UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

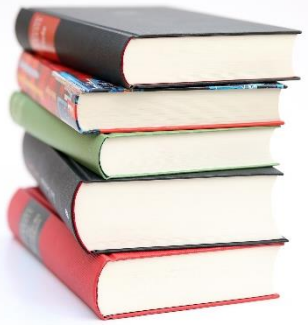
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Manažment, údržba a monitoring siete

Počítačové siete 2

Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU

Vytvorené v rámci projektu KEGA 026TUKE-4/2021



Čo nás dnes čaká

CCNA 3 (ENSA)

Kapitola 10: Network management
Objavovanie zariadení, správa, a údržba

- **10.1-2 Objavovanie zariadení**
  - Zmapovanie sieťovej topológie, CDP, LLDP
- **10.3-5 Správa zariadení**
  - NTP, SNMP, Syslog
- **10.6-7 Údržba zariadení**
  - Údržba konfiguračných a IOS súborov

Zabezpečenie LAN siete (krátke opakovanie z PS1)

- Útoky na LAN a zmierňovanie ich dopadov

Monitorovanie LAN siete (prídavok nad rámec Netacad curricula v 7.0)

- **Cisco Switch Port Analyzer (SPAN)**
  - Zrkadlenie prevádzky a jeho využitie

Samostatne si prečítať **kapitolu 12 Network Trobuleshooting** z portálu Netacad

Objavovanie zariadení

Netacad

- 10.1 CDP
- 10.2 LLDP

Objavovanie zariadení

CDP

- Prehľad CDP
  - Cisco Discovery Protocol
  - Objavovanie susedných fyzicky pripojených Cisco zariadení
- CDP konfigurácia a kontrola
  - **`show cdp neighbors`**
  - **`show cdp interface`**
  - **`cdp run`**
  - **`cdp enable`**
  - **`clear cdp counters, clear cdp table`**
- Objavovanie zariadení pomocou CDP
  - Identifikátory zariadení – názov susedného zariadenia
  - Identifikátor portu – názov lokálneho a vzdialeného portu
  - Zoznam funkcií – či zariadenie je smerovač alebo prepínač
  - Platforma – hardvérová platforma zariadenia

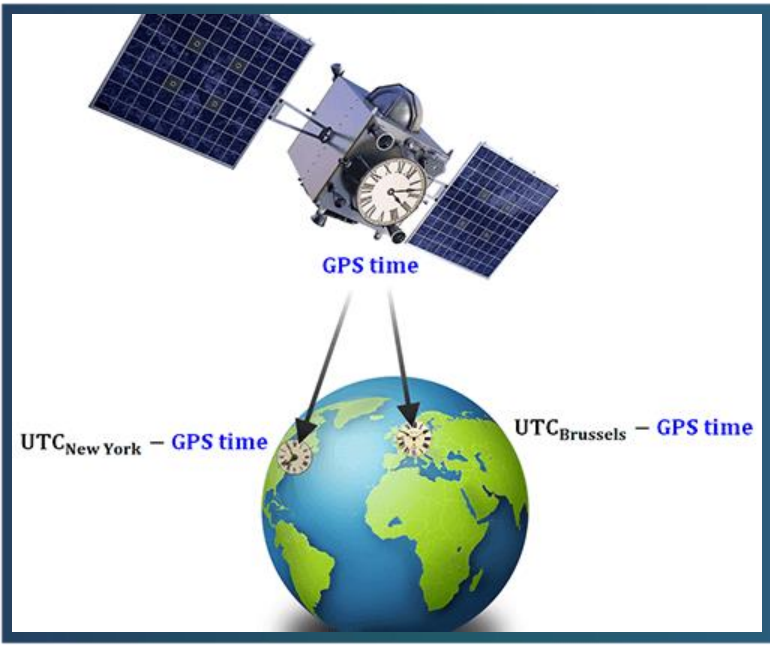
LLDP

- Prehľad LLD
  - Protokol na objavovanie susedov, nezávislý od výrobcu, podobný ako CDP
- LLDP konfigurácia a kontrola
  - **`show lldp`**
  - **`lldp run`**
  - **`lldp transmit`**
  - **`lldp receive`**
- Objavovanie zariadení pomocou LLDP
  - **`show lldp neighbors`**

Správa zariadení

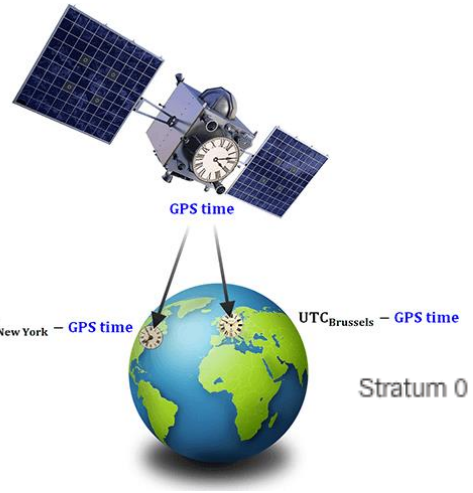
Netacad

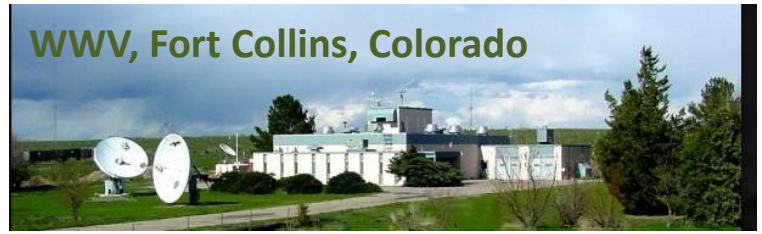
10.3 NTP
10.5 Syslog
10.4 SNMP



NTP

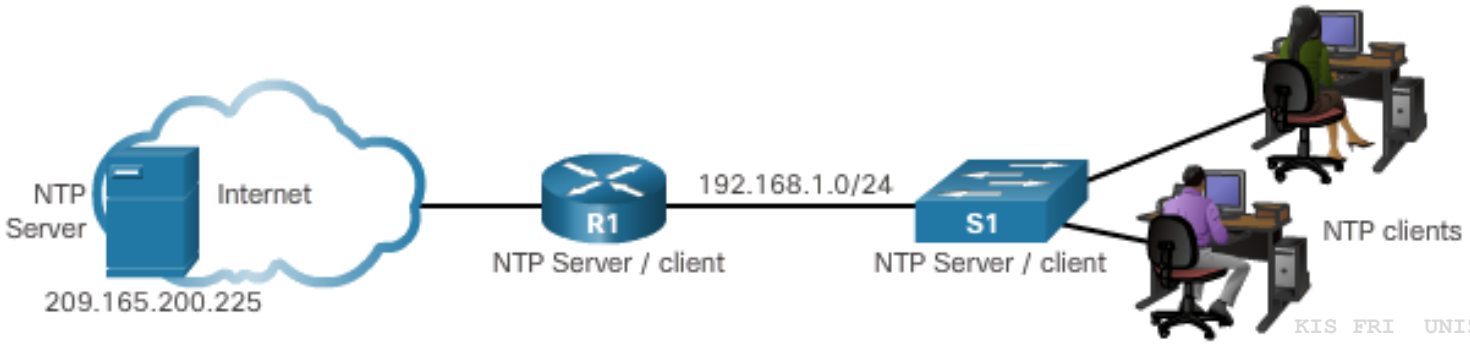
Implementácia NTP





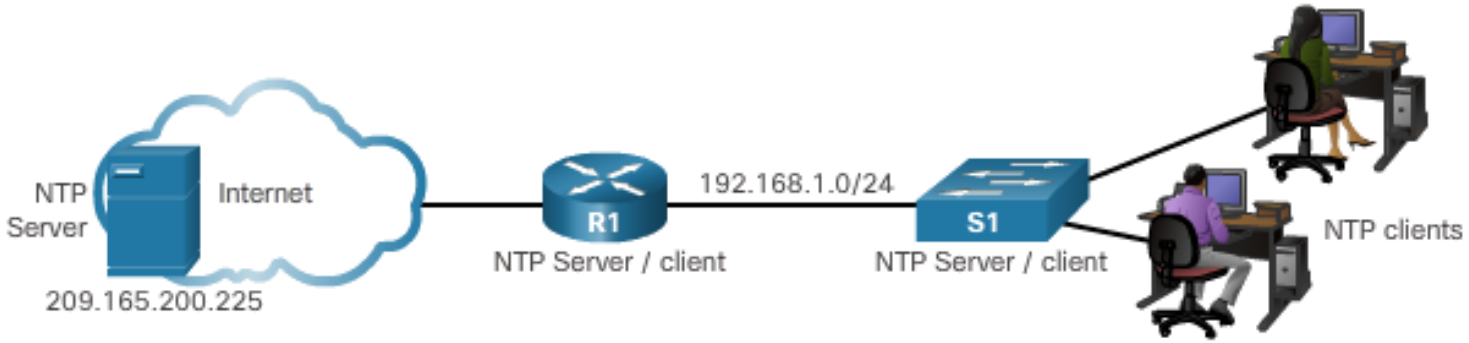
Reference clock (malé, alebo žiadne oneskorenie – **GPS**, CDMA, **WWV**, ...) – nie je network device

- 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. je 15, 16 = nesynchornizovaný
- Konfigurácia a overenie NTP
  - **`ntp server`** *`ip-address`*
  - **`show ntp associations`**
  - **`show ntp status`**
  - **`show clock [detail]`**



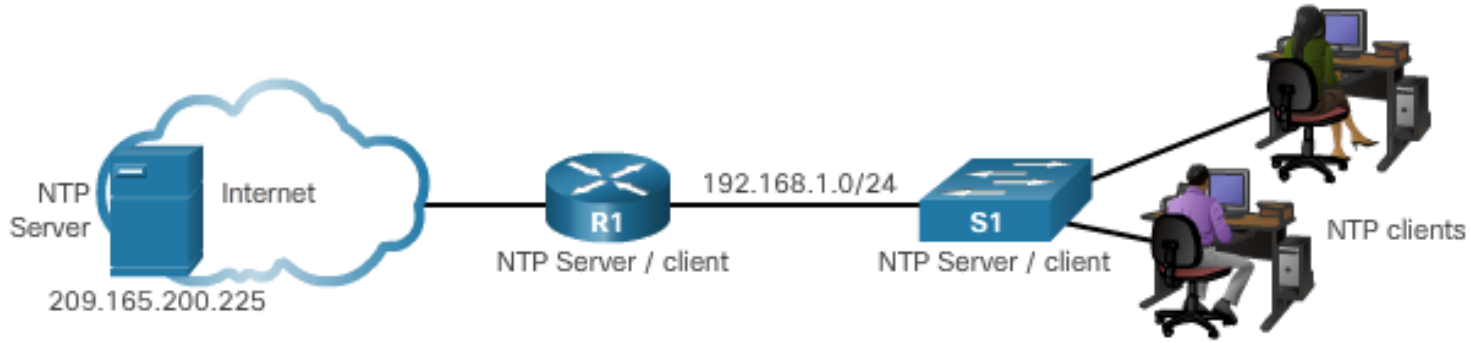
Implementácia NTP

```
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.
```

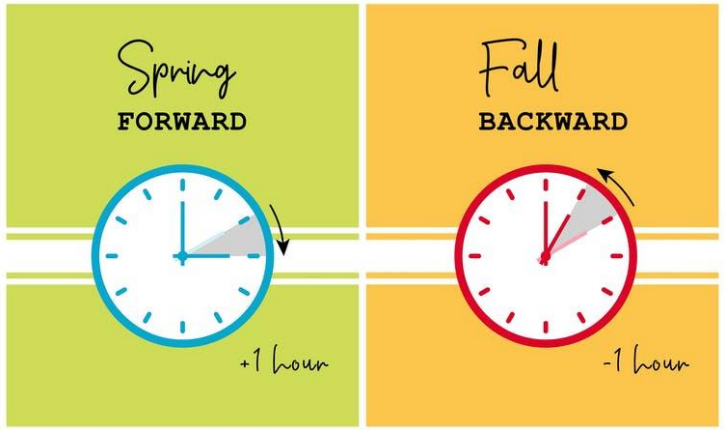
Implementácia NTP

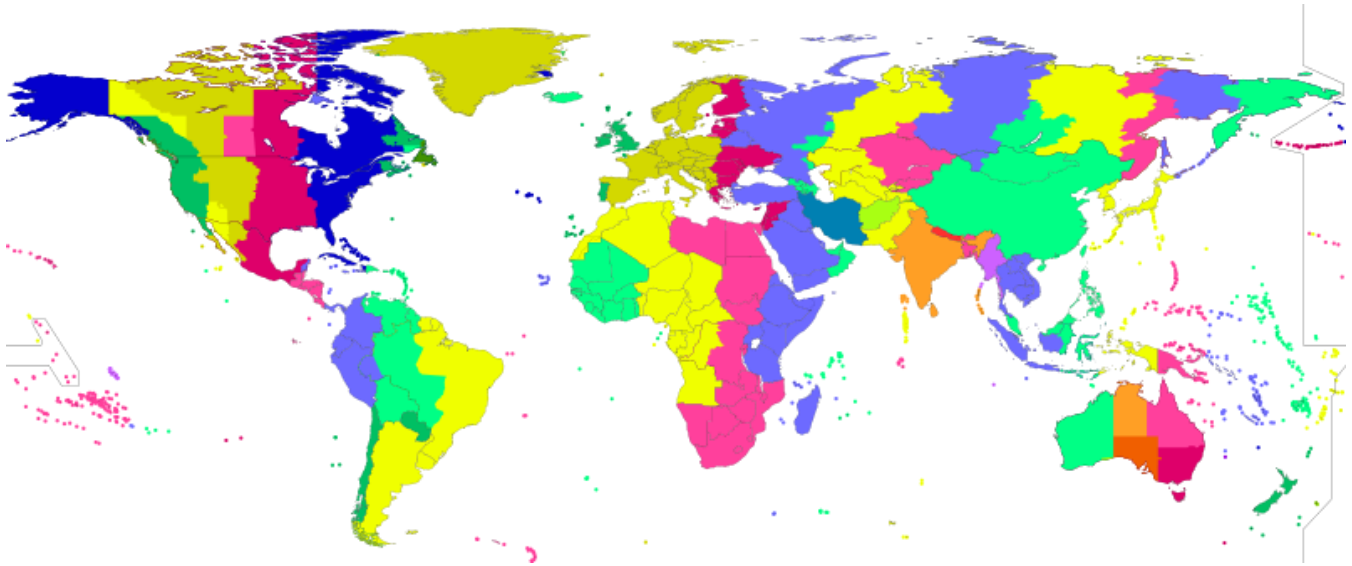



```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations

  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.
```

Ako NTP zvláda prechod na letný čas (DST)?

- Pri NTP nie je potrebné:
  - prepínanie na letný čas
  - nerozlišuje ani časové pásma
- Dôvod:
  - NTP je založený na UTC
  - UTC nemá prechod na letný čas
  - za prechod z/do DST sú výhradne zodpovedné OS serverov a klientov
  - aj za manipuláciu s časovými pásmami

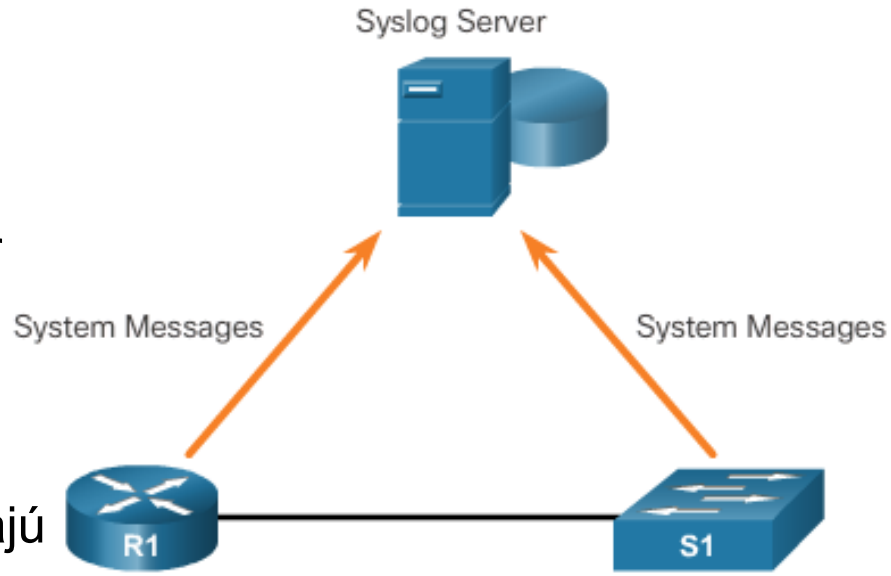


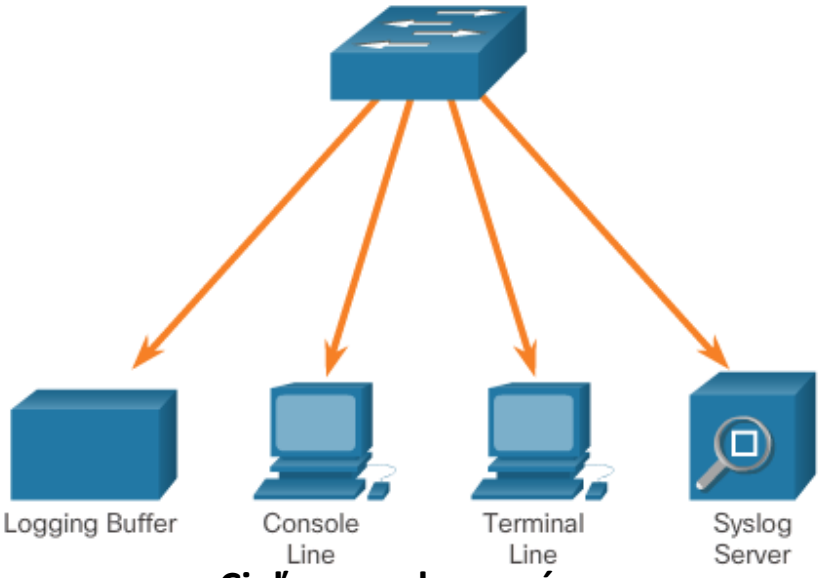


Syslog

Syslog

- Popip protokolu Syslog (UDP/514, RFC 3164)
  - Umožňuje zariadeniam posielať správy na syslog server
  - Podporovaný väčšinou sieťových zariadení
  - Hlavné funkcie:
    - **Zber informácií** pre monitorovanie a riešenie problémov
    - Výber **typu** zapisovaných informácií ktoré sa zaznamenajú
    - Určenie **cieľa** zaznamenaných syslog správ
- Formát Syslog správy
  - Stupeň závažnosti od 0 po 7
  - Facility – identifikácia služby
- Časová pečiatka služby
  - Vylepšuje ladenie a správu v reálnom čase
  - Protokoly môžu byť označené časovou pečiatkou a je možné nastaviť zdrojovú adresu správ syslog.
  - `service timestamps log datetime msec`





Cieľ pre syslog správy

Konfigurácia Syslog-u

- Syslog Server
  - Analyzuje výstup a umiestňuje správy do vopred určených stĺpcov
  - Časové pečiatky sa zobrazujú, ak sú nakonfigurované na sieťových zariadeniach, ktoré generovali správy výpisu
  - Umožňuje správcom siete navigovať sa vo veľkom množstve zhromaždených údajov
- Predvolené zapisovanie
  - Posielať správy protokolu všetkých stupňov závažnosti do konzoly
  - **`show logging`**
  - **`logging monitor`** *`LEVEL`* `! Do CLI mi zobrazí správy danej úrovne a vyššej`
    - Keď sme vzdialene pripojený na zariadení, tak je to potrebné, keď chceme aj debug správu, vtedy: 7
- Príkazy na smerovač/prepínači pre nastavenie ako Syslog klientov
  - **`logging`** *`ip-address`*
  - **`logging`** `trap` *`level`*
  - **`logging source-interface`** *`source-interface interface-number`*
- Syslog kontrola
  - **`show logging`**
  - Použite “|” na obmedzenie množstva zobrazených správ

Formát správy syslog

- Niektoré bežné oblasti syslog správ hlásených na Cisco IOS smerovačoch zahŕňajú:
  - IP
  - OSPF protokol
  - SYS operačný systém
  - IPsec
  - IP rozhranie (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

- 2 hlavné formáty syslog správ:
  - BSD format (RFC3164)
  - “nový” formát (RFC5424)

Konfigurácia Syslog

Predvolené zaznamenávanie

```
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
```

Konfigurácia Syslog

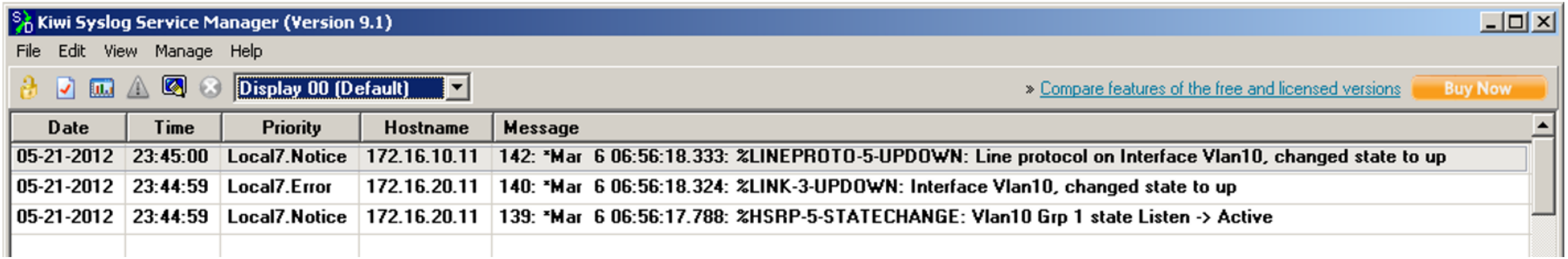
Príkazy smerovačov a prepínačov pre Syslog klientov

```
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)#
```

Severity Name	Severity Level
Emergency	Level 0
Alert	Level 1
Critical	Level 2
Error	Level 3
Warning	Level 4
Notification	Level 5
Informational	Level 6
Debugging	Level 7

Príklady syslog správ

```
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
```



Konfigurácia Syslog

Kontrola 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#
```

Rôzne projekty: syslog, rsyslog, syslog-ng

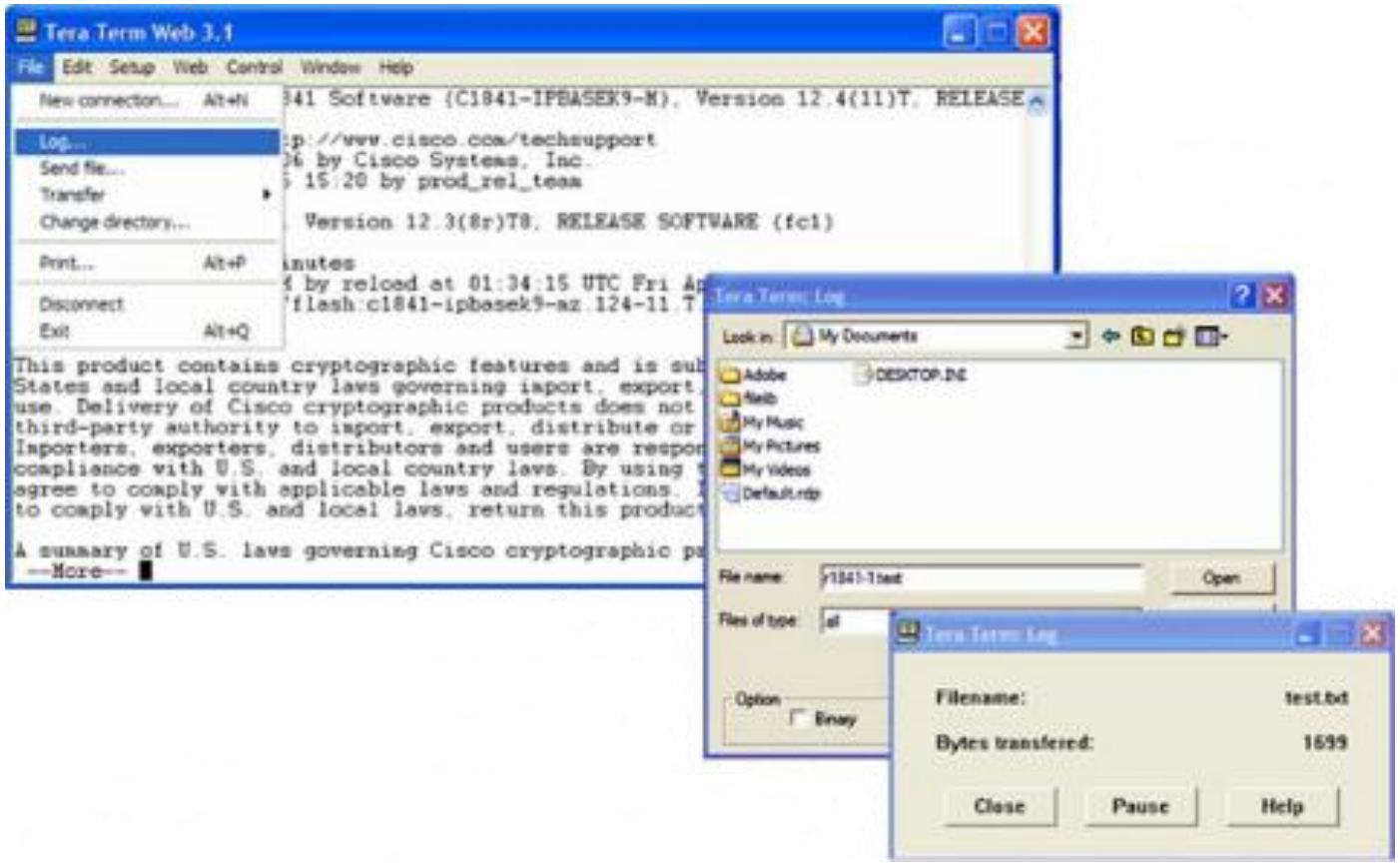
- všetky umožňujú získavanie údajov z rôznych typov systémov do centrálneho úložiska
- Syslog
  - Prvý (root) projekt, 1980, jednoduchý protokol, podporuje iba UDP = nezaručuje doručenie správ
- Syslogng (dnes asi najvyspelejší projekt)
  - 1998, rozšíril syslog o nové funkcie:
    - filtrovanie na základe obsahu
    - logovanie priamo do databázy
    - TCP pre transport
    - TLS šifrovanie
- Rsyslog
  - 2004, rozšíril syslog o nové funkcie:
    - Podpora protokolu RELP (application-level ACK)
    - Podpora prevádzky vo vyrovnávacej pamäti

Údržba zariadení

Netacad: 10.6, 10.7 IOS a config súbory

Správa súborov na smerovačoch a prepínačoch

- Súborové systémy merovačov a prepínačov
  - **`show file systems`** – zobrazí všetky dostupné súborové systémy
  - **`dir`** – zobrazí obsah súborového systému
  - **`pwd`** – overí aktuálny pracovný priečinok
  - **`cd`** – zmení aktuálny priečinok
- Záloha a obnova pomocou textových súborov

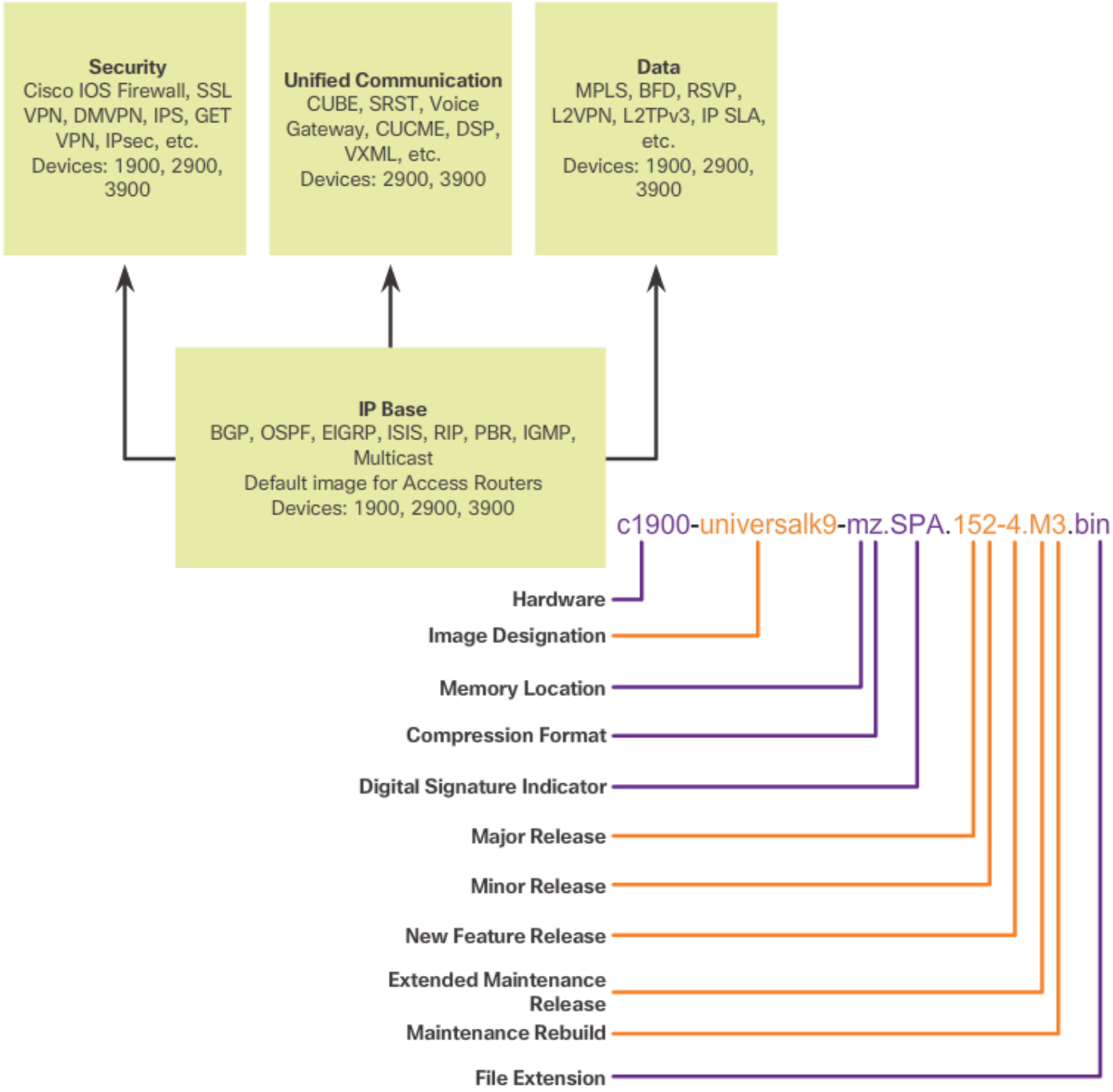


Správa súborov na smerovačoch a prepínačoch (pokrač.)

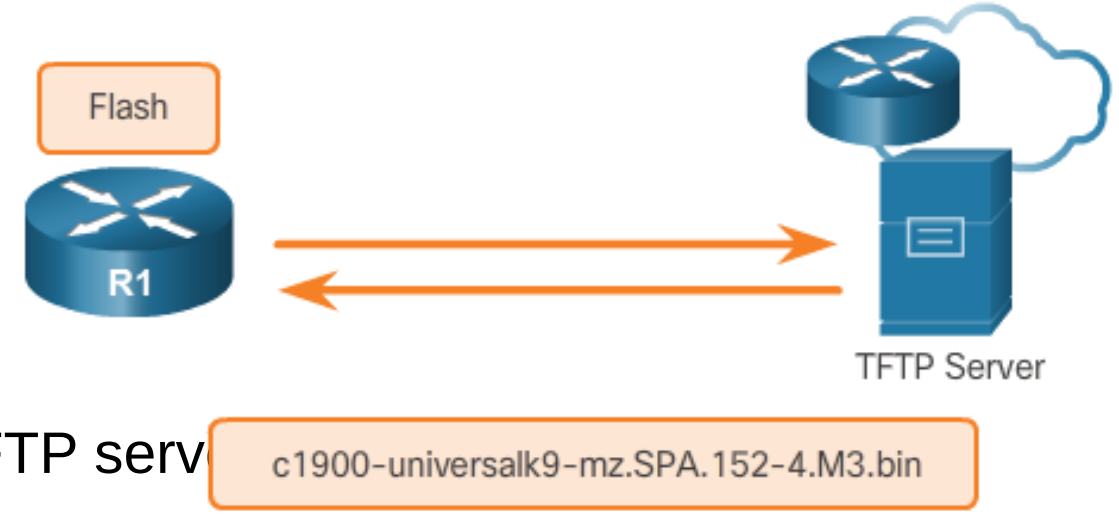
- Záloha a obnova pomocou TFTP
  - `copy running-config tftp`
  - `copy startup-config tftp`
- Použitie USB portov na zálohu a obnovu
  - `show file systems`
  - `dir usbflash0:`
  - `copy run usbflash0:/`
- Obnova hesla
  - Vstúpte do ROMMON režimu
  - Zmeňte konfiguračný register na 0x2142
  - Reštartujte zariadenie
  - Urobte zmeny do pôvodnej konfigurácie po štarte
  - Uložte novú konfiguráciu

IOS systémové súbory

- Balíčky systémových obrazov pre IOS ver. 15
  - universalk9
  - universalk9_npe
  - technologické balíčky:
    - IP Base
    - Data, UC, SEC
      - aktivované pomocou licencie
- Čo je v názvoch IOS obrazov
  - Sady funkcií a verzia
  - **`show flash`**



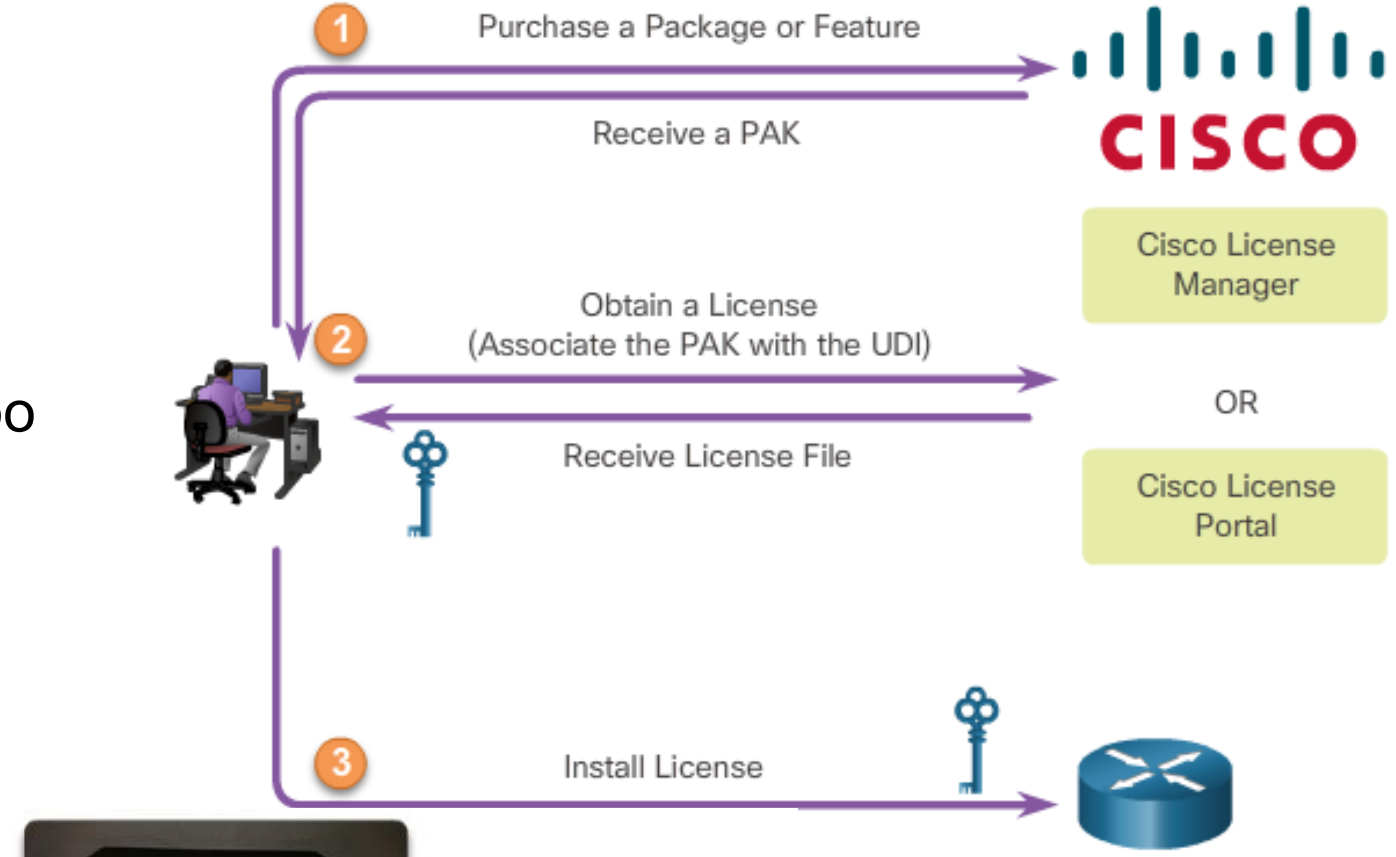
IOS správa obrazov

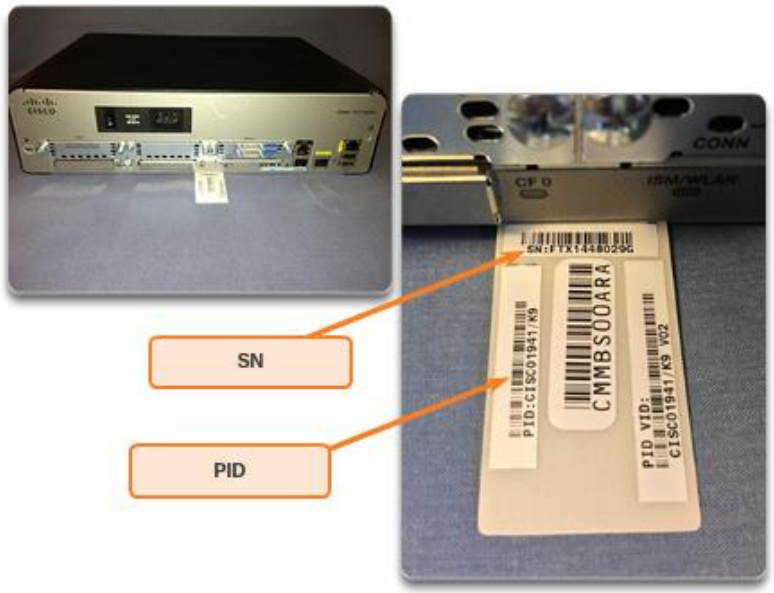


- TFTP servery pre umiestnenie záloh
  - pre IOS obrazy a konfiguračné súbory
- Kroky potrebné pre zálohu IOS obrazu na TFTP serv
  - Skontrolujte prístup na TFTP server
  - Skontrolujte dostatočné množstvo voľného miesta na disku
  - Skopírujte obraz na TFTP server
    - **`copy`** *`source-url`* **`tftp:`**
- Kroky na kopírovanie IOS obrazu na zariadenie
  - Stiahnite IOS obraz z Cisco.com a preneste ho na TFTP server
  - Overte prístup na TFTP server zo zariadenia
  - Skontrolujte dostatočné množstvo voľného miesta na zariadení
  - Skopírujte obraz z TFTP servera
    - **`copy tftp:`** *`destination-url`*
- Použite príkaz **`boot system`**
  - Príkaz na načítanie nového obrazu počas bootovania
  - **`boot system`** *`file-url`*

Licencovanie softvéru

- Proces licencovania
  - Zakúpte si balíček softvéru alebo funkcie na inštaláciu
  - Získajte licenciu
    - Cisco License Manager
    - Cisco License Portal
    - Vyžaduje PAK číslo a UDI
      - **`show license udi`**
  - Nainštalujte licenciu
    - **`license install`** *`stored-location-url`*
    - **`reload`**





Overenie a správa licencie

- Kontrola licencie
  - **show version**
  - **show license**
- Aktivácia hodnotiacej right-to-use licencie
  - **license accept end user agreement**
  - **license boot module** *module-name* **technology-package** *package-name*
- Záloha licencie
  - **license save** *file-sys://lic-location*
- Odinštalovanie licencie
  - Zakázanie licencie
    - **license boot module** *module-name* **technology-package** *package-name* **disable**
  - Odstránenie licencie
    - **license clear** *feature-name*
    - **no license boot module** *module-name* **technology-package** *package-name* **disable**

Bezpečnosť LAN (krátke opakovanie)

LAN Bezpečnostné útoky

- Medzi bežné útoky na infraštruktúru LAN vrstvy 2 patria:
  - CDP Prieskumné útoky
  - Telnet útoky
  - Útoky pomocou zahltenia MAC Address tabuľky
  - VLAN útoky
  - DHCP útoky

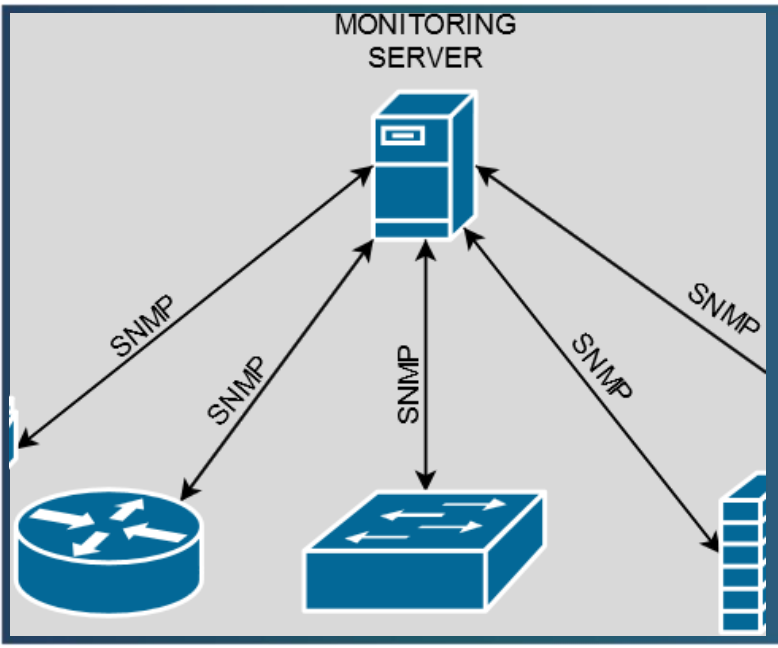
Čím zmierniť tieto hrozby?

Odporúčané postupy zabezpečenia LAN

- Táto téma sa zaoberá niekoľkými bezpečnostnými riešeniami vrstvy 2:
  - Zaránenie útokom zaplavením tabuľky MAC adries pomocou zabezpečenia portov
  - Zabránenie útokom na VLAN zakázaním DTP a dodržiavaním základných pokynov pre konfiguráciu hlavných portov.
  - Zabránenie útokom na DHCP pomocou DHCP snooping-u
  - Zabezpečenie administratívneho prístupu pomocou AAA
  - Zabezpečenie prístupu k zariadeniu pomocou overenia portu 802.1X

Odporúčané postupy zabezpečenia LAN

- Existuje niekoľko stratégií, ktoré pomáhajú zabezpečiť vrstvu 2 v sieti :
  - Vždy používajte bezpečné varianty týchto protokolov, ako sú SSH, SCP, SSL, SNMPv3 a SFTP.
  - Vždy používajte silné heslá a často ich meňte.
  - Povoľte CDP iba na vybraných portoch.
  - Zakážte prístup cez Telnet.
  - Použite vyhradenú VLAN pre manažment, kde sa nenachádza nič iné ako manažmentová prevádzka.
  - Na filtrovanie nežiaduceho prístupu používajte ACL.

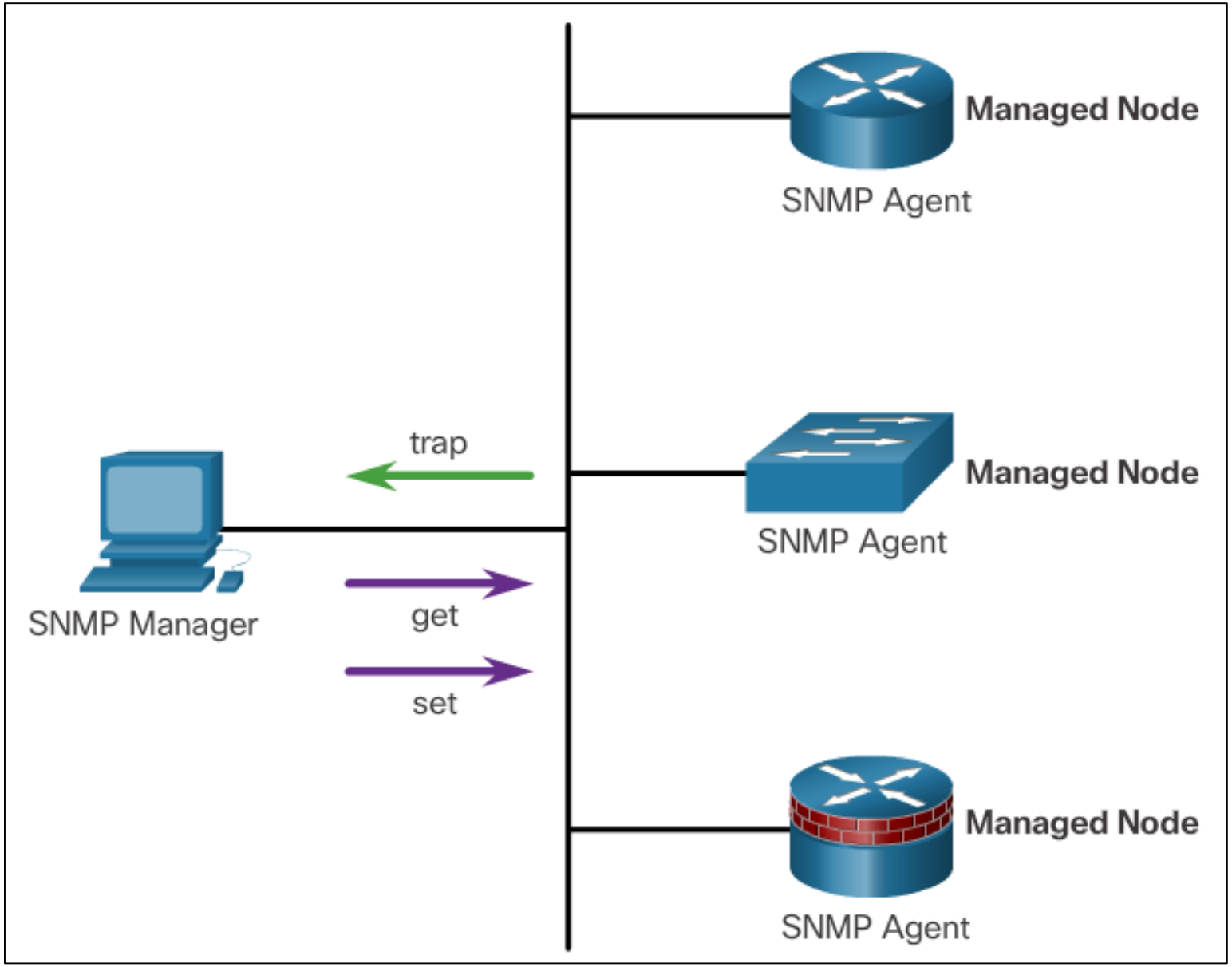


SNMP

Netacad: 10.4 SNMP

Fungovanie SNMP

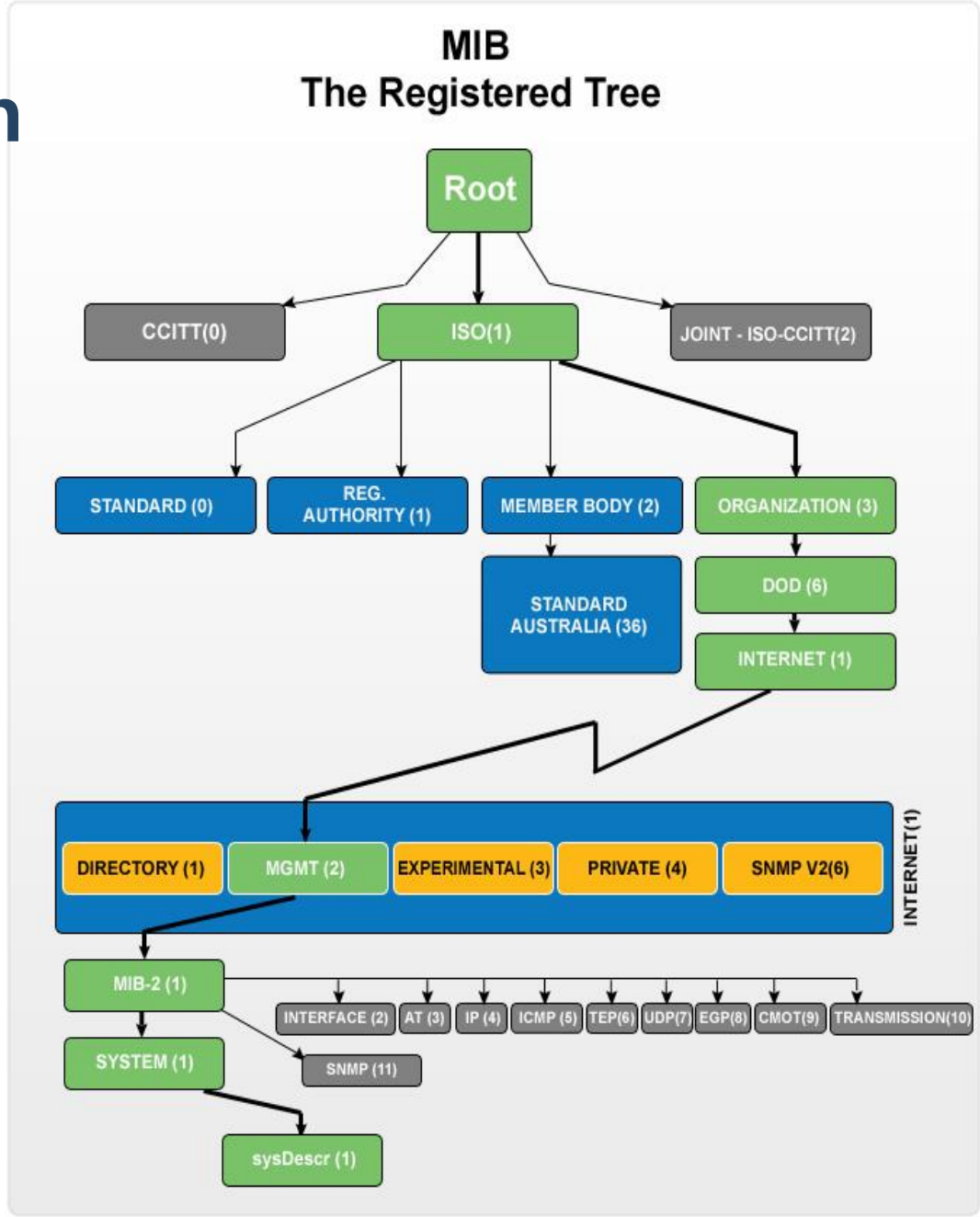
- Protokol SNMP umožňuje správcom spravovať a monitorovať zariadenia v sieti.
- SNMP prvky
  - SNMP Manager
  - SNMP Agent
  - MIB
- SNMP Operácie
  - Trap
  - Get
  - Set



MIB – Management Information Base

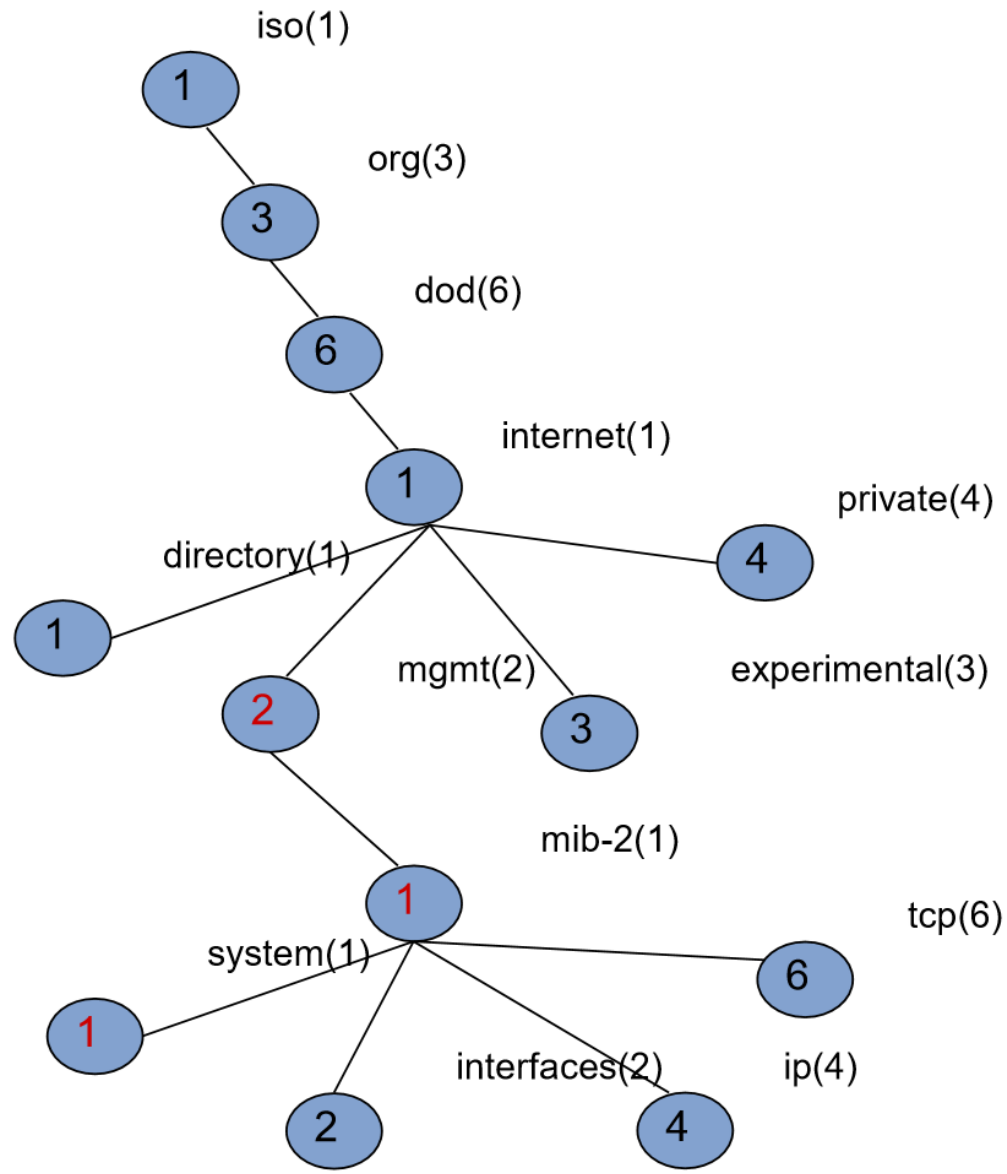
- Objekty na agentovi majú svoje identifikátory OID (Object IDentifier)
  - OID sú usporiadané v stromovej štruktúre
  - Vrcholy majú číselný i slovný názov
  - Konkrétny objekt je adresovaný cestou od koreňa stromu
- Príklad: .1.3.6.1.2.1.1

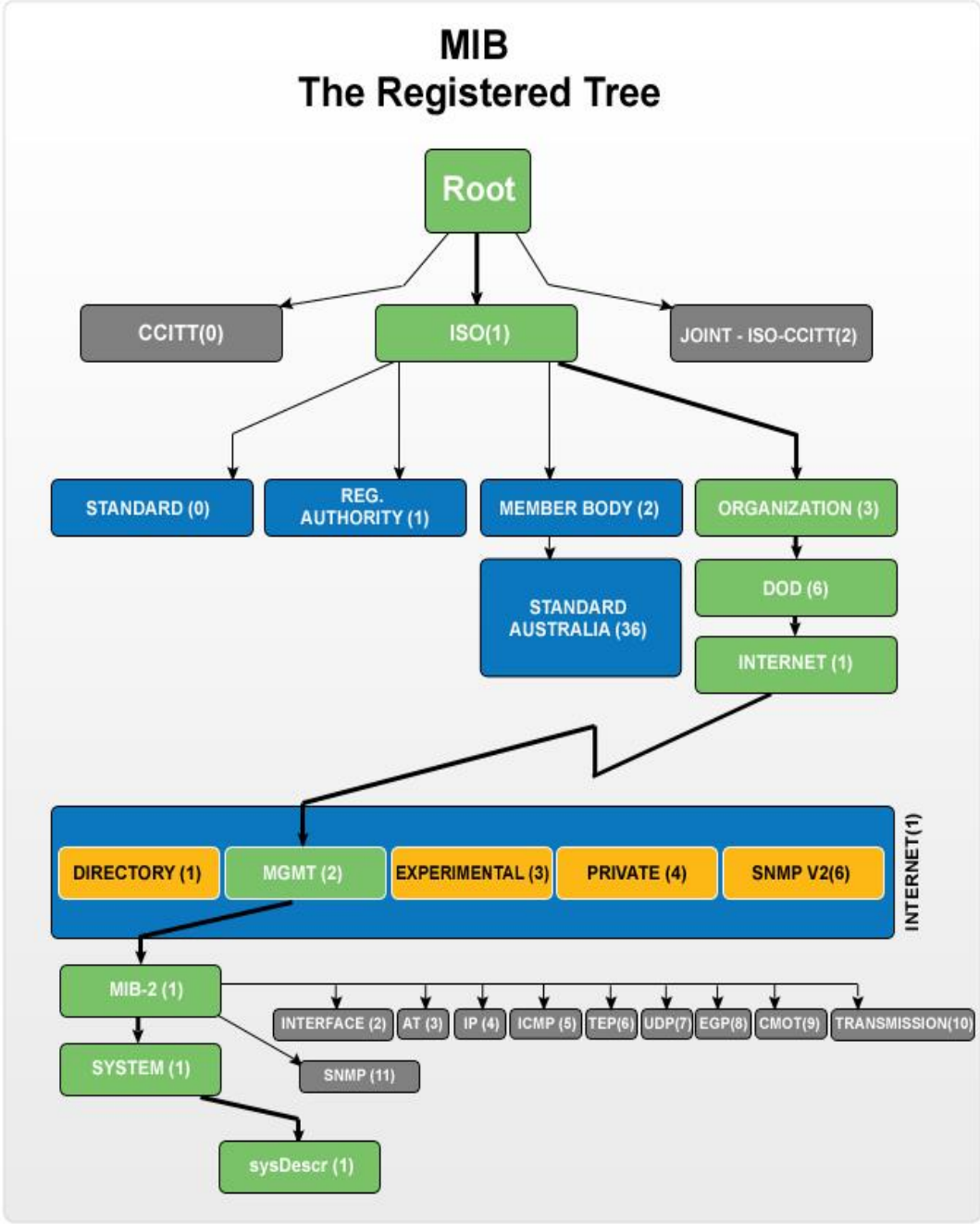
  iso(1) org(3) dod(6) internet(1)
  mgmt(2)
  mib-2 (1)
  system (1)



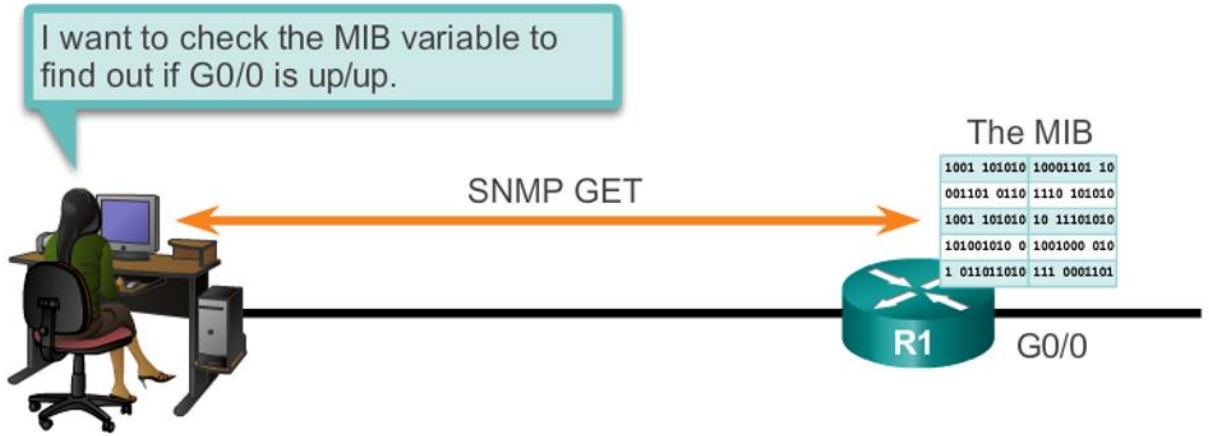
Hierarchická stromová štruktúra

MIB



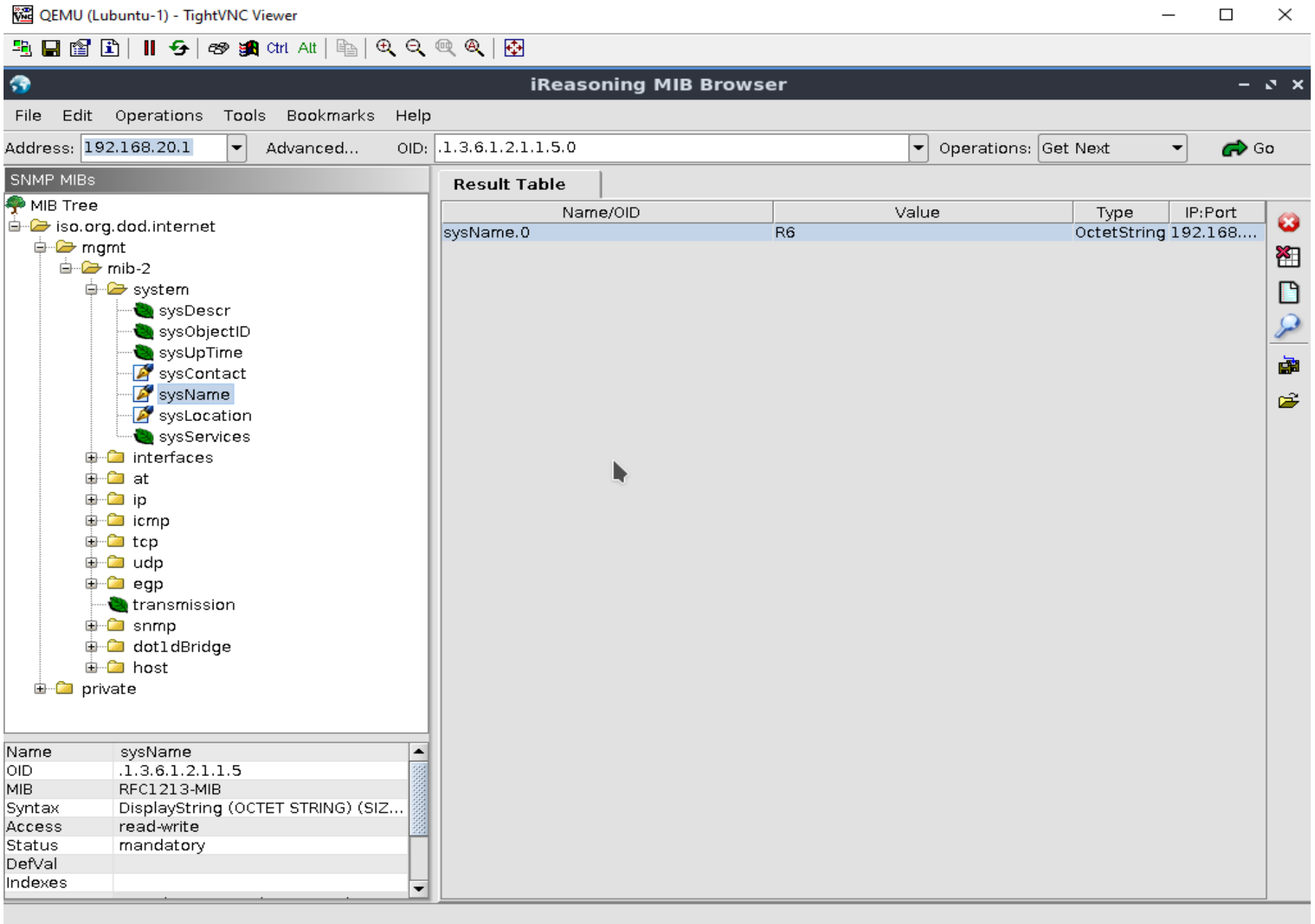


Fungovanie SNMP



Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table; the SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
get-bulk-request	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (Only works with SNMPv2 or later.)
get-response	Replies to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Stores a value in a specific variable.

iReasoning MIB Browser

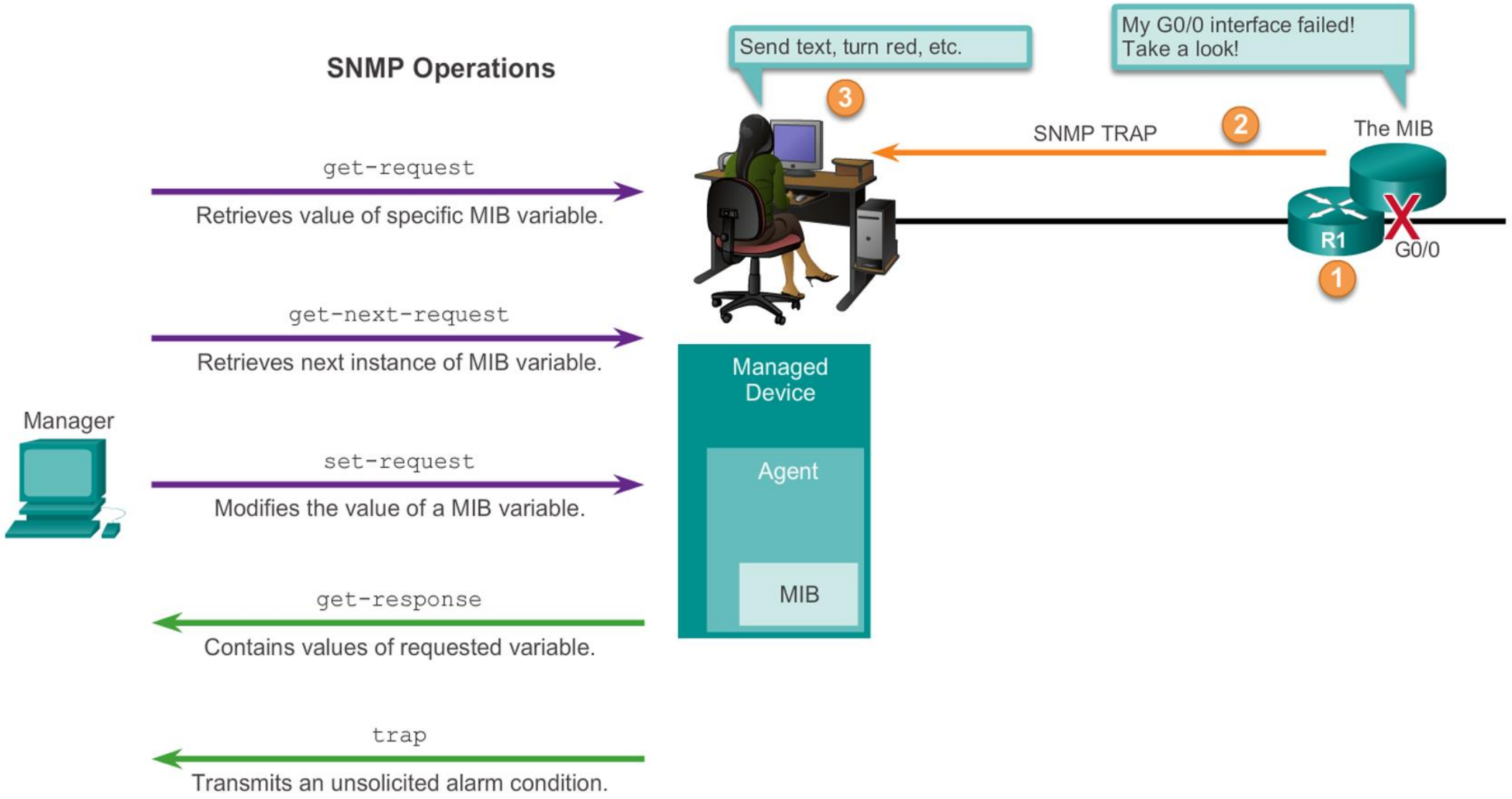


Konzolové výpisy

snmpget –v2c –c *COM_STRING* 192.168.255.14 .1.3.6.1.2.1.1.1.0

```
┌──(kali㉿kali)-[~]
└─$ snmpget -v2c -c  com_string  192.168.255.14 1.3.6.1.2.1.1.1.0
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 15.0(1)SE2, RELEAS
E SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 22-Dec-11 00:16 by prod_rel_team"
```

SNMP Agent Traps



Fungovanie SNMP

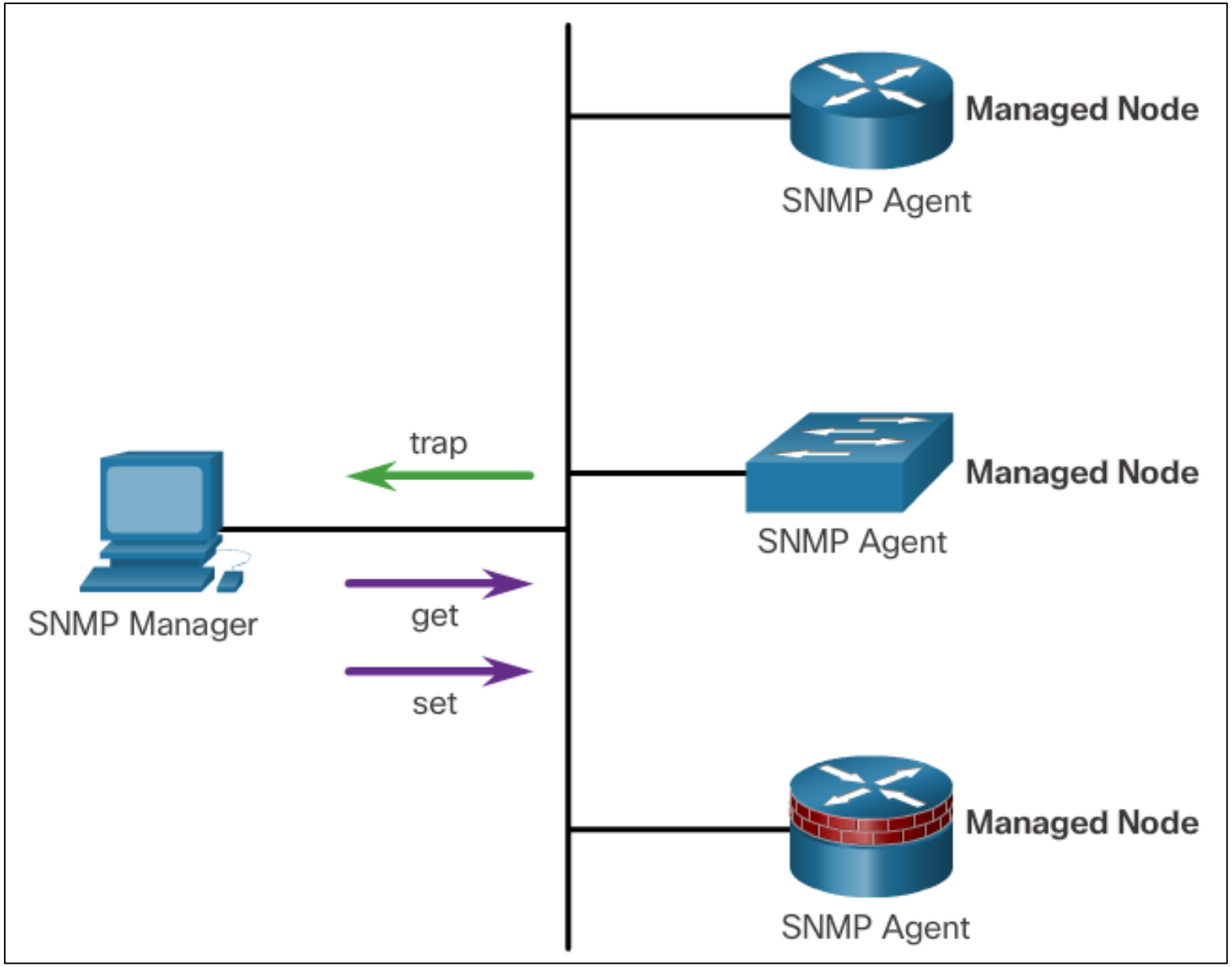
- SNMP Bezpečnostný model a úrovne
  - **SNMPv1** - RFC 1157.
  - **SNMPv2c** - RFC od 1901 do 1908; používa community-string-based administratívny framework
  - **SNMPv3** - RFC od 2273 do 2275; Zahŕňa **integritu správy**, aby sa zabezpečilo, že počas prepravy nedošlo k manipulácii s paketom; **autentifikáciu** na určenie, že správa je z platného zdroja, a **šifrovanie**, ktoré zabráni čítaniu obsahu správy neoprávneným zdrojom.

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

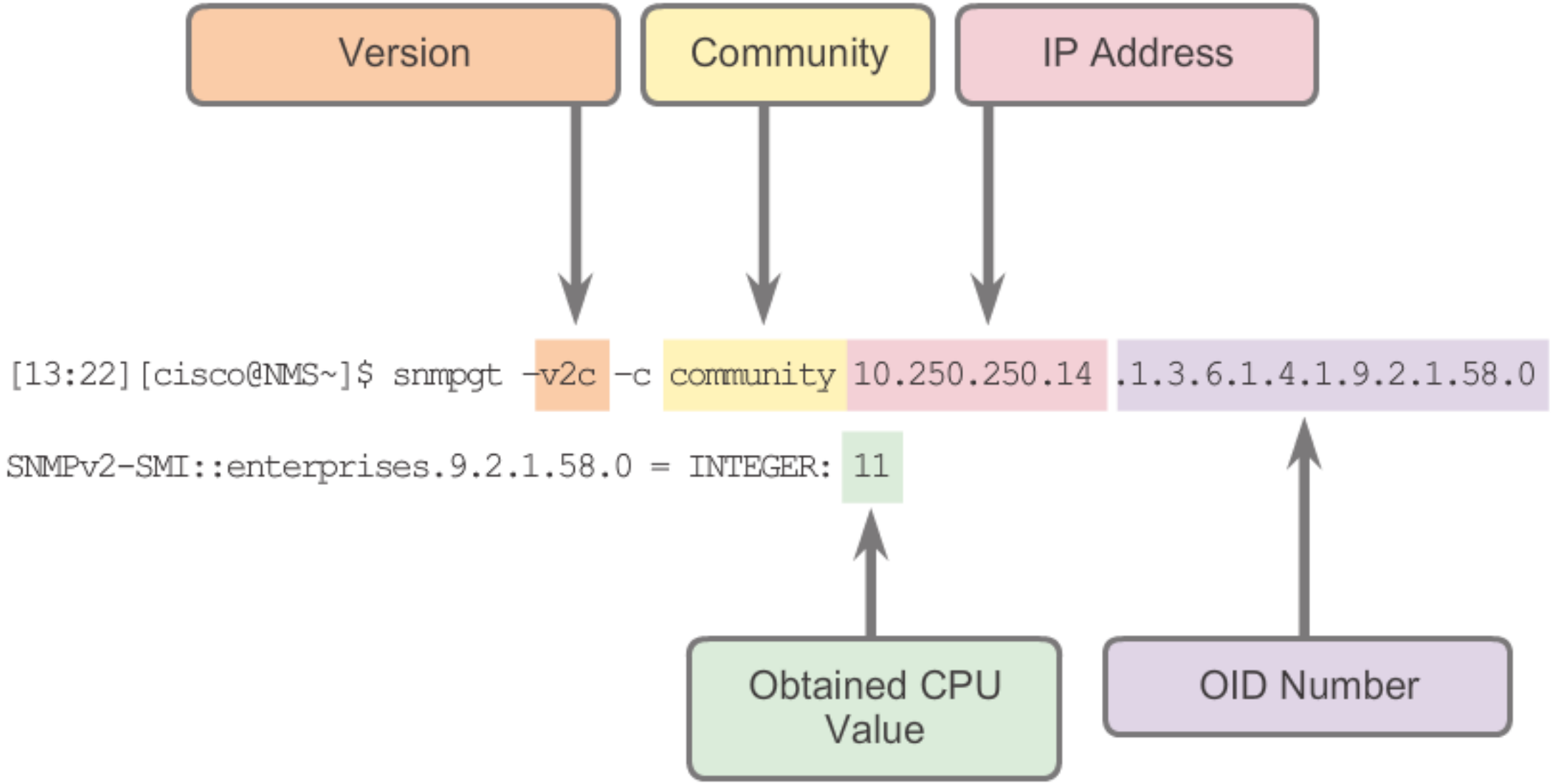
Komunitné reťazce

Existujú dva typy komunitných reťazcov:

- **Read-only (ro)** – Poskytuje prístup k premenným MIB, ale neumožňuje tieto premenné meniť, iba čítať. Pretože vo verzii 2c je zabezpečenie také slabé, mnoho organizácií používa protokol SNMPv2c v režime iba na čítanie.
- **Read-write (rw)** – Poskytuje prístup na čítanie a zápis na všetky objekty v MIB.



Management Information Base Object ID



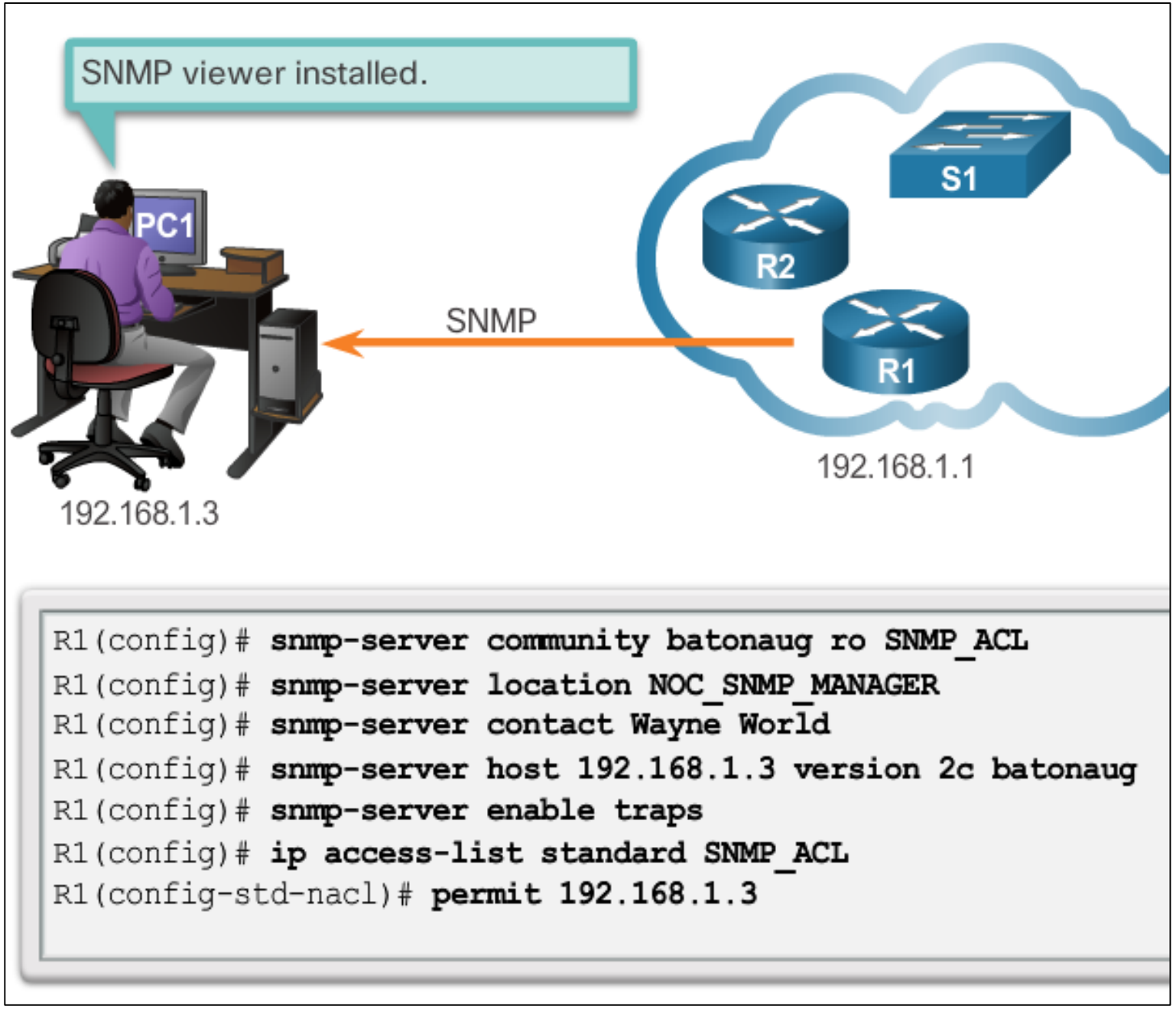
Konfigurácia SNMP

- 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 ?
```

Konfigurácia SNMP

- Kroky konfigurácie
  - (Povinné) Konfigurácia komunitného reťazca a úrovne prístupu (iba na čítanie alebo na čítanie aj zápis)
  - Document location of device
  - Document system contact
  - Obmedzte prístup SNMP na hostiteľov NMS (správcov SNMP), ktorí sú povolení zoznamom ACL.
  - Zadajte príjemcu SNMP traps
  - Povoľte traps na agentovi SNMP




```
R1(config)# snmp-server community batonaug ro SNMP_ACL
R1(config)# snmp-server location NOC_SNMP_MANAGER
R1(config)# snmp-server contact Wayne World
R1(config)# snmp-server host 192.168.1.3 version 2c batonaug
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.1.3
```

Konfigurácia SNMP

- Zabezpečenie 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
```

Konfigurácia SNMP

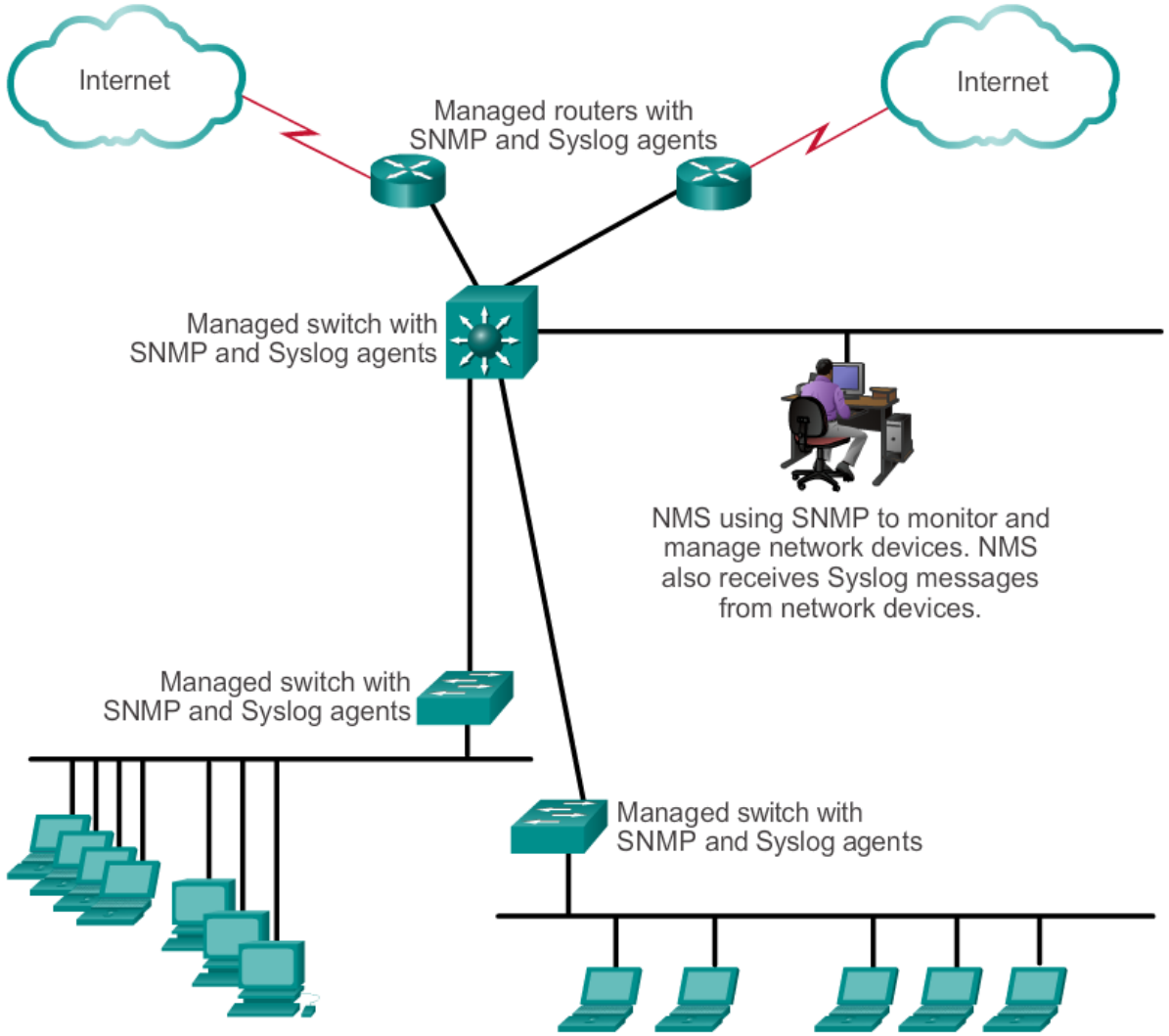
Kontrola SNMP Konfigurácie

```
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
```

Osvedčené bezpečnostné postupy

- Využívať SNMP, ideálne v3



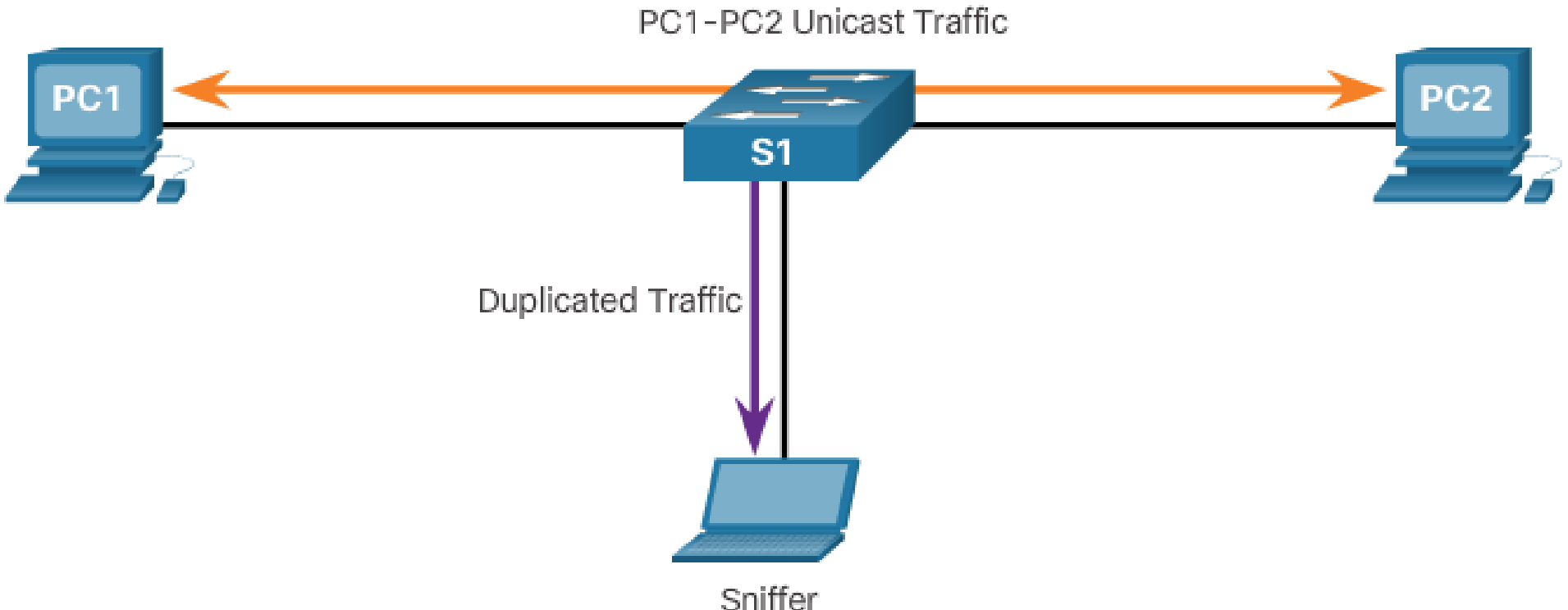
Cisco Switch Port Analyzer (SPAN)

Veľmi používaná technika pre monitorovanie v LAN

(aktuálne nie je zahrnutá v Netacad curricule, máte ju len tu v pptx, je ale potrebné ovládať ju)

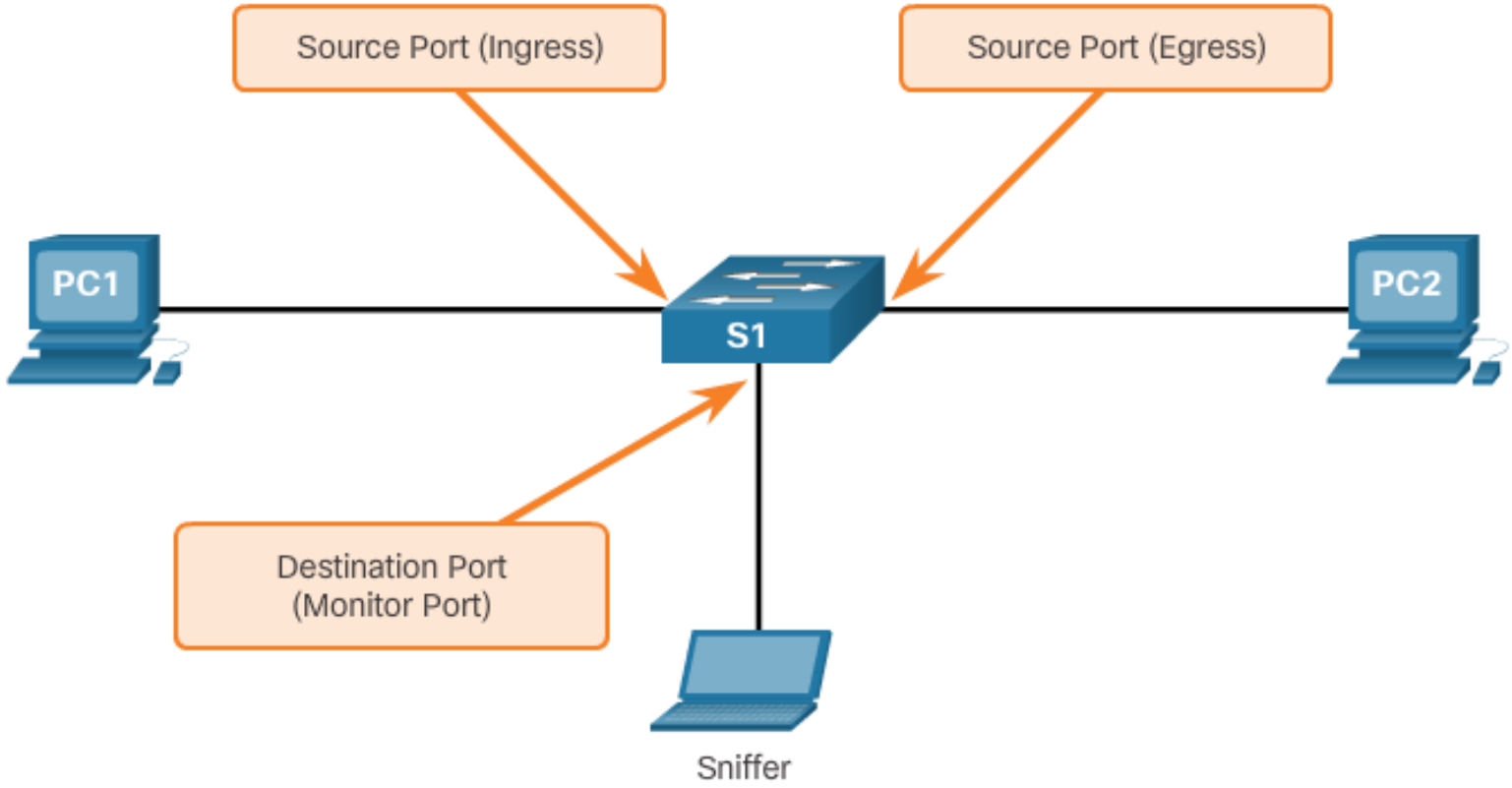
Popis využitia SPAN

- Port mirroring (zrkadlenie)
  - Umožňuje prepínačom kopírovať a odosielať eternetové rámce zo špecifického portov do cieľového portu pripojeného k analyzátoru paketov. Pôvodný rámec pokračuje ďalej obvyklým spôsobom.
  - Bežne sa implementuje na podporu prevádzkových analyzátorov alebo IDS zariadení



SPAN

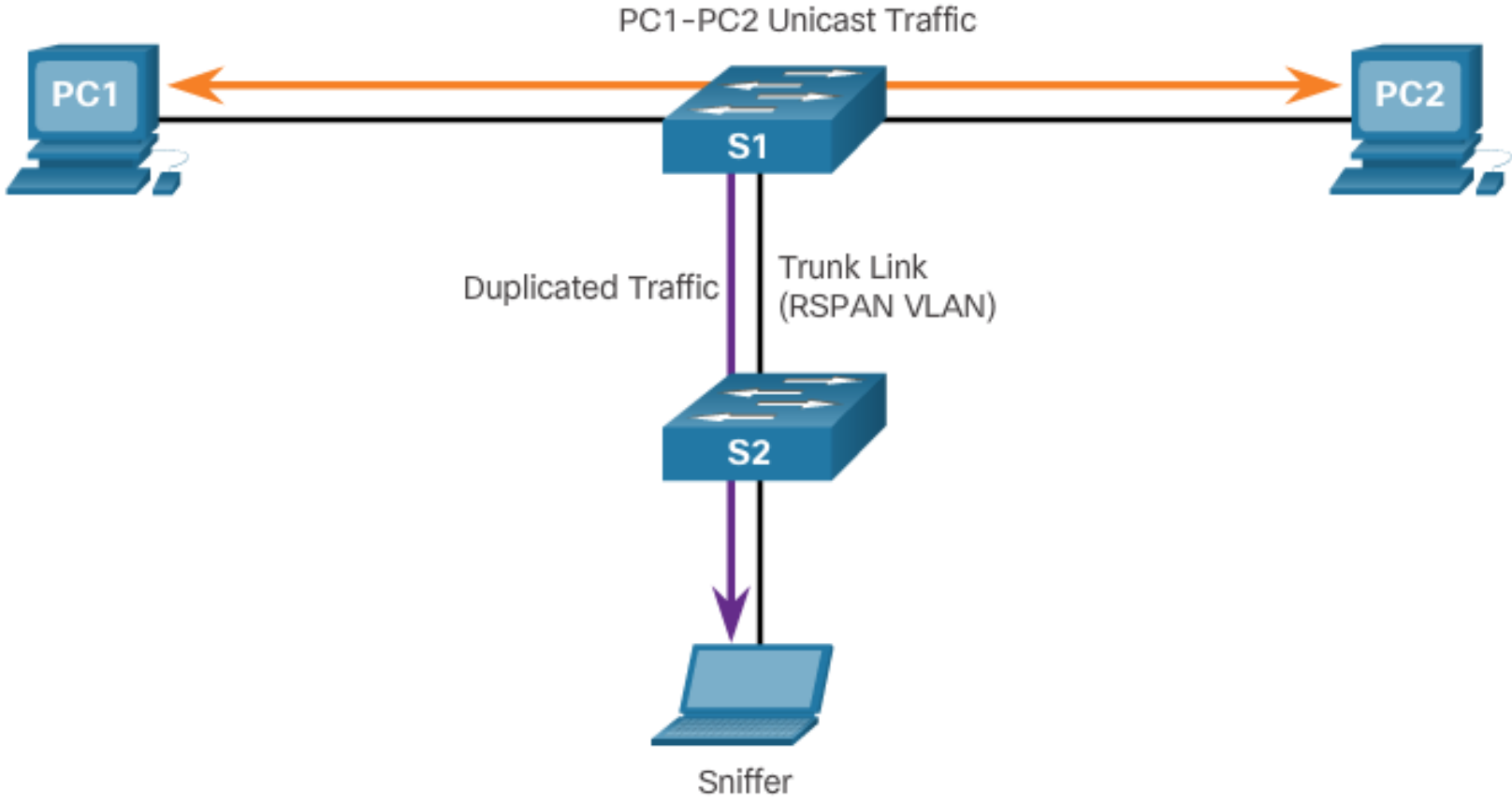
- SPAN terminológia



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.

SPAN

- RSPAN terminológia



Term	Definition
RSPAN source session	This is the source port/VLAN to copy traffic from.
RSPAN destination session	This is the destination VLAN/port to send the traffic to.
RSPAN VLAN	• A unique VLAN is required to transport the traffic from one switch to another. • The VLAN is configured with the `remote-span` vlan configuration command. • This VLAN must be defined on all switches in the path and must also be allowed on trunk ports between the source and destination.

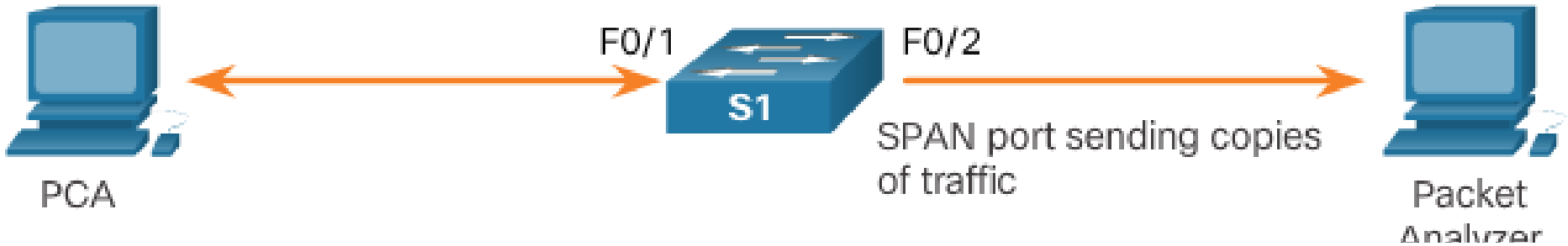
SPAN Konfigurácia

Associate a SPAN session with a source port

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

Associate a SPAN session with a destination port

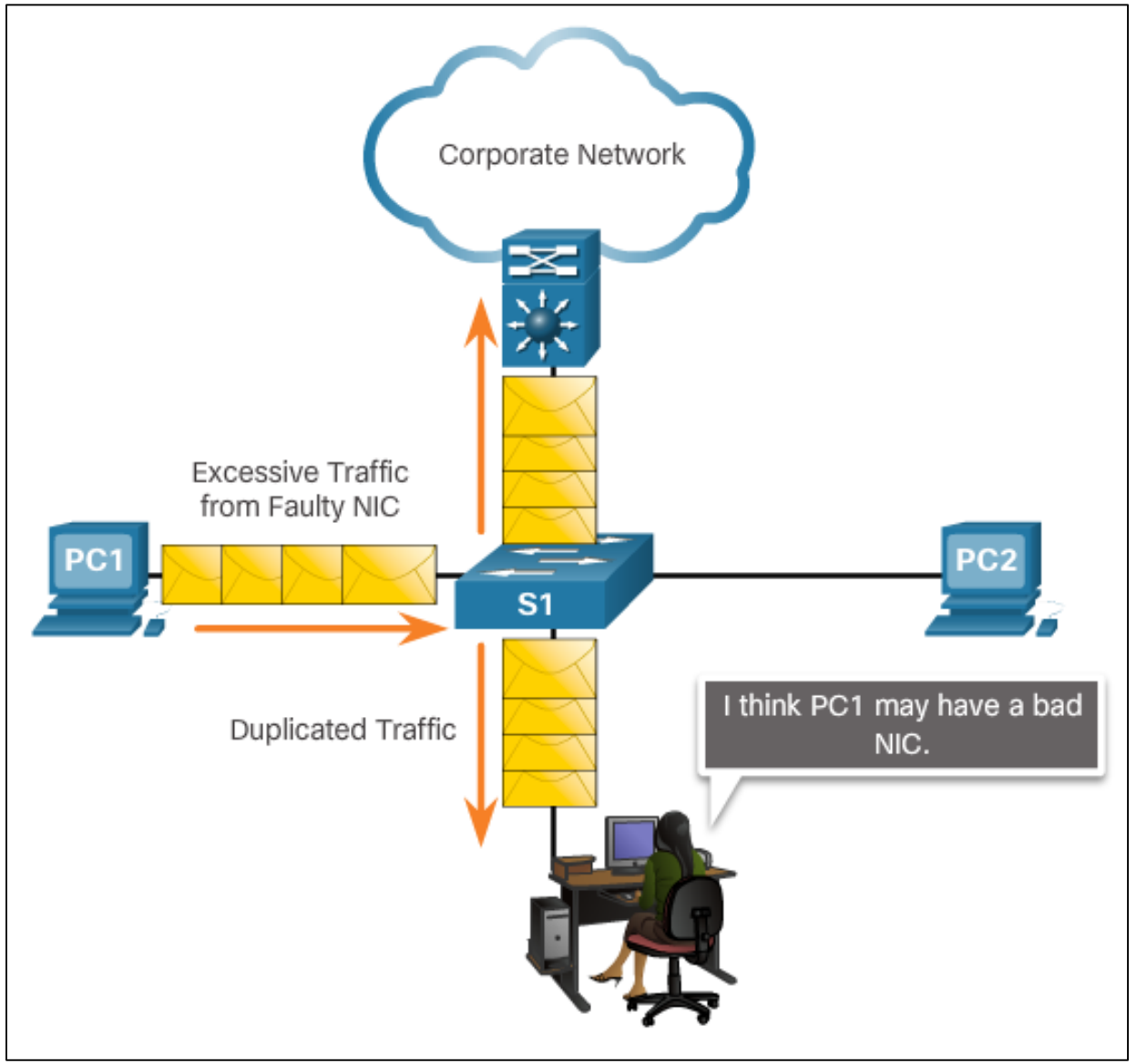
```
Switch(config)# monitor session number destination [ interface interface | vlan vlan ]
```




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

SPAN pre troubleshooting

- Použitím SPAN môže správca:
  - riešiť problémy so sieťou
  - použiť SPAN na duplikovania a presmerovanie prevádzky do analyzátora paketu
  - analyzovať prevádzku zo všetkých zariadení a vyriešiť tak neoptimálnu prevádzku sieťových aplikácii



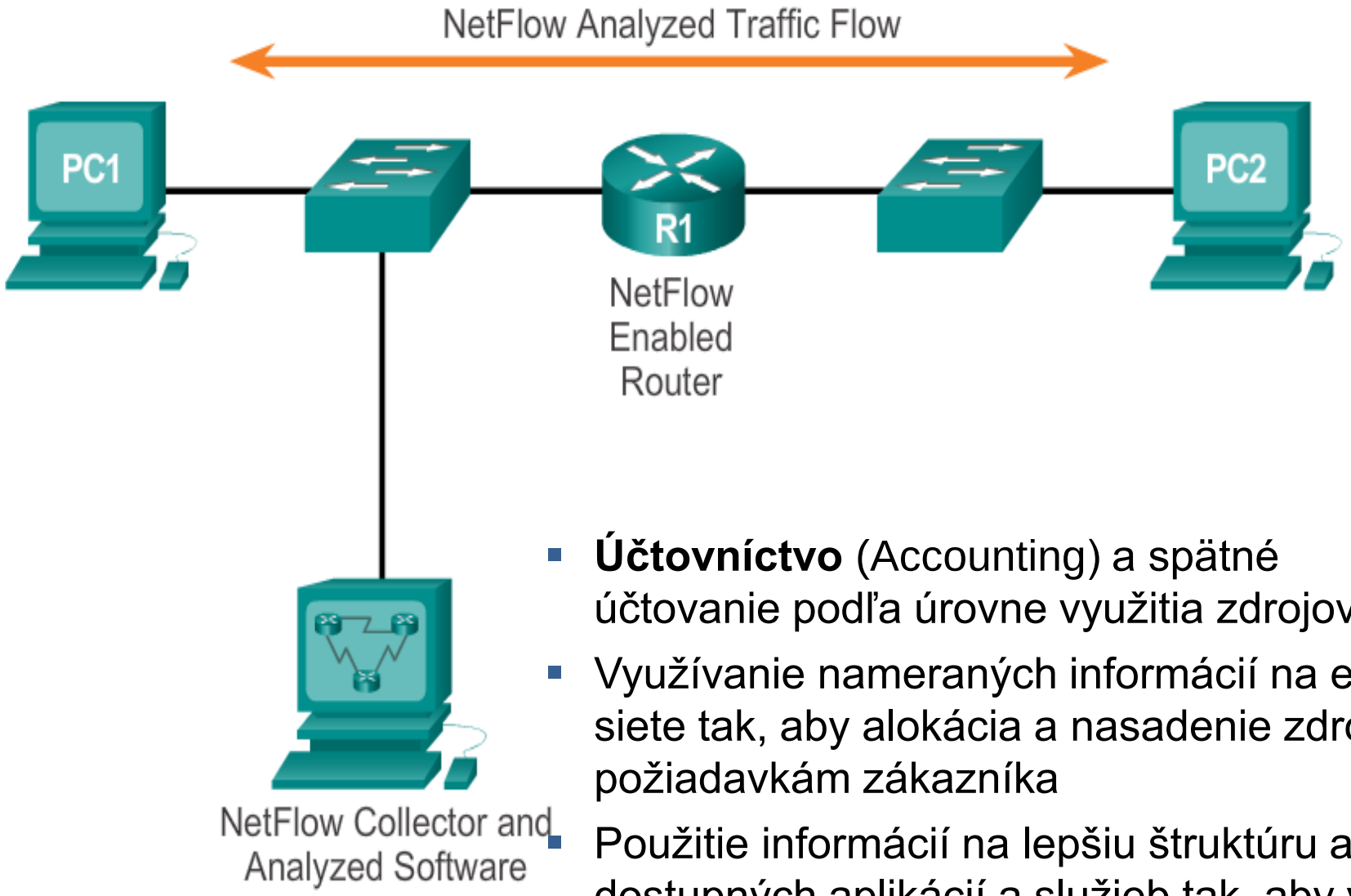
Prídavok: NetFlow

Nie je v aktuálnej verzii Netacad curricula (CCNA v7)

Nebude na skúške, ani v priebežnom teste

Uvádzame to ako rozšírenie témy - Monitoring siete, kde tento protokol svojou funkciou spadá. V domácej úlohe je aj jedna dobrovoľná úloha s Netflow.

Úvod do NetFlow



- Využitie nameraných informácií na efektívnejšie plánovanie siete (network **planning**), aby alokácia zdrojov bola podľa zákazníkových požiadaviek.
- Použitie informácií na lepšiu štruktúru a prispôsobenie dostupných aplikácií a služieb tak, aby vyhovovali potrebám používateľov a zákazníckych služieb.

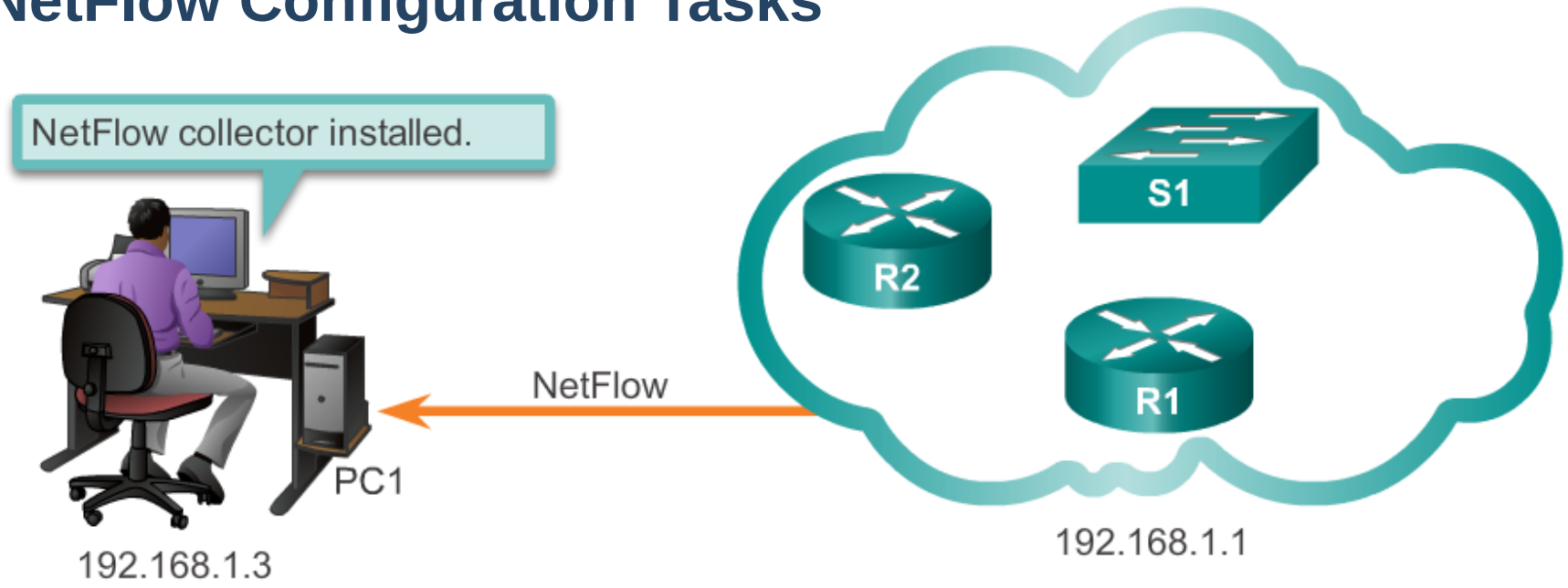
- **Účtovníctvo** (Accounting) a spätné účtovanie podľa úrovne využitia zdrojov.
- Využívanie nameraných informácií na efektívnejšie plánovanie siete tak, aby alokácia a nasadenie zdrojov vyhovovali požiadavkám zákazníka
- Použitie informácií na lepšiu štruktúru a prispôsobenie dostupných aplikácií a služieb tak, aby vyhovovali potrebám používateľov a požiadavkám zákazníckych služieb.

Network Flows

Súčasná NetFlow technológia má za sebou už niekoľko generácií, pričom každá poskytovala sofistikovanejšie definovanie internetovej prevádzky. “Originálny NetFlow“ rozlišoval typ prevádzky pomocou kombinácie siedmych faktorov.

- Zdrojová a cieľová IP adresa
- Zdrojové a cieľové číslo portu
- Typ protokolu (tretia vrstva)
- Typ služby (ToS) značenie
- Vstupné logické rozhranie

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

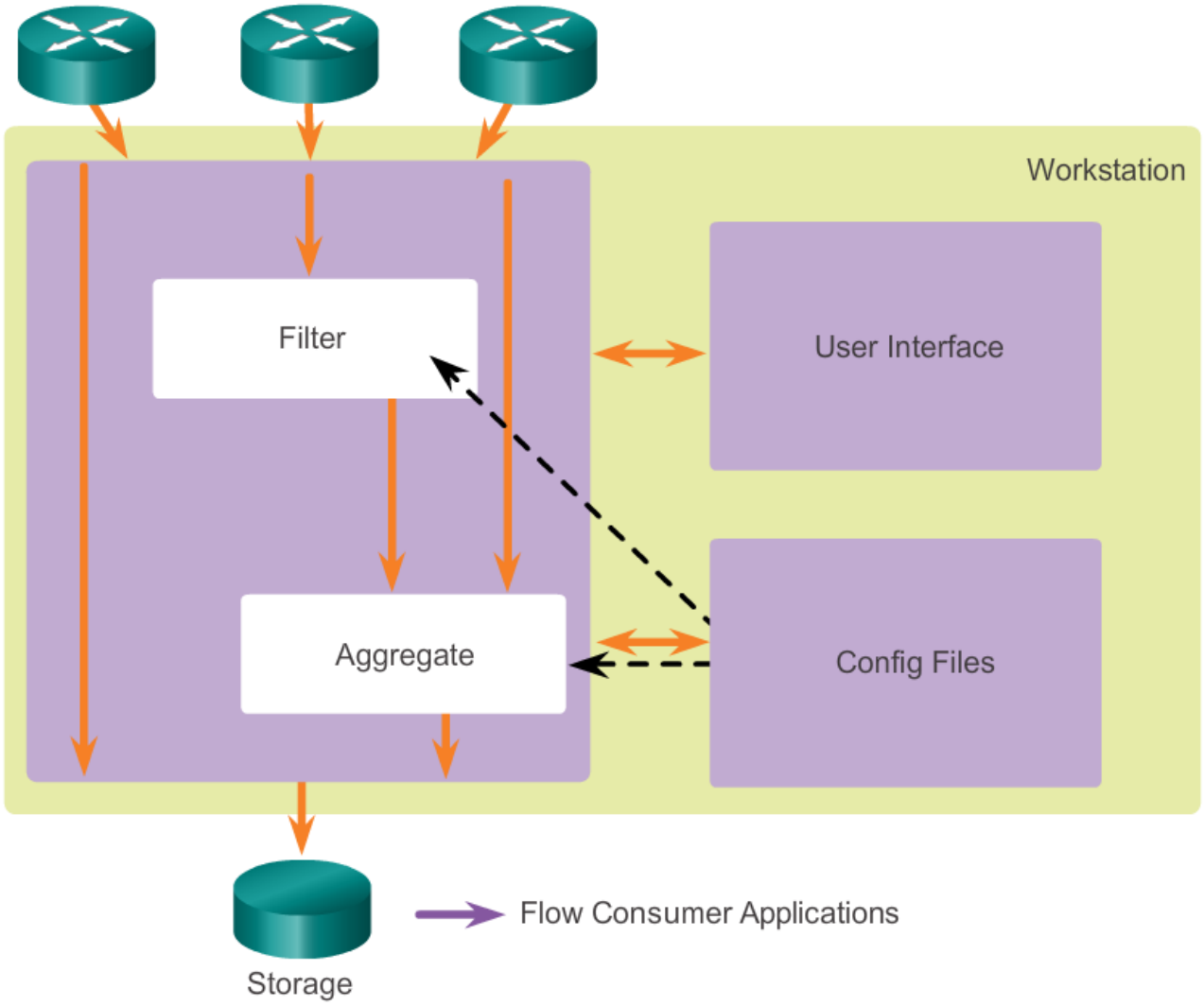
Overenie NetFlow

```
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
```

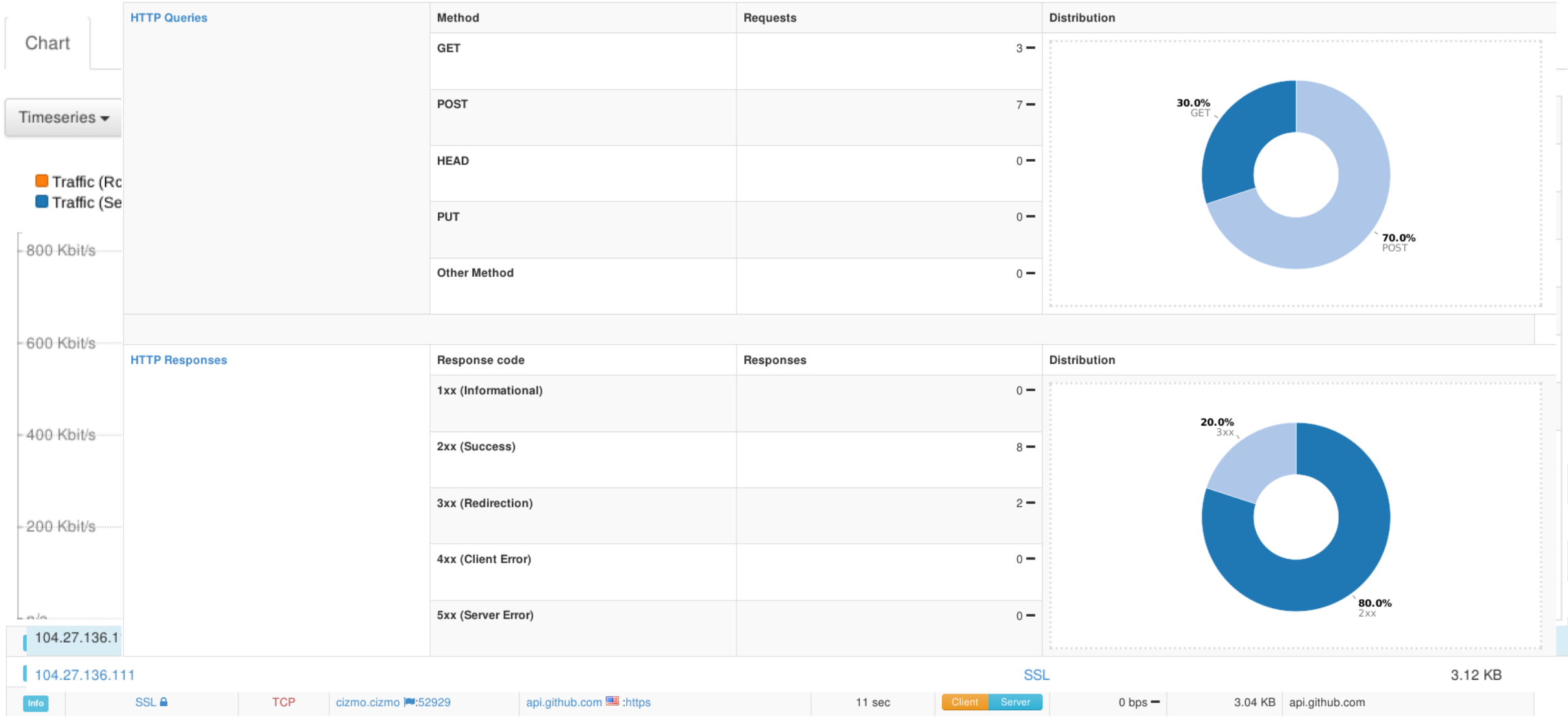
```
R1# show ip flow interface
GigabitEthernet0/1
  ip flow ingress
  ip flow egress
```

```
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 Funkcie



NetFlow analýza s NetFlow Collector



UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť.

Obsahom bola **kapitola 10** Network Management z kurzu CCNA 3 ENSA.
Samostatne treba naštudovať **kapitolu 12** (Network Trobuleshooting).

Spravte si kvíz na Netacade z ENSA_10 a ENSA_12.

Vyjadrite svoj názor na prednášku tohto týždňa (alebo cvičenie).

Vytvorené v rámci projektu KEGA 026TUKE-4/2021