Chapter 8: Monitoring the Network

Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 8

8.0 Introduction

8.1 Syslog

8.2 SNMP

8.3 NetFlow

8.4 Summary

Chapter 8: Objectives

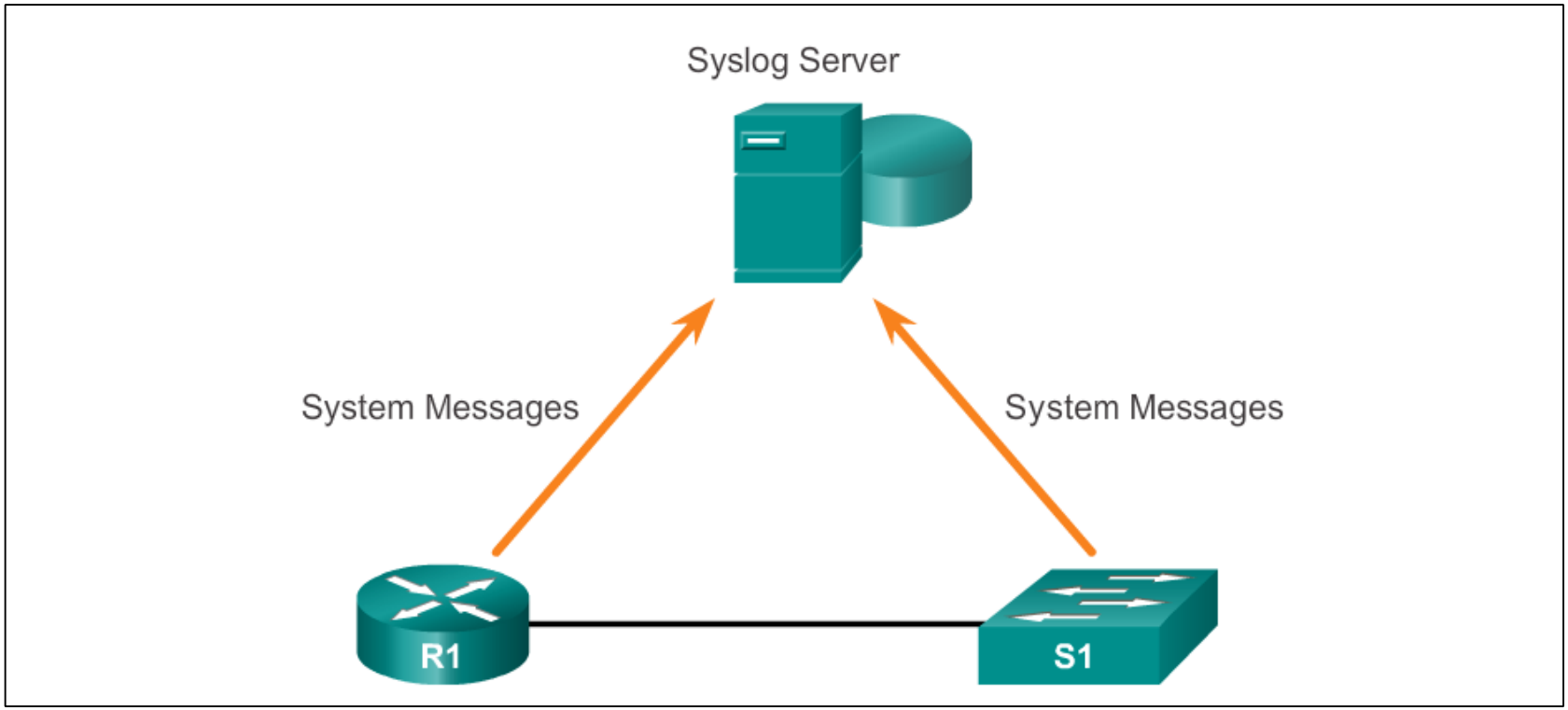
- Explain syslog operation in a small-to-medium-sized business network.
- Configure syslog to compile messages on a small-to-medium-sized business network management device.
- Explain syslog operation in small-to-medium-sized business network.
- Configure SNMP to compile messages on a small-to-medium-sized business network.
- Describe NetFlow operation in a small-to-medium-sized business network.
- Configure NetFlow data export on a router.
- Examine sample NetFlow data to determine traffic patterns.

8.1 Syslog

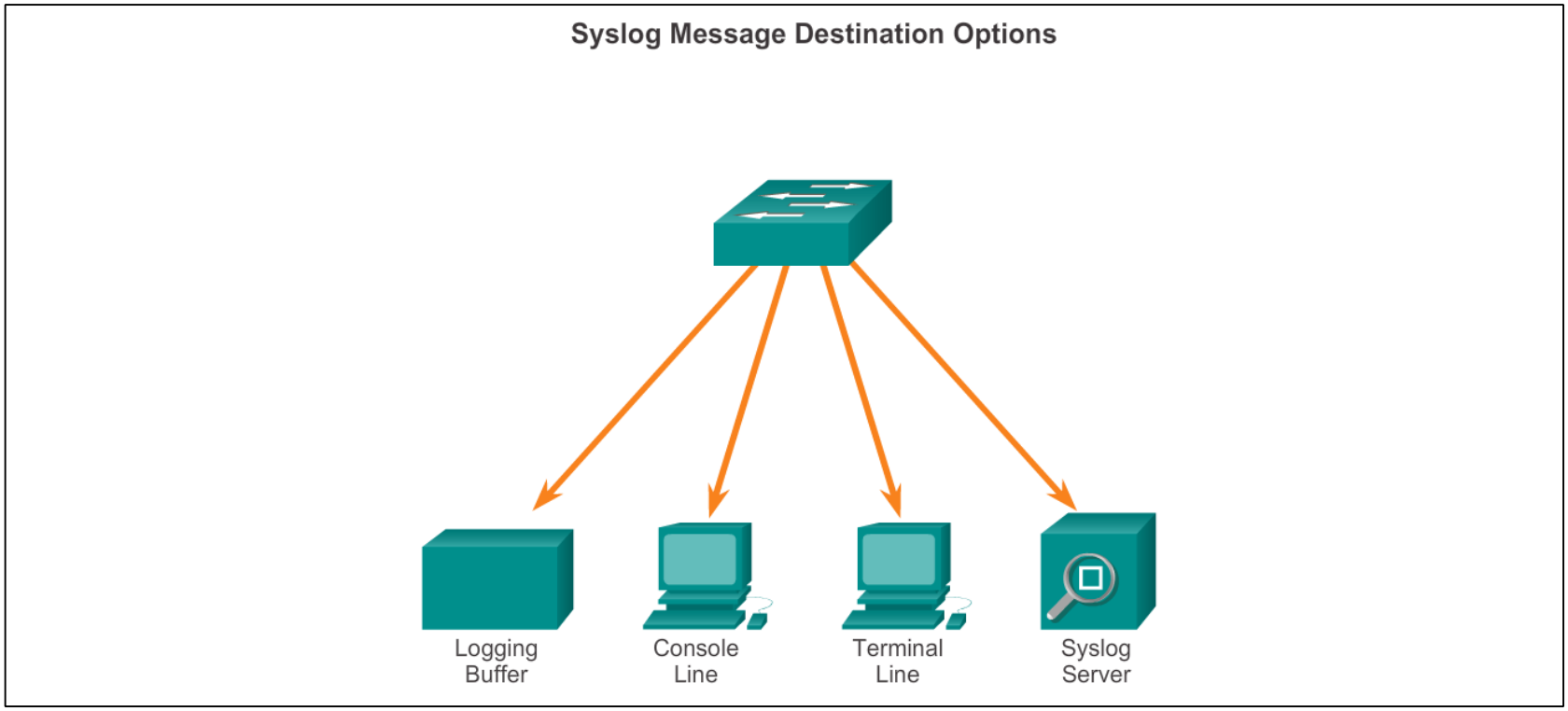
Cisco | Networking Academy®
Mind Wide Open™

Syslog Operation

Introduction to Syslog



Syslog Operation



Syslog Operation

Syslog Message Format

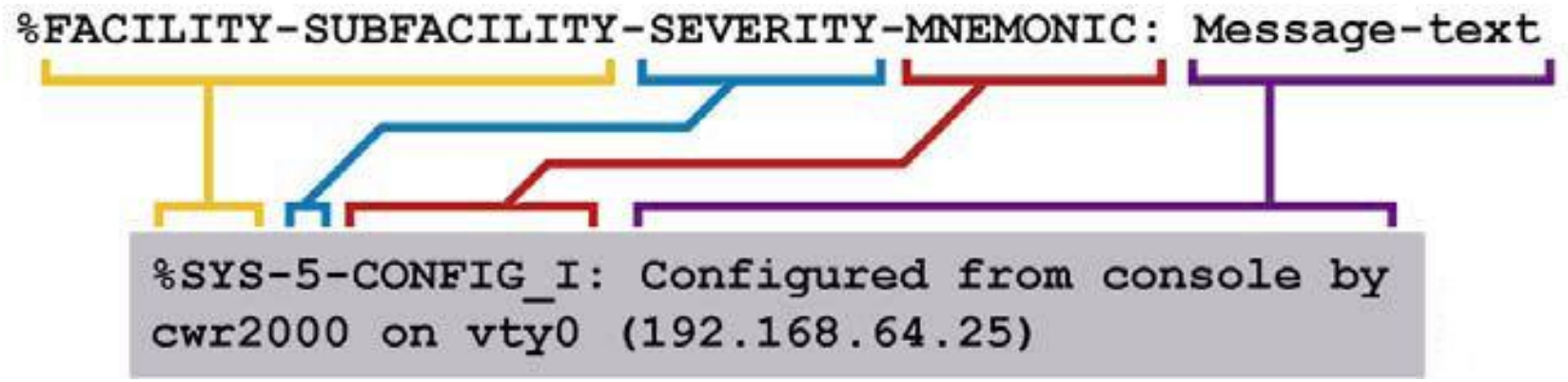
Syslog Severity Level

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

Syslog Message Format

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.

Formát Syslog správ



- Systémová správa začína so znakom percento (%)
- **Facility**
  - Dve alebo viac písmen identifikujúci hw zariadenie, protocol, alebo sw modul
- **Severity**
  - Kód od 0-7, ktorá indikuje úroveň závažnosti
- **Mnemonic**
  - Kód jednoznačne identifikujúci správu
- **Message-text**
  - Text popisujúci daný stav. Môže obsahovať detailnejší popis danej udalosti, zahŕňajúci portové číslo, terminal, meno používateľa apod

Syslog Operation

Service Timestamp

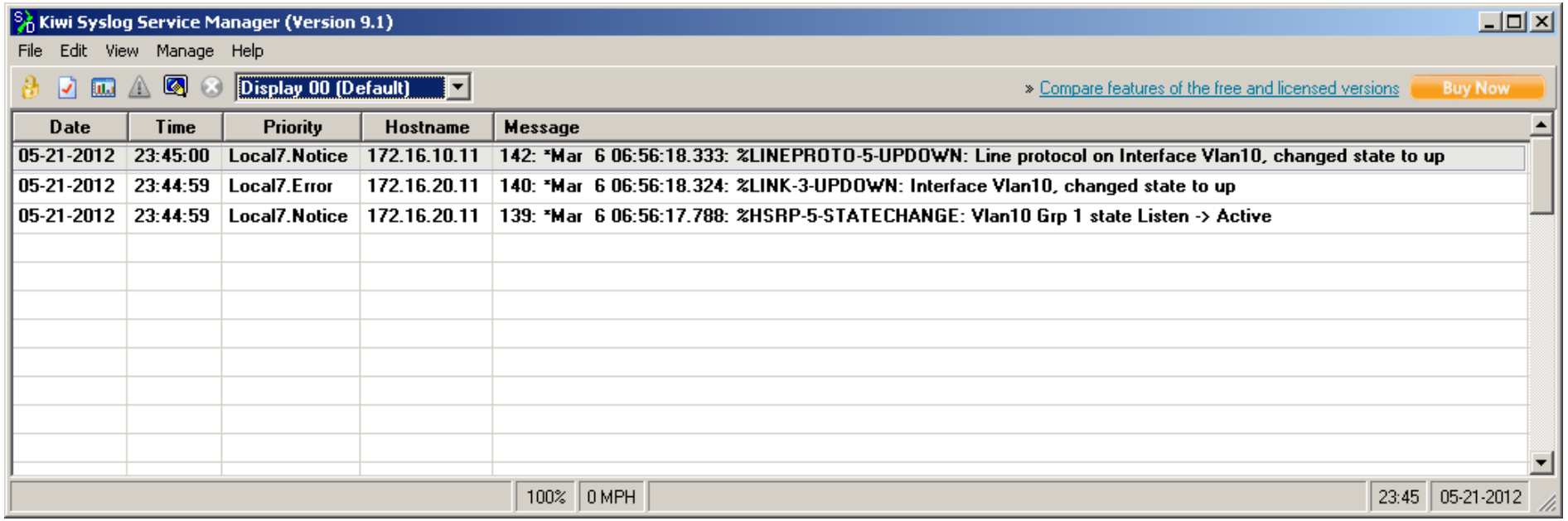
- Log messages can be time-stamped and the source address of syslog messages can be set. This enhances real-time debugging and management.
- The **`service timestamps log datetime`** command entered in global configuration mode should be entered on the device.
- In this chapter, it is assumed that the clock has been set and the **`service timestamps log datetime`** command has been configured on all devices.

Syslog Server

- The syslog server provides a relatively user-friendly interface for viewing syslog output.
- The server parses the output and places the messages into pre-defined columns for easy interpretation. If timestamps are configured on the networking device sourcing the syslog messages, then the date and time of each message displays in the syslog server output.
- Network administrators can easily navigate the large amount of data compiled on a syslog server.

Sample Syslog Messages

```
08:01:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
08:01:23: %DUAL-5-NBRCHANGE: EIGRP-IPv4:(1) 1: Neighbor 10.1.1.1 (Vlan1) is up: new adjacency
08:02:31: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to up
08:18:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
08:18:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
08:18:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
08:18:24: %ILPOWER-5-IEEE_DISCONNECT: Interface Fa0/2: PD removed
08:18:26: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down
08:19:49: %ILPOWER-7-DETECT: Interface Fa0/2: Power Device detected: Cisco PD
08:19:53: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
08:19:53: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```



Configuring Syslog

Default Logging

```
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
```

Configuring Syslog

Router and Switch Commands for Syslog Clients

```
R1(config)# logging 192.168.1.3
R1(config)# logging trap 4
R1(config)# logging source-interface gigabitEthernet 0/0
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)#
```

Configuring Syslog

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
```

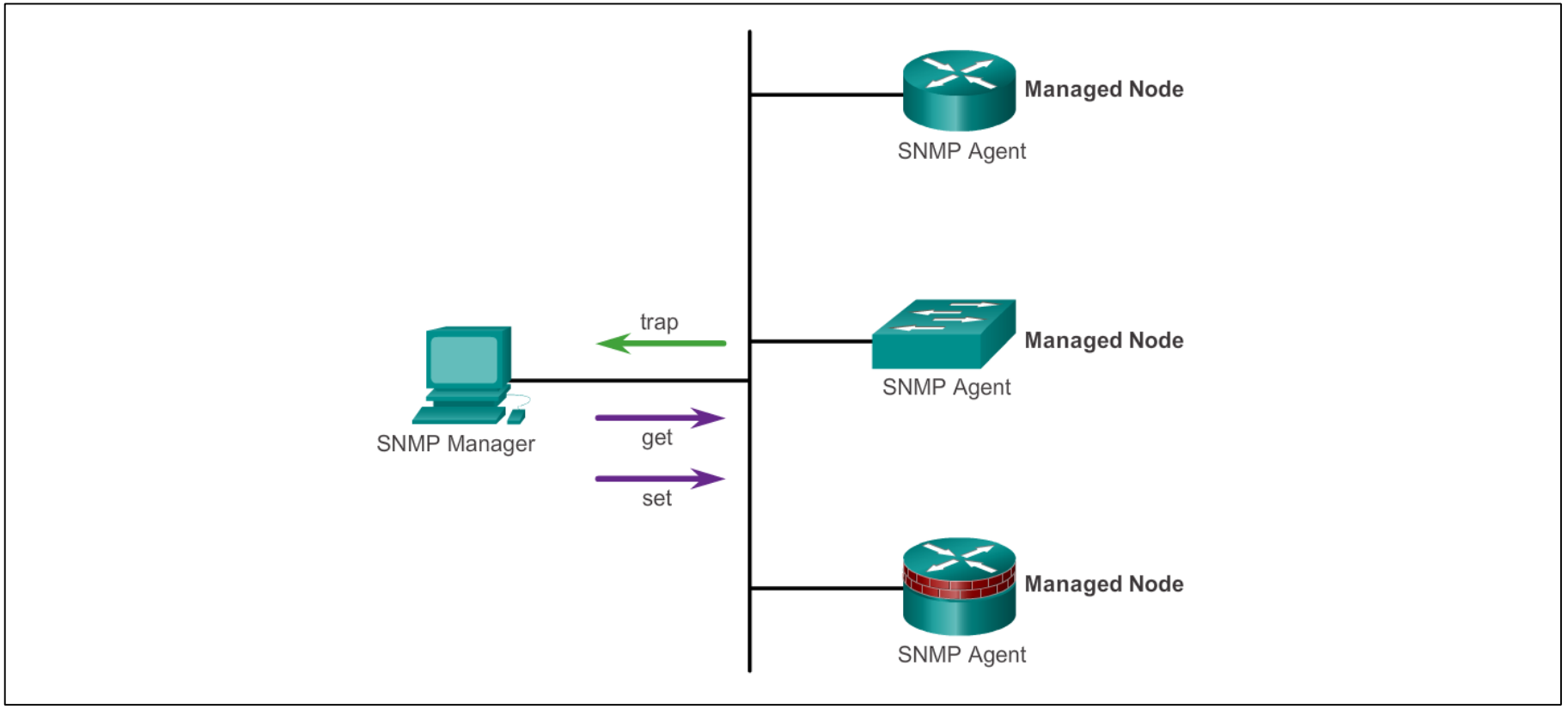
```
R1# show logging | begin Jun 12 22:35
*Jun 12 22:35:46.206: %LINK-5-CHANGED: Interface Loopback0,
changed state to administratively down
*Jun 12 22:35:47.206: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to down
*Jun 12 22:35:55.926: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:35:56.926: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:49:52.122: %SYS-5-CONFIG_I: Configured from console by
console
*Jun 12 23:15:48.418: %SYS-5-CONFIG_I: Configured from console by
console
R1#
```

8.2 SNMP

Cisco | Networking Academy®
Mind Wide Open™

SNMP Operation

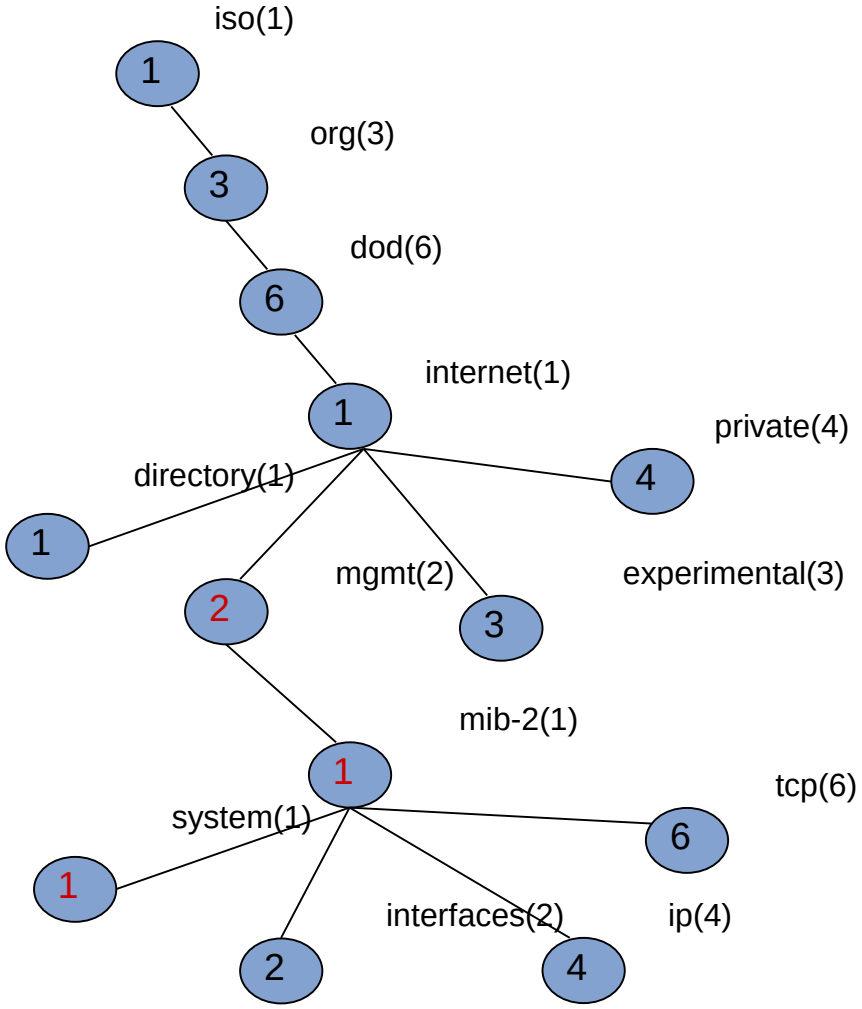
Introduction to SNMP



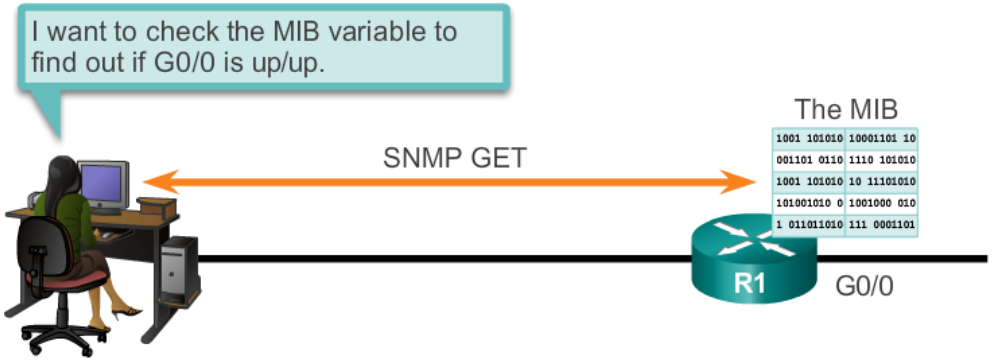
MIB – Management Information Base

- Objekty na agentovi majú svoje identifikátory OID (Object IDentifier)
  - OID sú usporiadané v stromovej štruktúre
  - Vrcholy majú číselný i slovný názov
  - Konkrétny objekt je adresovaný cestou od koreňa stromu
- Príklad: .1.3.6.1.2.1.1

iso(1) org(3) dod(6) internet(1)
mgmt(2)
mib-2 (1)
system (1)



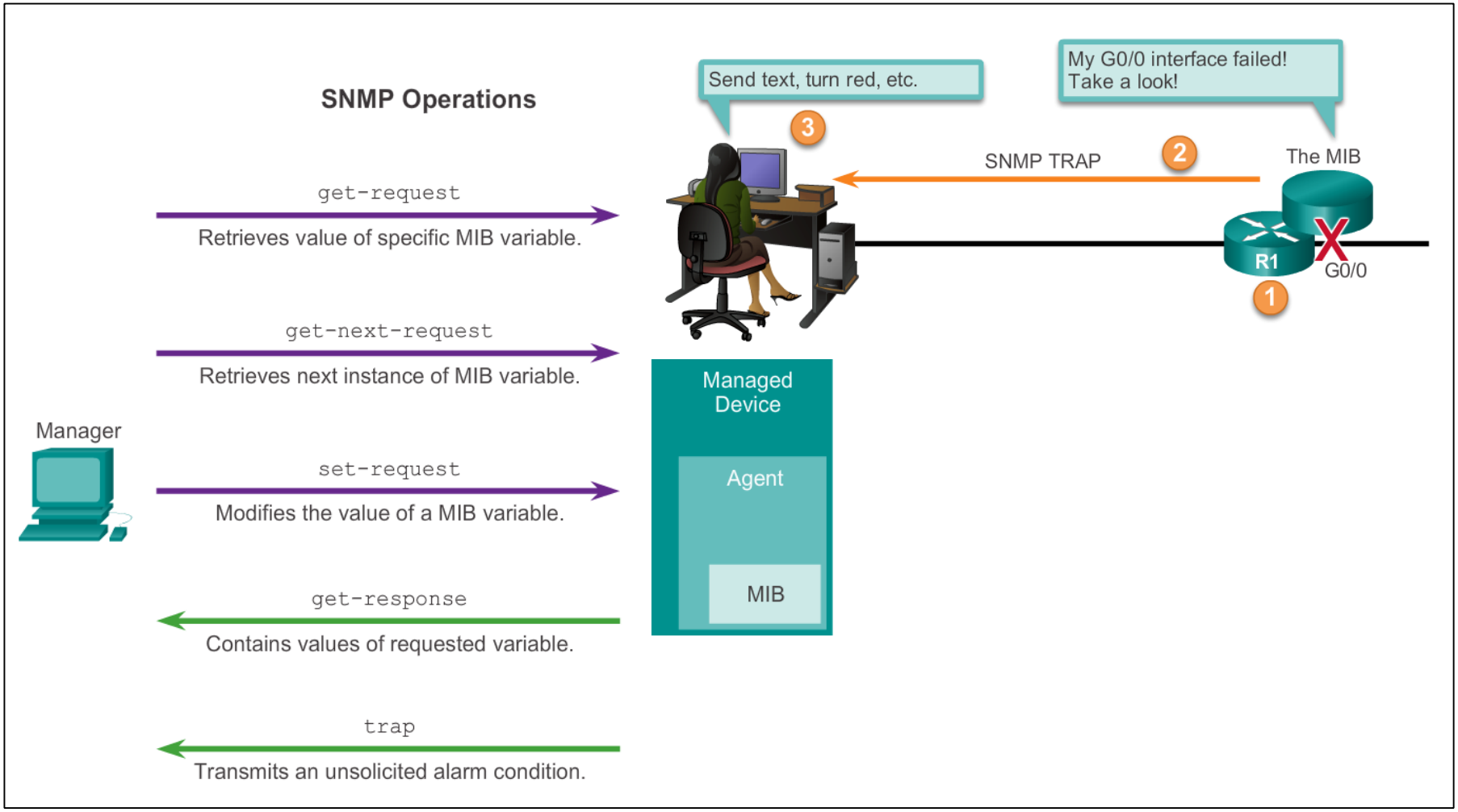
SNMP Operation



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



SNMP Operation

SNMP Versions

There are several versions of SNMP, including:

- **SNMPv1** - The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.
- **SNMPv2c** - Defined in RFCs 1901 to 1908; utilizes community-string-based Administrative Framework.
- **SNMPv3** - Interoperable standards-based protocol originally defined in RFCs 2273 to 2275; provides secure access to devices by authenticating and encrypting packets over the network. It includes these security features: message integrity to ensure that a packet was not tampered with in transit; authentication to determine that the message is from a valid source, and encryption to prevent the contents of a message from being read by an unauthorized source.

SNMP Operation

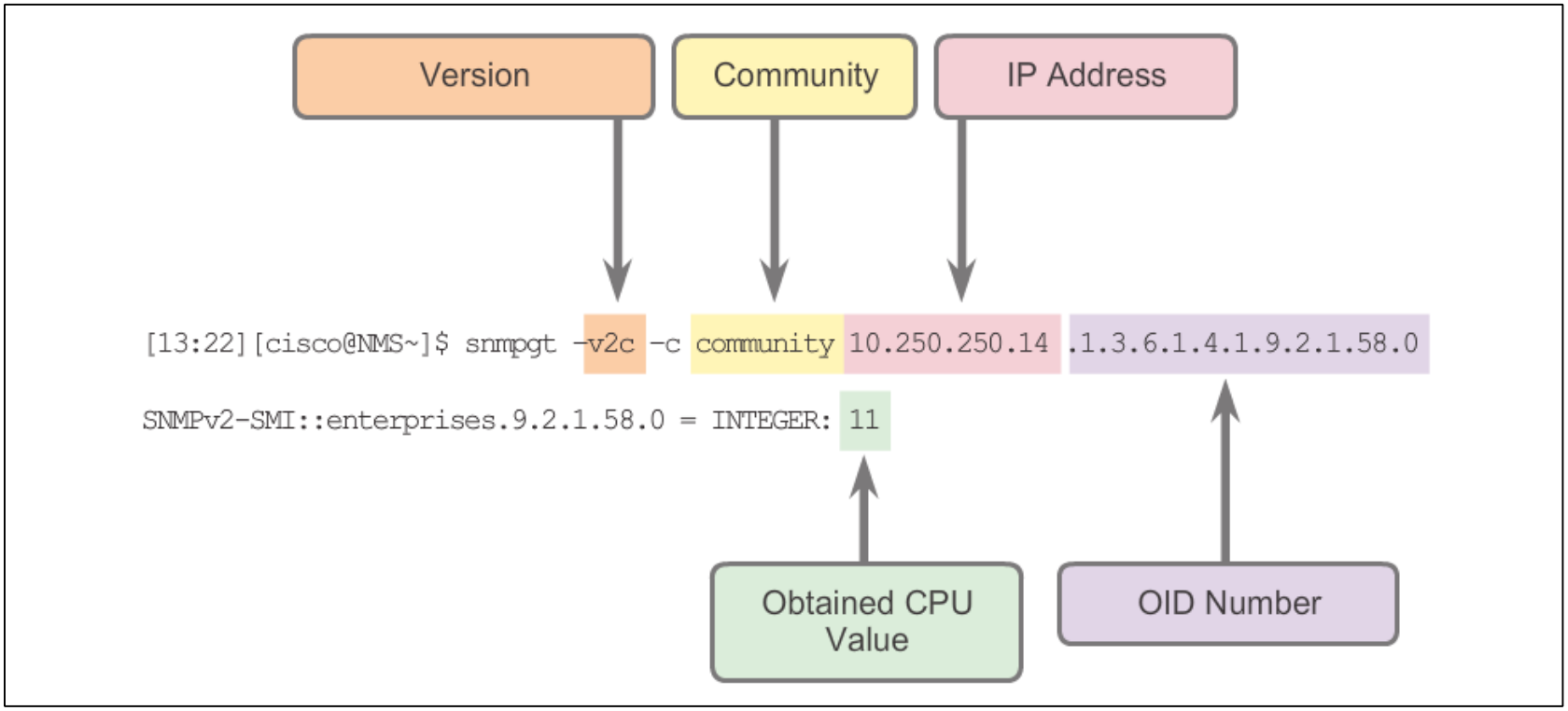
Community Strings

There are two types of community strings:

- **Read-only (ro)** – Provides access to the MIB variables, but does not allow these variables to be changed, only read. Because security is so weak in version 2c, many organizations use SNMPv2c in read-only mode.
- **Read-write (rw)** – Provides read and write access to all objects in the MIB.

SNMP Operation

Management Information Base Object ID



Steps for Configuring SNMP

Step 1. (Required) Configure the community string and access level (read-only or read-write) with the **snmp-server community** *string* **ro | rw** command.

Step 2. (Optional) Document the location of the device using the **snmp-server location** *text* command.

Step 3. (Optional) Document the system contact using the **snmp-server contact** *text* command.

Steps for Configuring SNMP (cont.)

Step 4. (Optional) Restrict SNMP access to NMS hosts (SNMP managers) that are permitted by an ACL. Define the ACL and then reference the ACL with the **snmp-server community** *string access-list-number-or-name* command.

Step 5. (Optional) Specify the recipient of the SNMP trap operations with the **snmp-server host** *host-id* [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* command. By default, no trap manager is defined.

Step 6. (Optional) Enable traps on an SNMP agent with the **snmp-server enable traps** *notification-types* command.

Konfigurácia SNMP

- Vytvorenie ACL pre limitovaný prístup k SNMP agentovi
- Nastavenie SNMP komunít
- Nastavenie cieľa pre zasielanie správ SNMP Trap
- Aktivácia konkrétnych SNMP Trap správ

```
Switch(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Switch(config)# snmp-server community cisco RO 1
Switch(config)# snmp-server community xyz123 RW 1
Switch(config)# snmp-server host 10.1.1.50 xyz123
Switch(config)# snmp-server enable traps ?
```

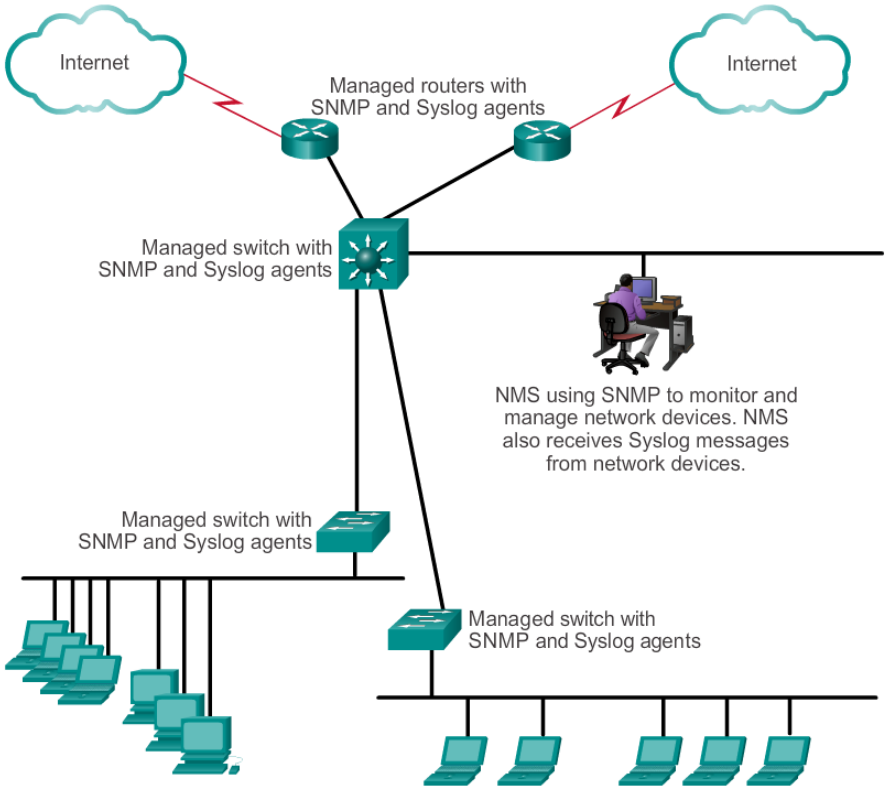
Configuring SNMP

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
```

```
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
```

Security Best Practices

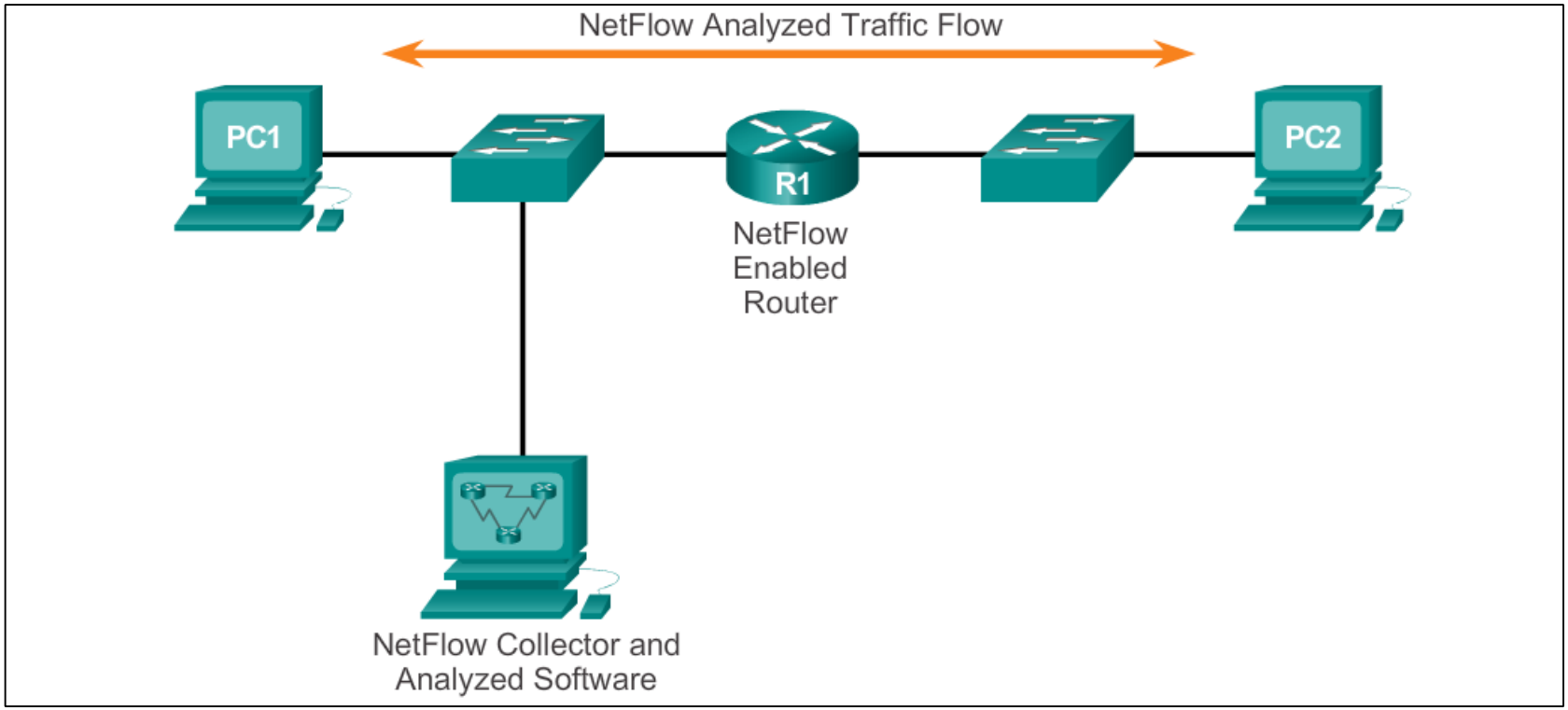


8.3 NetFlow

Cisco | Networking Academy®
Mind Wide Open™

NetFlow Operation

Introduction to NetFlow



Purpose of NetFlow

Most organizations use NetFlow for some or all of the following key data collection purposes:

- Efficiently measuring who is using what network resources for what purpose.
- Accounting and charging back according to the resource utilization level.
- Using the measured information to do more effective network planning so that resource allocation and deployment is well-aligned with customer requirements.
- Using the information to better structure and customize the set of available applications and services to meet user needs and customer service requirements.

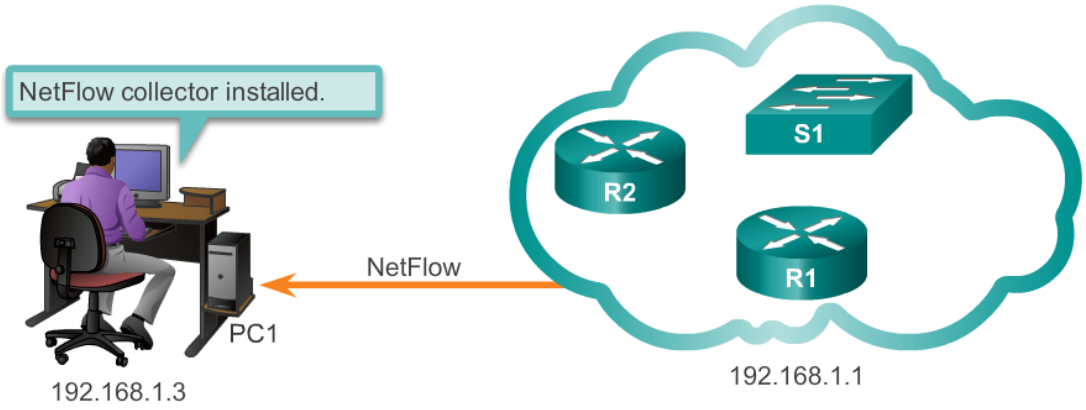
Network Flows

NetFlow technology has seen several generations that provide more sophistication in defining traffic flows, but “original NetFlow” distinguished flows using a 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

Configuring NetFlow

NetFlow Configuration Tasks




```
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
```

Examining Traffic Patterns

Verifying NetFlow

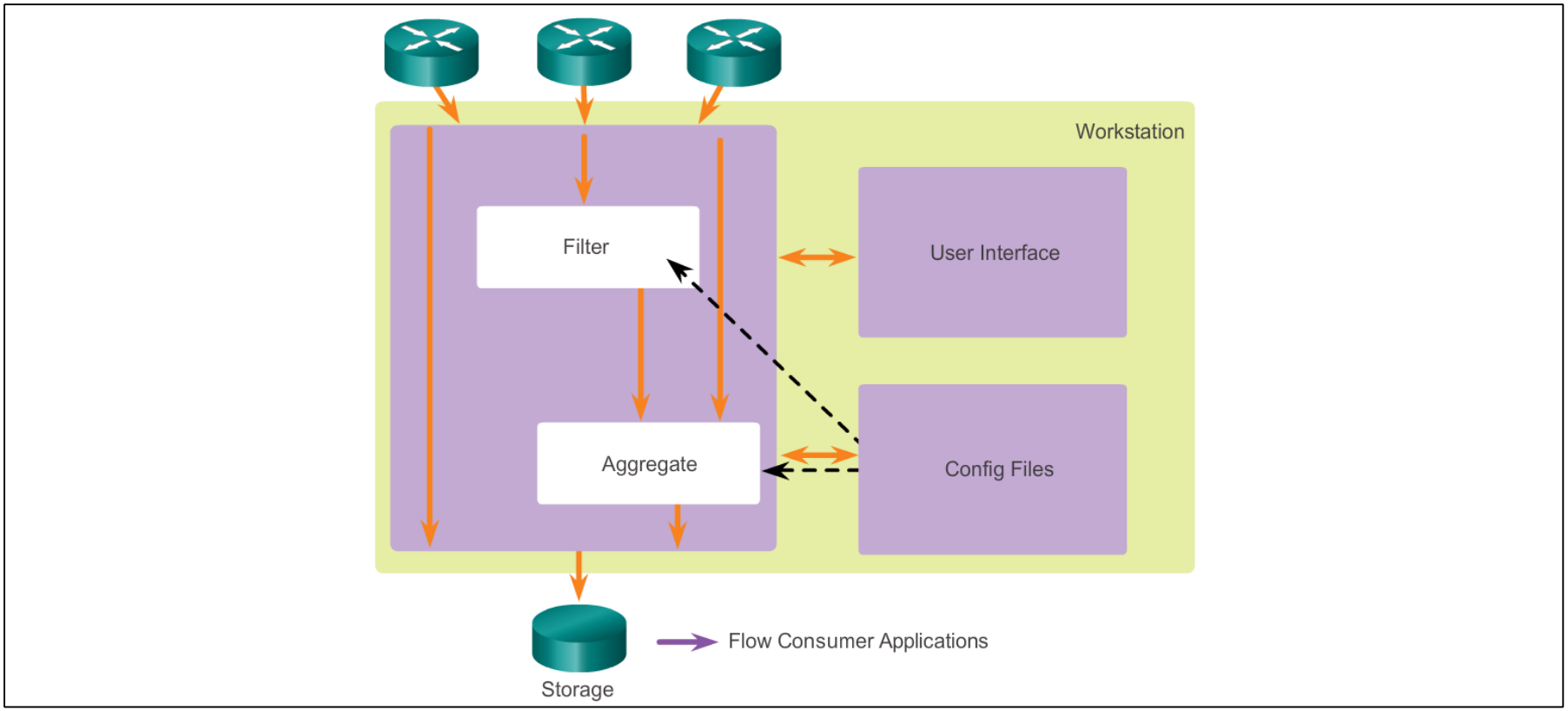
```
R1# show ip cache flow
IP packet size distribution (178617 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .002 .080 .008 .005 .001 .000 .001 .001 .000 .000 .000 .000 .000 .000 .000

    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
```

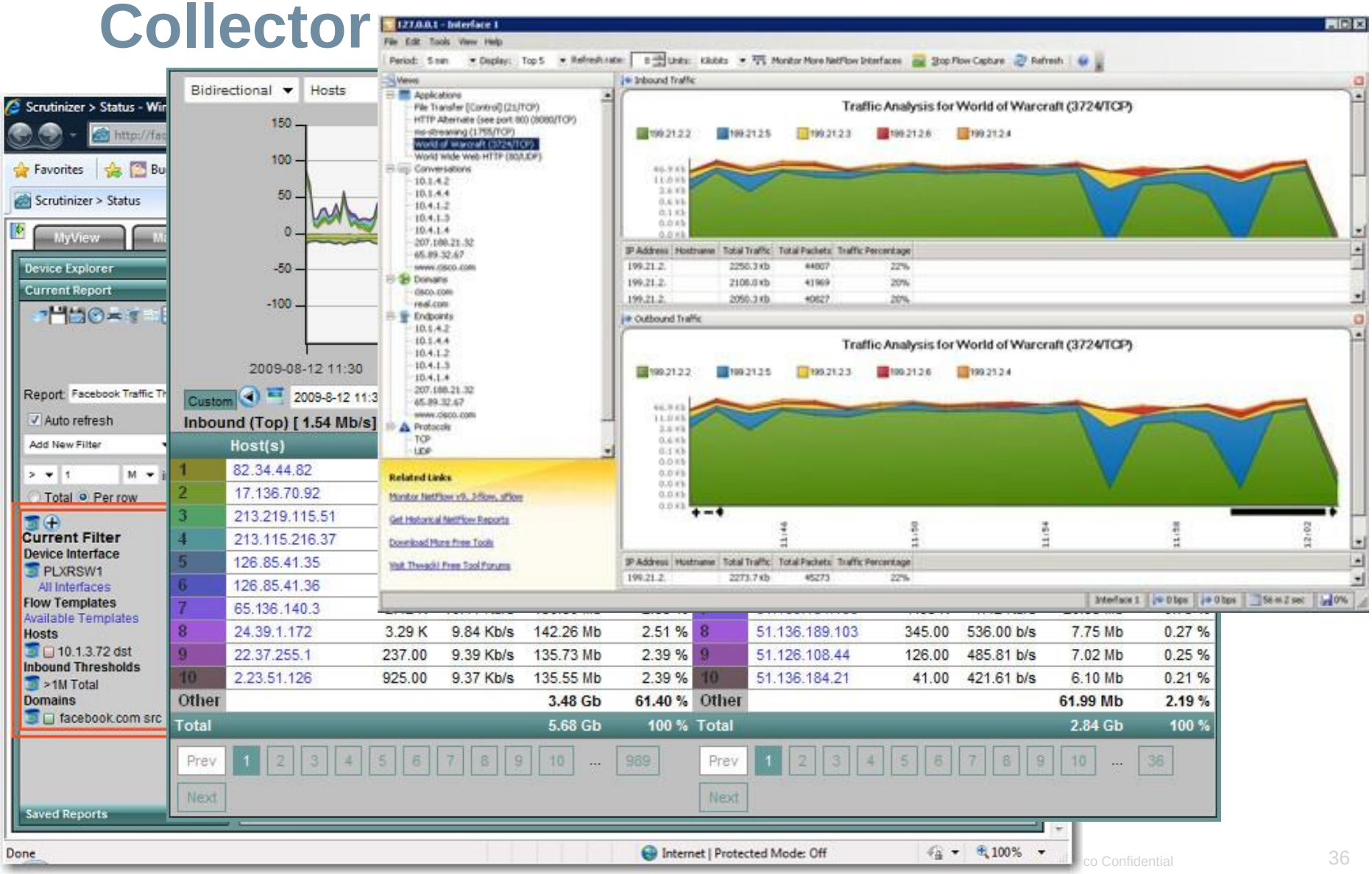
```
R1# show ip flow export
Flow export v5 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.1.3 (2055)
  Version 5 flow records
  1764 flows exported in 532 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets 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
```

Examining Traffic Patterns

NetFlow Collector Functions



NetFlow Analysis with a NetFlow Collector



Chapter 8: Summary

- Syslog, SNMP, and NetFlow are the tools a network administrator uses in a modern network to manage the collection, display, and analysis of events associated with the networking devices.
- Syslog provides a rudimentary tool for collecting and displaying messages as they appear on a Cisco device console display.
- SNMP has a very rich set of data records and data trees to both set and get information from networking devices.
- NetFlow and its most recent iteration, Flexible NetFlow, provides a means of collecting IP operational data from IP networks.
- NetFlow provides data to enable network and security monitoring, network planning, traffic analysis, and IP accounting.
- NetFlow collectors provide sophisticated analysis options for NetFlow data.