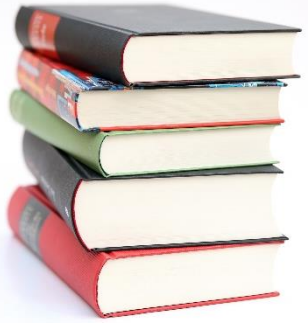
MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Manažment, údržba a monitoring siete

Počítačové siete 1

Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU

Vytvorené v rámci projektu KEGA 011STU - 4/2017.



Čo nás dnes čaká

CCNA 2

Chapter 10: Device Discovery, Management, and Maintenance

- **10.1 Device Discovery**
  - Zmapovanie sieťovej topológie
- **10.2 Device Management**
  - NTP, Syslog
- **10.3 Device Maintenance**
  - Údržba konfiguračných a IOS súborov

CCNA 4:

Chapter 5: Network Security and Monitoring

- **5.1 LAN Security**
  - Útoky na LAN a zmierňovanie ich dopadov
- **5.2 SNMP**
  - SNMP pre monitorovanie sieťových operácií
- **5.3 Cisco Switch Port Analyzer (SPAN)**
  - Zrkadlenie prevádzky a jeho využitie

\+ **NetFlow**

10.1 Device Discovery

Device Discovery

CDP

- CDP Overview
  - Cisco Discovery Protocol
  - Neighbor discovery of physically connected Cisco devices
- Configure and Verify CDP
  - **`show cdp neighbors`**
  - **`show cdp interface`**
  - **`cdp run`**
  - **`cdp enable`**
  - **`clear cdp counters, clear cdp table`**
- Discover Devices Using CDP
  - Device identifiers - The host name of the neighbor device
  - Port identifier - The name of the local and remote port
  - Capabilities list - Whether the device is a router or a switch
  - Platform - The hardware platform of the device

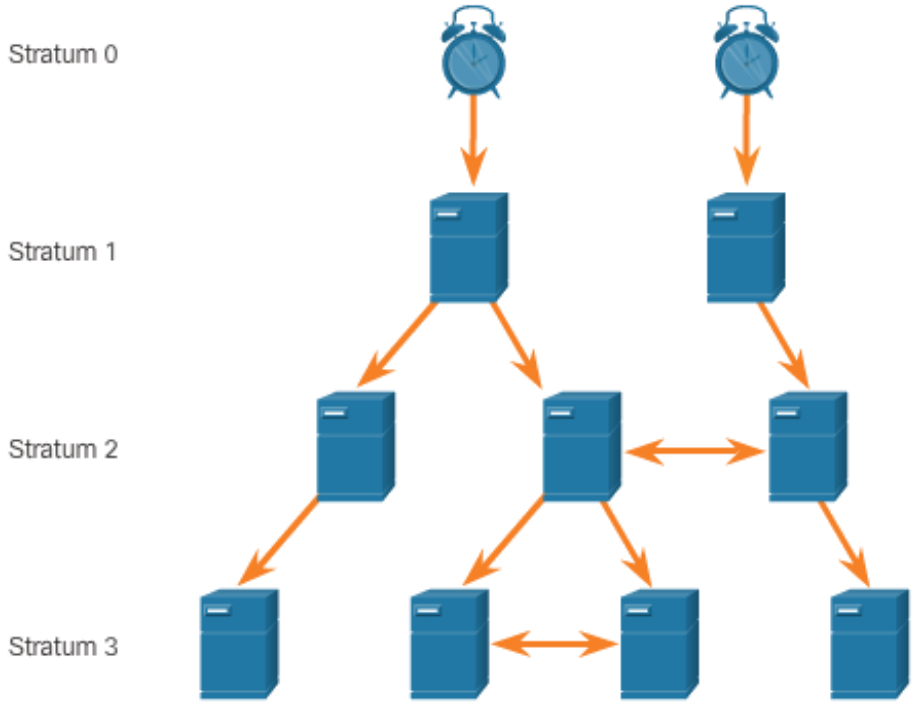
LLDP

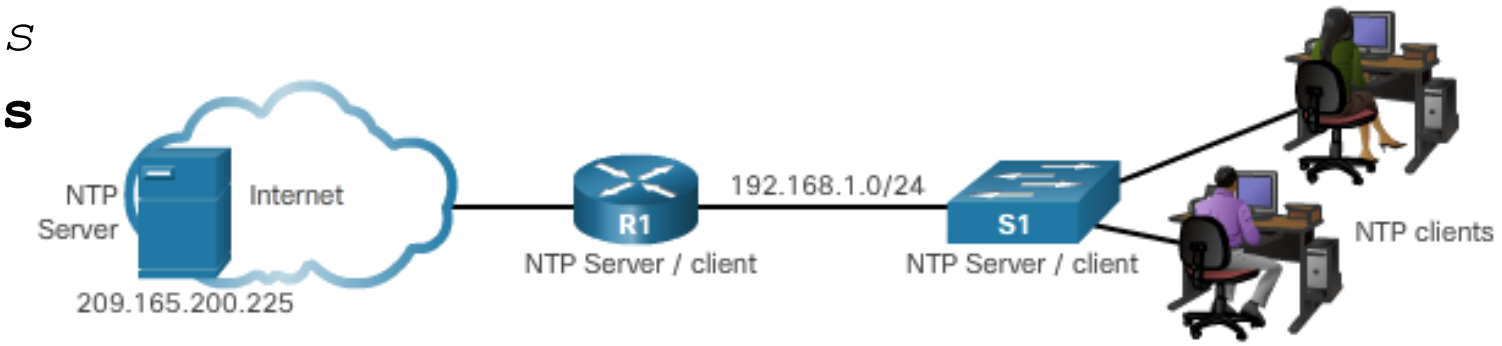
- LLDP Overview
  - A vendor neutral layer 2 neighbor discovery protocol, similar to CDP
- Configure and Verify LLDP
  - **`show lldp`**
  - **`lldp run`**
  - **`lldp transmit`**
  - **`lldp receive`**
- Discover Devices Using LLDP
  - **`show lldp neighbors`**

10.2 Device Management

Implementácia NTP

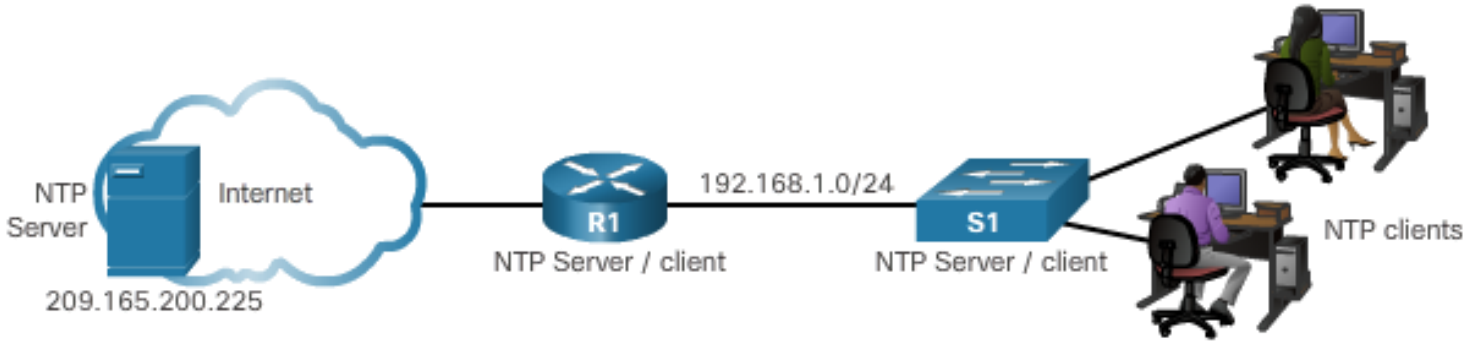
- Ako nastaviť systémové hodiny
  - Manuálne (reboot?)
  - Nakonfigurovať NTP
- Ako funguje NTP (UDP/123, RFC 1305)
  - Hierarchický systém zdrojov času
  - Stratum 0 – autoritatívny zdroj
  - Iné čísla – ako ďaleko je daný server od zdroja
    - Max. 15, 16 = nesynchornizovaný
- Konfigurácia a overenie NTP
  - **`ntp server`** *`ip-address`*
  - **`show ntp associations`**
  - **`show ntp status`**
  - **`show clock [detail]`**





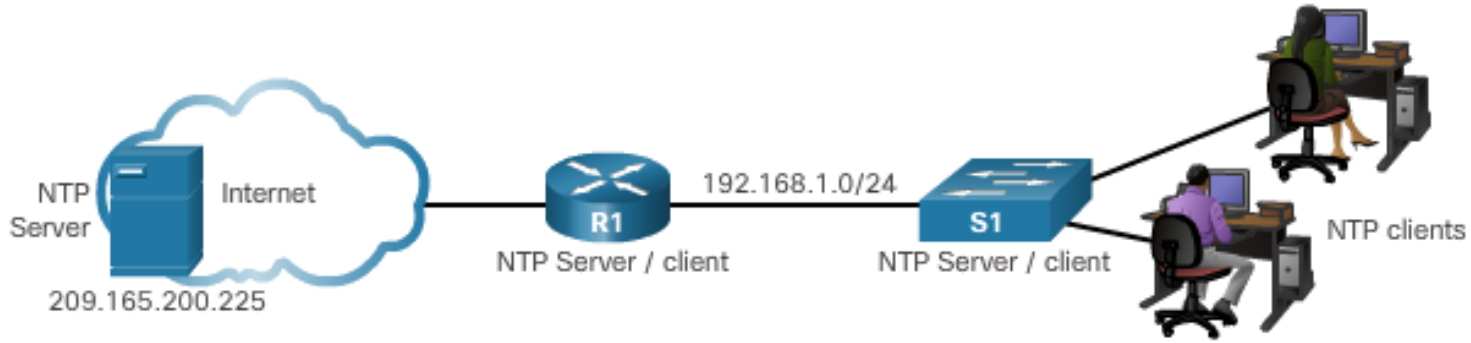
Implementácia NTP

```
R1# show clock detail
20:55:10.207 UTC Fri Dec 11 2015
Time source is user configuration
R1(config)# ntp server 209.165.200.225
R1(config)# end
R1# show clock detail
21:01:34.563 UTC Fri Dec 11 2015
Time source is NTP
```




```
R1# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~209.165.200.225 .GPS.           1     61     64   377  0.481   7.480  4.261
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
ntp uptime is 589900 (1/100 of seconds), resolution is 4016
reference time is DA088DD3.C4E659D3 (13:21:23.769 PST Tue Dec 1 2015)
clock offset is 7.0883 msec, root delay is 99.77 msec
root dispersion is 13.43 msec, peer dispersion is 2.48 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000001803 s/s
system poll interval is 64, last update was 169 sec ago.
```

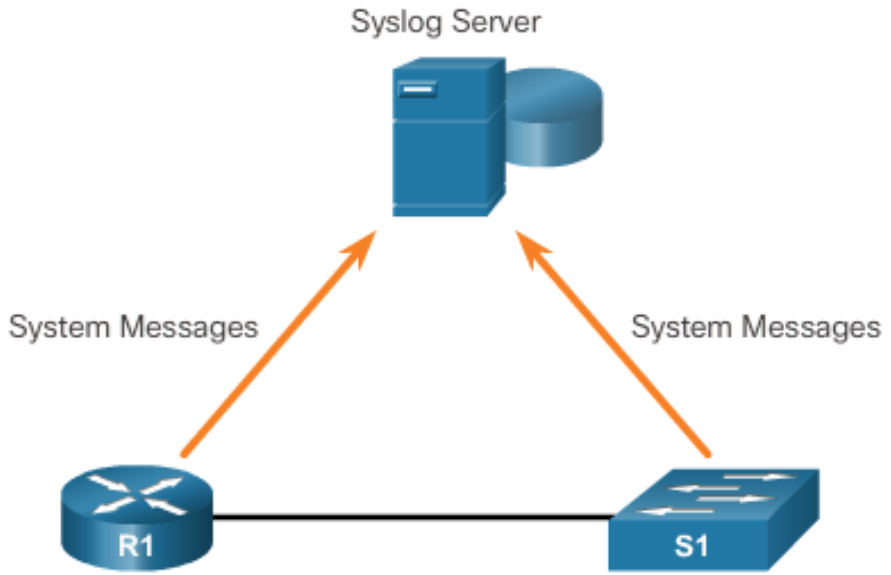
Implementácia NTP

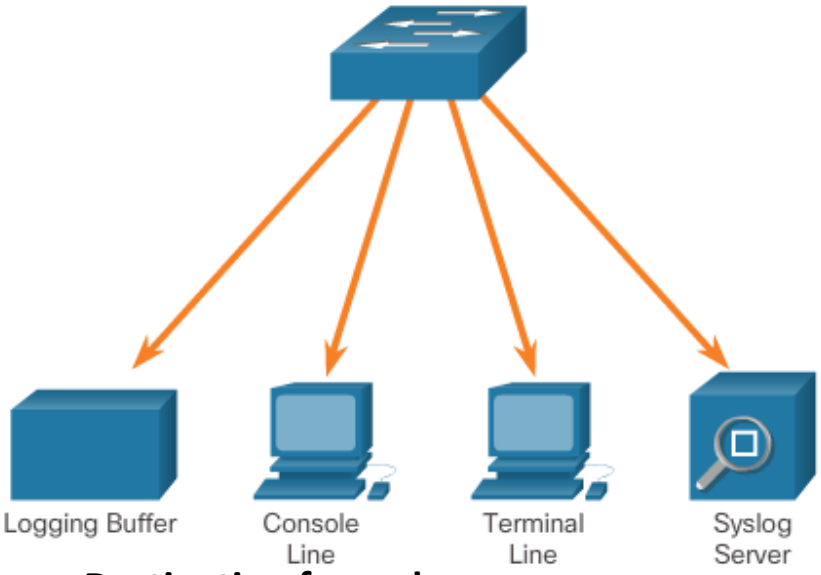



```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~C192.168.1.1     209.165.200.225  2     12     64   377  1.066  13.616  3.840
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

S1# Cshow ntp status
CClock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2**17
reference time is DA08904B.3269C655 (13:31:55.196 PST Tue Dec 1 2015)
clock offset is 18.7764 msec, root delay is 102.42 msec
root dispersion is 38.03 msec, peer dispersion is 3.74 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000003925 s/s
system poll interval is 128, last update was 178 sec ago.
```

Syslog

- Introduction to Syslog (UDP/514, RFC 3164)
  - Allows devices to send their messages to syslog server
  - Supported by most networking devices
  - Primary functions:
    - **log information** for monitoring and troubleshooting
    - select the **type** of logging information that is captured
    - specify the **destinations** of captured syslog messages
- Syslog Message Format
  - Severity level from 0 – 7
  - Facility – service identifiers
- Service Timestamp
  - Enhances real-time debugging and management
  - Log messages can be time-stamped and the source address of syslog messages can be set.
  - **`service timestamps log datetime msec`**





Destination for syslog messages

Syslog Configuration

- Syslog Server
  - Parses the output and places the messages into pre-defined columns
  - Timestamps are displayed if configured on networking devices that generated the log messages
  - Allows the network administrators to navigate the large amount of data compiled on a syslog server.
- Default Logging
  - Send log messages of all severity level to the console
  - **`show logging`**
- Router and Switch Commands for Syslog Clients
  - **`logging`** *`ip-address`*
  - **`logging`** `trap` *`level`*
  - **`logging source-interface`** *`source-interface interface-number`*
- Verifying Syslog
  - **`show logging`**
  - Use the pipe (|) to limit the amount of displayed log messages

Syslog Message Format

- Some common syslog message facilities reported on Cisco IOS routers include:
  - IP
  - OSPF protocol
  - SYS operating system
  - IP security (IPsec)
  - Interface IP (IF)

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.

```
seq no: timestamp: %facility-severity-MNEMONIC: description
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

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

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
```

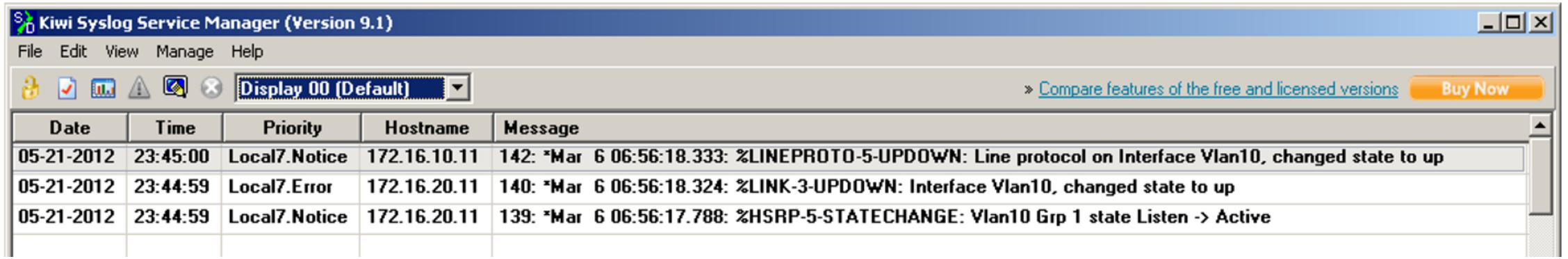
Configuring Syslog

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)#
```

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

Verifying Syslog

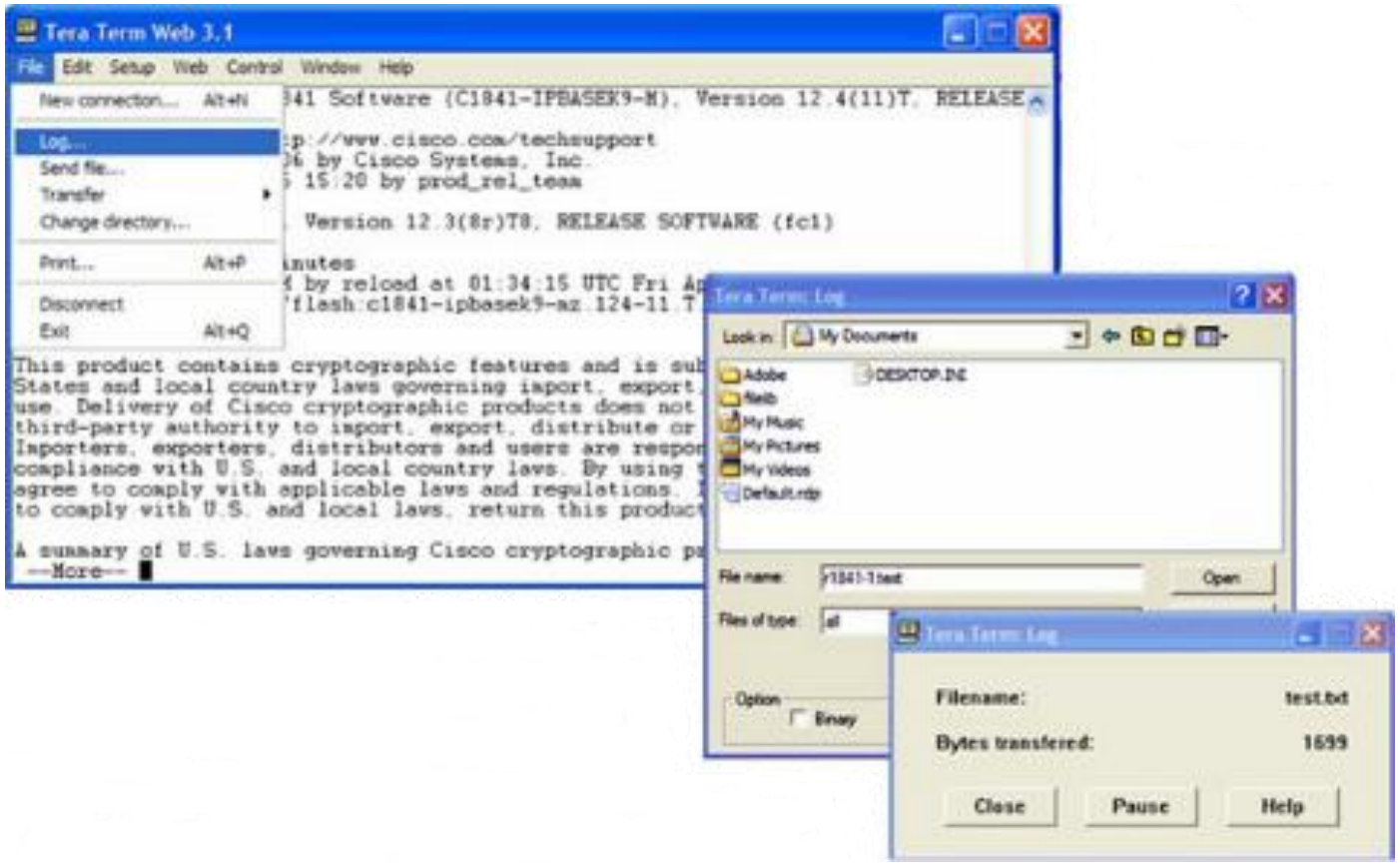
```
R1# show logging | include changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface Seri
changed state to up
*Jun 12 17:46:27.263: %LINEPROTO-5-UPDOWN: Line prot
Interface GigabitEthernet0/1, changed 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#
```

10.3 Device Maintenance

Router and Switch File Maintenance

- Router and Switch File Systems
  - **`show file systems`** – lists all available file system
  - **`dir`** – lists the content of the file system
  - **`pwd`** – verify the present working directory
  - **`cd`** – changes the current directory
- Backing up and Restoring using Text Files

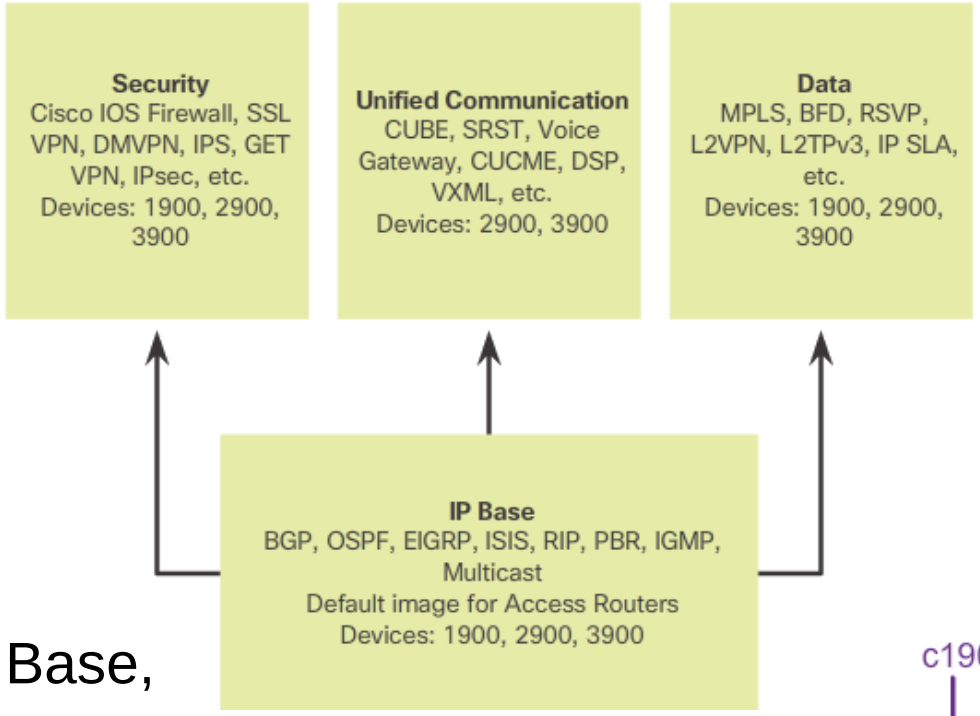


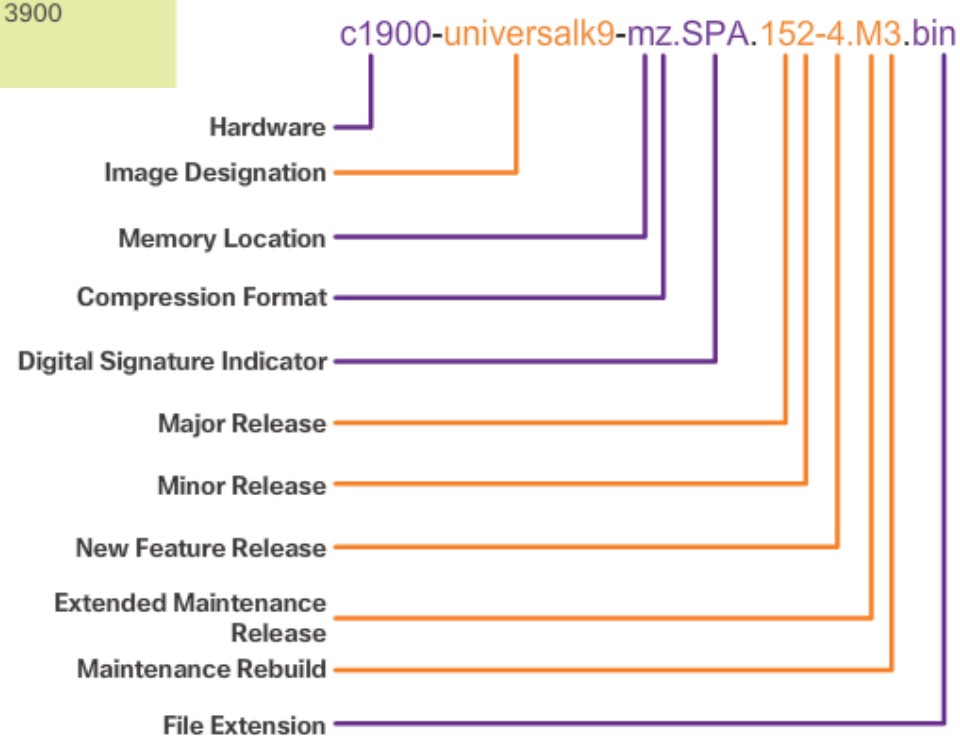
Router and Switch File Maintenance (Cont.)

- Backing up and Restoring using TFTP
  - `copy running-config tftp`
  - `copy startup-config tftp`
- Using USB Ports for Backing Up and Restoring
  - `show file systems`
  - `dir usbflash0:`
  - `copy run usbflash0:/`
- Password Recovery
  - Enter ROMMON mode
  - Change configuration register to 0x2142
  - Make changes to the original startup config
  - Save the new configuration

IOS System Files

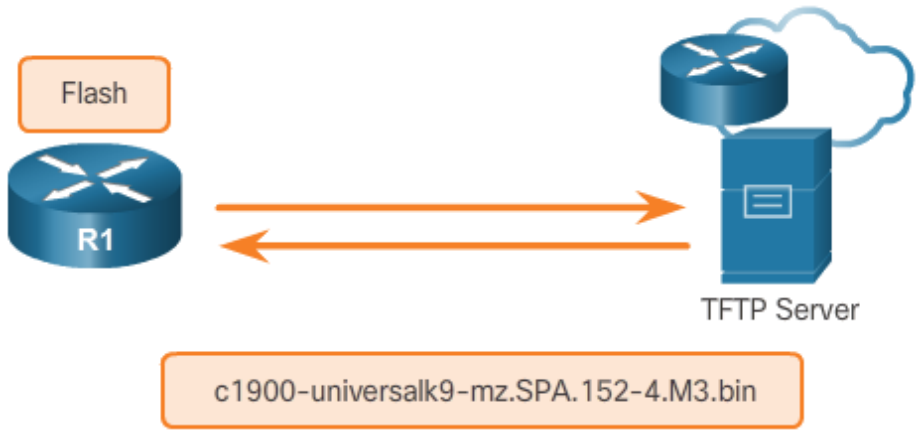
- IOS 15 System Image Packaging
  - universalk9 images
  - universalk9_npe images
  - Technology packages: IP Base, Data, UC, SEC
  - Data, UC, and SEC technology packages are activated through licensing
- IOS Image Filenames
  - Feature sets and version
  - **`show flash`**





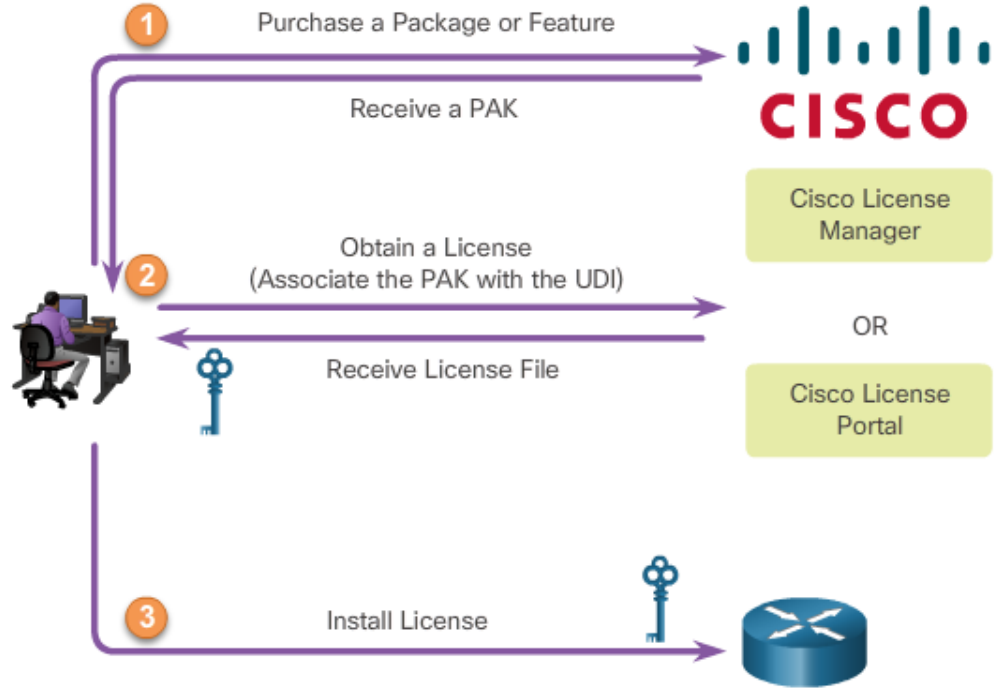
IOS Image Management

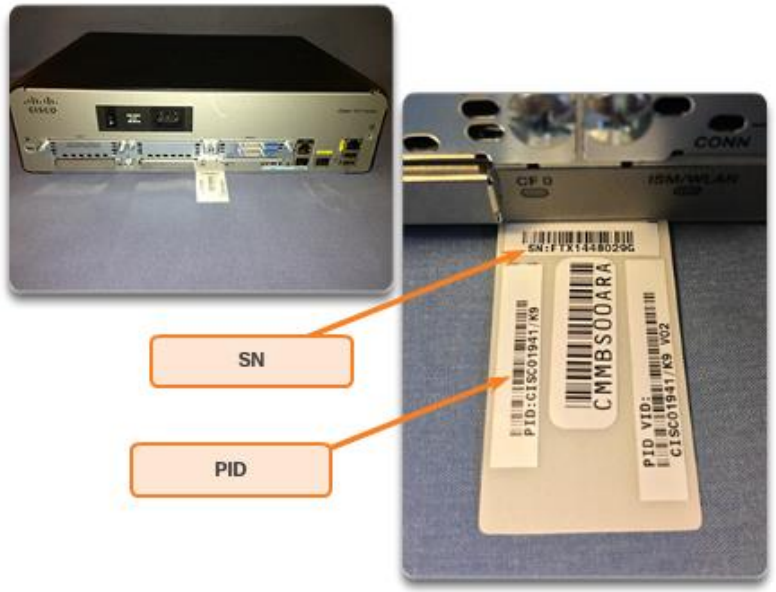
- TFTP Servers as a Backup Location
  - Backup location for IOS images and configuration files
- Steps to Backup IOS Image to TFTP Server
  - Verify access to TFTP server
  - Verify sufficient disk space
  - Copy the image to the TFTP server
    - **`copy`** *`source-url`* **`tftp:`**
- Steps to Copy an IOS Image to a Device
  - Download IOS image from Cisco.com and transfer it to TFTP server
  - Verify access to TFTP server from device
  - Verify sufficient disk space on device
  - Copy the image from the TFTP server
    - **`copy tftp:`** *`destination-url`*
- The **`boot system`** Command
  - Command to load the new image during bootup
  - **`boot system`** *`file-url`*



Software Licensing

- Licensing Process
  - Purchase the software package or feature to install
  - Obtain a license
    - Cisco License Manger
    - Cisco License Portal
    - Requires PAK number and UDI
      - **`show license udi`**
  - Install the license
    - **`license install`** *`stored-location-url`*
    - **`reload`**





License Verification and Management

- License verification
  - **`show version`**
  - **`show license`**
- Activate an evaluation right-to-use license
  - **`license accept end user agreement`**
  - **`license boot module`** *`module-name`* **`technology-package`** *`package-name`*
- Back up the license
  - **`license save`** *`file-sys://lic-location`*
- Uninstall the license
  - Disable the license
    - **`license boot module`** *`module-name`* **`technology-package`** *`package-name`* **`disable`**
  - Clear the license
    - **`license clear`** *`feature-name`*
    - **`no license boot module`** *`module-name`* **`technology-package`** *`package-name`* **`disable`**

5.1 LAN Security

LAN Security Attacks

- Common attacks against the Layer 2 LAN infrastructure include:
  - CDP Reconnaissance Attacks
  - Telnet Attacks
  - MAC Address Table Flooding Attacks
  - VLAN Attacks
  - DHCP Attacks

Čím zmierniť tieto hrozby?

LAN Security Best Practices

- This topic covers several Layer 2 security solutions:
  - Mitigating MAC address table flooding attacks using port security
  - Mitigating VLAN attacks by disabling DTP and following basic guidelines for configuring trunk ports.
  - Mitigating DHCP attacks using DHCP snooping
  - Securing administrative access using AAA
  - Securing device access using 802.1X port authentication

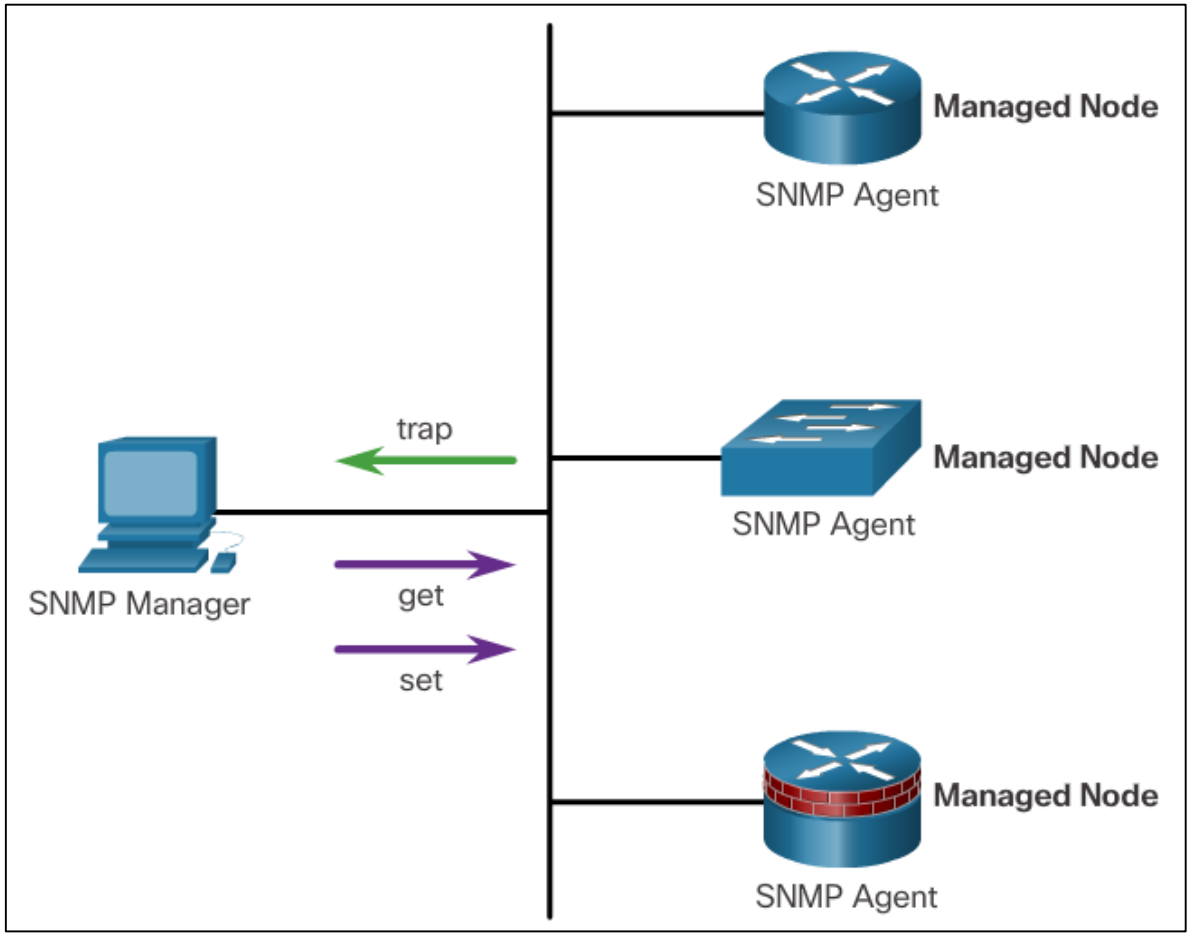
LAN Security Best Practices

- 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 SFTP.
  - Always use strong passwords and change them often.
  - Enable CDP on select ports only.
  - Secure Telnet access.
  - Use a dedicated management VLAN where nothing but management traffic resides.
  - Use ACLs to filter unwanted access.

5.2 SNMP

SNMP Operation

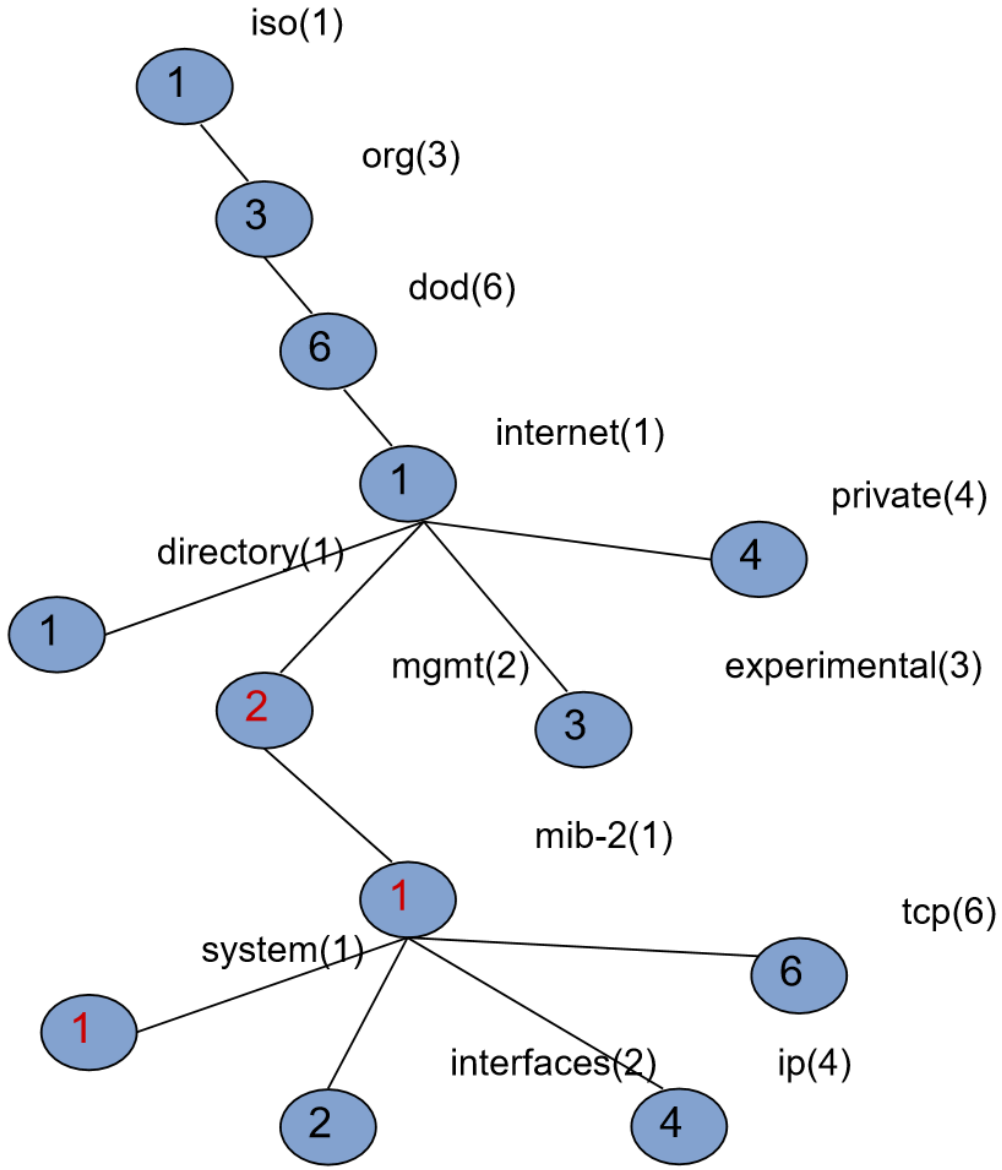
- SNMP allows administrators to manage and monitor devices on an IP network.
- SNMP Elements
  - SNMP Manager
  - SNMP Agent
  - MIB
- SNMP Operation
  - Trap
  - Get
  - Set



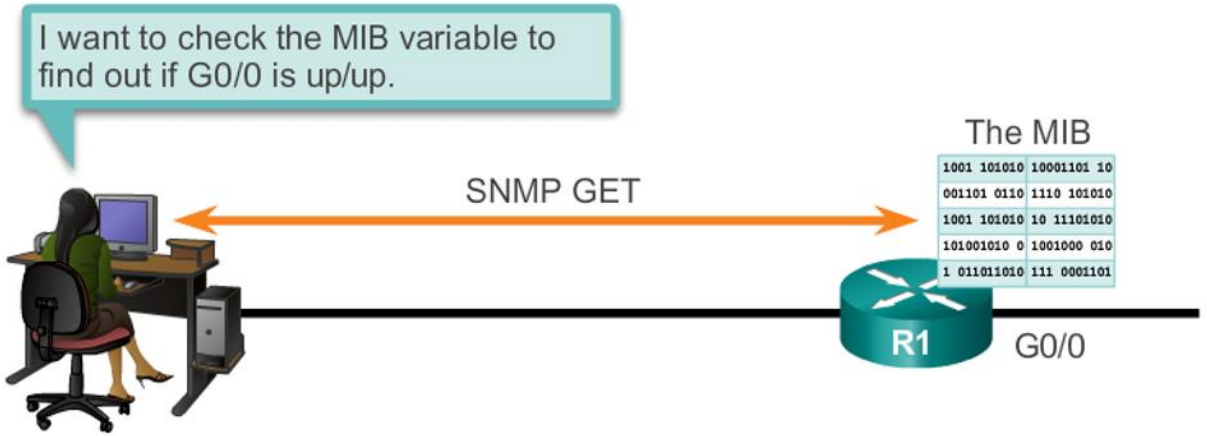
MIB – Management Information Base

- 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)

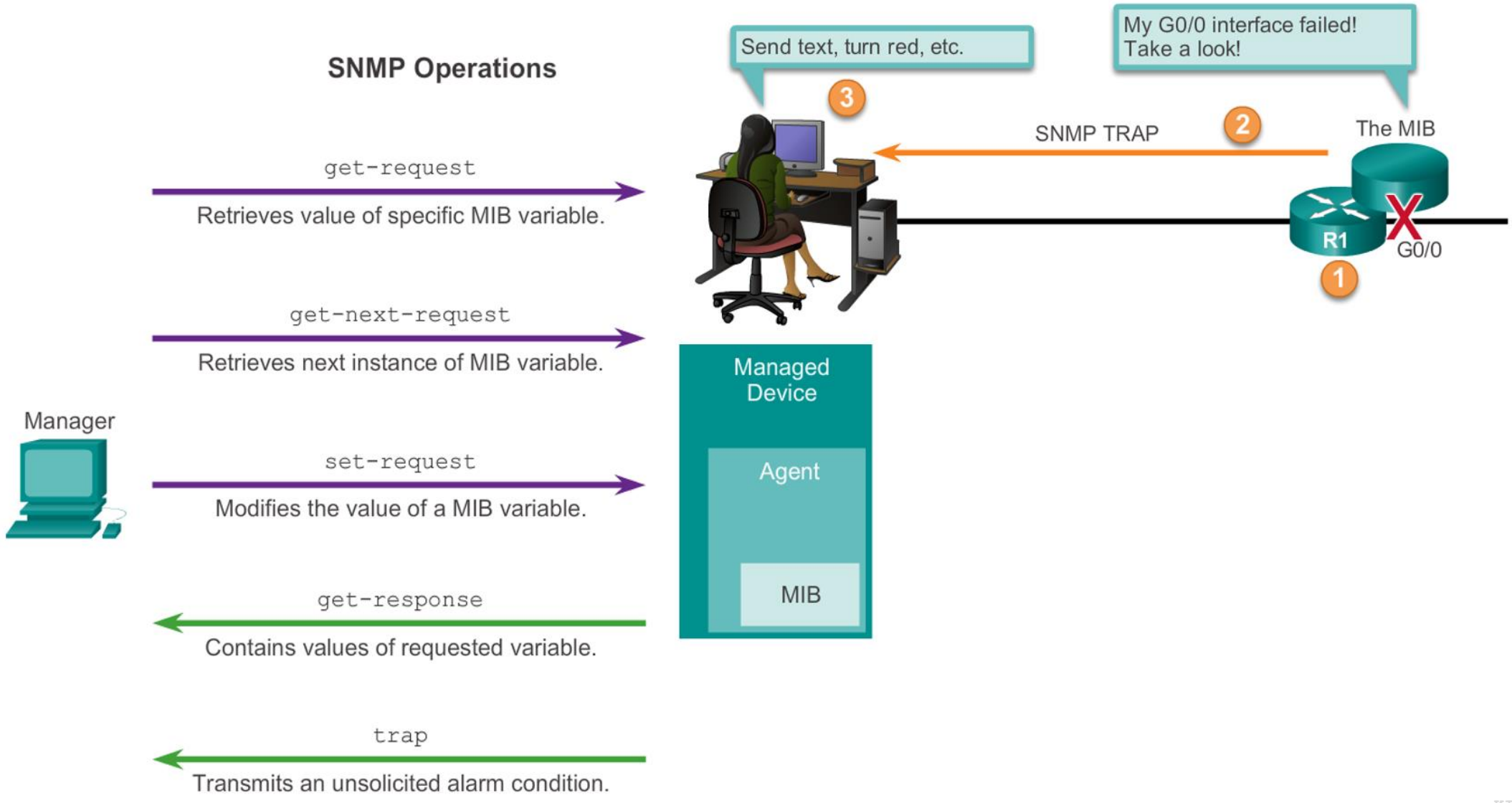


SNMP Operation



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 Agent Traps



SNMP Operation

- SNMP Security Model and Levels
  - **SNMPv1** - RFC 1157.
  - **SNMPv2c** - RFCs 1901 to 1908; utilizes community-string-based Administrative Framework.
  - **SNMPv3** - RFCs 2273 to 2275; It includes **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.

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

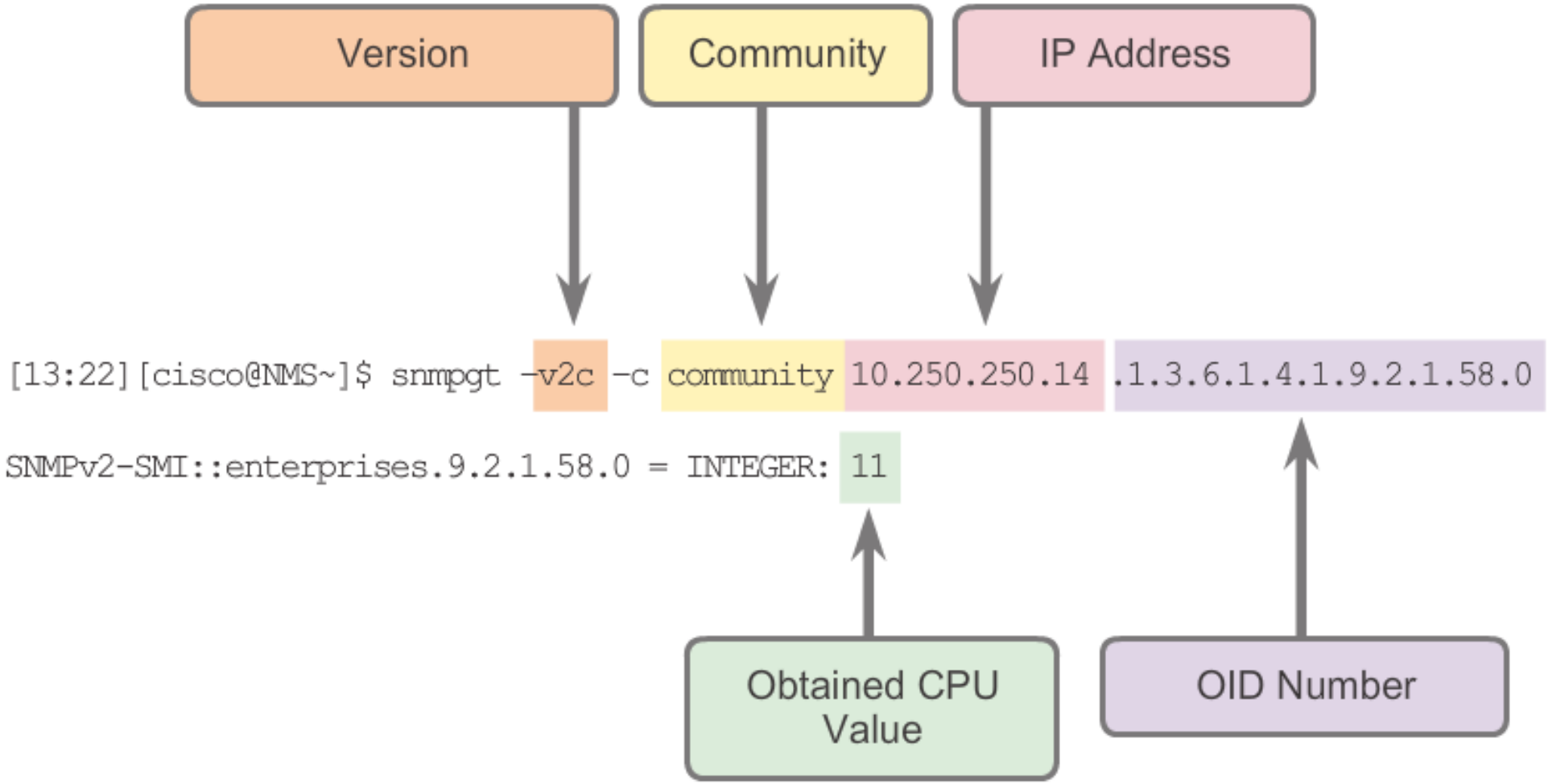
Community Strings

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



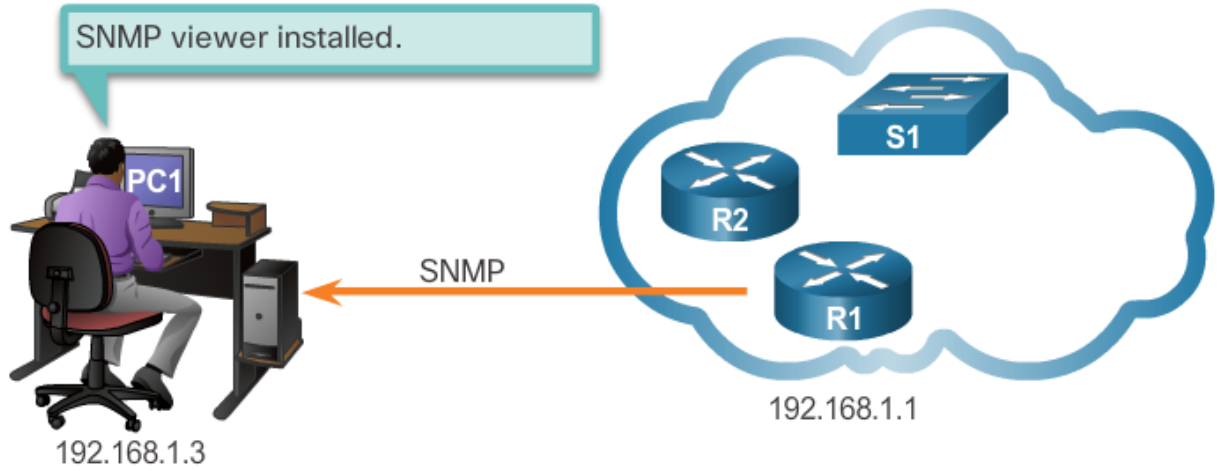
Konfigurácia SNMP

- 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

- Configuration steps
  - (Required) Configure the community string and access level (read-only or read-write)
  - Document location of device
  - Document system contact
  - Restrict SNMP access to NMS hosts (SNMP managers) that are permitted by an ACL.
  - 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
```

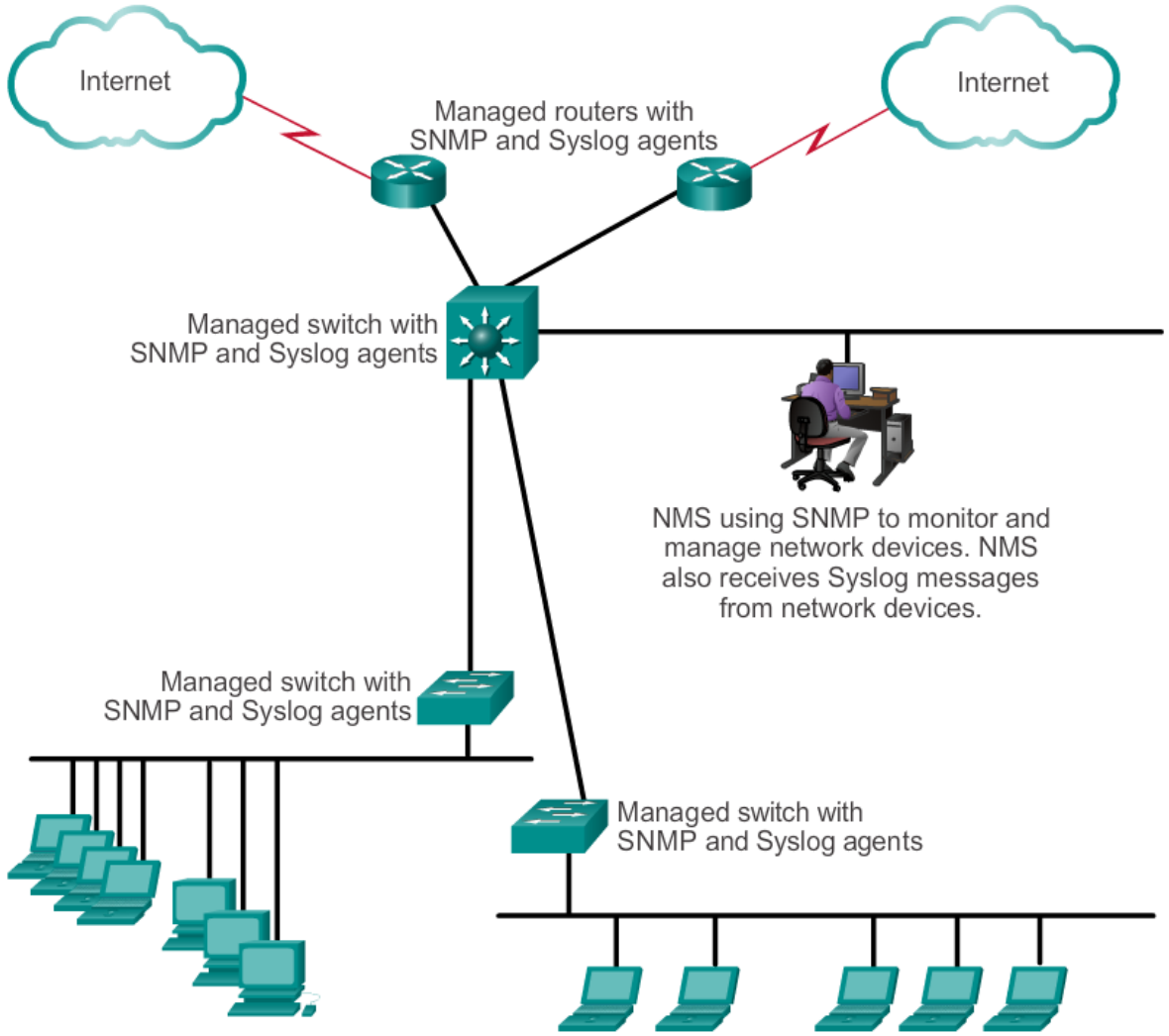
Configuring SNMP

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



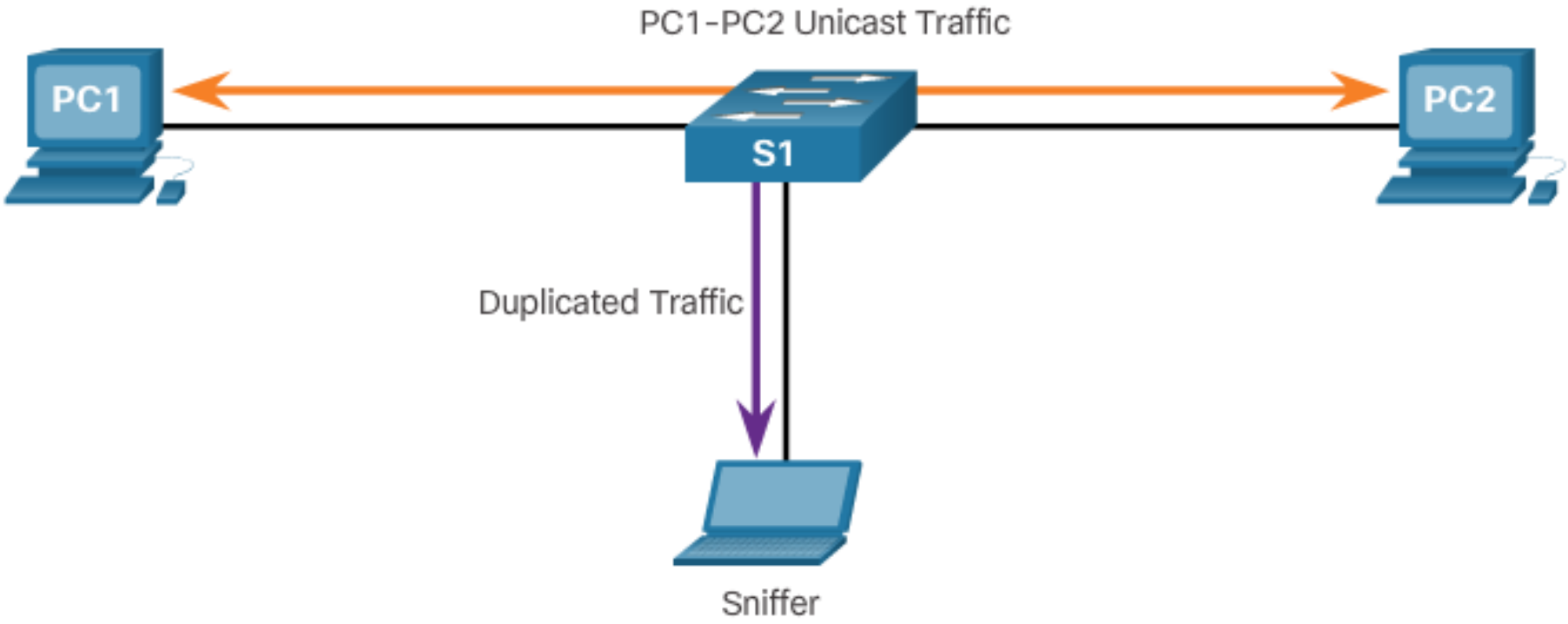
MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

5.3 Cisco Switch Port Analyzer (SPAN)

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

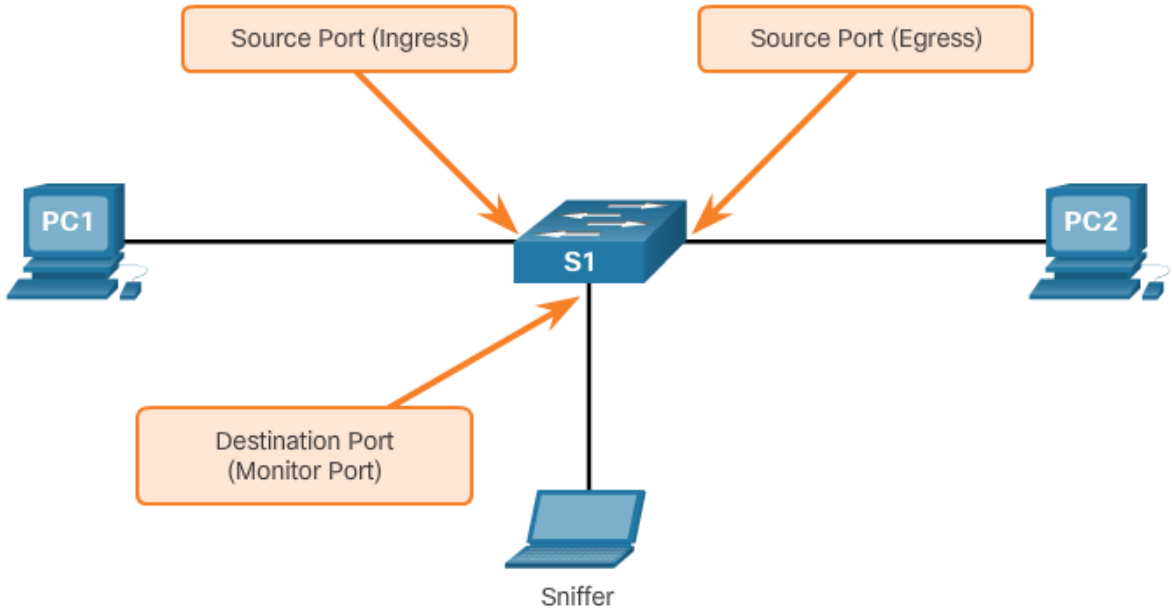
Cisco Switch Port Analyzer
SPAN Overview

- Port mirroring
  - 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.
  - It is commonly implemented to support traffic analyzers or IPS devices.



Cisco Switch Port Analyzer SPAN Overview

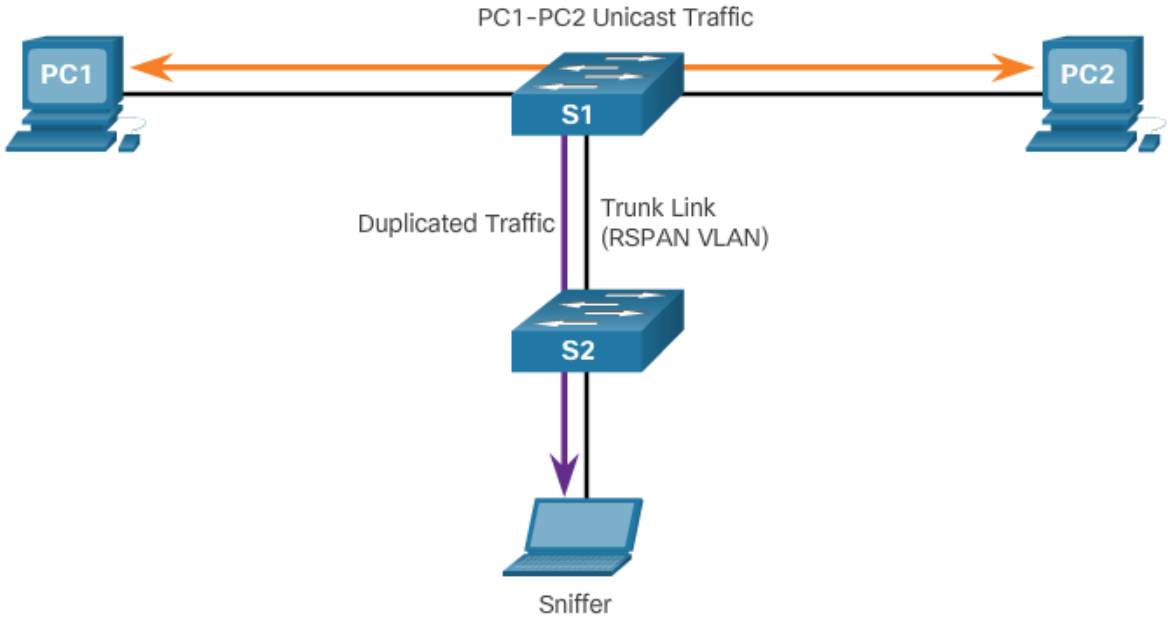
- SPAN terminology



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.

Cisco Switch Port Analyzer SPAN Overview

- RSPAN terminology



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.

Cisco Switch Port Analyzer
SPAN Configuration

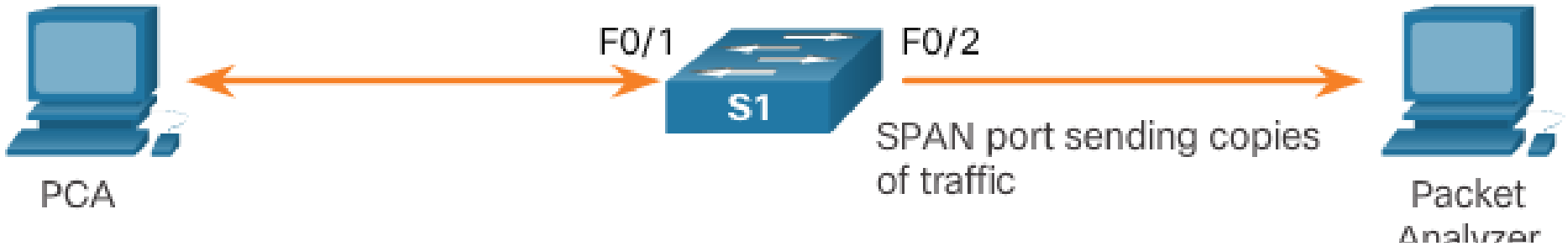
- Use monitor session global configuration command

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

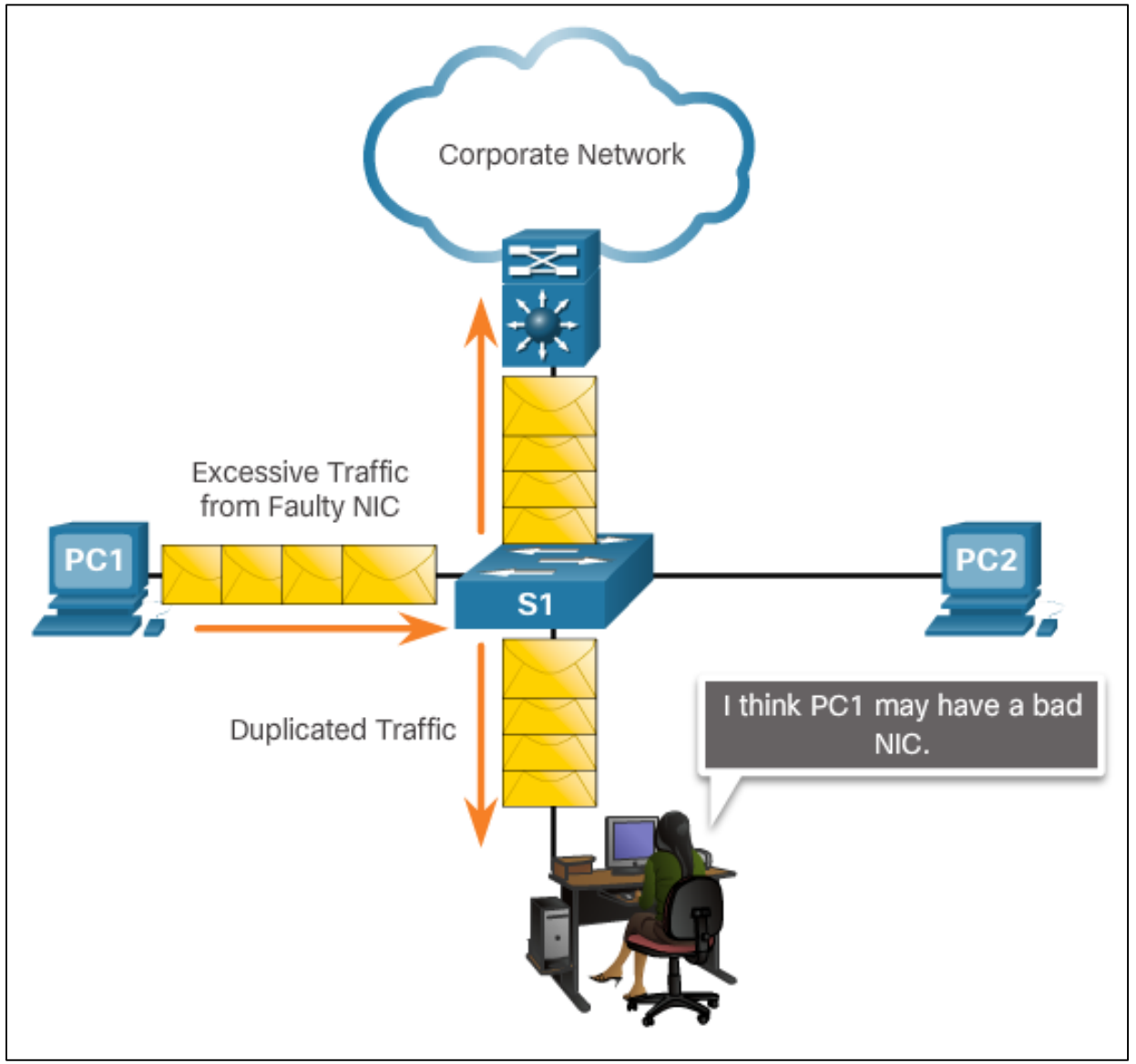
```
Switch(config)# monitor session number destination [ interface interface | vlan vlan ]
```




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

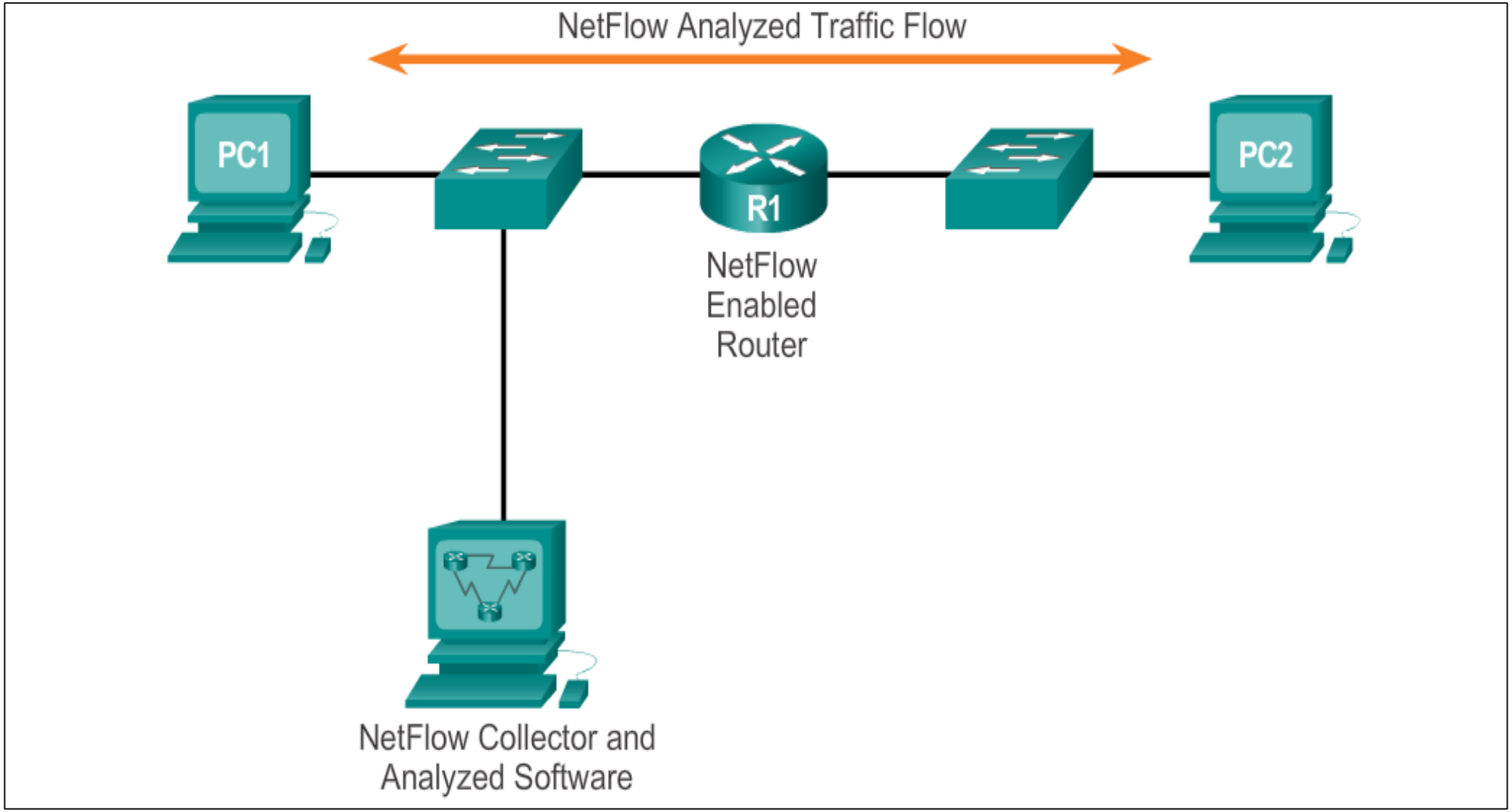
Cisco Switch Port Analyzer
SPAN as a Troubleshooting Tool

- 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



Prídavok: NetFlow

Introduction to NetFlow



Purpose of NetFlow

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

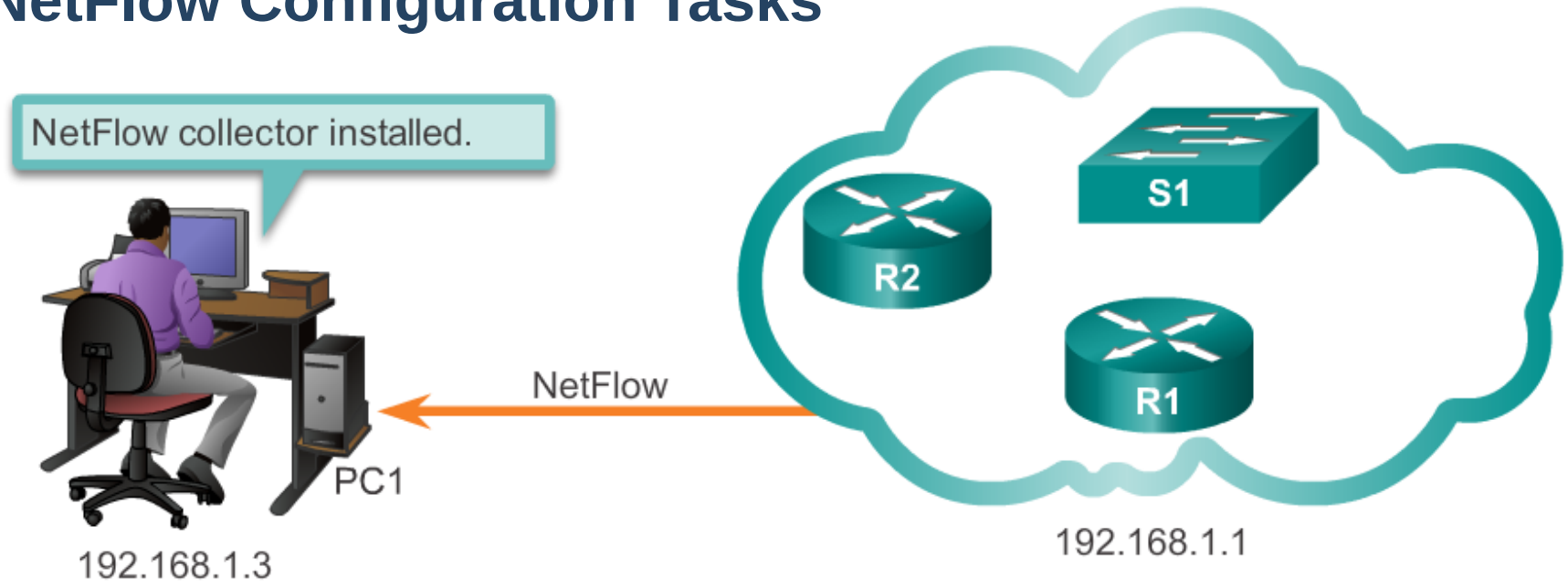
- Efficiently **measuring** who is using what network resources for what purpose.
- **Accounting** and charging back according to the resource utilization level.
- Using the measured information to do more effective network **planning** so that resource allocation and deployment is well-aligned with 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

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

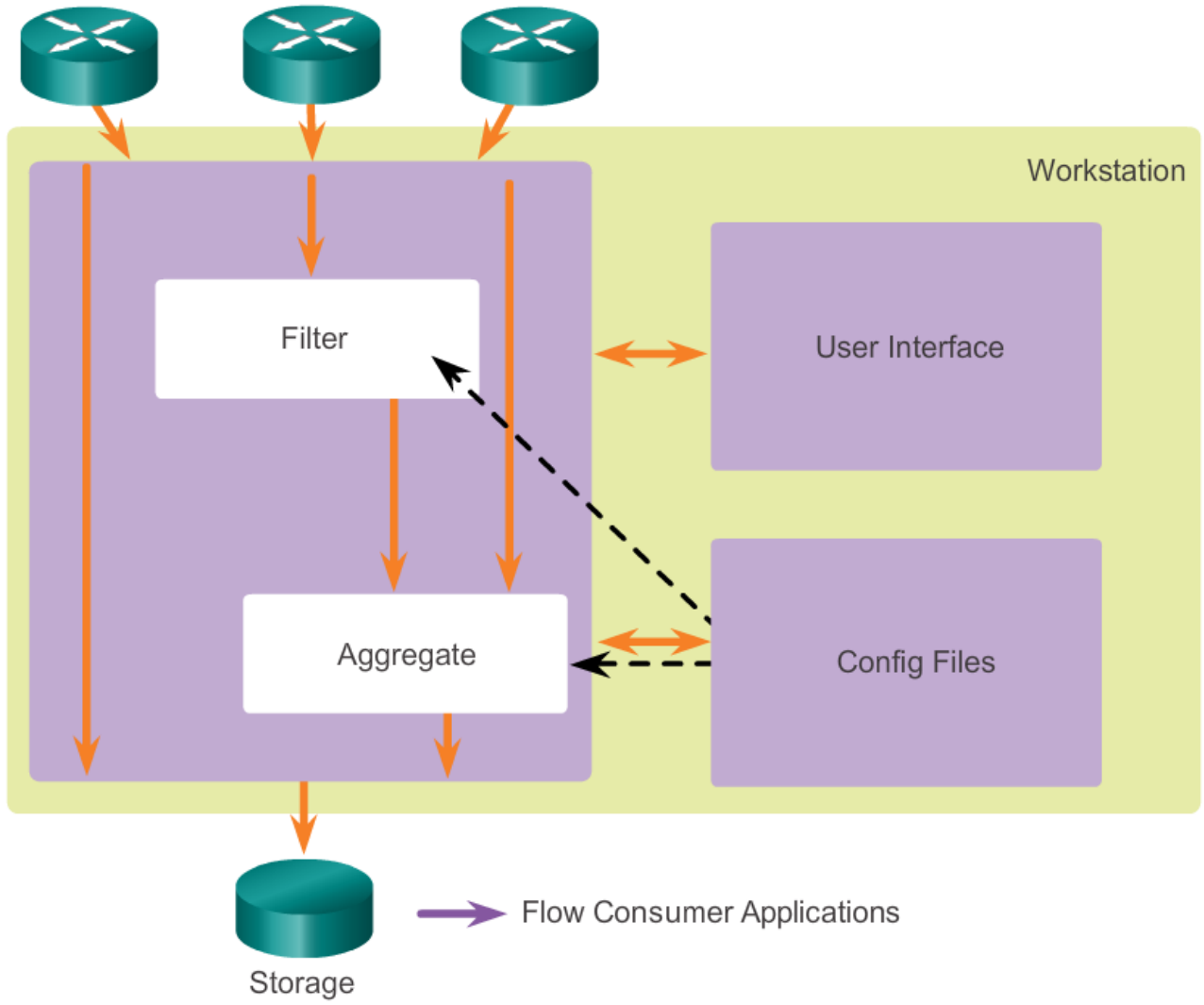
Verifying NetFlow

```
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

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 Functions



NetFlow Analysis with a NetFlow Collector

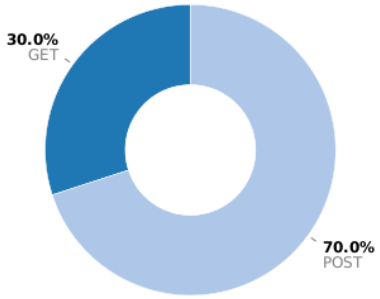
Chart

Timeseries

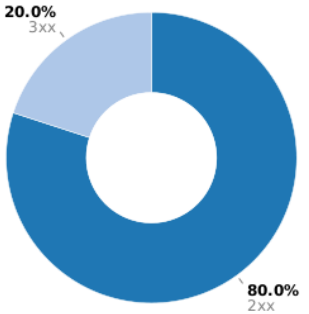
Traffic (Rc
Traffic (Se

800 Kbit/s
600 Kbit/s
400 Kbit/s
200 Kbit/s

HTTP Queries	Method	Requests	Distribution
	GET	3	
	POST	7	
	HEAD	0	
	PUT	0	
	Other Method	0	



HTTP Responses	Response code	Responses	Distribution
	1xx (Informational)	0	
	2xx (Success)	8	
	3xx (Redirection)	2	
	4xx (Client Error)	0	
	5xx (Server Error)	0	



104.27.136.1
104.27.136.111 SSL 3.12 KB

Info | SSL | TCP | cizmo.cizmo :52929 | api.github.com :https | 11 sec | Client | Server | 0 bps | 3.04 KB | api.github.com

Ďakujem za pozornosť!

Ohodnoť našu CNA na google:

- https://goo.gl/maps/BAnFvQKYCBpffcEX7

--