Cisco Switch Port Analyzer (SPAN)
  - Troubleshoot a network problem using SPAN.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

5.1 LAN Security

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved.

LAN Security

- Physical Damage
  - Dropping, ESD, Lightning, UPS use, Theft
  - Physically securing devices
  - Environmental threats
- Common attacks against the Layer 2 LAN infrastructure include:
  - CDP Reconnaissance Attacks (shut down CDP)
  - Telnet Attacks (Close telnet access, complex passwords, ssh, acl)
  - MAC Address Table Flooding Attacks (shutdown unused ports, configure port security)
  - VLAN Attacks (put unused ports in unused vlan, hardcode access, change default vlan, port security)
  - DHCP Attacks (DHCP snooping, port security)

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

LAN Security Best Practices

- This topic covers several Layer 2 security solutions:
  - Mitigating MAC address table flooding attacks
    - using port security
    - Limit mac address numbers allowed
  - Mitigating VLAN attacks (don't use default native vlan1)
  - Mitigating DHCP attacks using DHCP spoofing
    - Uses ip-helper address across networks
    - DHCP snooping command – restricts replies from untrusted switch ports
    - Limit number of DHCP requests
  - Securing administrative access using AAA
    - authentication, authorization, accounting – local or remote server
    - Configure aaa server, either: Radius or TACACS+
  - Securing device access using 802.1X port-based authentication
    - Radius (open/UDP/one-way), TACACS+ (Cisco/TCP/two-way): username/password server
    - EAP encryption (optional)

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

LAN Security Best Practices

- Review - There are several strategies to help secure Layer 2 of a network:
  - Always use secure variants of these protocols such as SSH, SCP, SSL, SNMPv3, and Secure FTP (SFTP).
  - Always use strong passwords and change them often.
    - Can be configured/enforced
  - Enable CDP on select ports only.
    - Or LLDP (Link Layer Discovery Protocol IEEE 802.1AB)
  - Secure Telnet access.
  - Use a dedicated management VLAN where nothing but management traffic resides.
  - Use ACLs to filter unwanted access to management vlan/access ports
  - Hard code Access or Trunk ports

© 2008 Cisco Systems, Inc. All rights reserved.

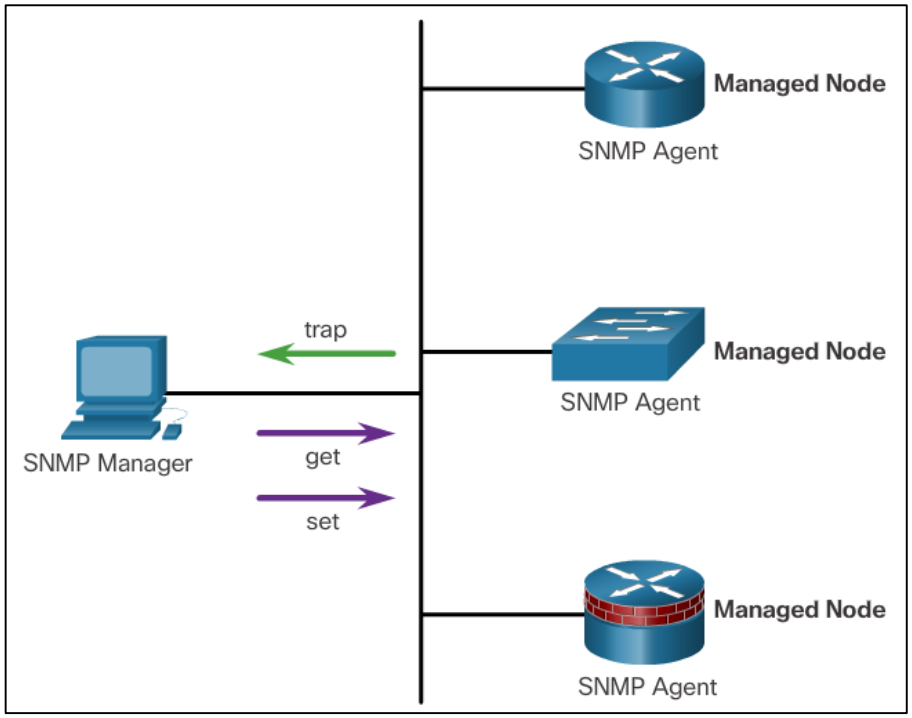
5.2 SNMP

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved.

SNMP Operation

- SNMP allows administrators to manage and monitor devices on an IP network.
- SNMP Elements
  - SNMP Manager (server polls)
  - SNMP Agent (network device reports)
  - MIB (device management info base saved locally)
- SNMP Operation
  - Trap (trap notification to mngr)
  - Get (collects information)
  - Set (change configurations)
  - Ports UDP 161 & 162



© 2008 Cisco Systems, Inc. All rights reserved.

SNMP Operation

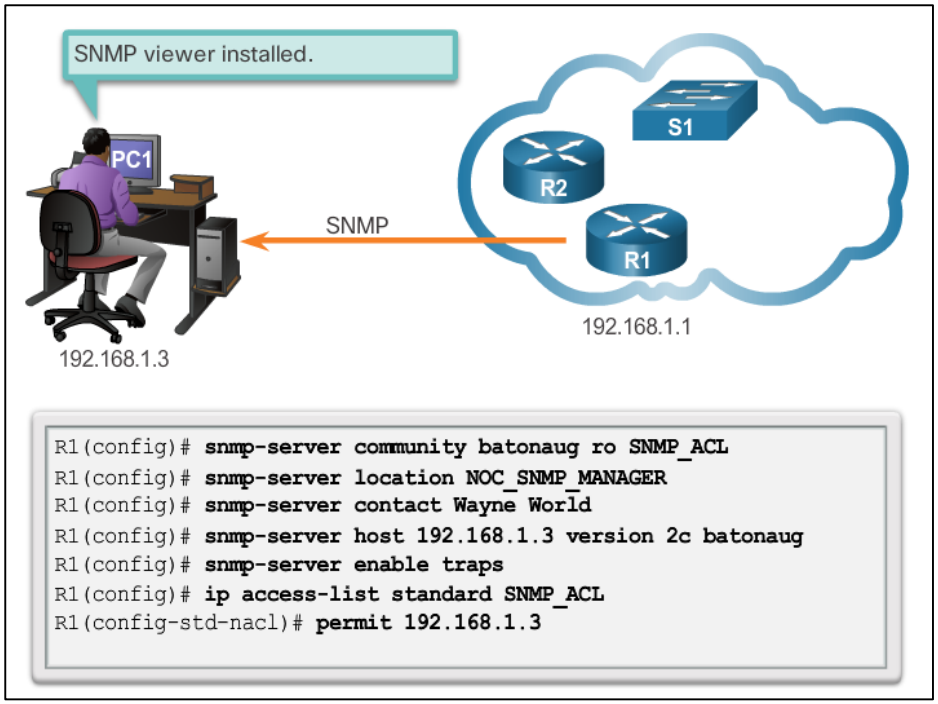
- SNMP Security Model and Levels

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.

© 2008 Cisco Systems, Inc. All rights reserved.

Configuring SNMP

- Configuration steps
  - Configure community string
  - Document location of device
  - Document system contact
  - Restrict SNMP Access
  - Specify recipient of SNMP Traps
  - Enable traps on SNMP agent




```
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
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Configuring SNMP

- Securing 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
```


© 2008 Cisco Systems, Inc. All rights reserved.

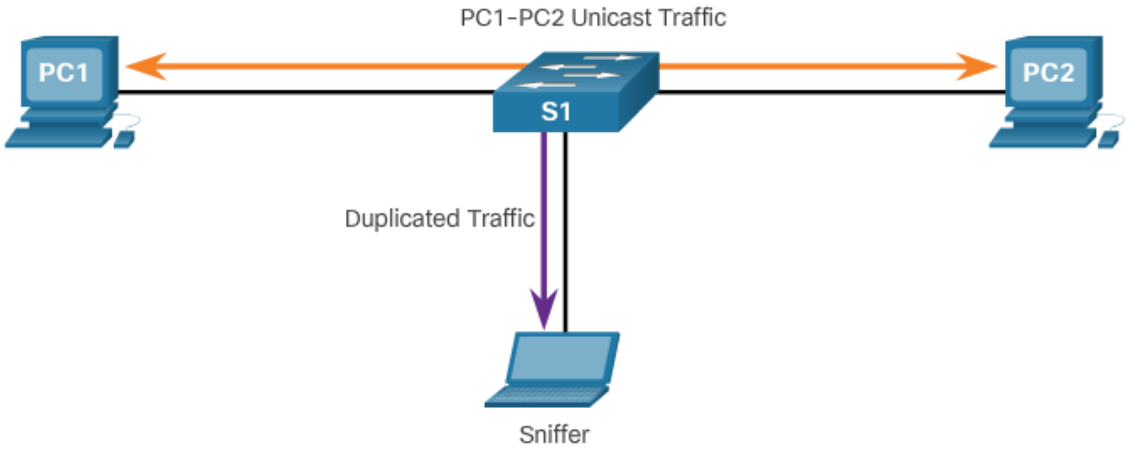
5.3 Cisco Switch Port Analyzer (SPAN)

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved.

SPAN Overview

- 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.

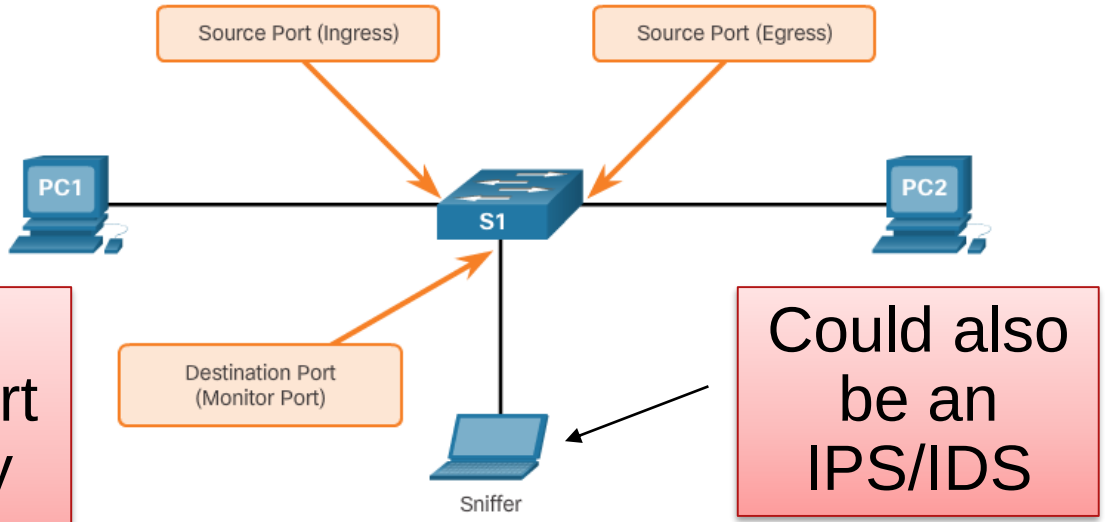


© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

SPAN Overview

- SPAN terminology

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 is part of security course

Could also be an IPS/IDS

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco Switch Port Analyzer

SPAN Configuration

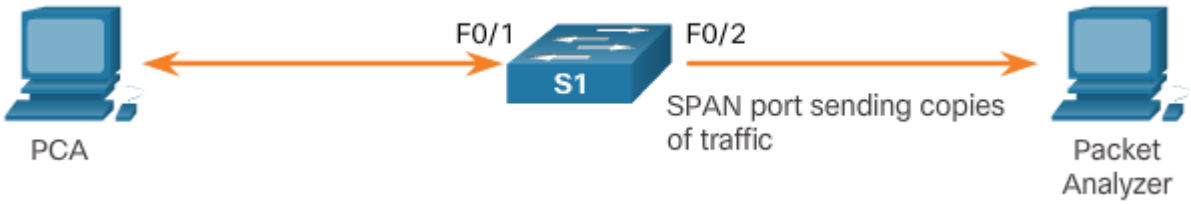
- Use **monitor session** global configuration command

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 ]
```

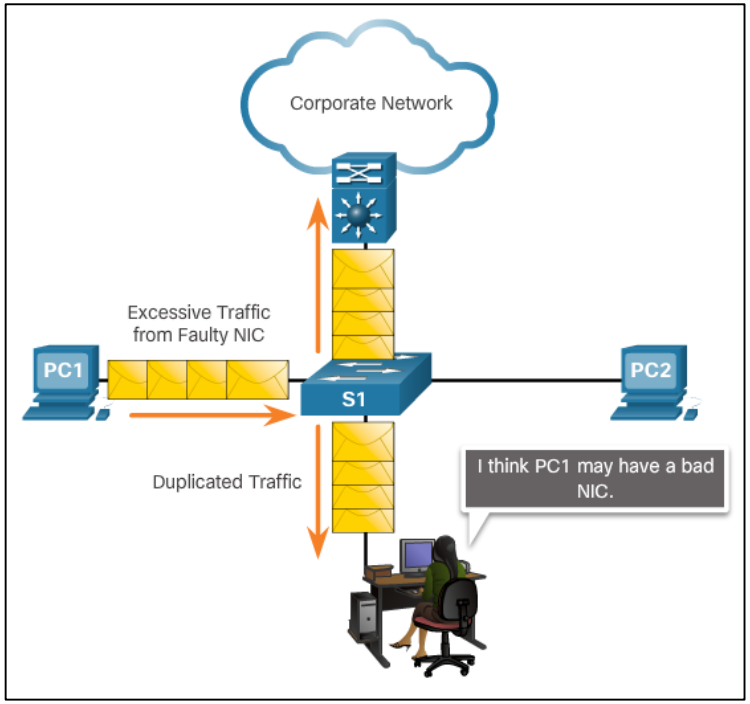



```
S1(config)# monitor session 1 source interface fastethernet 0/1
S1(config)# monitor session 1 destination interface fastethernet 0/2
```


© 2008 Cisco Systems, Inc. All rights reserved.

SPAN as a Troubleshooting Tool

- SPAN allows administrators to troubleshoot network issues
- Administrator can use SPAN to duplicate and redirect traffic to a packet analyzer
- Administrator can analyze traffic from all devices to troubleshoot sub-optimal operation of network applications



© 2008 Cisco Systems, Inc. All rights reserved.

© 2008 Cisco Systems, Inc. All rights reserved.

© 2008 Cisco Systems, Inc. All rights reserved.