Switching Features and Technologies for the Campus Network

CCNP SWITCH: Implementing Cisco IP Switched Networks

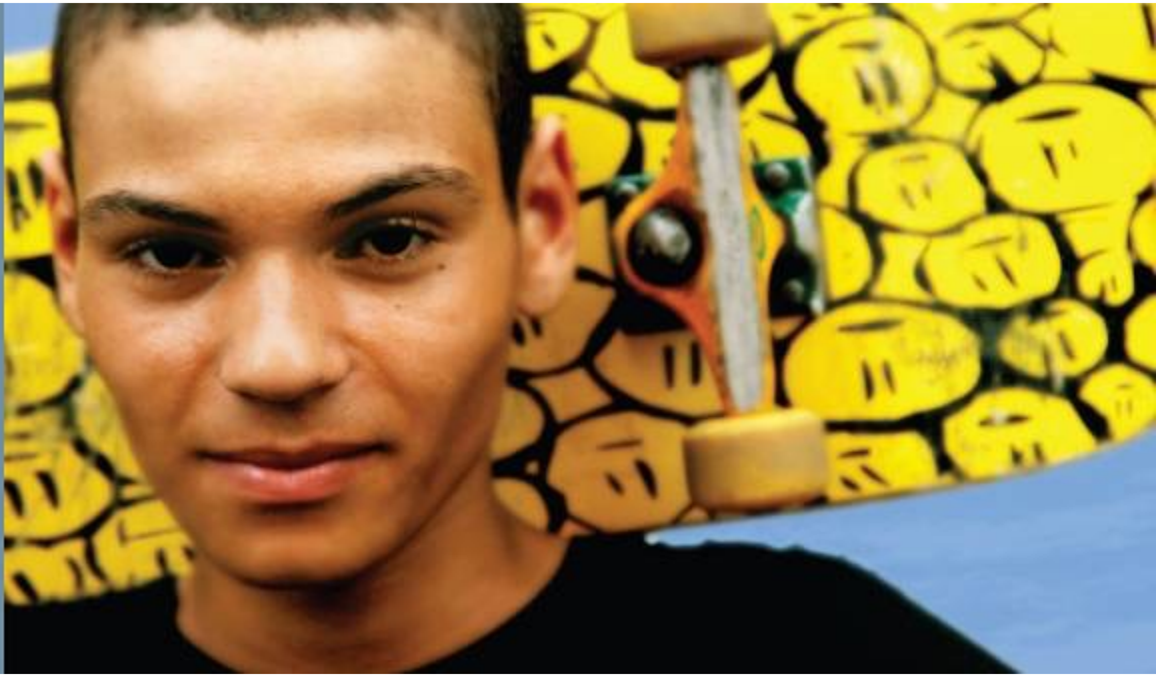
Cisco | Networking Academy®
Mind Wide Open™

Chapter 8 Objectives

This chapter covers the following Cisco Catalyst switch features:

- Discovery protocols
- Unidirectional Link Detection
- Power over Ethernet
- SDM templates
- Monitoring features
- IP SLA

Discovery Protocols



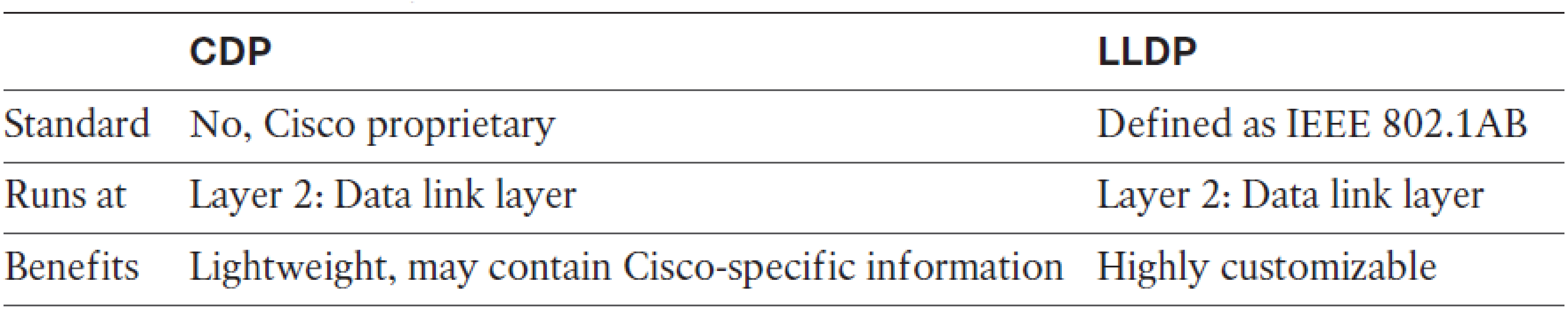
Discovery Protocols

This section on discovery protocols covers the following topics:

- Introduction to LLDP and comparison to CDP
- Basic configuration of LLDP
- Discovering neighbors using LLDP

Introduction to LLDP

- LLDP is an industry standard protocol for neighbor discovery.
- All current Cisco devices support LLDP, and only legacy and end-of-sale platforms may not support LLDP.



	CDP	LLDP
Standard	No, Cisco proprietary	Defined as IEEE 802.1AB
Runs at	Layer 2: Data link layer	Layer 2: Data link layer
Benefits	Lightweight, may contain Cisco-specific information	Highly customizable

Introduction to LLDP

- This protocol can advertise details such as configuration information, device capabilities, IP address, hostname, and device identity.
- LLDP is used for a plethora of information sharing, it is not architected to send out real-time information such as performance data or counter data.
- An advantage of LLDP over CDP is that it allows for customization. LLDP can carry a lot of information that is relevant to your network.
- One drawback of LLDP in comparison to CDP is that it is not very lightweight.

Introduction to LLDP

The following list captures a few important implementation properties of LLDP:

- LLDP is unidirectional.
- LLDP operates only in an advertising mode.
- LLDP does not solicit for information or monitor state changes between LLDP nodes.
- LLDP leverages a Layer 2 multicast frame to notify neighbors of itself and its properties.
- LLDP will receive and record all information it receives about its neighbors.
- LLDP uses 01:80:c2:00:00:**0e**, 01:80:c2:00:00:**03**, or 01:80:c2:00:00:**00** as the destination multicast MAC address.

Introduction to LLDP

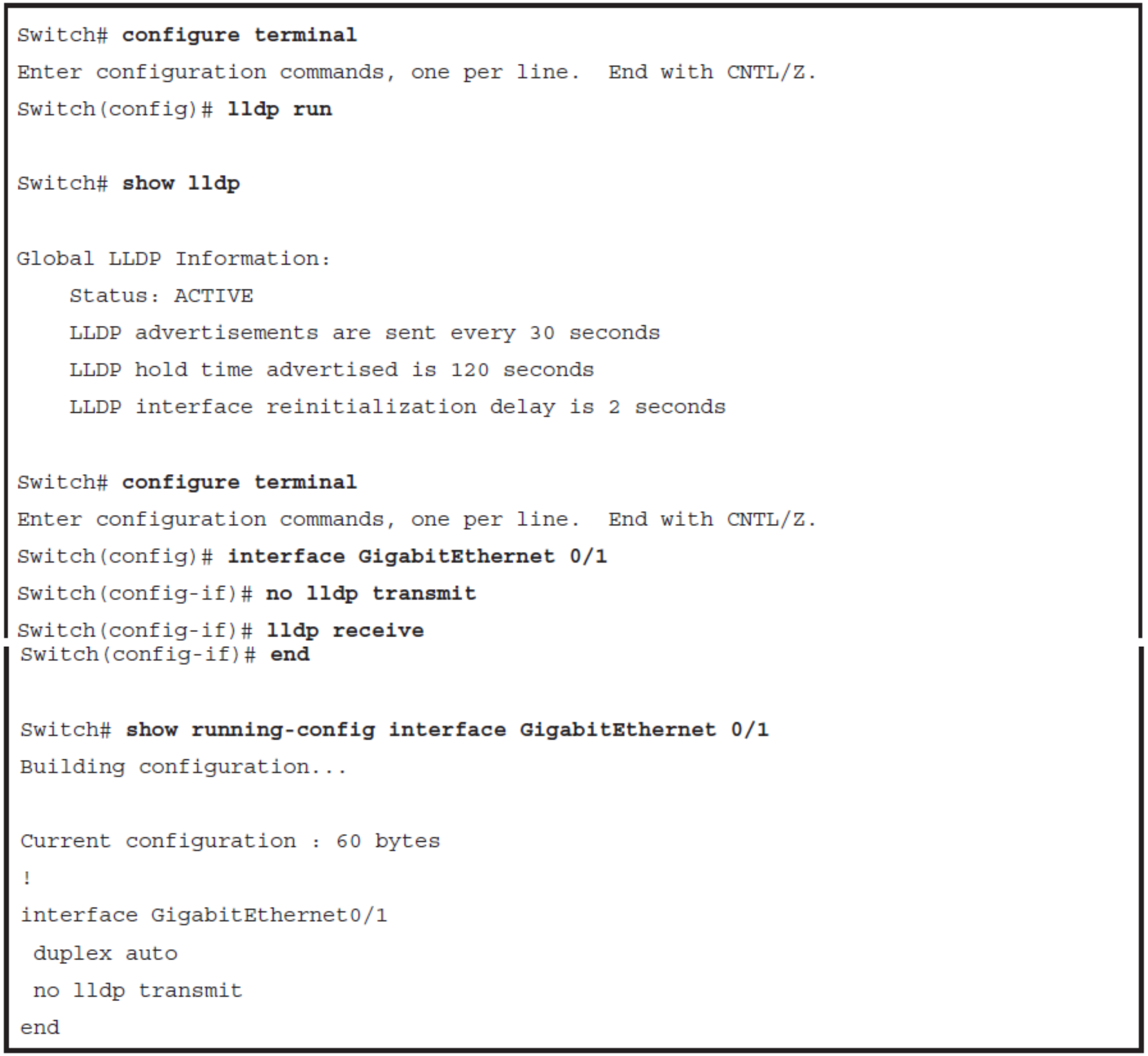
The following list defines the most common information exchanged with LLDP with campus switches:

- System name and description
- Port name and description
- Port VLAN and VLAN name
- Management IP address
- System Capabilities (Wi-Fi, routing, switching, and so on)
- Power over Ethernet
- Link aggregation

Basic Configuration of LLDP

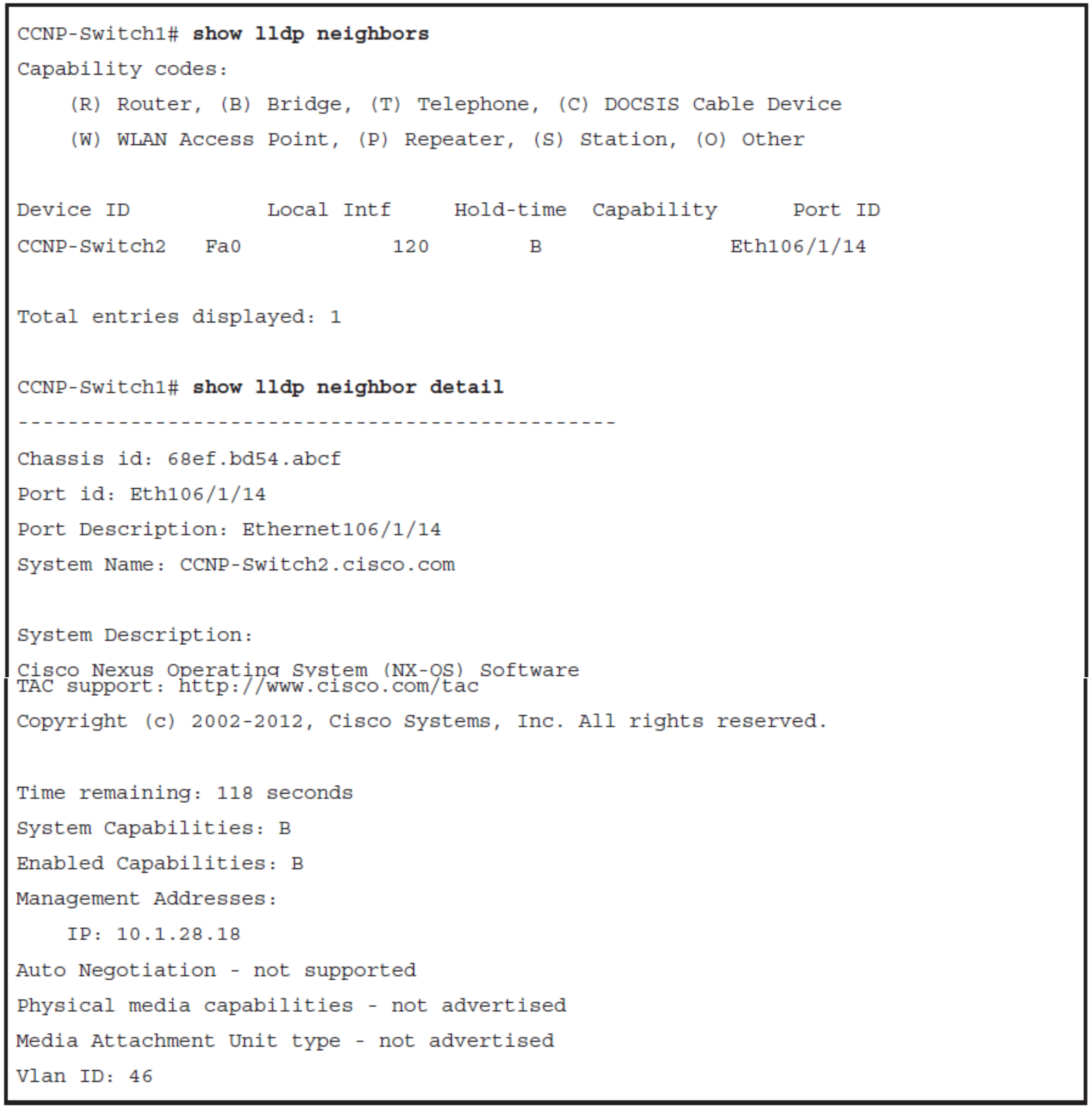
- CDP is enabled by default on all Cisco devices, but LLDP may be either enabled or disabled by default, depending on the hardware platform and software version.
- Therefore, to enable LLDP on a device, use the command **lldp run** in global configuration mode. To disable it, use **no lldp run.**
- To disable LLDP on a specific interface, you need to disable both LLDP from receiving or transmitting LLDP by issuing both the **no lldp receive** and **no lldp transmit** commands.

Basic Configuration of LLDP



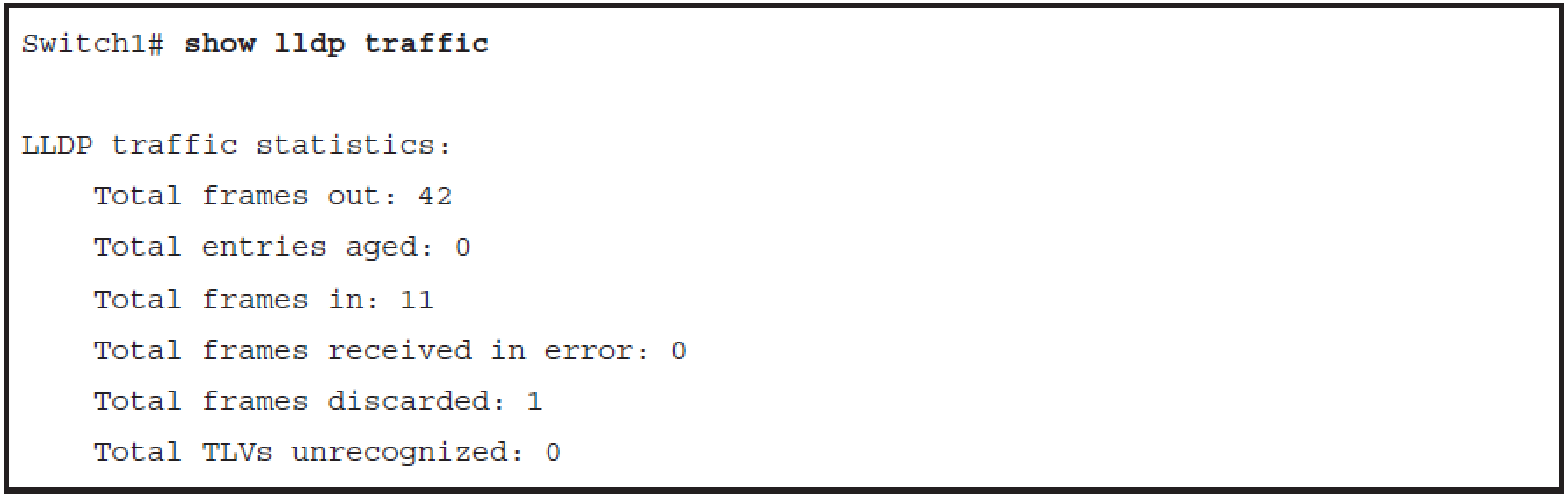
```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# lldp run

Switch# show lldp

Global LLDP Information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialization delay is 2 seconds

Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface GigabitEthernet 0/1
Switch(config-if)# no lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end

Switch# show running-config interface GigabitEthernet 0/1
Building configuration...

Current configuration : 60 bytes
!
interface GigabitEthernet0/1
 duplex auto
 no lldp transmit
end
```

LLDP Neighbors



```
CCNP-Switch1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
CCNP-Switch2    Fa0             120        B               Eth106/1/14

Total entries displayed: 1

CCNP-Switch1# show lldp neighbor detail
------------------------------------------------
Chassis id: 68ef.bd54.abcf
Port id: Eth106/1/14
Port Description: Ethernet106/1/14
System Name: CCNP-Switch2.cisco.com

System Description:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.

Time remaining: 118 seconds
System Capabilities: B
Enabled Capabilities: B
Management Addresses:
    IP: 10.1.28.18
Auto Negotiation - not supported
Physical media capabilities - not advertised
Media Attachment Unit type - not advertised
Vlan ID: 46
```

LLDP Traffic Info



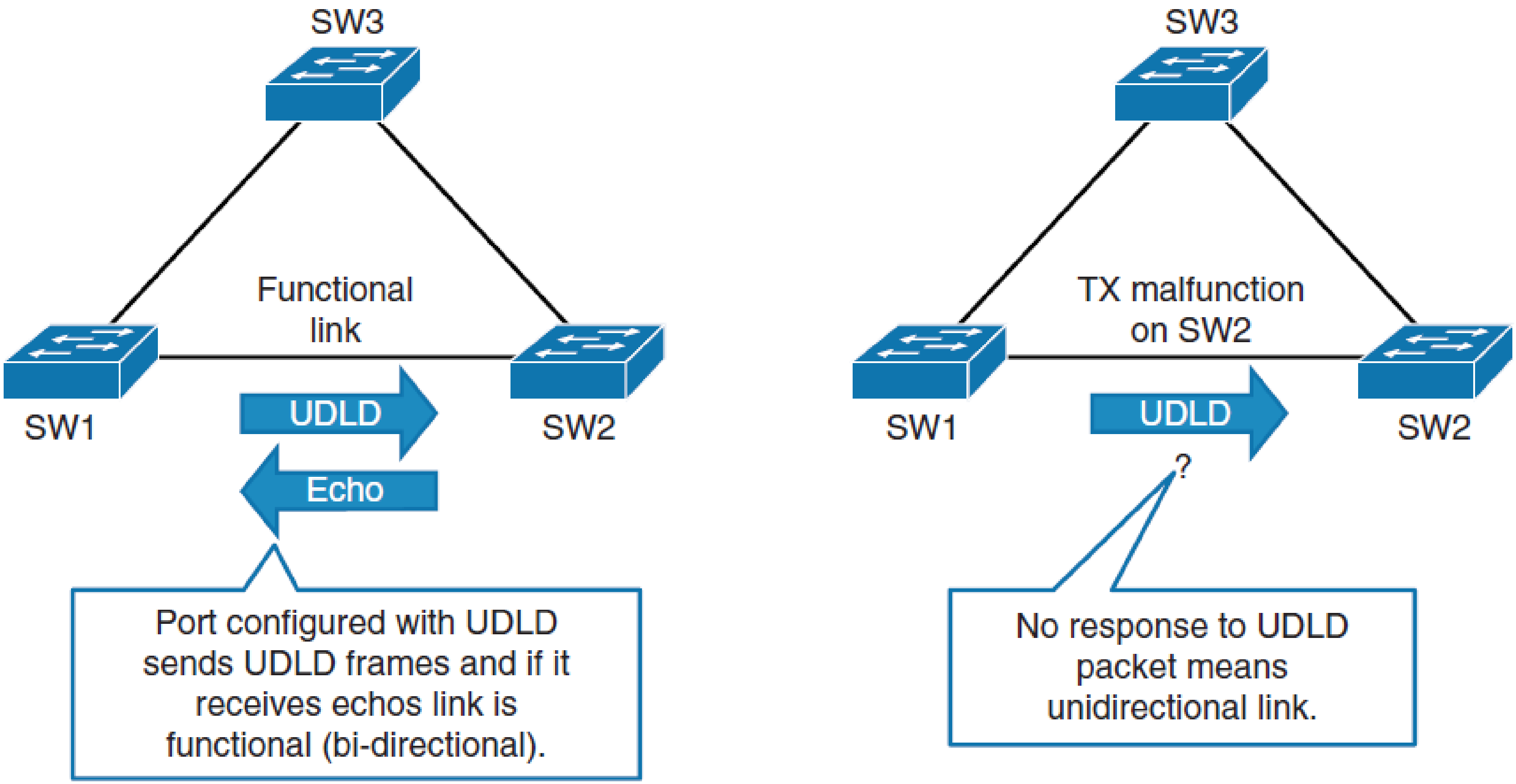
```
Switch1# show lldp traffic


LLDP traffic statistics:
    Total frames out: 42
    Total entries aged: 0
    Total frames in: 11
    Total frames received in error: 0
    Total frames discarded: 1
    Total TLVs unrecognized: 0
```

LLDP Key Features

- LLDP allows network management applications to automatically discover and learn about network devices.
- LLDP is the industry standard alternative to the CDP.
- LLDP supports enabling or disabling either transmitting or receiving capabilities per port.
- To view LLDP neighbors, use the **show lldp neighbors** [**detail**] command.

Unidirectional Link Detection

UDLD (Unidirectional Link Detection)



Port configured with UDLD sends UDLD frames and if it receives echos link is functional (bi-directional).

No response to UDLD packet means unidirectional link.

UDLD

- The unidirectional condition at Layer 2 is disastrous for any network because it will lead to either spanning tree not blocking on a forwarding port or a routing black hole.
- In either of these situations, the network will exhibit a total failure, become instable, and eventually create a complete loss of connectivity for end users.
- UDLD may protect the network from the following problems:
  - Transient hardware condition
  - Hardware failure
  - Optic/GBIC anomalous behavior or failure
  - Miswired cabling
  - Software defect or condition
  - Misconfigured or malfunction of inline tap or sniffer

UDLD Mechanisms and Specifics

- UDLD is supported on all current Cisco Catalyst and Nexus switches.
- UDLD functions by transmitting Layer 2 packets to the well-known MAC address 01:00:0C:CC:CC:CC.
- If the packets are not echoed back within a specific time frame, the link is flagged as unidirectional.
- Devices on both ends of the link must support UDLD for the protocol to successfully identify and disable unidirectional links.
- UDLD messages are sent at regular intervals.
  - This timer can be modified.
  - The default setting varies between platforms; however, the typical value is 15 seconds.

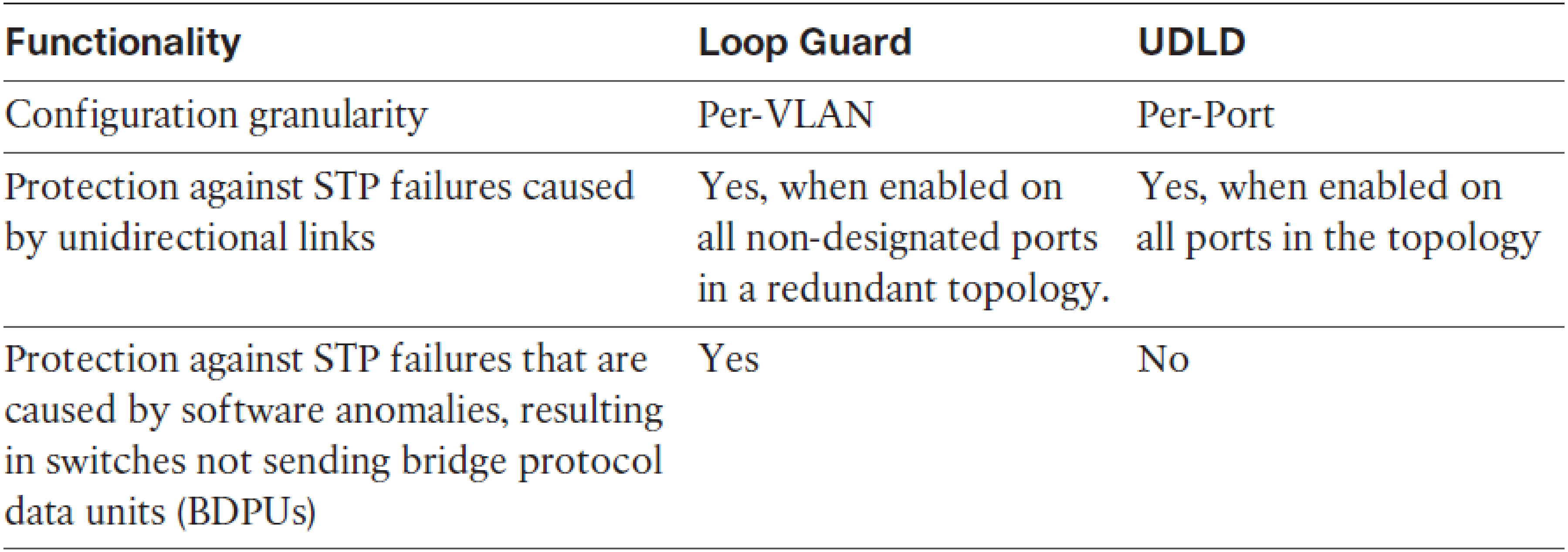
UDLD Behavior

- The behavior of UDLD after it detects a unidirectional link is dependent on its operation mode, either normal mode or aggressive mode. The modes are described as follows:
  - **Normal mode**
    - When a unidirectional link is detected the port is allowed to continue its operation. UDLD just marks the port as having an undetermined state. A syslog message is generated.
  - **Aggressive mode**
    - When a unidirectional link is detected the switch tries to reestablish the link. It sends one message a second, for 8 seconds. If none of these messages are sent back, the port is placed in error-disabled state.

UDLD Configuration

- To configure a Cisco Catalyst switch for UDLD normal mode, use the **udld enable** command.
- Similarly, to enable UDLD in aggressive mode, use the **udld aggressive** keyword.
- To display the UDLD status for the specified interface or for all interfaces, use the **show udld** [*interface slot/number*] privileged EXEC command.
- To view UDLD neighbors, use the **show udld neighbors** .
- In addition, use **udld reset** command to reset all the interfaces that were shut down by UDLD.
  - You can also achieve a UDLD reset by first shutting down the interface and then bringing it back up (that is, **shut** , then **no shut**).

Loop Guard and UDLD Functionality Comparison

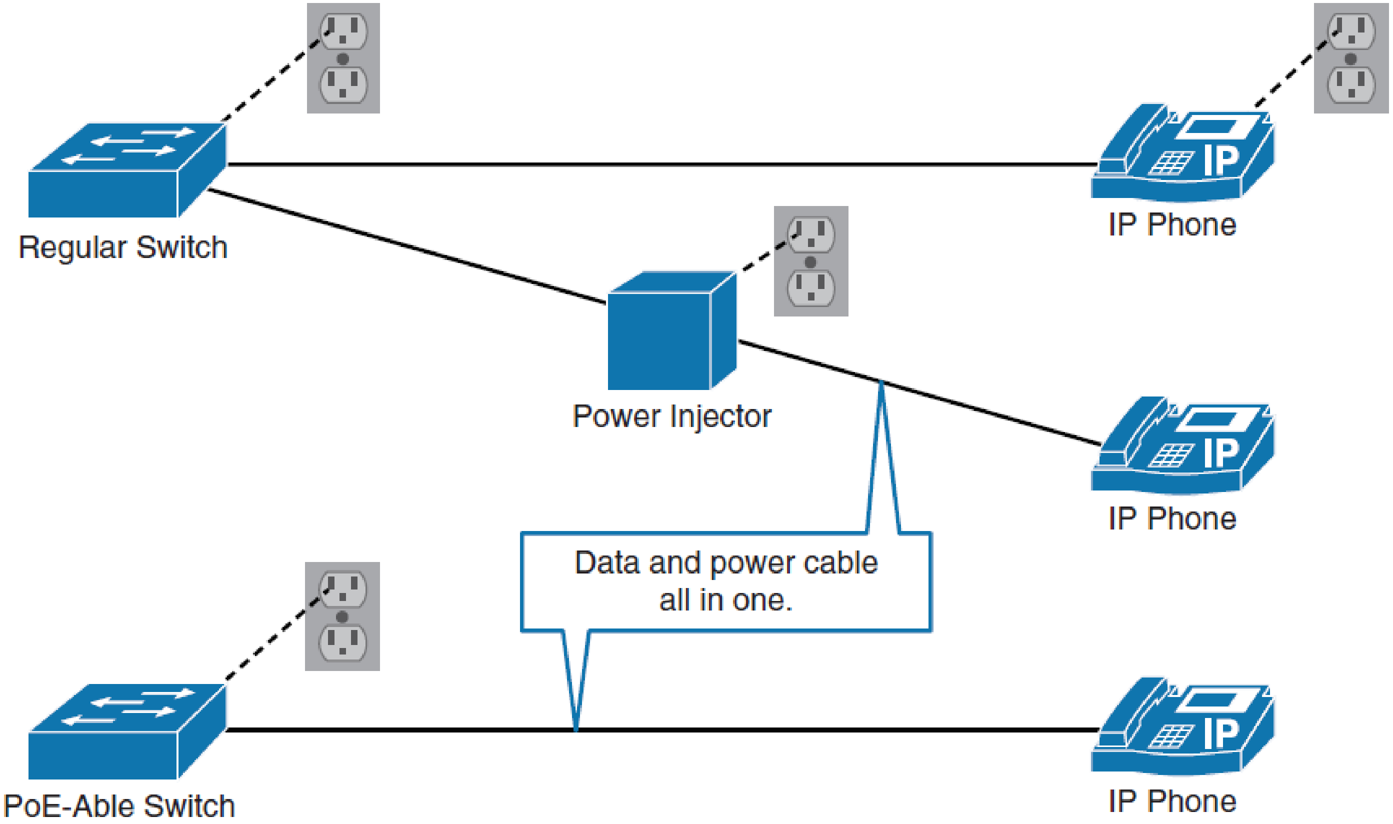


Functionality	Loop Guard	UDLD
Configuration granularity	Per-VLAN	Per-Port
Protection against STP failures caused by unidirectional links	Yes, when enabled on all non-designated ports in a redundant topology.	Yes, when enabled on all ports in the topology
Protection against STP failures that are caused by software anomalies, resulting in switches not sending bridge protocol data units (BDPUs)	Yes	No

Power over Ethernet

Power over Ethernet

- Power over Ethernet (PoE) supplies power through the same cable as data.



Data and power cable all in one.

PoE benefits

- PoE switches support remote management where power adapters and injectors do not.
- PoE switches allow for centralized methods of backup power.
- PoE requires less configuration than a local power adapter or injector.
- PoE leverages the data cabling infrastructure, and no additional power cable is required as with the case with power adapters or injectors.

PoE Components

PoE terminology refers to three types of components:

- Power-sourcing devices
  - Cisco Catalyst switches and power injectors
- Powered devices
  - Access points, IP phones, and IP cameras.
  - Thin clients, sensors, wall clocks, and so on.
  - Even switches can be powered through PoE itself.
- Ethernet cabling.
  - As with standard Ethernet, the distance of PoE is limited to 100 meters with Category 5 cabling.

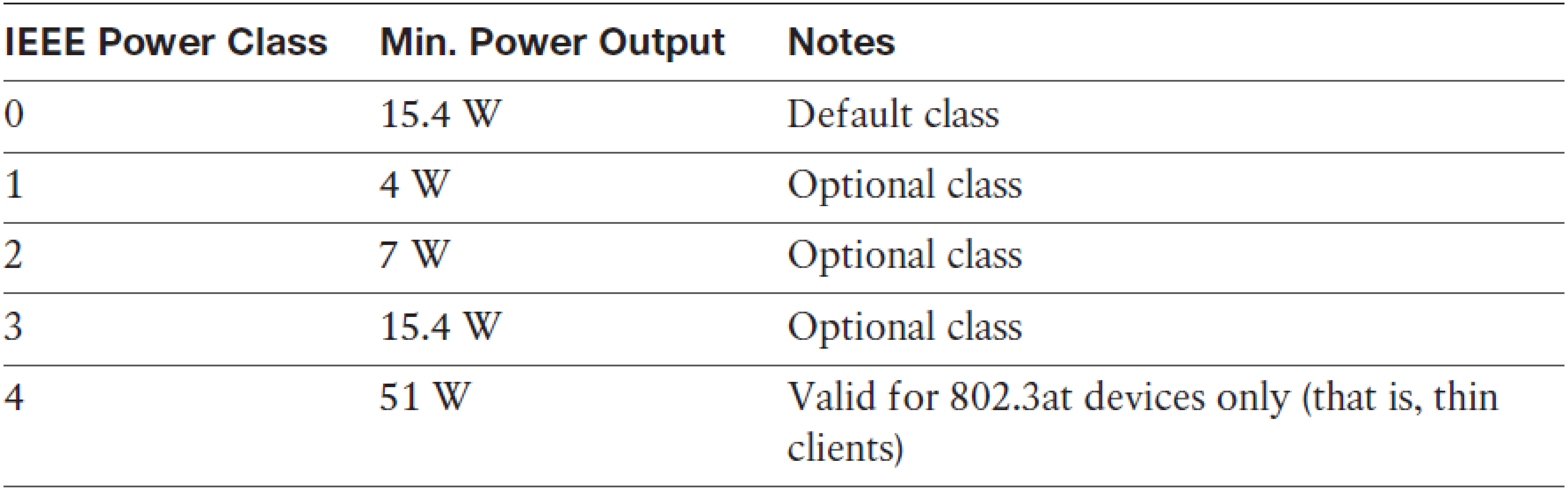
PoE Standards

- **IEEE 802.3af (ratified 2003)**
  - This standard provides interoperability between different vendors.
  - Up to 15.4 W of DC power is available for each powered device.
- **IEEE 802.3at (ratified 2009)**
  - This standard is an improvement over the 802.3af standard, and can provide powered devices with up to 25.5 W of power.
  - This number can be increased to 50 W and more with implementations that are outside the standard.
  - This standard is also known as PoE+ or PoE Plus.

PoE Negotiation

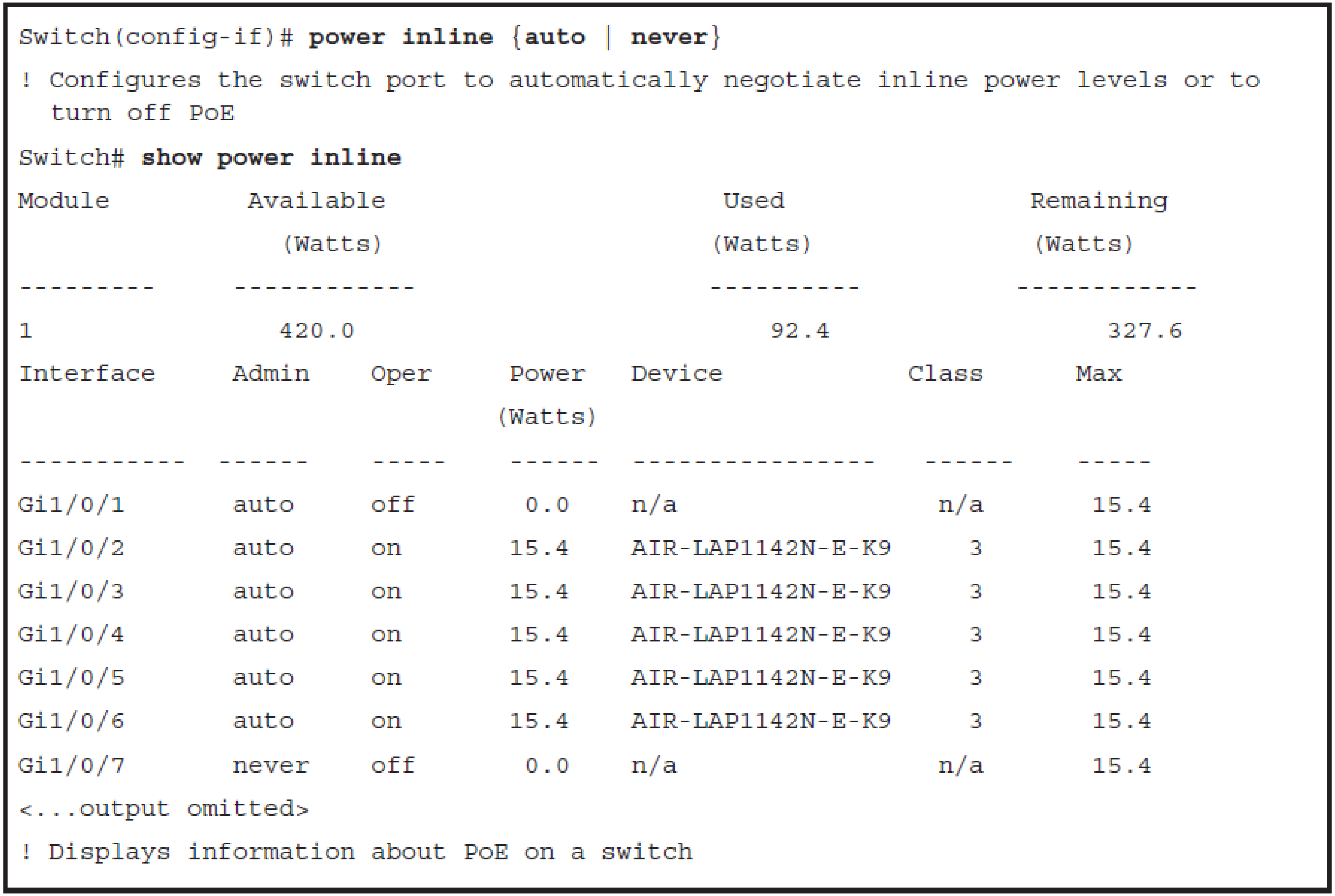
- The Cisco switches do not supply power to a port unless it specifically detects the need by the end device.
- This prevents wasting of unnecessary power and so on.
- With 802.3af and 802.3at, the switch tries to detect the powered device by supplying a small voltage across the Ethernet cable.
- The switch then measures the resistance. If the measured resistance is 25KΩ, a powered device is present.
- The powered device can provide the switch with a power class information.
- The default class of 0 is used if either the switch or the powered device does not support power class discovery

PoE Power Classes



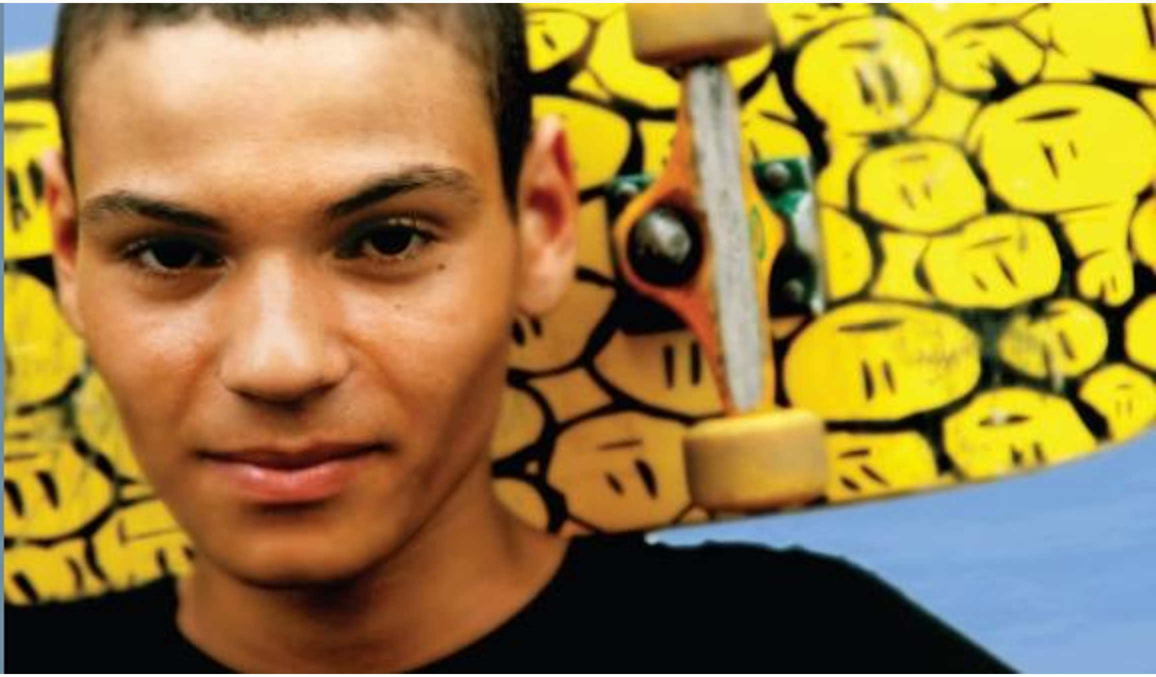
IEEE Power Class	Min. Power Output	Notes
0	15.4 W	Default class
1	4 W	Optional class
2	7 W	Optional class
3	15.4 W	Optional class
4	51 W	Valid for 802.3at devices only (that is, thin clients)

Configuring and Verifying PoE



```
Switch(config-if)# power inline {auto | never}
! Configures the switch port to automatically negotiate inline power levels or to
  turn off PoE
Switch# show power inline
Module         Available                        Used                Remaining
                 (Watts)                       (Watts)              (Watts)
---------     ------------                   ----------           ------------
1                420.0                          92.4                  327.6
Interface      Admin     Oper      Power    Device                 Class      Max
                                  (Watts)
-----------  ------    -----     ------   ----------------      ------     -----
Gi1/0/1        auto      off        0.0    n/a                      n/a        15.4
Gi1/0/2        auto      on        15.4    AIR-LAP1142N-E-K9          3        15.4
Gi1/0/3        auto      on        15.4    AIR-LAP1142N-E-K9          3        15.4
Gi1/0/4        auto      on        15.4    AIR-LAP1142N-E-K9          3        15.4
Gi1/0/5        auto      on        15.4    AIR-LAP1142N-E-K9          3        15.4
Gi1/0/6        auto      on        15.4    AIR-LAP1142N-E-K9          3        15.4
Gi1/0/7        never     off        0.0    n/a                      n/a        15.4
<...output omitted>
! Displays information about PoE on a switch
```

SDM Templates



SDM Templates

Upon completing this section on SDM templates, you will be able to do the following:

- Describe the typical SDM template types
- Change the SDM template
- Describe precautions to take when changing the SDM templates

SDM Templates

- The Switching Database Manager (SDM) templates on specific access layer switches (such as Cisco Catalyst 2960, 3560, or 3750) manages how Layer 2 and Layer 3 switching information is maintained in the Ternary Content-Addressable Memory (TCAM). So, different Cisco SDM templates are used for optimal use of system resources for specific features or feature set combination. Although the default SDM is configured for optimal use of all features simultaneously, SDM may be tweaked for those corner-case or specific scenarios.
- As an example, the most common SDM default modification action is when deploying a combination of both IPv4 and IPv6 (dual stack) because IPv6 functionality is not supported with the default template.

SDM Template Types

SDM templates modify system resources such as CAM and TCAM.

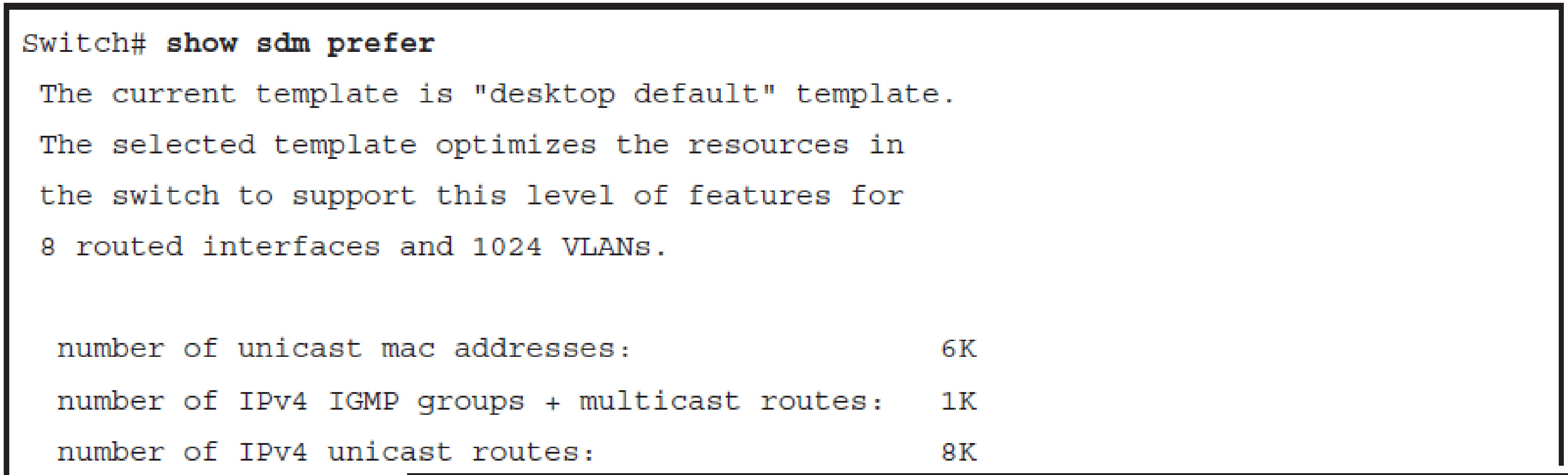
SDM templates:

- **Default**
  - The default template; this template provides for a mix of unicast routes, connected, and host routes.
- **Routing**
  - As one example, you would enable this template if the device is performing routing in the distribution or core of the network. The device is able to carry numerous routes, but only for IPv4.
- **Access**
  - You would enable this template if you have many VLANs. In turn, this template reduces the resources that are allocated to routing.

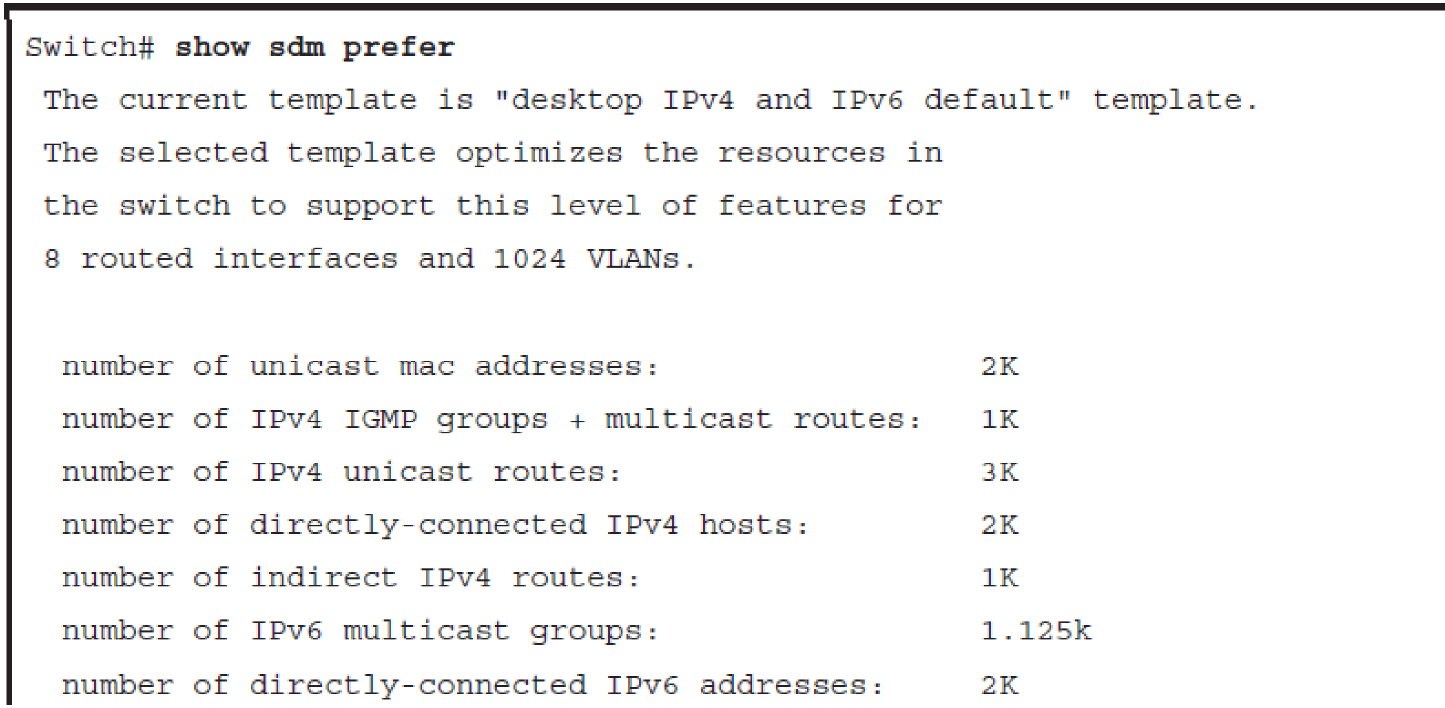
SDM Template Types

- **VLAN**
  - When you enable this template, you allocate most of the table space to Layer 2 unicasts. You would use this when you have large subnets with many MAC addresses.
- **Dual IPv4 and IPv6**
  - You would enable this template if you want to turn on the IPv6 capabilities of the device. When enabling this template, you have to choose between default, routing, and VLAN:
  - **Default**
    - More space is reserved for IPv6 routing and security. There is less reserved space for Layer 2 unicast.
  - **Routing**
    - More space is reserved for IPv6 routing than IPv4 routing.
  - **VLAN**
    - Suitable for when you are running a dual-stack environment with lots of VLANs.

Displaying SDM Resources



```
Switch# show sdm prefer
 The current template is "desktop default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  6K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    8K
  number of directly-
  number of indirect
  number of IPv4 poli
  number of IPv4/MAC
  number of IPv4/MAC
```



```
Switch# show sdm prefer
 The current template is "desktop IPv4 and IPv6 default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  2K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    3K
  number of directly-connected IPv4 hosts:          2K
  number of indirect IPv4 routes:                   1K
  number of IPv6 multicast groups:                  1.125k
  number of directly-connected IPv6 addresses:      2K
```

Choosing the Right SDM Template

- It is a best practice to change the SDM template only if you have a good reason to do so.
- Before changing the template, investigate whether the change is needed or if it is just a workaround for poor design choices.
- As another best practice, always investigate the amount of systems resources being used prior to considering changes to the SDM template.
- To verify how much of the system resources are being used, use the command **`show platform tcam utilization`** .
- If the TCAM utilization is close to maximum for any of the parameters, check if any of the other template features can optimize for that parameter:
  - **`show sdm prefer { access | default | dual-ipv4-and-ipv6 | routing | vlan }`**.
- Another common reason for changing the SDM template is because you are running out of a specific resource.
  - For example, the use of the switch in a large Layer 2 domain with many ACLs may require a change to the access SDM template.

System Resource Configuration on Other Platforms

SDM templates configure the switch for specific allocation of finite resources.

The use of SDM templates is summarized as follows:

- To verify the amount of resources being used, use the command **`show platform tcam utilization`**.
- To verify the SDM template that is currently in use, use the command **`show sdm prefer`**.
- To change the template to dual stack, use the command **`sdm prefer dual-ipv4-and-ipv6 default.`**
  - When changing the SDM template, a reload of the switch is required.

Monitoring Features

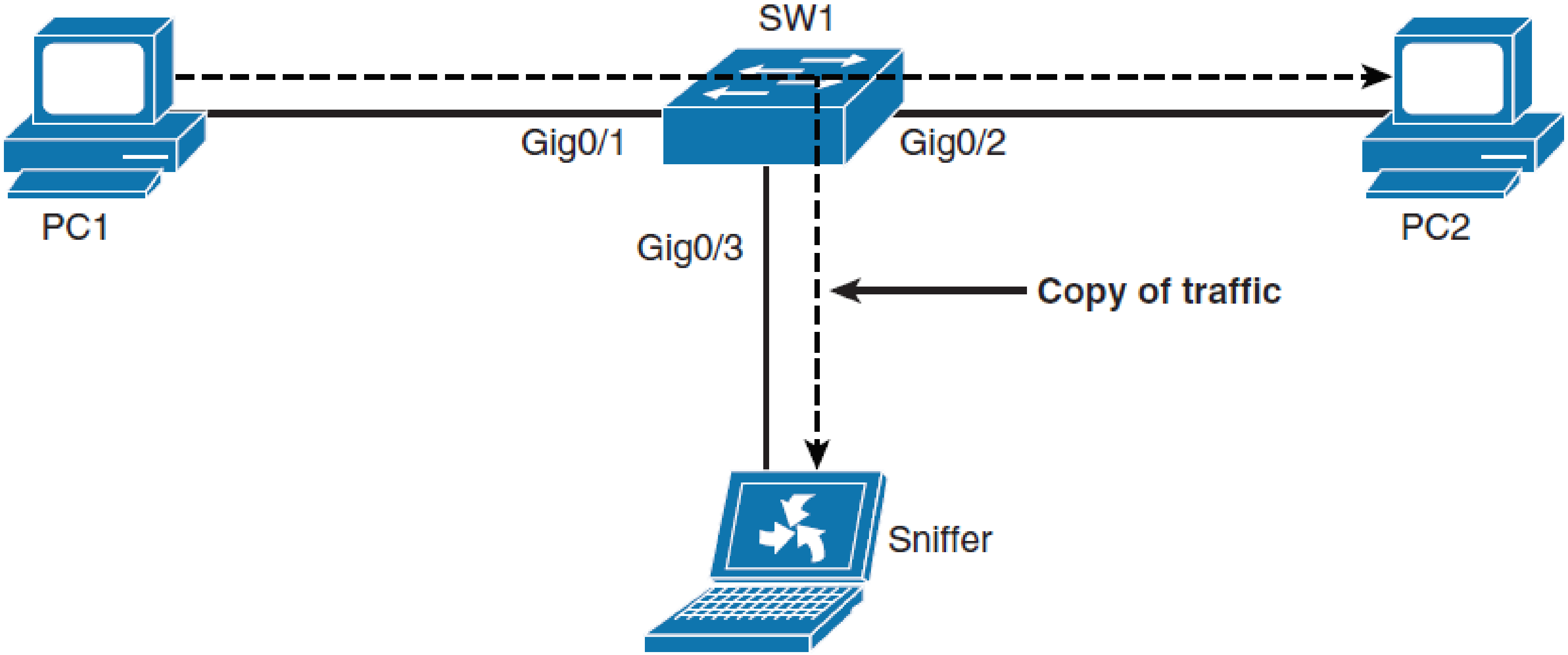
Monitoring Features

Upon completing this lesson, you will be able to meet these objectives:

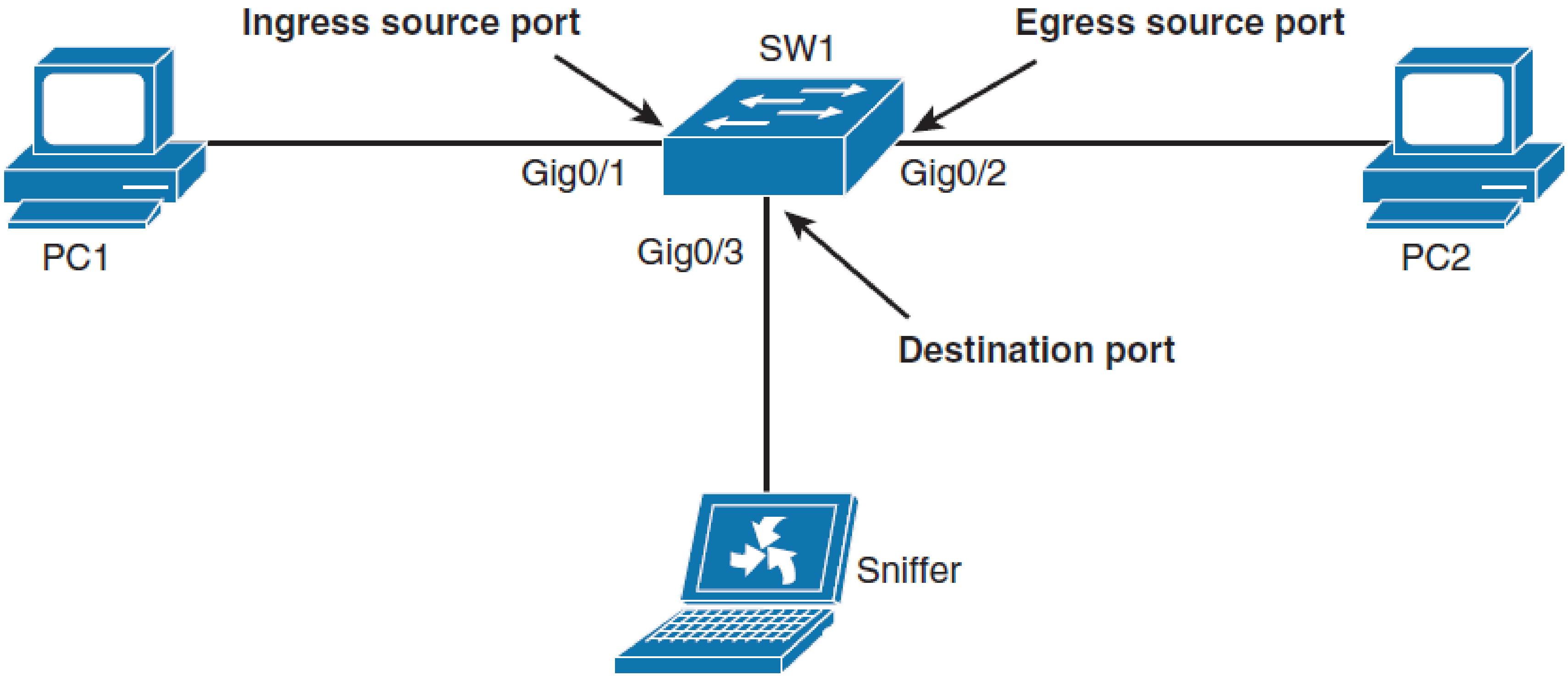
- Describe SPAN (Switch Port Analyzer)
- Describe SPAN terminology
- Describe different versions of SPAN
- Configure SPAN
- Verify local SPAN configuration
- Configure RSPAN
- Verify RSPAN configuration

SPAN and RSPAN Overview

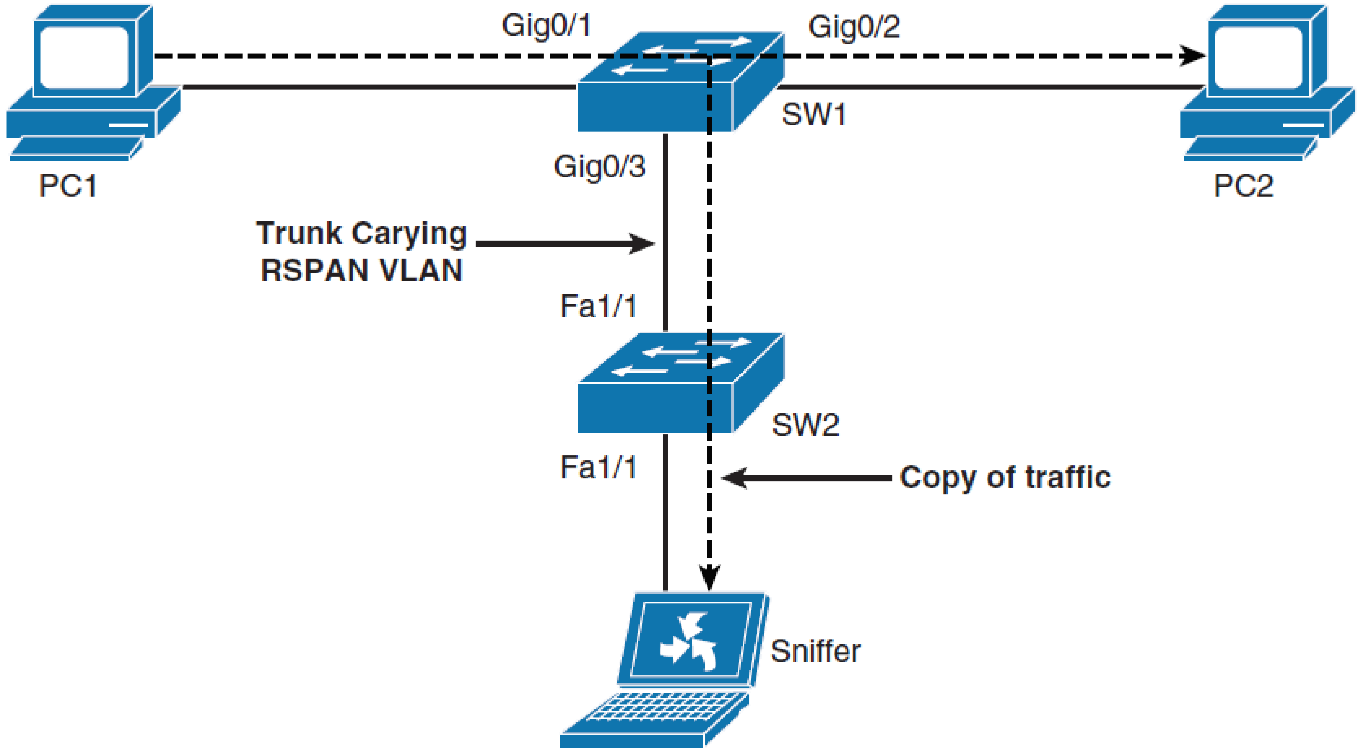
- **SPAN session:** An association of a destination port with source ports.
- **Source VLAN:** VLAN monitored for traffic analysis.



SPAN Terminology



Remote SPAN Overview



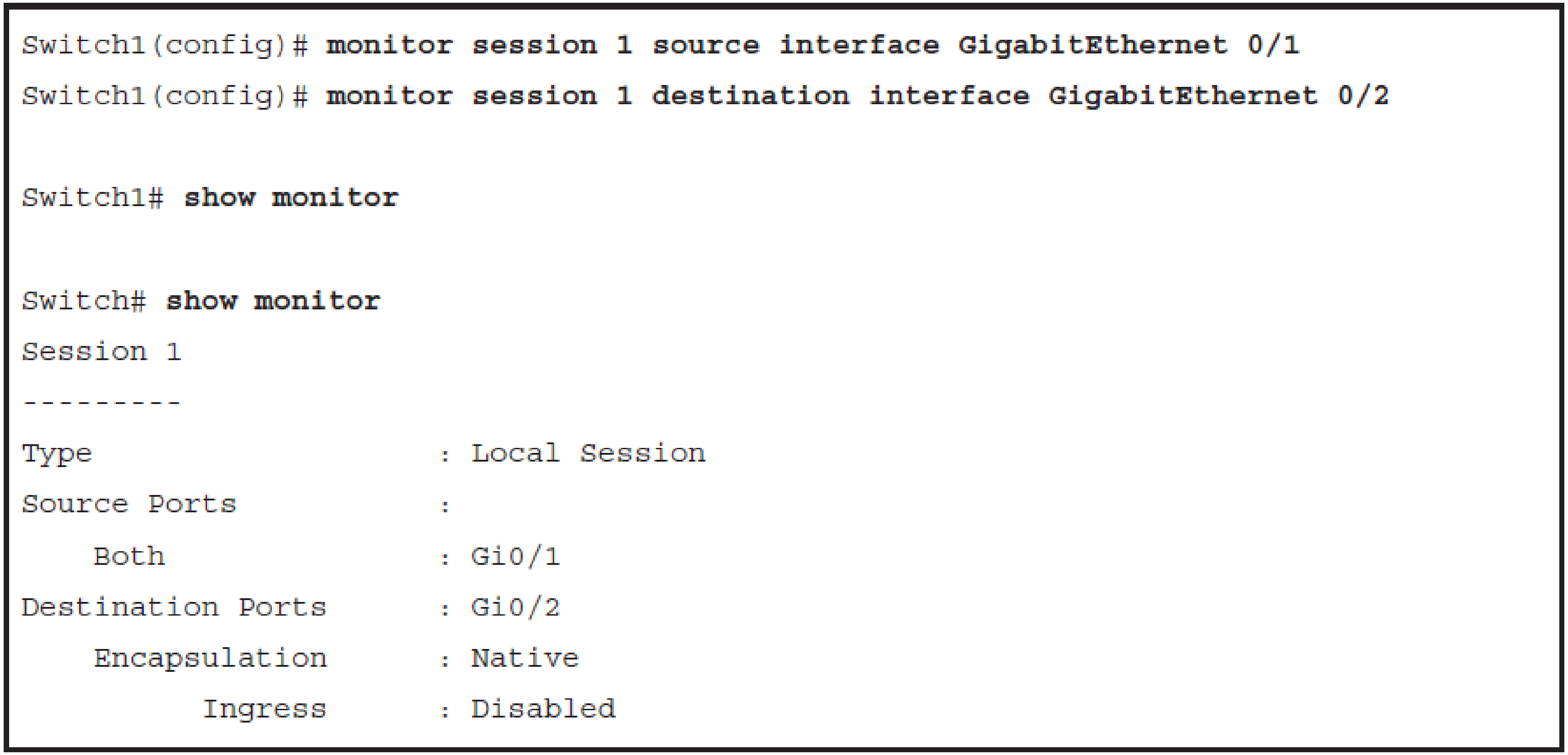
- Remote SPAN supports source and destination ports on different switches, while local SPAN supports only source and destination ports on the same switch.

SPAN Configuration

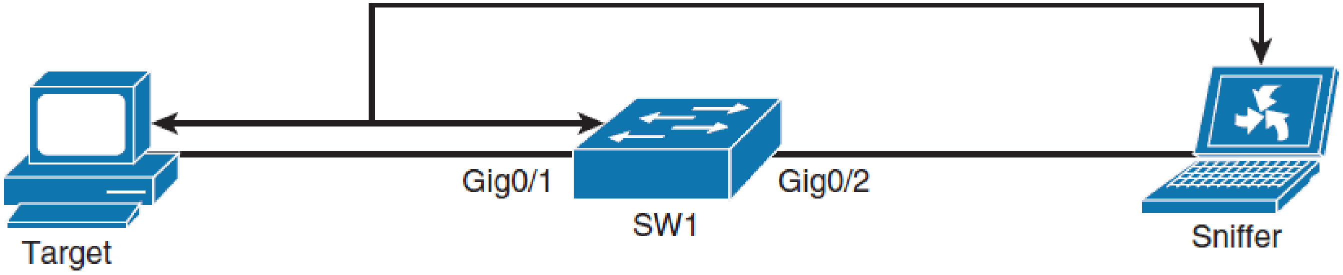
SPAN adheres to the following caveats

- A destination port cannot be a source port or vice versa.
- The number of destination ports is platform dependent; some platforms allow for more than one destination.
- Destination ports do not act as normal ports and do not participate in spanning tree and so on.
- Normal traffic flows through a destination.
- Be careful not to connect anything besides an end device to a SPAN destination port.

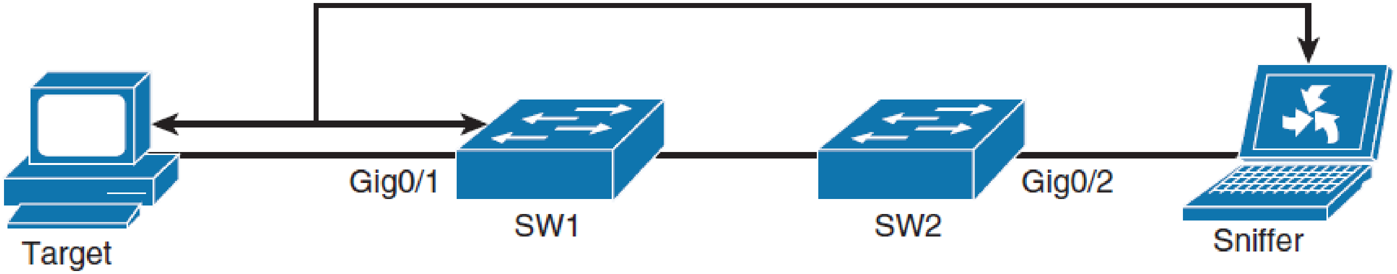
SPAN Configuration



```
Switch1(config)# monitor session 1 source interface GigabitEthernet 0/1
Switch1(config)# monitor session 1 destination interface GigabitEthernet 0/2


Switch1# show monitor


Switch# show monitor
Session 1
---------
Type                    : Local Session
Source Ports            :
    Both                : Gi0/1
Destination Ports       : Gi0/2
    Encapsulation       : Native
          Ingress       : Disabled
```

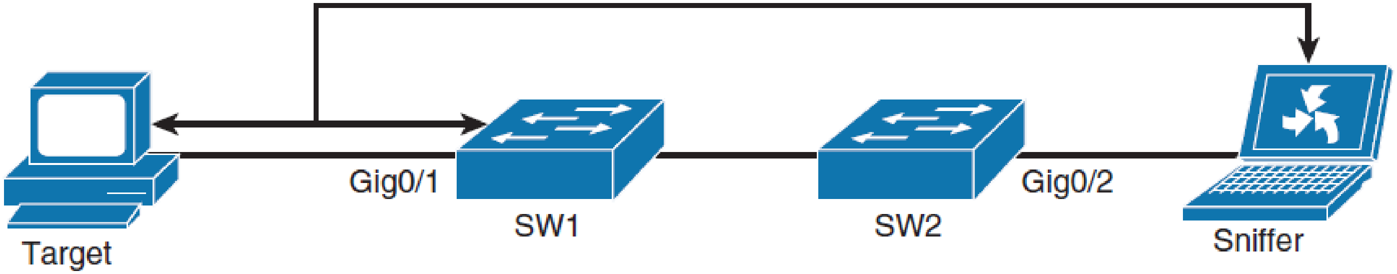


RSPAN Configuration



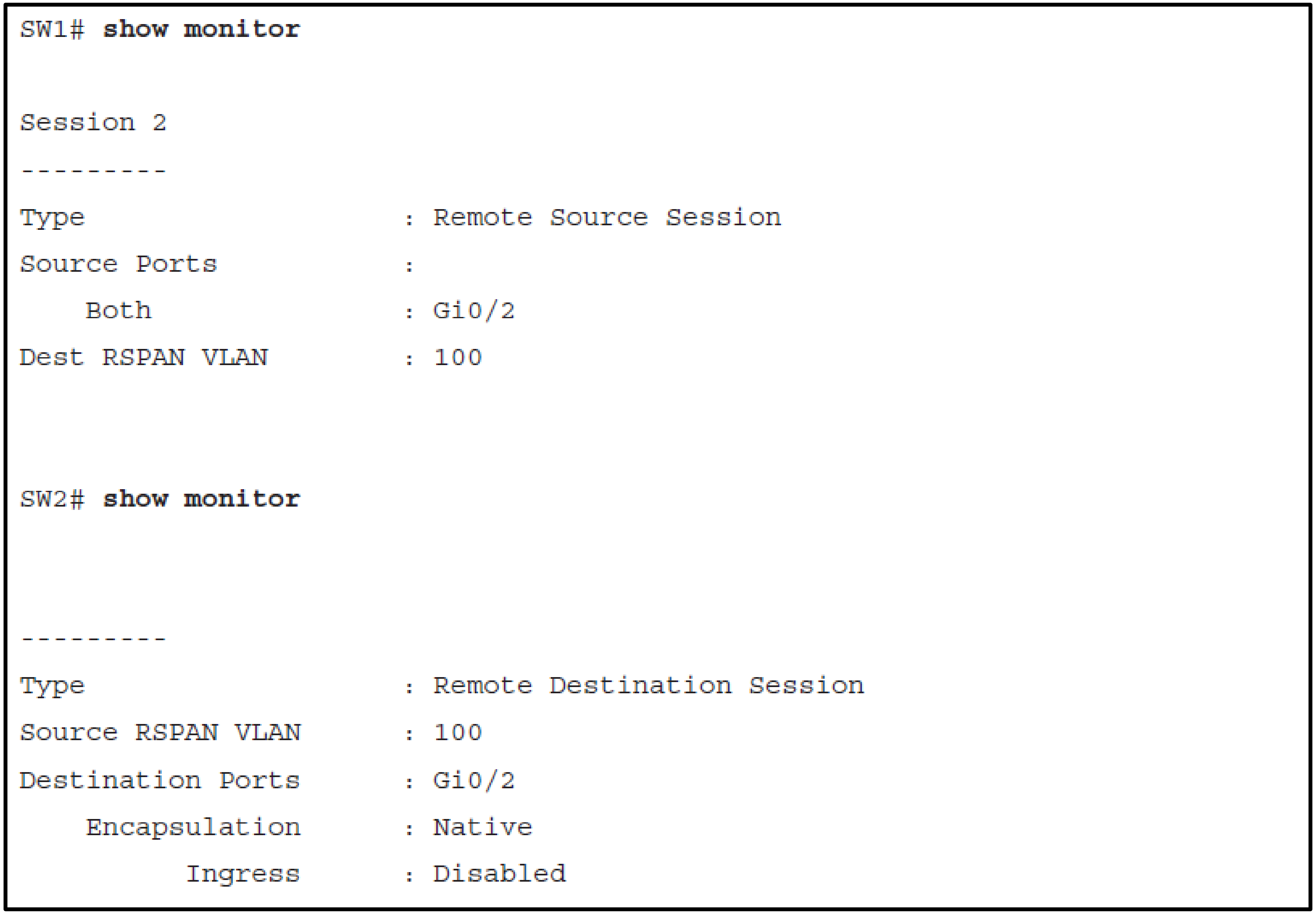
- SW1(config)# **vlan 100**
- SW1(config-vlan)# **name RSPAN-VLAN**
- SW1(config-vlan)# **remote-span**
- SW1(config-vlan)# **exit**
- SW1(config)# **monitor session 2 source interface Giga0/1**
- SW1(config)# **monitor session 2 destination remote vlan 100**

RSPAN Configuration



- SW2(config)# **vlan 100**
- SW2(config-vlan)# **name RSPAN-VLAN**
- SW2(config-vlan)# **remote-span**
- SW2(config-vlan)# **exit**
- SW2(config)# **monitor session 2 destination interface Giga 0/2**
- SW2(config)# **monitor session 2 source remote vlan 100**

RSPAN Verification



```
SW1# show monitor

Session 2
---------
Type                    : Remote Source Session
Source Ports            :
    Both                : Gi0/2
Dest RSPAN VLAN         : 100


SW2# show monitor



---------
Type                    : Remote Destination Session
Source RSPAN VLAN       : 100
Destination Ports       : Gi0/2
    Encapsulation       : Native
          Ingress       : Disabled
```

IP SLA

IP SLA

Upon completion of this section, you will understand the following:

- Basic use cases of IP SLA
- What an IP SLA source and responder are
- Basic example of an ICMP IP SLA configuration and a UDP configuration

Introduction to IP SLA

- An SLA (service level agreement) is a contract between the network provider and its customers, or between a network department and internal corporate customers. It provides a form of guarantee to customers about the level of user experience.
- SLA may contain specifics about connectivity and performance agreements for an enduser service from a service provider.
- An SLA typically outlines the minimum level of service and the expected level of service.

Introduction to IP SLA

- An SLA can also be used as the basis for planning budgets and justifying network expenditures.
- Overall, the IP SLA feature provides real-time feedback about network reachability. For features such as voice and video, network availability with stable jitter and latency are important.
- The IP SLA provides the feedback necessary to ensure the network can sustain real-time applications as well as mission-critical applications such as web portal or ordering.

IP SLA Additional Uses

Additional functions and uses for IP SLA are as follows:

- Edge-to-edge network availability monitoring.
- Network performance monitoring and network performance visibility
- Voice over IP (VoIP), video, and virtual private network (VPN) monitoring
- SLA monitoring
- IP service network health
- MPLS network monitoring
- Troubleshooting of network operation

IP SLA Options

```
Switch(config) ip sla operation-number
Switch(config-ip-sla)# ?
IP SLAs entry configuration commands:
      dhcp          DHCP Operation
      dns           DNS Query Operation
      exit          Exit Operation Configuration
      ftp           FTP Operation
      http          HTTP Operation
      icmp-echo     ICMP Echo Operation
      path-echo     Path Discovered ICMP Echo Operation
      path-jitter   Path Discovered ICMP Jitter Operation
      tcp-connect   TCP Connect Operation
      udp-echo      UDP Echo Operation
      udp-jitter    UDP Jitter Operation
```

IP SLA Source and Responder

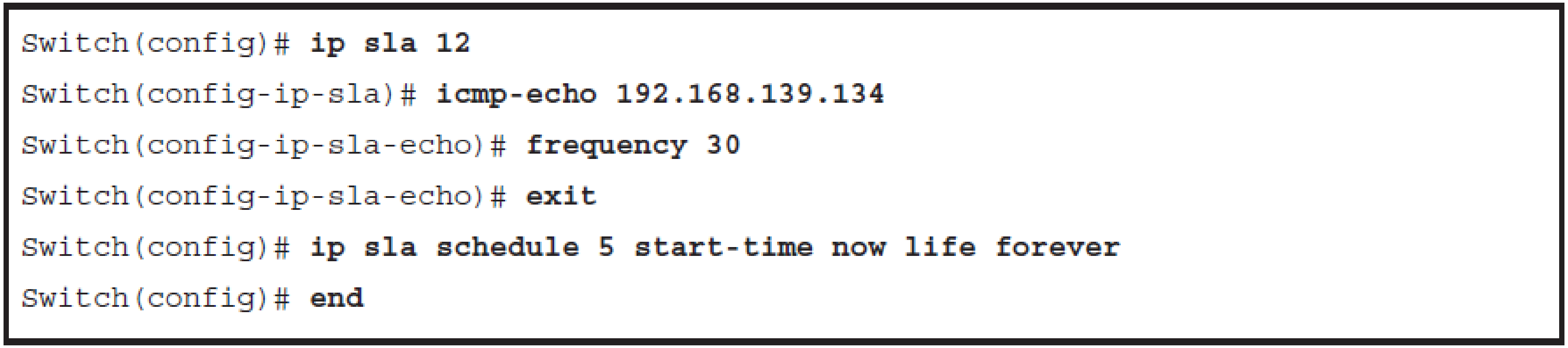
- The source is the Cisco IOS device that sends probe packets.
- The destination of the probe may be another Cisco device or another network target such as a web server or IP host.
- Although the destination of the majority of the tests can be any IP device, the measurement accuracy of some of the tests can be improved with an IP SLA responder.
- An IP SLA responder is a device that runs Cisco IOS Software.
- The responder adds a time stamp to the packets sent so the IP SLA source can take into account any latency that occurred while the responder is processing the test packets.
- For this test to work properly, both the source and responder clocks need to be synchronized through Network Time Protocol (NTP).

IP SLA Configuration

To implement IP SLA network performance measurement, you need to perform the following tasks:

- **Step 1.** Enable the IP SLAs responder, if required.
- **Step 2.** Configure the required IP SLA’s operation type.
- **Step 3.** Configure any options available for the specified operation type.
- **Step 4.** Configure threshold conditions, if required.
- **Step 5.** Schedule the operation to run, and then let the operation run for a period of time to gather statistics.
- **Step 6.** Display and interpret the results of the operation using the Cisco IOS CLI or a network management system (NMS) with SNMP.

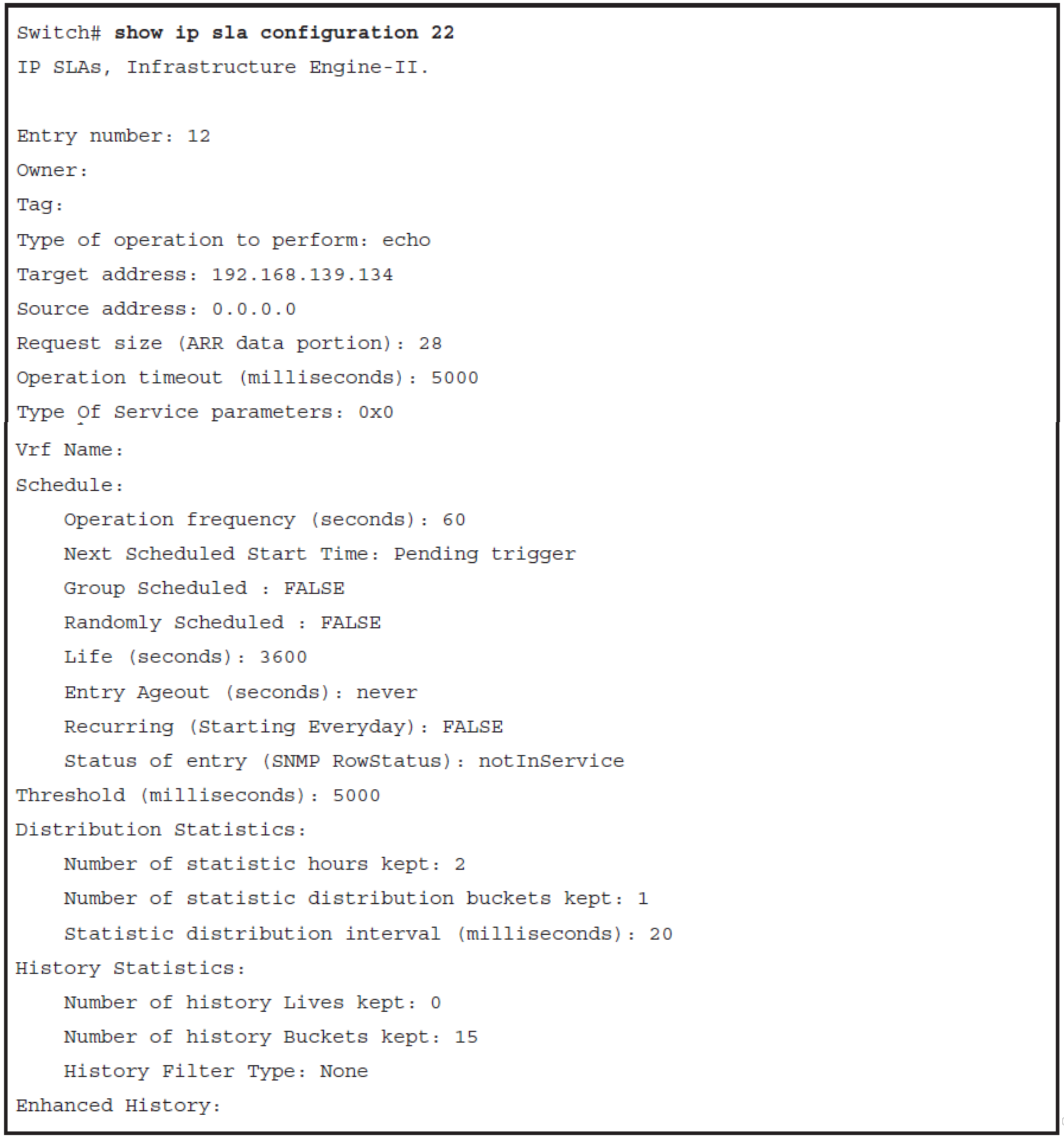
IP SLA ICMP Echo Configuration Example



```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 192.168.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
```

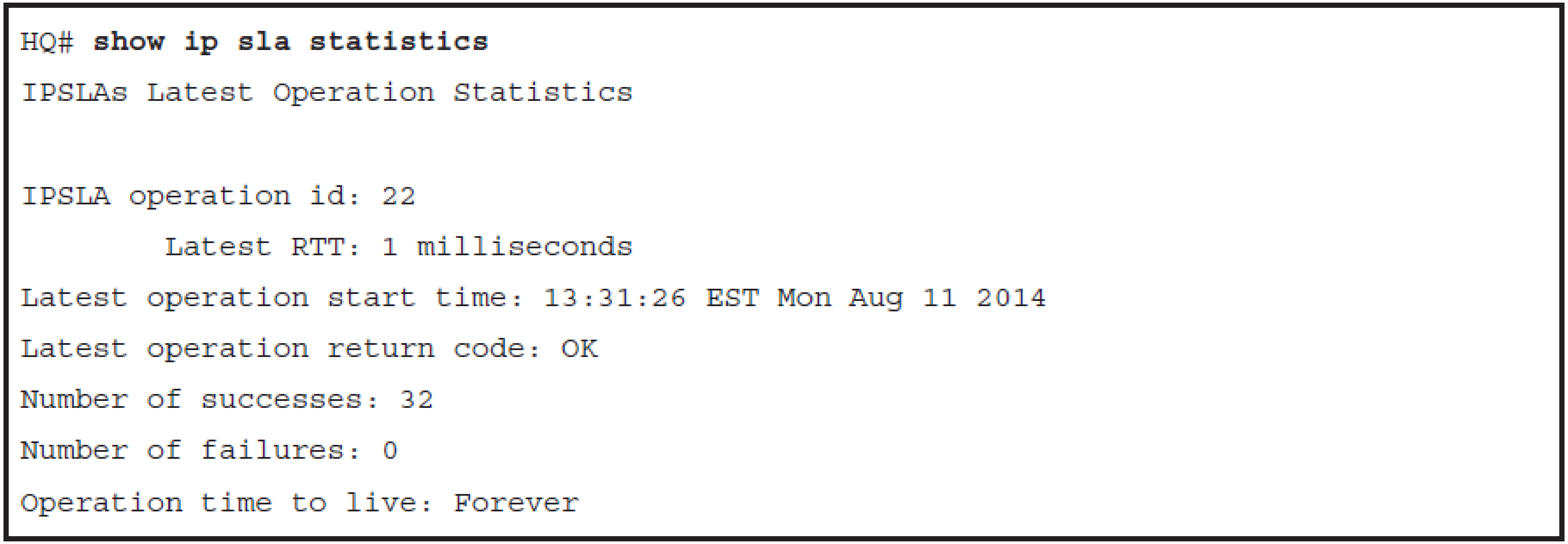
- The **icmp-echo** command has many options.
- In Example, the echoes will occur every 30 seconds.
- The **ip sla schedule** controls the scheduling parameters of the individual IP SLA operation. The full syntax of the command is as follows: **ip sla schedule** *operation-number* [**life** { **forever** | *seconds* }] [**start-time** { *hh* : *mm* [: *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*].
- In Example 8-8 , the IP SLA will start immediately after the command is issued and will run **forever** . As indicated in the command options, IP SLA supports specific start times, end times, age out, and reoccurrence.

Verify IP SLA Configuration



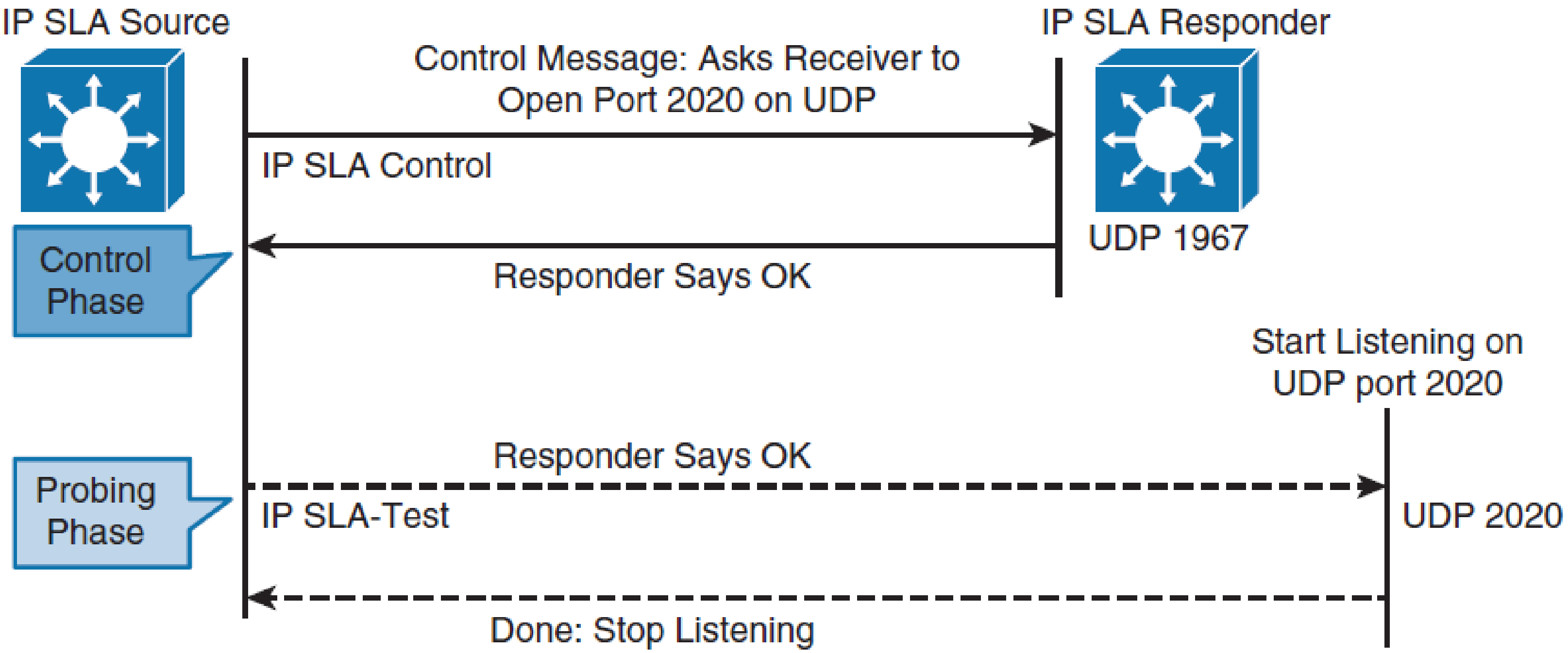
```
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.139.134
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Vrf Name:
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

Verify IP SLA Configuration

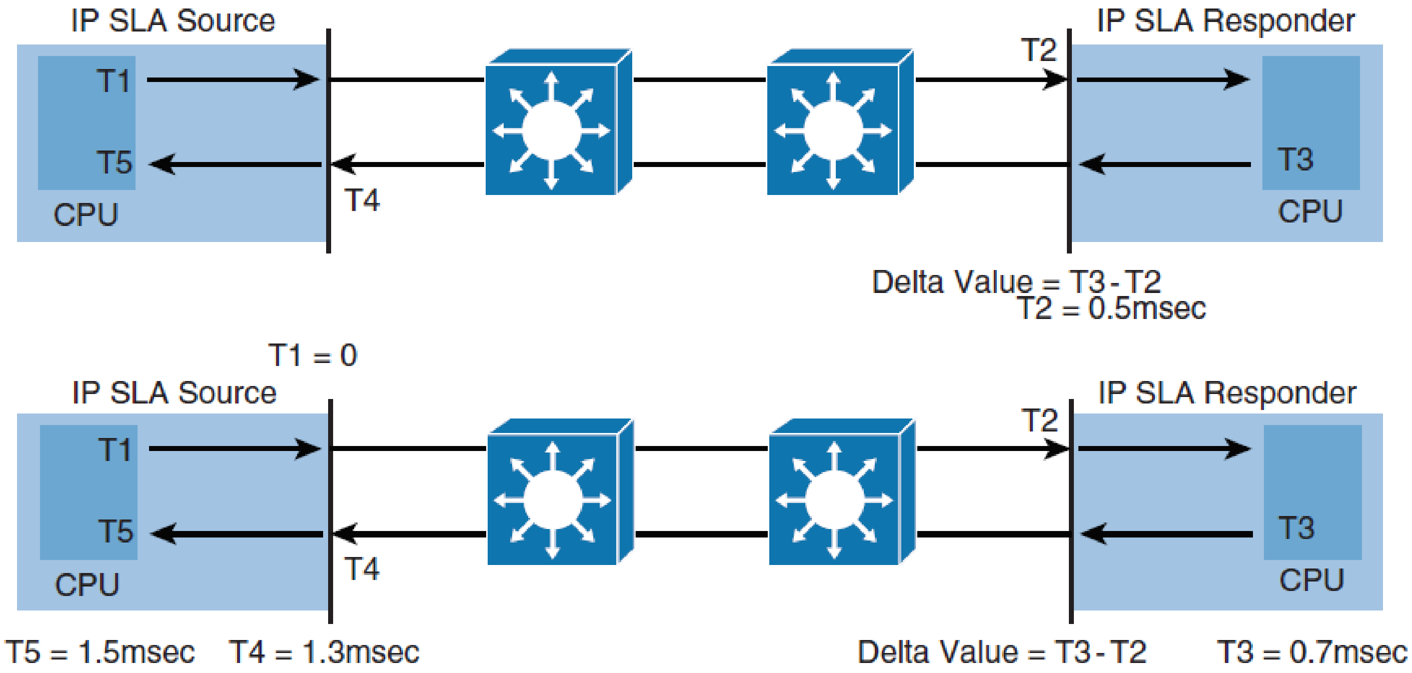


```
HQ# show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 22
        Latest RTT: 1 milliseconds
Latest operation start time: 13:31:26 EST Mon Aug 11 2014
Latest operation return code: OK
Number of successes: 32
Number of failures: 0
Operation time to live: Forever
```

IP SLA Operation with Responder



IP SLA Time Stamps

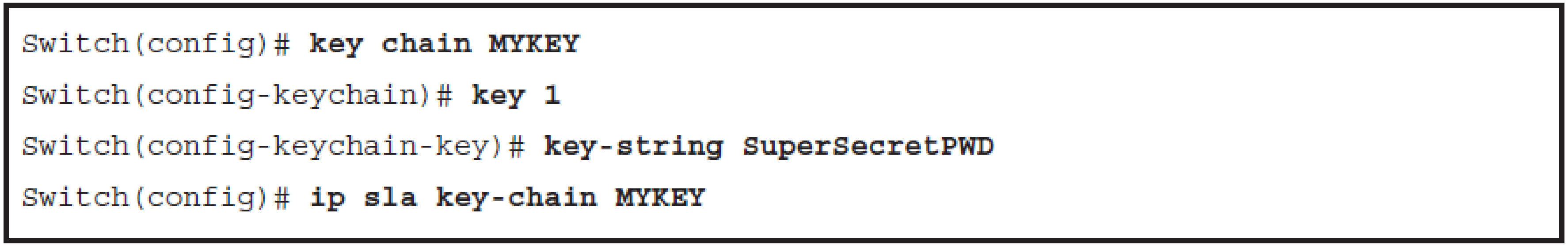


T1 time is marked from 0 in milliseconds for simplicity.

The RTT in this example is calculated as

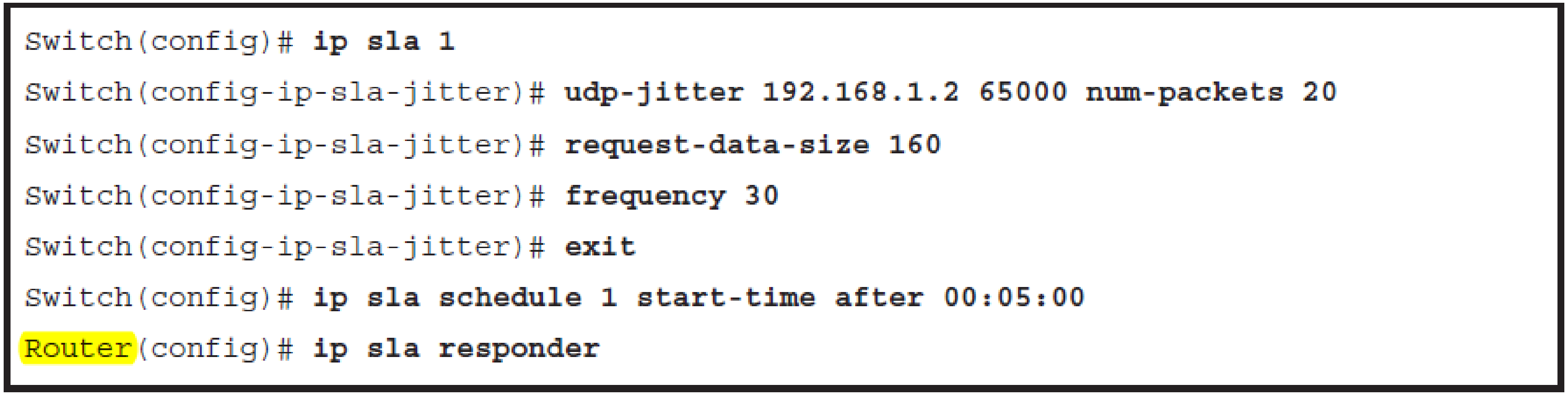
RTT = T5 – (T5-T4) - (T3-T2) = 1.5msec – (1.5msec-1.3msec) – (0.7msec - 0.5msec) = 1.1msec .

Configuring Authentication for IP SLA



```
Switch(config)# key chain MYKEY
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string SuperSecretPWD
Switch(config)# ip sla key-chain MYKEY
```

IP SLA UDP Jitter Example



```
Switch(config)# ip sla 1
Switch(config-ip-sla-jitter)# udp-jitter 192.168.1.2 65000 num-packets 20
Switch(config-ip-sla-jitter)# request-data-size 160
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 1 start-time after 00:05:00
Router(config)# ip sla responder
```

Chapter 8 Summary

- LLDP and the legacy CDP features are useful for discovering neighbor adjacencies and their details.
- The UDLD aggressive mode feature is useful in adding resiliency to networks to avoid disasters in case of anomalous behaviors.
- SPAN and RSPAN are common debugging and traffic capture features that are also leveraged to capture traffic for network analytics.
- The IP SLA

Chapter 8 Labs

- **CCNPv7.1 SWITCH Lab8.1 IP SLA SPAN**

Cisco | Networking Academy®

Mind Wide Open™

Acknowledgment

- *Some of the images and texts are from Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: (CCNP SWITCH 300-115)* by Richard Froom and Erum Frahim (1587206641)
- Copyright © 2015 – 2016 Cisco Systems, Inc.
- Special Thanks to *Bruno Silva*