Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Koncept funkčného monitorovania

Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza (Blok VI)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk

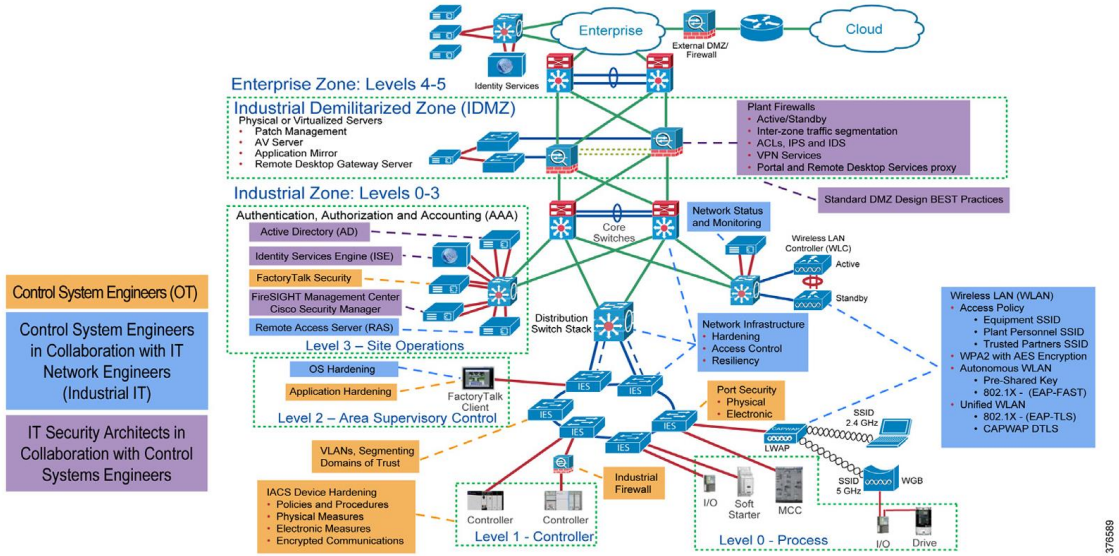
Ciele

- Protokoly a technológie využívané pre monitorovanie (SNMP, NetFlow, port mirror, TAPs, NTP, Syslog)

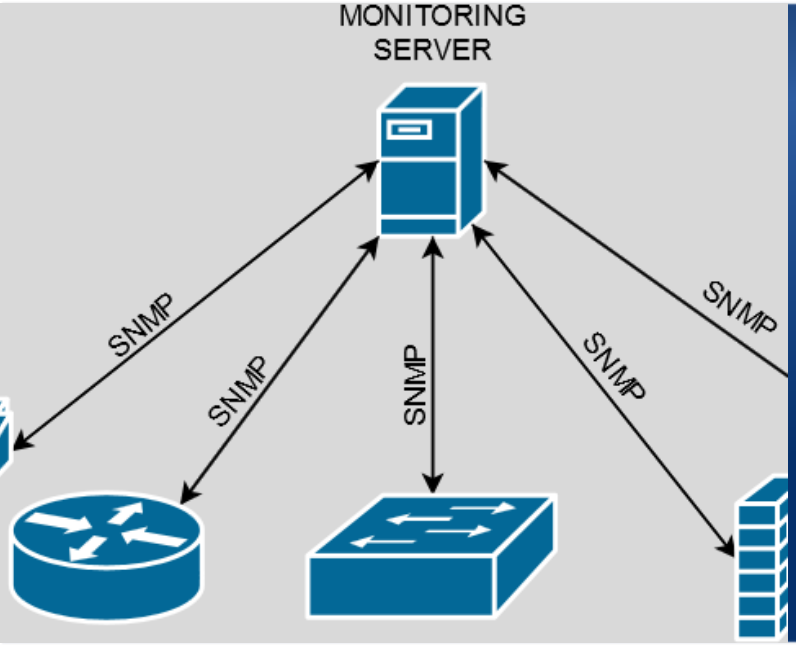
Metódy monitorovania sietí

- Každodenné činnosti siete pozostávajú z:
  - Tokov sieťovej prevádzky
  - Využívania šírky pásma
  - Prístupu k zdrojom

na identifikáciu bežného správania siete a identifikáciu odchýlok, anomálií, a incidentov



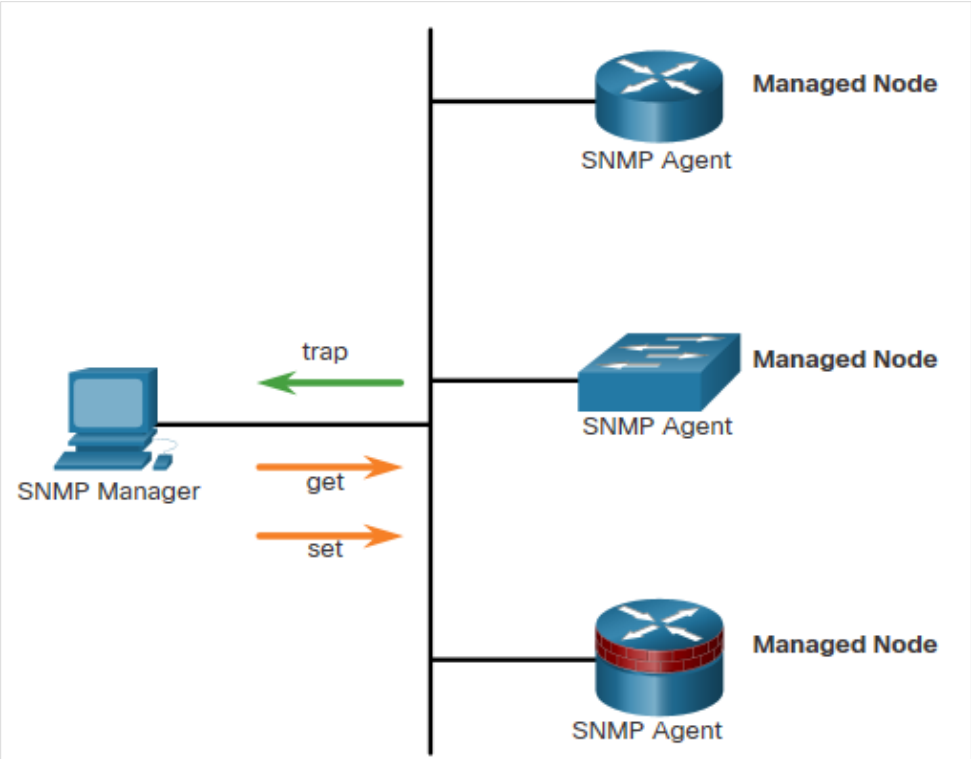
- AKO to zabezpečiť:
  - Implementáciou monitorovania siete
- KTORÝMI nástrojmi:
  - **Pre zaznamenanie:**
    - prevádzky a odoslanie do NMS zariadení
      - TAPs (Test Access Points)
      - Port mirror (SPAN)
    - informácií o toku paketov
      - Netflow
    - SNMP traps a info
    - Logov (+NTP)
  - **Pre analýzu:**
    - Packet sniffer
      - Wireshark / Tshark
      - Tcpdump
    - IDS
    - SIEM



SNMP

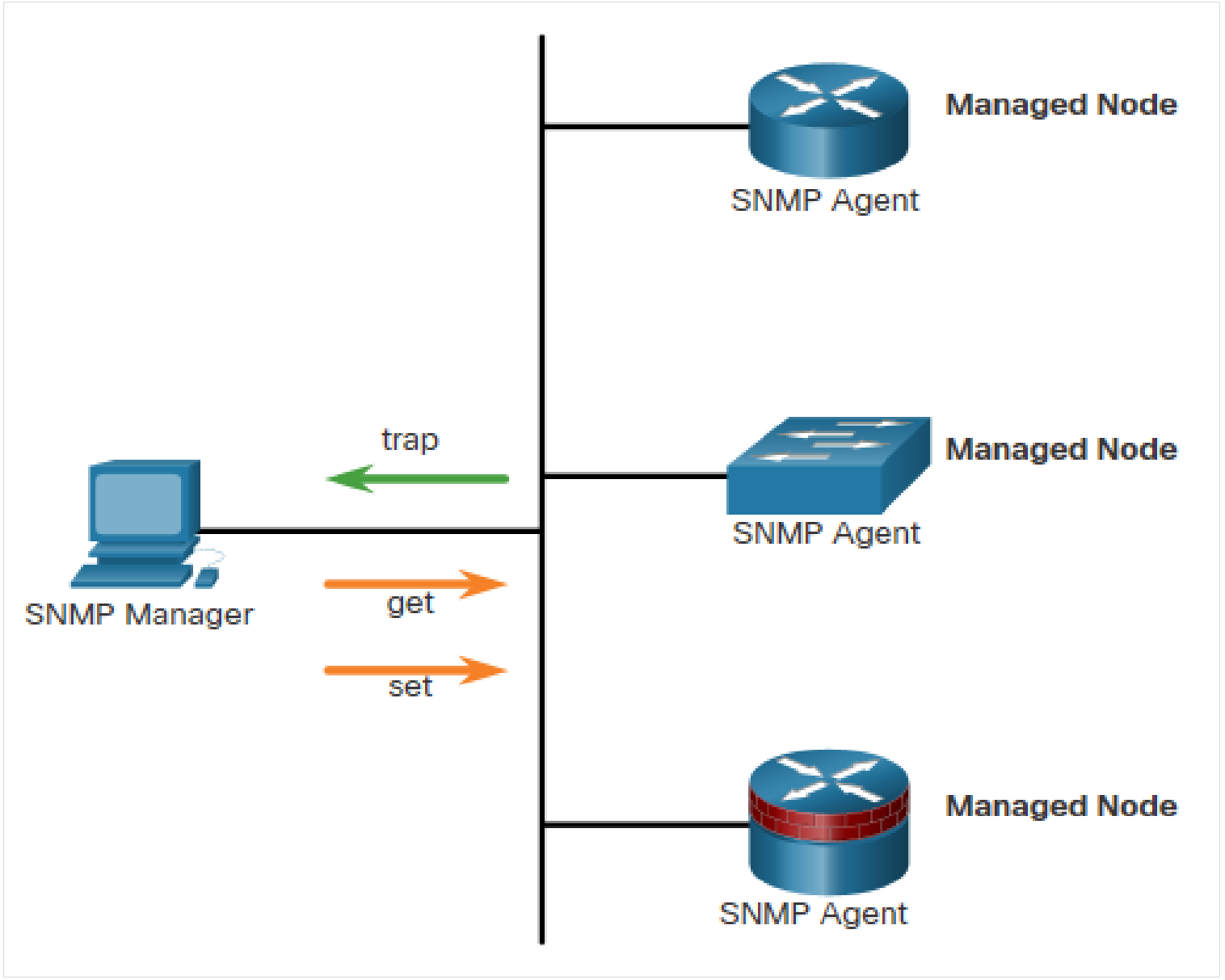
SNMP

- Simple Network Management Protocol (SNMP) je protokol aplikačnej vrstvy, ktorý poskytuje formát správ pre komunikáciu medzi SNMP manažérmi a SNMP agentmi.
- Umožňuje správcom sietí vykonávať:
  - Spravovanie koncových zariadení, ako sú servery, pracovné stanice, smerovače, prepínače a bezpečnostné zariadenia
  - Monitorovanie a riadenie výkonu siete
  - Hľadanie a riešenie sieťových problémov
  - Plánovanie rozširovania siete
- Systém SNMP pozostáva z dvoch prvkov:
  - **SNMP manažér:** prevádzkuje SNMP riadiaci softvér
  - **SNMP agent: s**tanice, ktoré sa monitorujú a spravujú



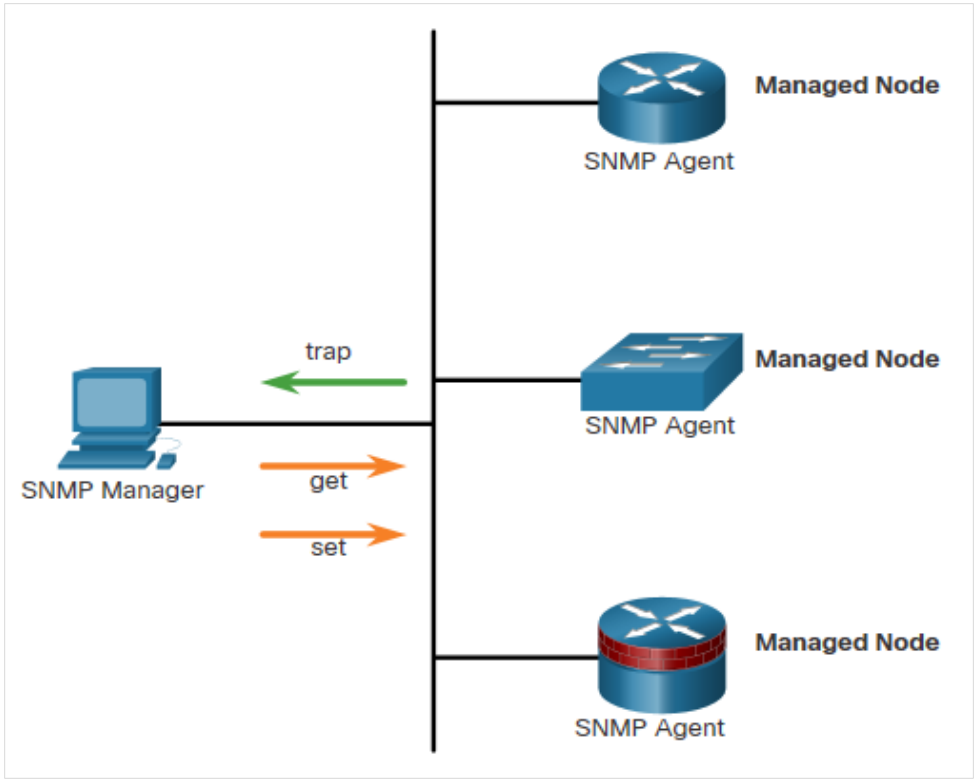
Fungovanie SNMP

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



SNMP

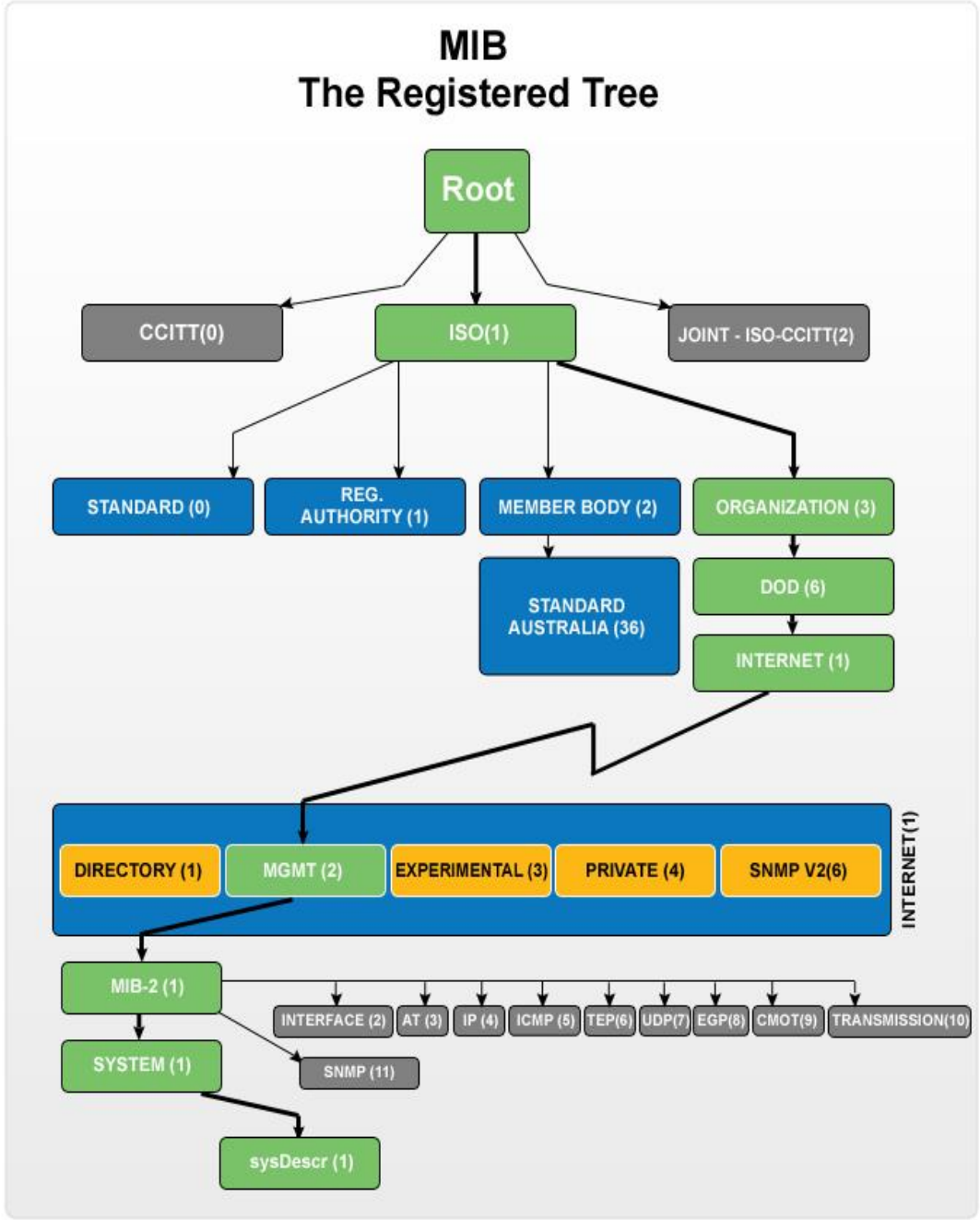
- dá sa využiť na zbieranie informácií z danej siete
- definuje operácie nad MIB bázou, ktorá má formu stromu
  - jej jednotlivé prvky sa definujú pomocou OID
  - prvky tejto bázy sa dajú rozdeliť na 2 typy údajov:
    - **Skalárne –** jeden údaj, ktorý obsahuje informáciu na základe daného OID
    - **Tabulárne –** viacero údajov, ktoré sa nachádzajú v predkovi svojho OID
  - Toto OID určuje konkrétny údaj, napríklad IP adresa, maska siete a podobne, alebo je to vrchol, ako napríklad systém
  - akými volaniami sa pristupuje na jednotlivé OID:
    - **snmget** – ktorý sa používa na prístup skalárnych typov
    - **snmpwalk** – ktorý sa používa primárne na prístup tabulárnych ale môže byť použitý aj na prístup skalárnych



MIB – Management Information Base

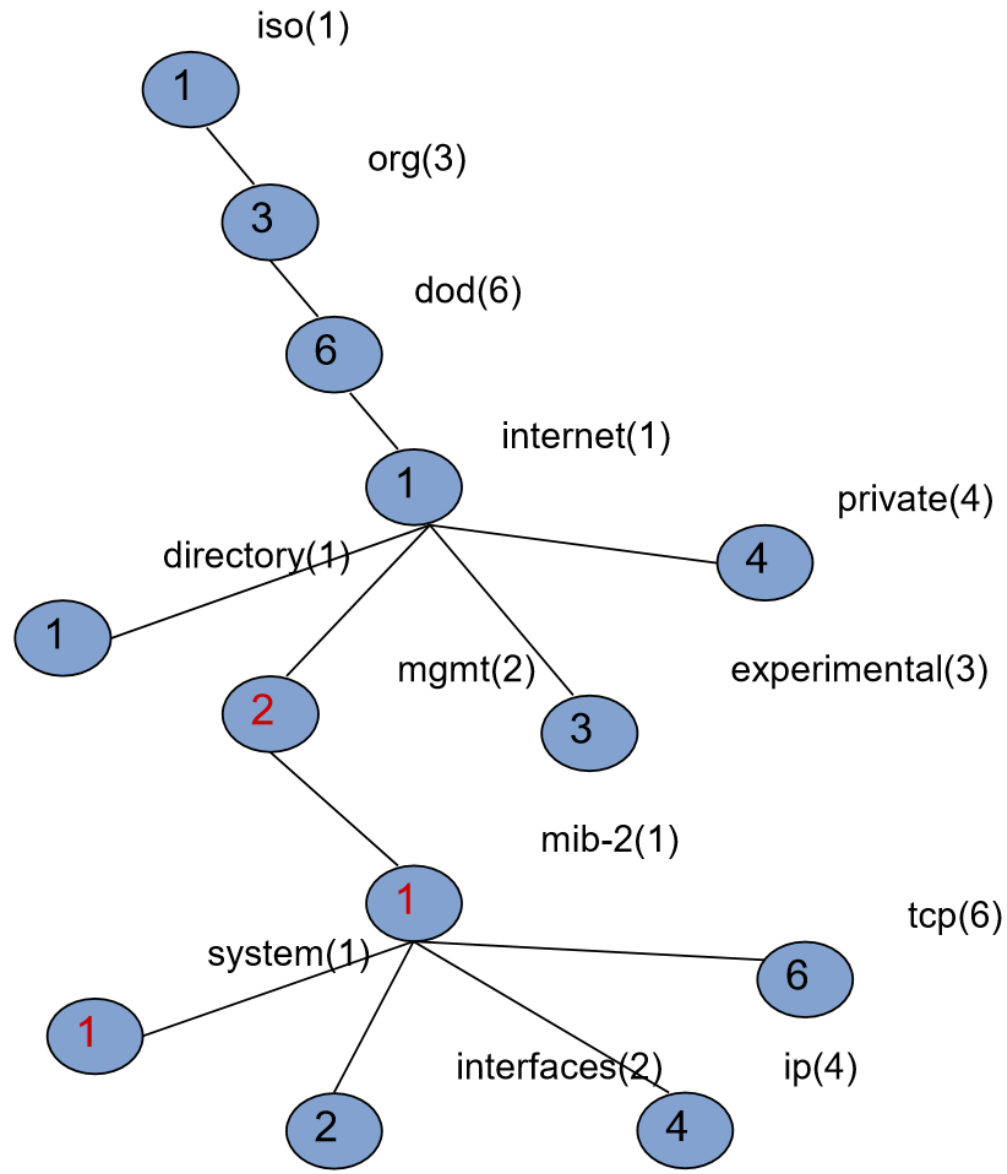
- Objekty na agentovi majú svoje identifikátory OID (Object IDentifier)
  - OID sú usporiadané v stromovej štruktúre
  - Vrcholy majú číselný i slovný názov
  - Konkrétny objekt je adresovaný cestou od koreňa stromu
- Príklad: .1.3.6.1.2.1.1

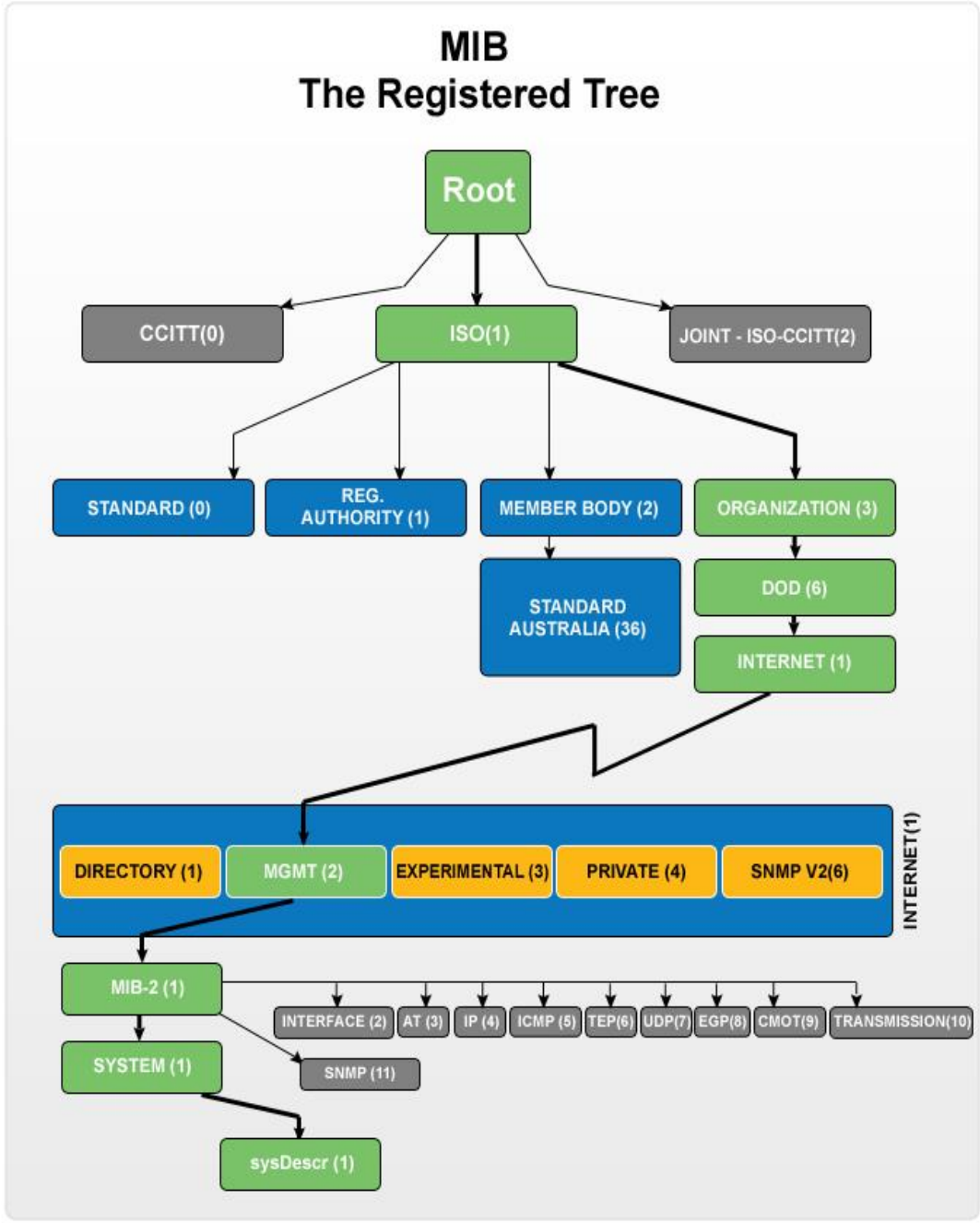
  iso(1) org(3) dod(6) internet(1)
  mgmt(2)
  mib-2 (1)
  system (1)



Hierarchická stromová štruktúra

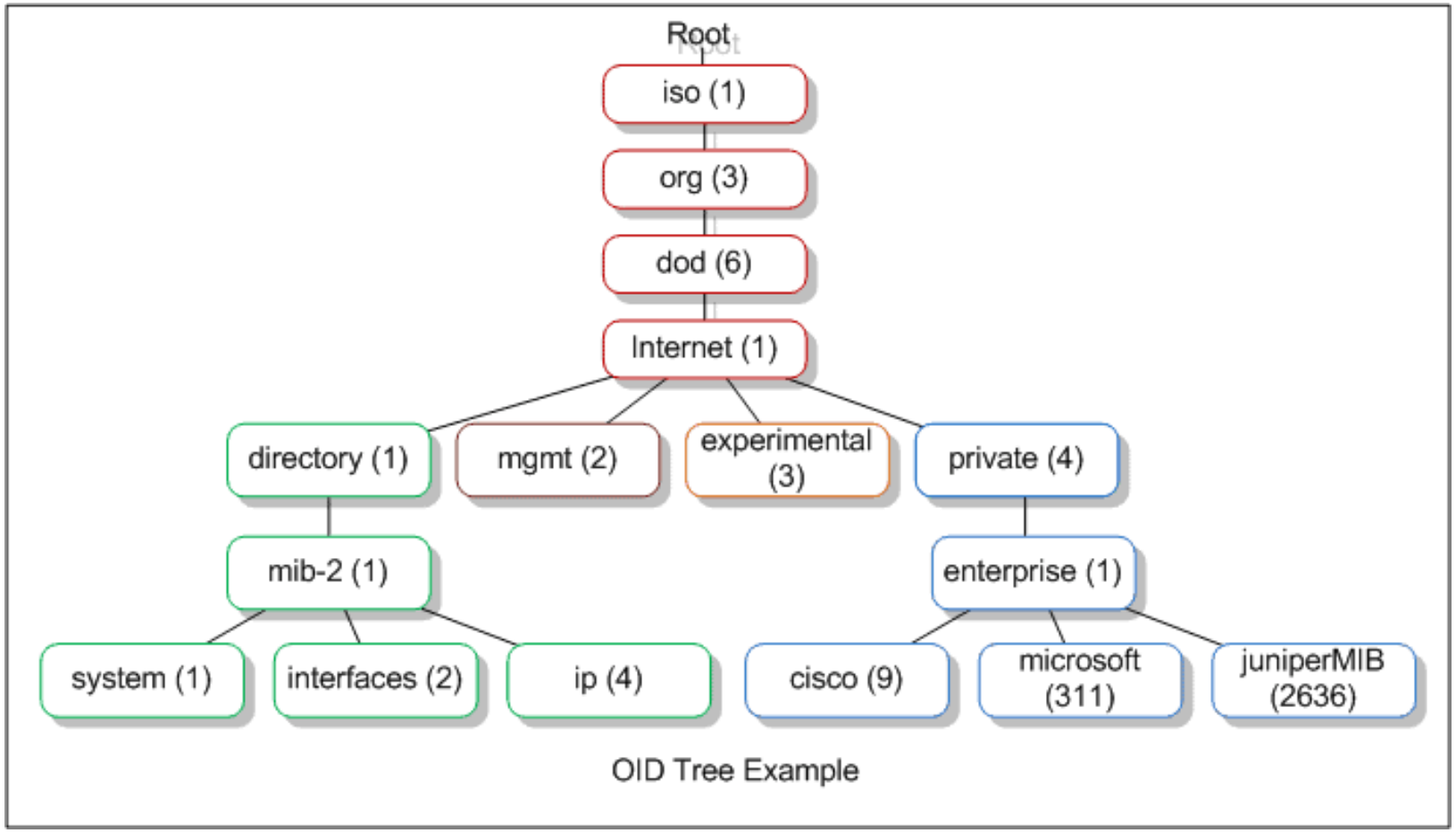
MIB





SNMP – MIB – verejná a privátna časť SNMP MIB databázy

- Úroveň ORG, má číslo „3“, keďže ide o tretí objekt pod ISO
- Väčšina SNMP hodnôt, o ktoré máme záujem, bude vždy začínať rovnakým súborom objektov – 1.3.6.1
- Stav rozhrania by mal OID 1.3.6.1.2.2.2.2.1.8
- MIB je ako prekladateľ, ktorý pomáha riadiacej stanici pochopiť odpovede získané zo sieťových zariadení
- Všetky zariadenia SNMP vo všeobecnosti podporujú MIB-2, ktorý je štandardným súborom objektov, ktoré možno monitorovať.



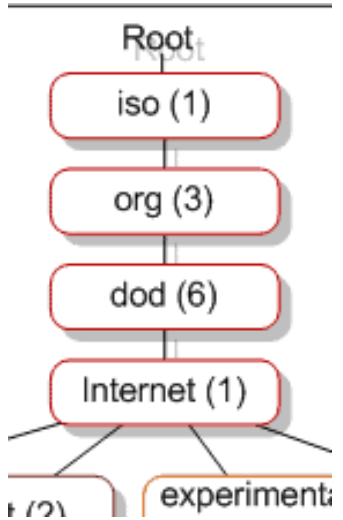
OID Tree Example

https://mibs.observium.org/

https://mibs.observium.org/all

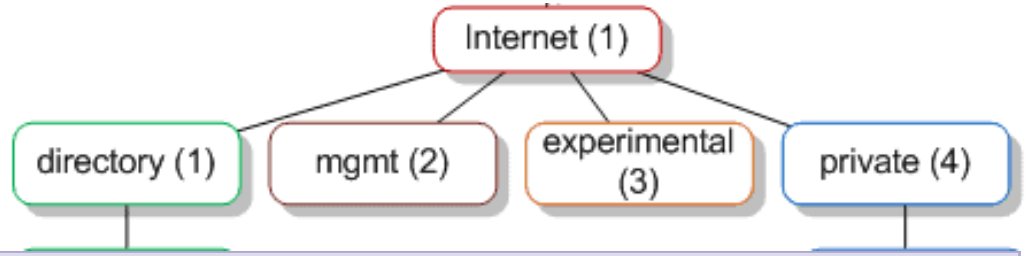
Prvé 4 úrovne MIB stromu (pod koreňom)

- SNMP prakticky vždy ide cestou:
  iso (1) → org (3) → dod (6) → internet (1)
- Ostatné vetvy existujú, ale v SNMP sa takmer nepoužívajú.



Úroveň	Názov	OID	Význam
1	**iso**	1	Globálny koreň OID stromu spravovaný organizáciou ISO, z ktorého vychádza celé hierarchické prideľovanie identifikátorov.
2	**org**	1.3	Vetva určená pre organizácie, umožňujúca delegovanie správy častí OID stromu jednotlivým subjektom.
3	**dod**	1.3.6	Historická vetva Ministerstva obrany USA, pod ktorou vznikli kľúčové sieťové technológie ako TCP/IP a SNMP.
4	**internet**	1.3.6.1	Vetva vyhradená pre internetové protokoly a technológie spravované IANA a IETF; základ pre všetky SNMP MIB.

Hlavné vetvy MIB (5. úroveň od koreňa)



OID	Názov vetvy	Význam
1.3.6.1.1	**directory**	Určená pre adresárové služby (napr. X.500); historická vetva, v praxi sa dnes takmer nepoužíva.
1.3.6.1.2	**mgmt**	Hlavná vetva pre štandardné SNMP objekty definované IETF; obsahuje MIB-II a predstavuje základ monitorovania zariadení naprieč výrobcami.
1.3.6.1.3	**experimental**	Priestor pre experimentálne a testovacie objekty; nie je určený pre produkčné nasadenie.
1.3.6.1.4	**private**	Vetva vyhradená pre výrobcovské (vendor-specific) MIB; obsahuje podstrom enterprises, kde má každý výrobca vlastné OID.
1.3.6.1.5	**security**	Objekty súvisiace s bezpečnostnými mechanizmami SNMP; v praxi málo využívaná vetva.
1.3.6.1.6	**snmpV2**	Objekty definované pre správu a štatistiky protokolu SNMPv2; slúži na monitorovanie samotného SNMP mechanizmu.

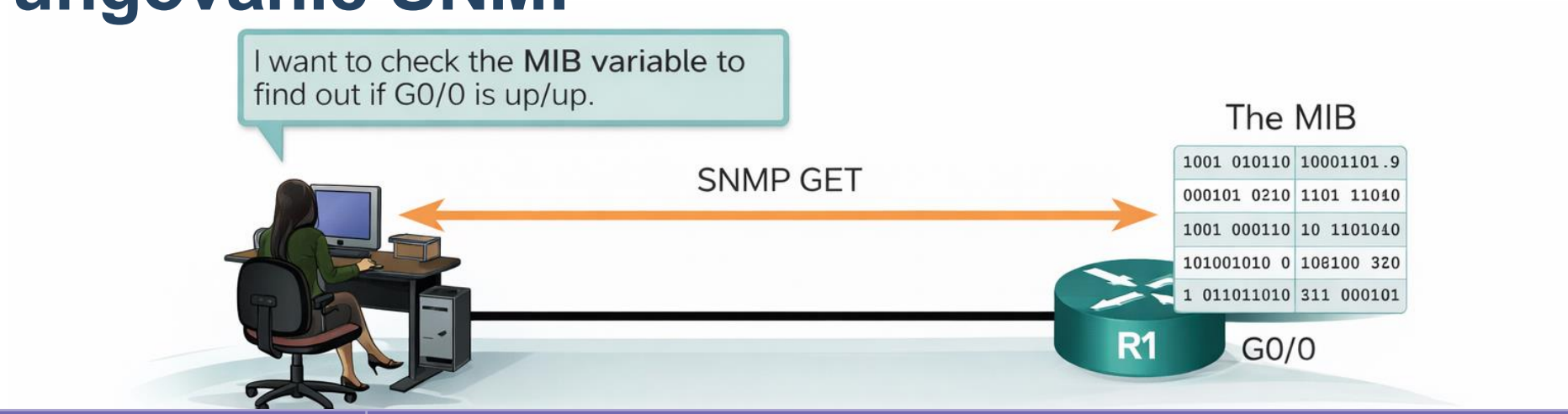
Pôvodný účel vetvy Security (1.3.6.1.5)

- Vetva **security** bola navrhnutá ako priestor pre **bezpečnostné mechanizmy súvisiace so SNMP**, najmä:
  - autentifikáciu,
  - autorizáciu,
  - riadenie prístupu k MIB objektom.
- Ide o **bezpečnosť SNMP protokolu**, nie bezpečnosť monitorovaných zariadení.
- **SNMPv1 mal problémy:**
  - používal len **community string** (plaintext),
  - žiadna skutočná autentifikácia,
  - žiadne šifrovanie,
  - veľmi slabá bezpečnosť.
- Preto vznikla snaha riešiť bezpečnosť **dodatočnými MIB mechanizmami**.

- **Prečo sa security vetva v praxi nepoužíva**
  - **Bezpečnosť sa presunula do SNMPv3**
  - SNMPv3 zaviedlo:
    - **User-based Security Model (USM)**,
    - **View-based Access Control Model (VACM)**,
    - autentifikáciu,
    - integritu,
    - šifrovanie.
  - Tieto mechanizmy sú definované:
    - v **SNMP-FRAMEWORK-MIB**,
    - v **SNMPv2 vetve (1.3.6.1.6)**,
    - nie v security.
- **Vetva ostala historickým artefaktom**
  - Dnes je **prakticky prázdna alebo nepoužívaná**.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

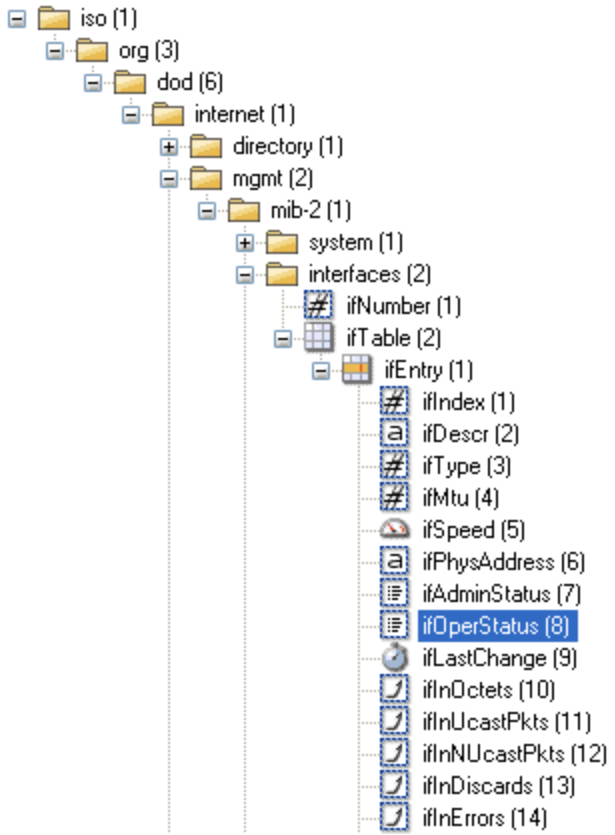
Fungovanie SNMP



Operácia	Popis
get-request	Získa hodnotu z konkrétnej MIB premennej.
get-next-request	Získa hodnotu z nasledujúcej premennej v tabuľke; SNMP manažér nemusí poznať presný názov premennej a prehľadáva tabuľku sekvenčne.
get-bulk-request	Získa veľké bloky dát (napr. viacero riadkov tabuľky) naraz, čím sa znižuje počet jednotlivých požiadaviek; dostupné len v SNMPv2 a novších verziách.
get-response	Odpoveď SNMP agenta na požiadavky typu get-request, get-next-request alebo set-request odoslané manažérom.
set-request	Uloží alebo zmení hodnotu v konkrétnej MIB premennej na zariadení.

SNMP – MIB files (not readable)

- Väčšina softvéru na manažment siete má schopnosť zobrazovať strom OID



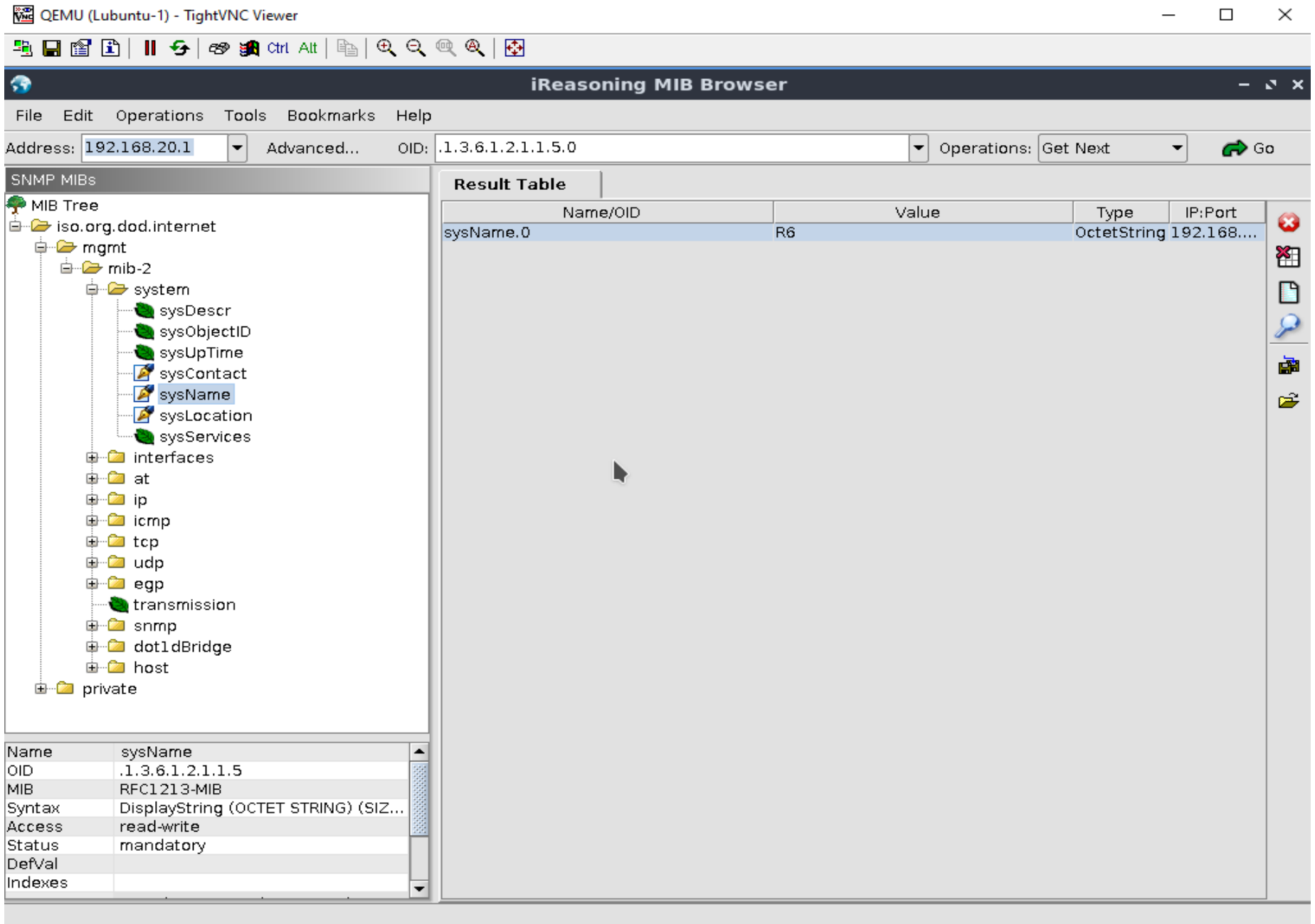
- Samotné MIB súbory sa ťažko čítajú, sú určené len na import alebo kompiláciu riadiacou stanicou.

```
ciscoEnvMonObjects 2 }▯▯ciscoEnvMonVoltageStatusEntry
OBJECT-TYPE▯        SYNTAX     CiscoEnvMonVoltageStatusEntry▯
    MAX-ACCESS not-accessible▯        STATUS     current▯
DESCRIPTION▯                "An entry in the voltage status
table, representing the status▯                of the associated
testpoint maintained by the environmental▯
monitor."▯        INDEX      { ciscoEnvMonVoltageStatusIndex }▯
      ::= { ciscoEnvMonVoltageStatusTable 1 }▯▯
CiscoEnvMonVoltageStatusEntry ::=▯        SEQUENCE {▯
    ciscoEnvMonVoltageStatusIndex   Integer32 (0..2147483647),▯
             ciscoEnvMonVoltageStatusDescr   DisplayString,▯
           ciscoEnvMonVoltageStatusValue   CiscoSignedGauge,▯
            ciscoEnvMonVoltageThresholdLow  Integer32,▯
       ciscoEnvMonVoltageThresholdHigh Integer32,▯
 ciscoEnvMonVoltageLastShutdown  Integer32,▯
ciscoEnvMonVoltageState         CiscoEnvMonState▯        }▯▯
ciscoEnvMonVoltageStatusIndex OBJECT-TYPE▯        SYNTAX
Integer32 (0..2147483647)▯        MAX-ACCESS not-accessible▯
   STATUS     current▯        DESCRIPTION▯
"Unique index for the testpoint being instrumented.▯
   This index is for SNMP purposes only, and has no▯
   intrinsic meaning."▯        ::= {
```

Cisco - SNMP Object Navigator

Cisco poskytuje užitočný zdroj na vyhľadávanie hodnôt OID a sťahovanie MIB súborov pre ktorékoľvek z ich zariadení: https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

iReasoning MIB Browser

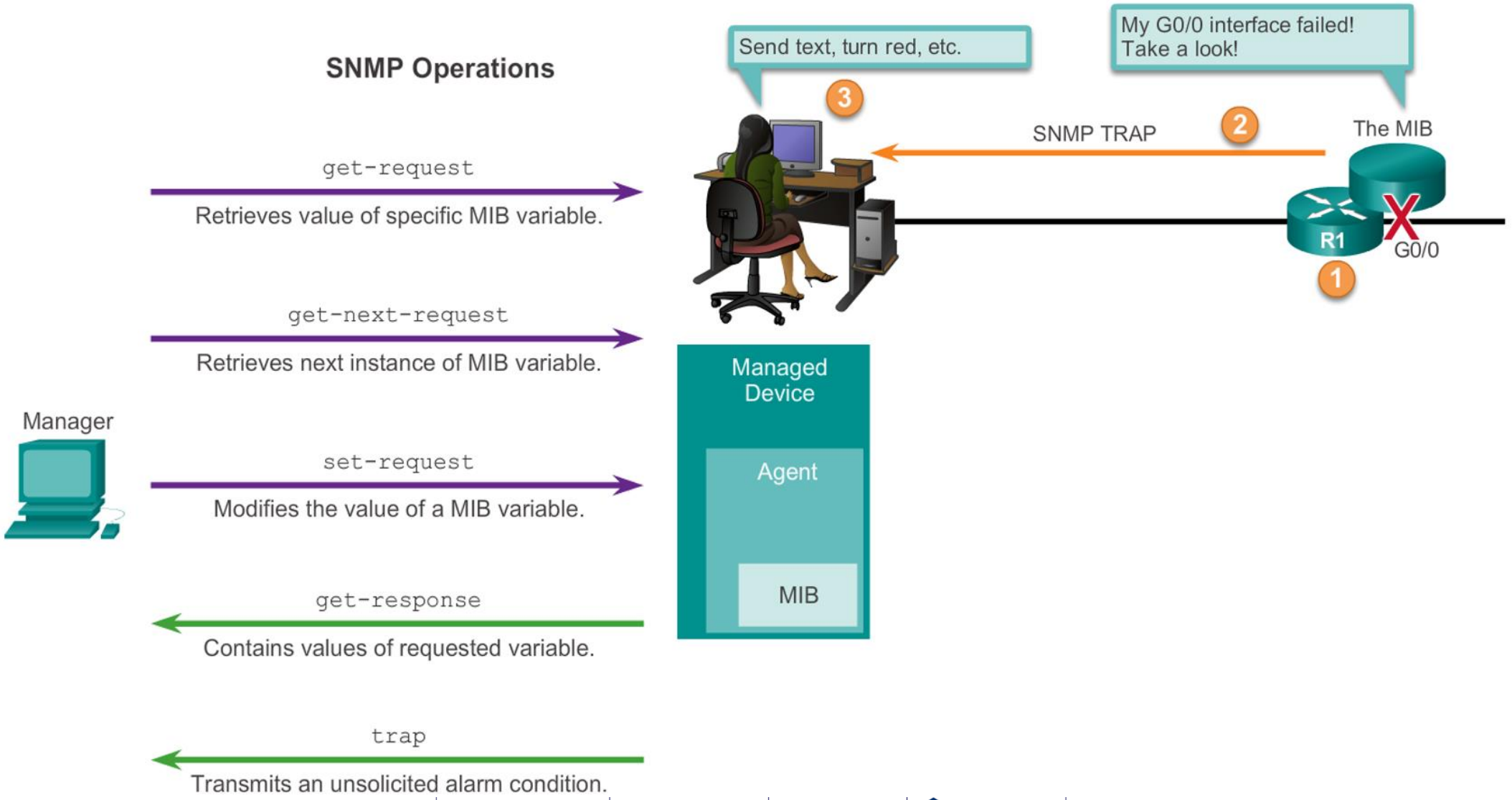


Konzolové výpisy

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



Verzie 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.

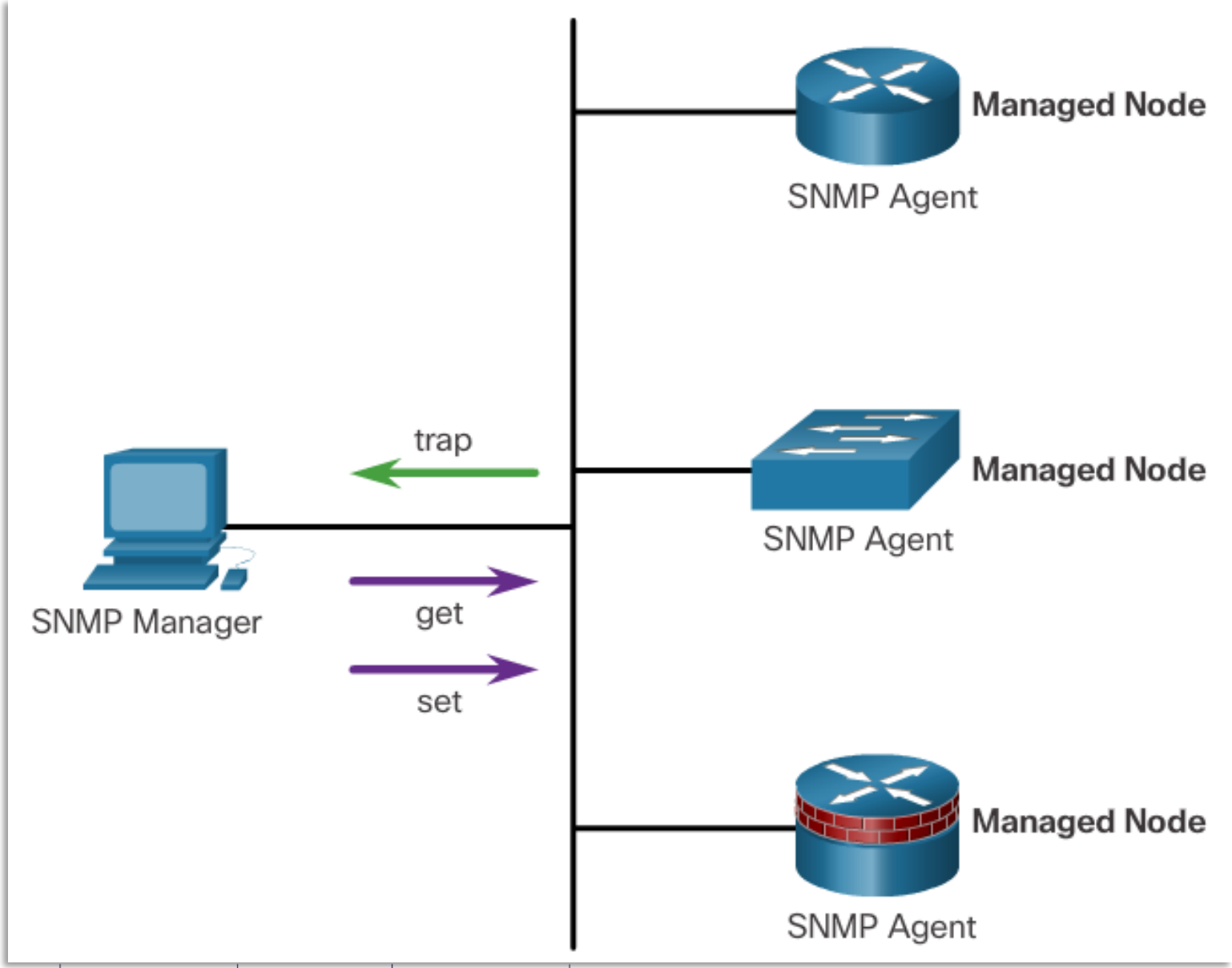
Model	Úroveň	Autentifikácia	Šifrovanie	Poznámka (aktuálny stav)
SNMPv1	noAuthNoPriv	Community string	Nie	**Neodporúčané** – bez zabezpečenia
SNMPv2c	noAuthNoPriv	Community string	Nie	**Neodporúčané** – plaintext
SNMPv3	noAuthNoPriv	Používateľské meno	Nie	Len minimálna ochrana
SNMPv3	authNoPriv	**SHA-1 / SHA-256**	Nie	Autentifikácia bez šifrovania
SNMPv3	authPriv	**SHA-256**	**AES-128 / AES-256**	**Odporúčaná konfigurácia**

Fungovanie SNMP

Komunitné reťazce

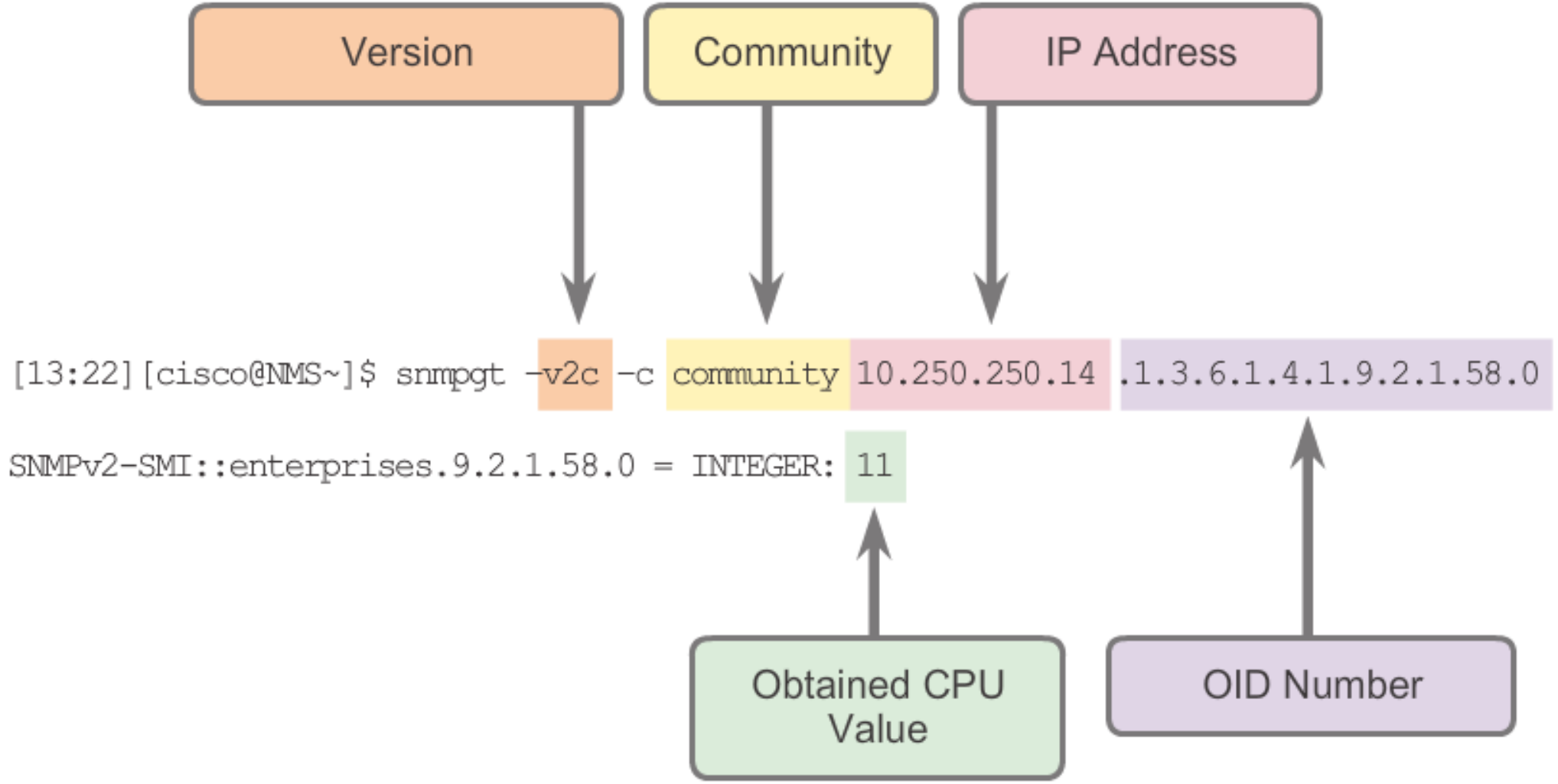
Existujú dva typy komunitných reťazcov:

- **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.



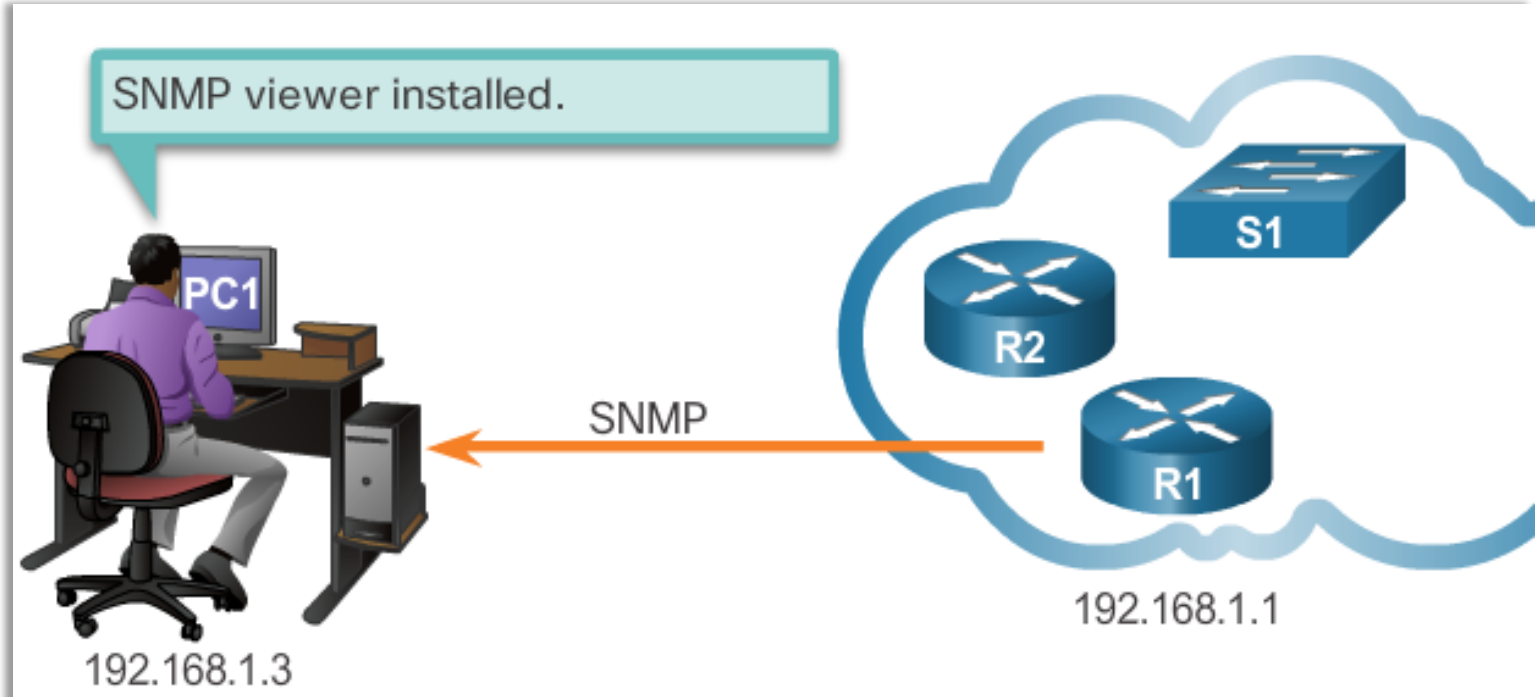
Fungovanie SNMP

Management Information Base Object ID



Konfigurácia SNMP – príklad 1

- Kroky konfigurácie
  - (Povinné) Konfigurácia komunitného reťazca a úrovne prístupu (iba na čítanie alebo na čítanie aj zápis)
  - Document location of device
  - Document system contact
  - Obmedzenie prístupu SNMP na NMS zariadenia (SNMP managers), ktorí sú povolení zoznamom ACL.
  - Špecifikácia príjemcu SNMP traps
  - Povolenie traps na SNMP agentovi




```
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

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
```

Konfigurácia SNMP- príklad 2

- Vytvorenie ACL pre limitovaný prístup k SNMP agentovi
- Nastavenie SNMP komunitných reťazcov
  - pre read only a read write
- Nastavenie cieľa pre zasielanie správ SNMP Traps
- 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 ?
```

Rozdiel medzi SNMP polling a SNMP traps

Vlastnosť	SNMP Polling	SNMP Traps
Spôsob iniciácie	Manažér (monitorovací systém) pravidelne **pýta** zariadenia o stav	Zariadenie **posiela** upozornenie samo, keď nastane udalosť
Reakcia na udalosť	Aktívne zisťovanie stavu (pull)	Pasívne upozornenie (push)
Frekvencia	Pravidelná, podľa nastaveného intervalu	Iba keď nastane konkrétna udalosť
Sieťová záťaž	Vyššia pri veľkom počte zariadení a krátkych intervaloch	Nízka, posielajú sa len upozornenia
Použitie	Zisťovanie **aktuálneho stavu** zariadení a trendov	Rýchle upozornenie na **významnú udalosť**
Príklad	Polling CPU load každých 5 minút	Trap pri výpadku prepínača alebo kritickej chybe

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.

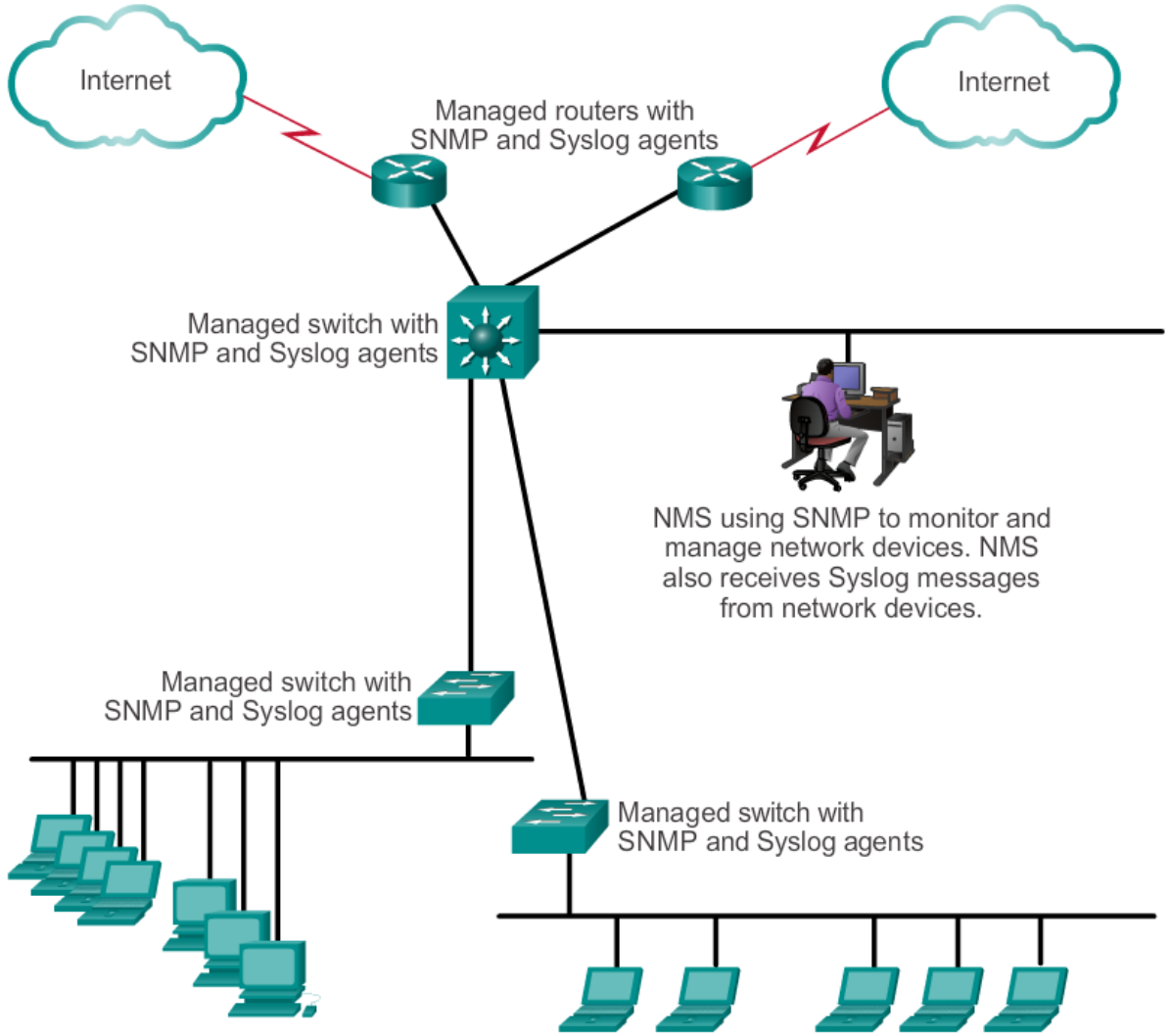
```
Router(config)# snmp-server group group-name v3
priv read view-name access [acl-number | acl-name]
```

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
```

Osvedčené bezpečnostné postupy

- Využívať SNMP, ideálne v3



Port mirroring a TAPs

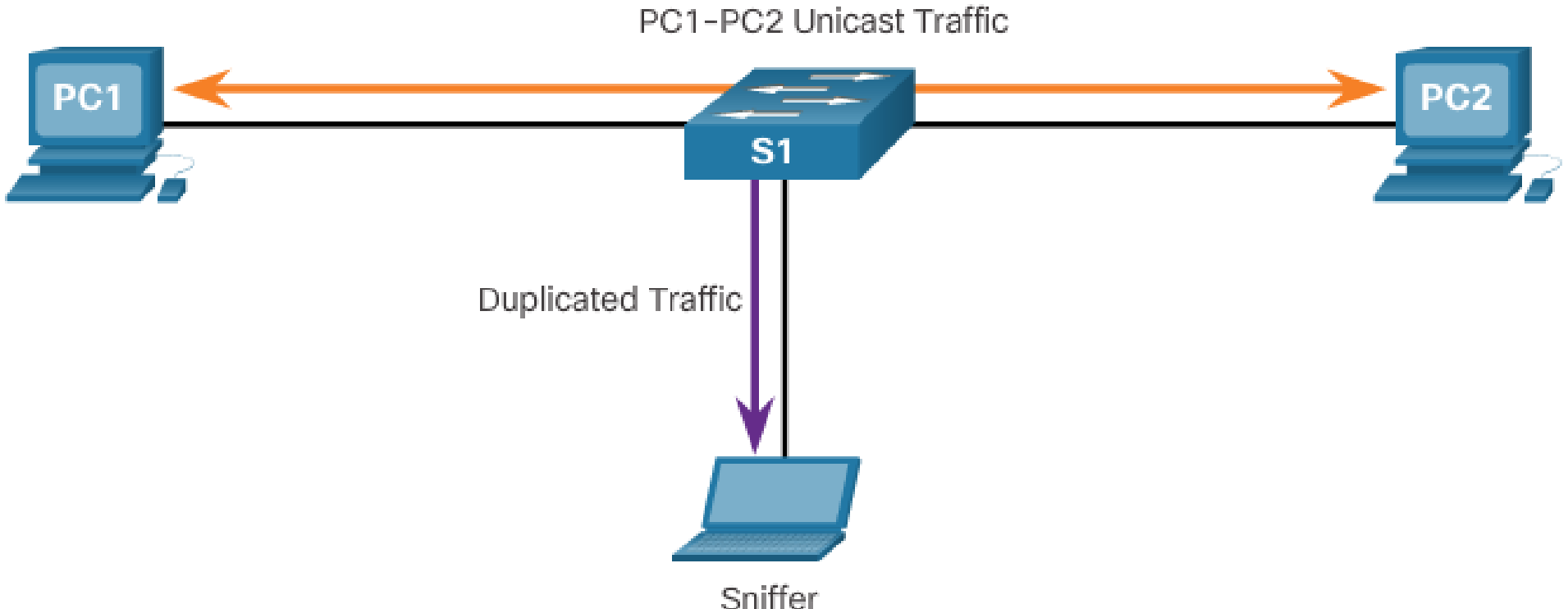
Často používaná technika pre monitorovanie v LAN

Cisco Switch Port Analyzer (SPAN)

Taps ako monitorovacie body

Popis využitia SPAN

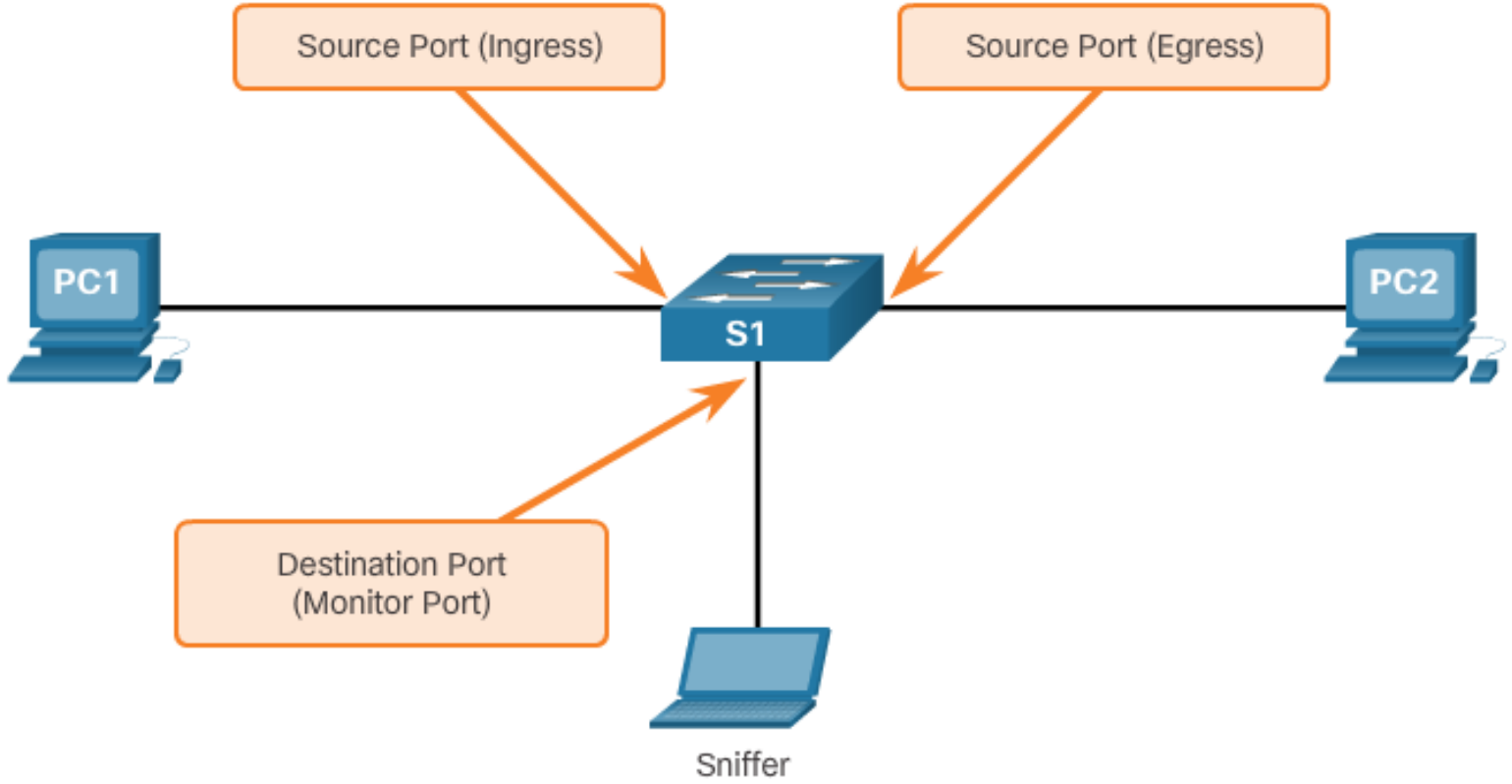
- Port mirroring (zrkadlenie)
  - Umožňuje prepínačom kopírovať a odosielať eternetové rámce zo špecifického portov do cieľového portu pripojeného k analyzátoru paketov. Pôvodný rámec pokračuje ďalej obvyklým spôsobom.
  - Bežne sa implementuje na podporu prevádzkových analyzátorov alebo IDS zariadení



Cisco Switch Port Analyzer

SPAN

- SPAN terminológia

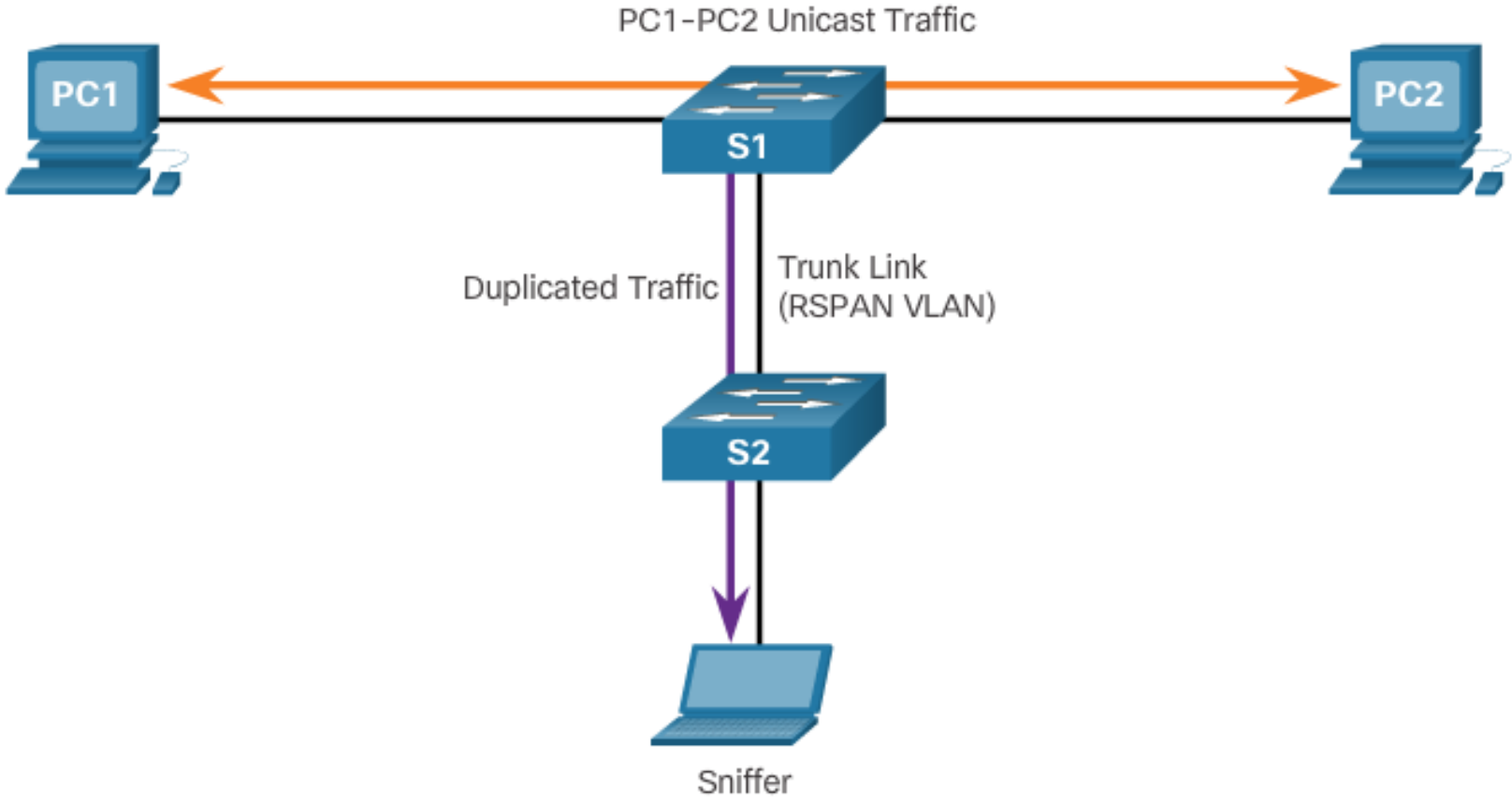


Term	Definition
Ingress traffic	This is traffic that enters the switch.
Egress traffic	This is traffic that leaves the switch.
Source (SPAN) port	This is a port that is monitored with use of the SPAN feature.
Destination (SPAN) port	This is a port that monitors source ports, usually where a packet analyzer, 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.

Cisco Switch Port Analyze

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.

Cisco Switch Port Analyzer

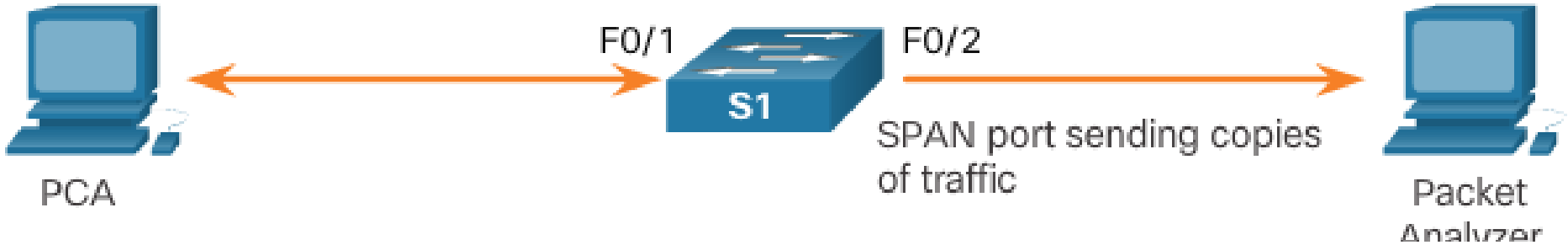
SPAN Konfigurácia

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

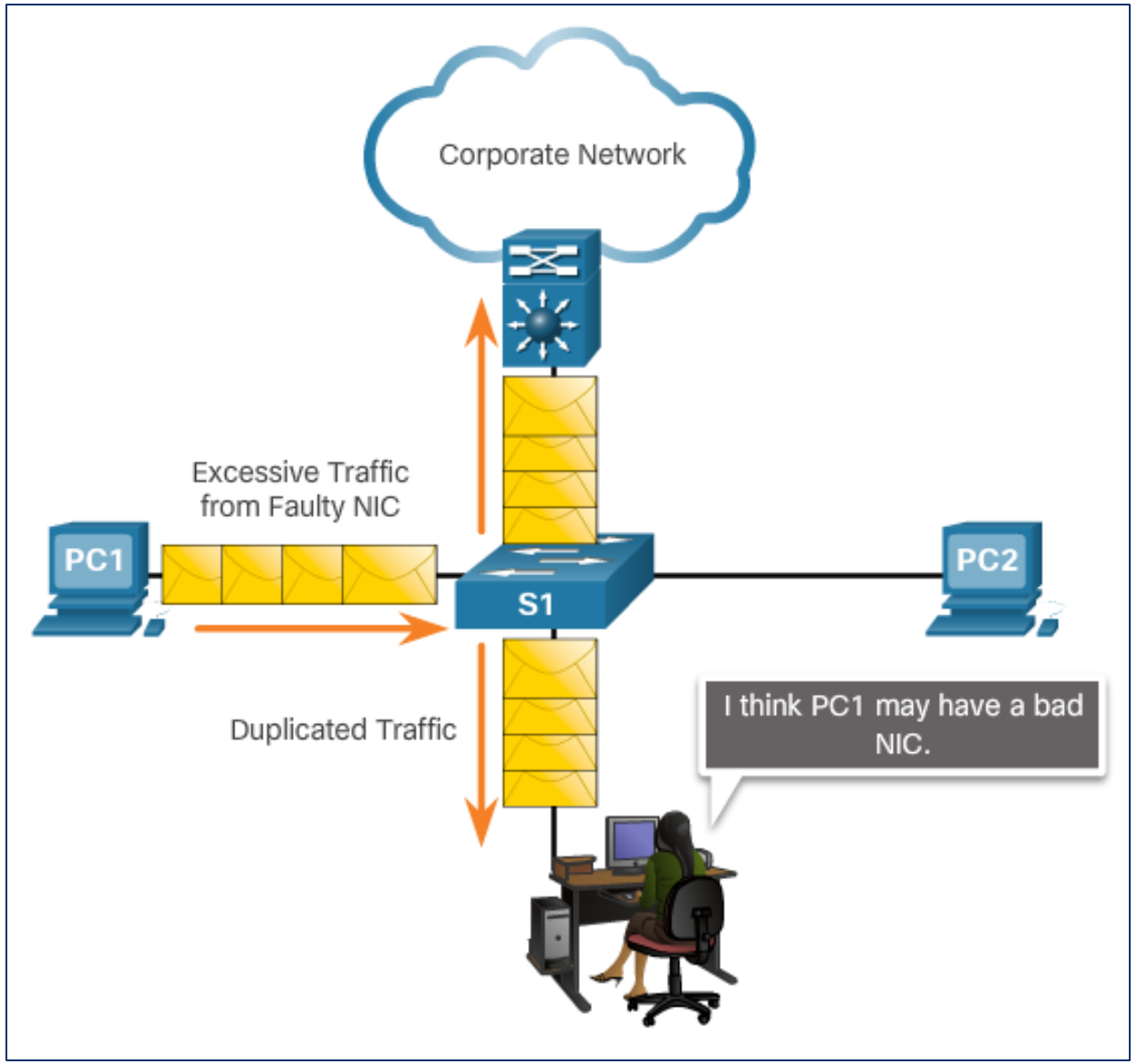
```
Switch(config)# monitor session number destination [ interface interface | vlan vlan ]
```




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

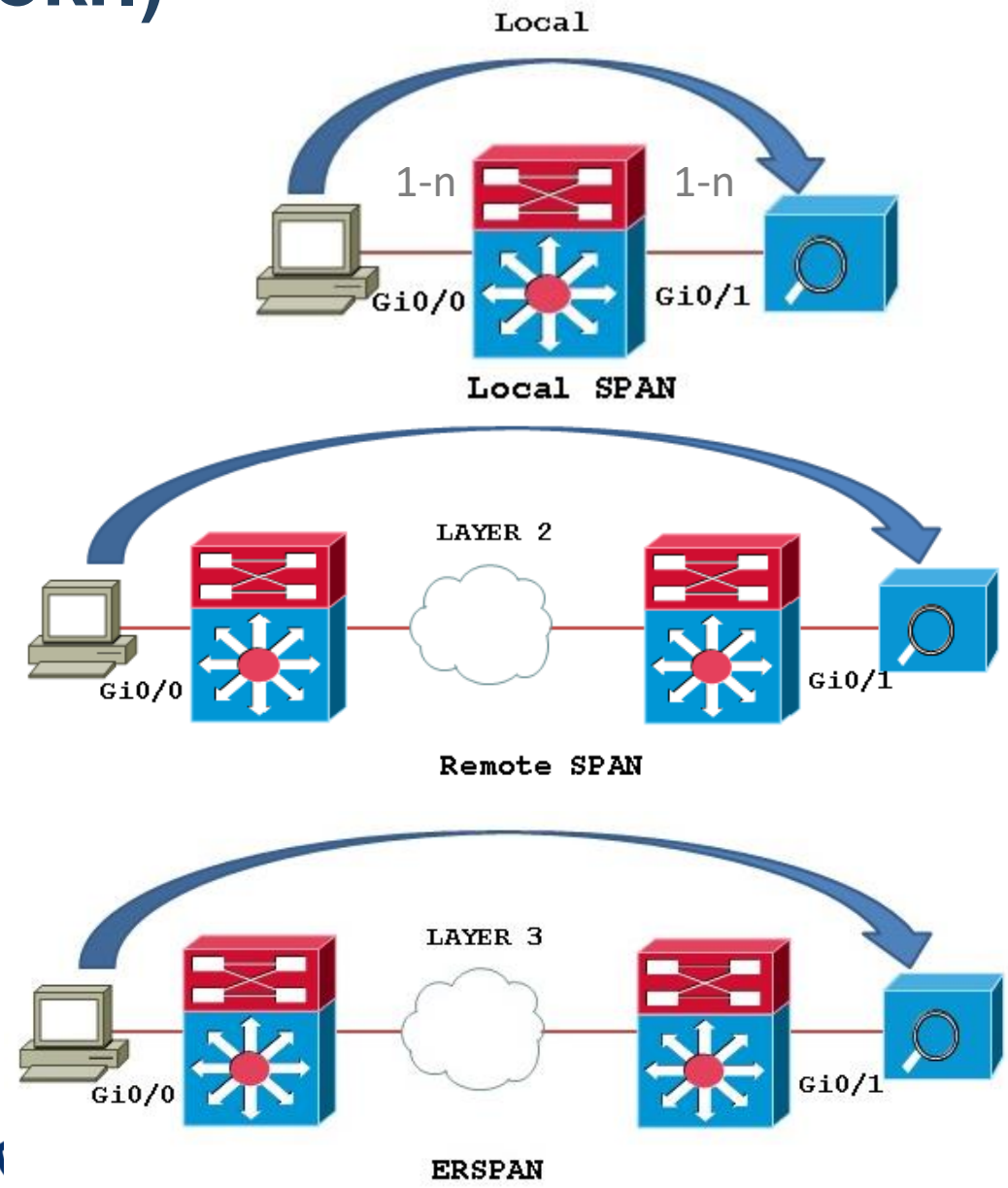
SPAN pre troubleshooting

- Použitím SPAN môže správca:
  - riešiť problémy so sieťou
  - použiť SPAN na duplikovania a presmerovanie prevádzky k nástroju pre analyzovanie paketov, a ich možnú archiváciu (napr. Arkime)
  - analyzovať prevádzku zo všetkých zariadení a vyriešiť tak neoptimálnu prevádzku sieťových aplikácii



Zrkadlenie prevádzky a SPAN (Pokr.)

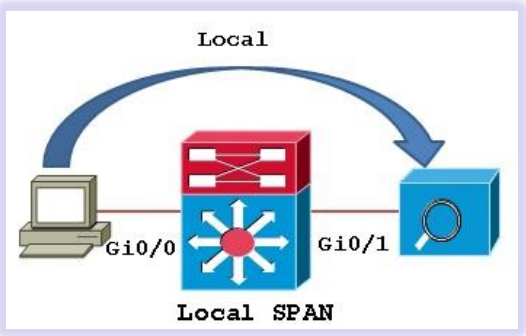
- **SPAN session =** spojenie medzi zdrojovými portmi a cieľovým portom
- Samostatná **lokálna SPAN** relácia:
  - Zdroj:
    - **jeden alebo viacero portov možno monitorovať, alebo:**
    - **zdrojová VLAN** môže byť špecifikovaná, čím sa stanú zdrojmi SPAN prevádzky všetky porty v tejto VLAN.
  - Cieľ:
    - V niektorých Cisco prepínačoch je možné zrkadliť prevádzku **na viacej cieľových portov**.
  - Varianty:
    - **Remote SPAN (RSPAN)** umožňuje správcovi siete využívať flexibilitu VLANs na monitorovanie prevádzky na vzdialených prepínačoch.
    - **Encapsulated Remote SPAN (ERSPAN)** zavádza GRE pre celú zachytenú prevádzku a umožňuje tak jej rozšírenie na 3. vrstvu
      - Musíme použiť **RSPAN VLAN**, tieto VLANs majú **špeciálne vlastnosti** a nemôžu byť priradené k žiadnym prístupovým prístavom.



SPAN konfigurácia

- **Local SPAN**

```
Switch1(config)# monitor session 1 source interface Gi0/0
Switch1(config)# monitor session 1 destination interface Gi0/1
```



- **Remote SPAN**

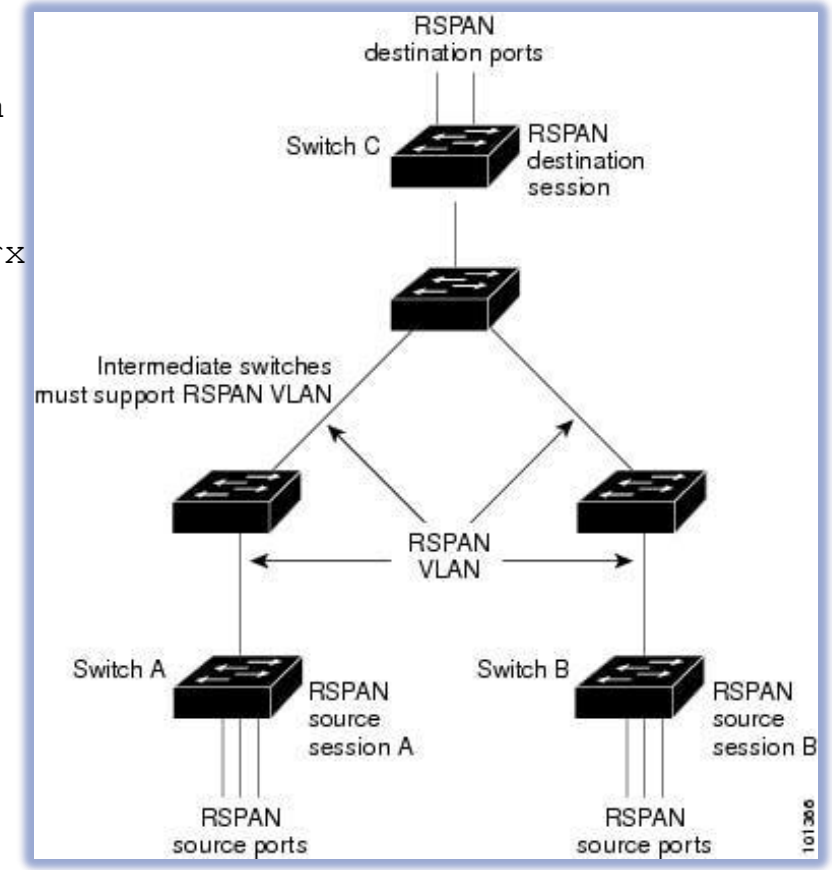
```
SwitchA(config)# vlan 200        ... SwitchC(config)# vlan 200
SwitchA(config-vlan)# remote-span ..SwitchC(config-vlan)# remote-span
```

Source switch:

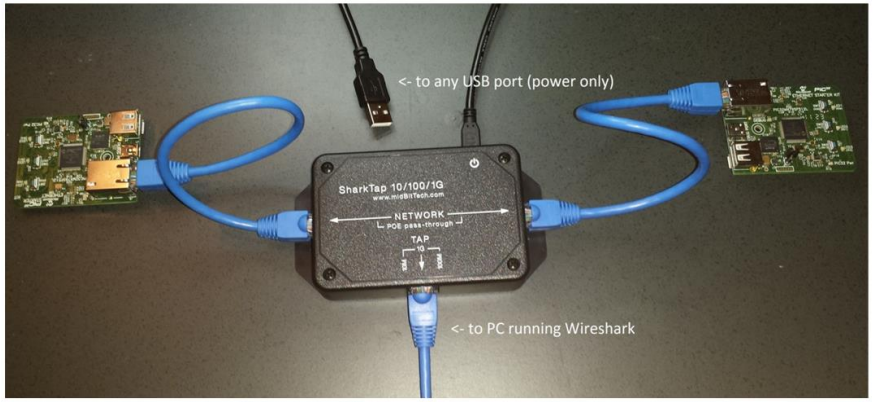
```
SwitchA(config)# monitor session 1 source interface fastEthernet0/2 rx
SwitchA(config)# monitor session 1 destination remote vlan 200
```

Destination switch (na ktorom je NMS)

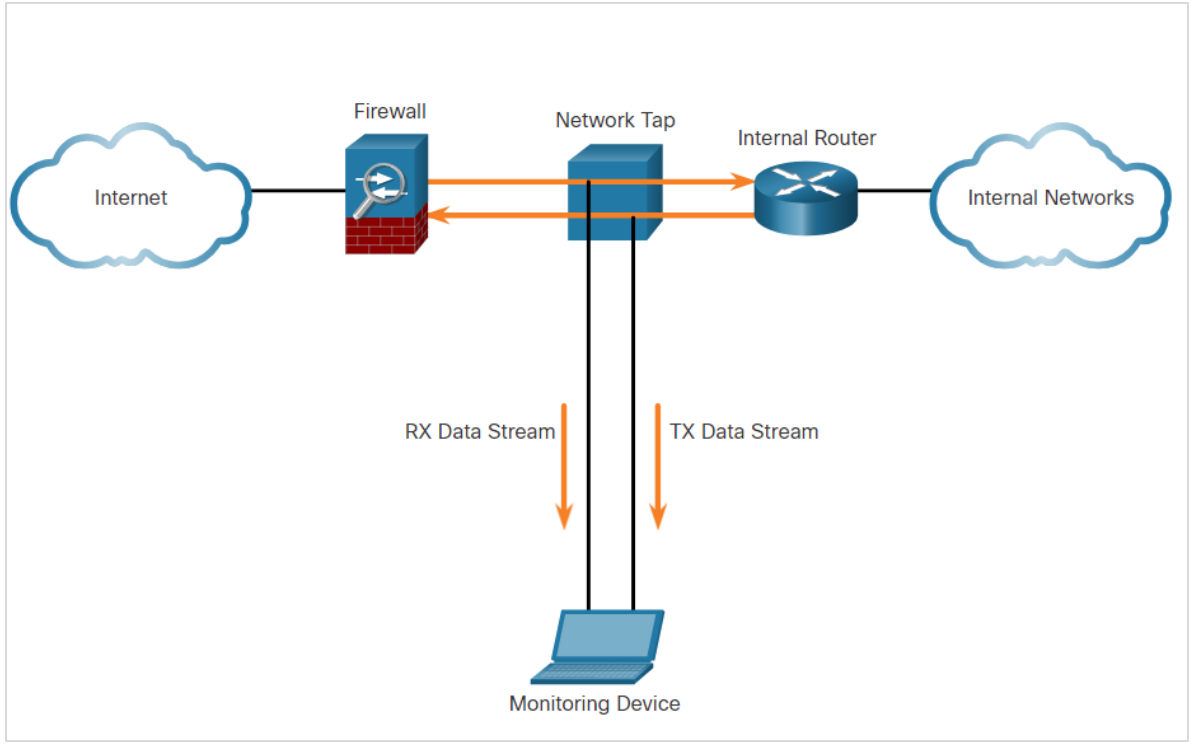
```
SwitchC(config)# monitor session 1 source remote vlan 200
SwitchC(config)# monitor session 1 destination interface fa0/3
```



Network Taps



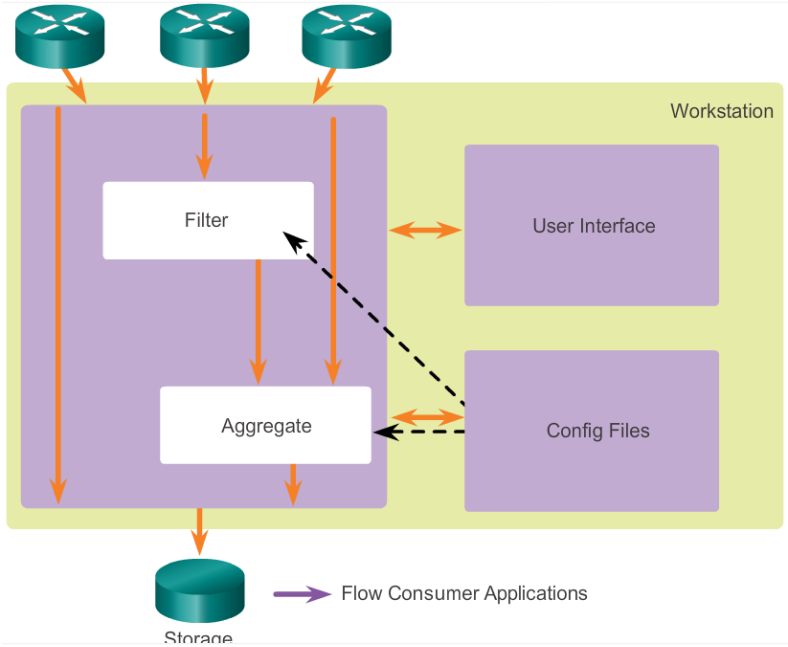
- Network tap (odpočúvacie zariadenie) je **pasívne rozdeľovacie zariadenie** implementované v línii medzi zariadením, ktoré odpočúvame, a sieťou.
- Network tap presmeruje všetku prevádzku **vrátane chýb fyzickej vrstvy** do analytického zariadenia a zároveň umožňuje, aby sa prevádzka dostala aj do pôvodného cieľa.
  - V tomto prípade odbočka súčasne posiela vysielací (**TX**) dátový tok z interného smerovača a prijímací (**RX**) dátový tok do interného smerovača na samostatných, vyhradených kanáloch.
  - Tým sa zabezpečí, že všetky údaje sa dostanú do monitorovacieho zariadenia **v reálnom čase.**
- Network taps sú **fail-safe**, čo znamená, že prevádzka medzi bránou firewall a interným smerovačom nie je ovplyvnená.



Implementácia TAP v jednoduchej sieti

TAP vs Port Mirroring (SPAN) z pohľadu presnosti a strát paketov

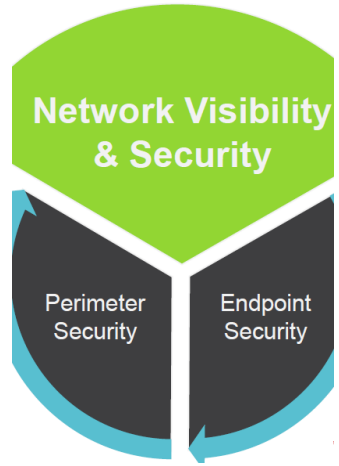
Vlastnosť	TAP (Test Access Point)	Port Mirroring / SPAN
Zpôsob odpočúvania	Fyzicky kopíruje všetky pakety z linky	Softvérovo duplikuje pakety z portu
Strata paketov	Žiadna strata, všetky pakety zachytené	Môžu sa stratiť pri vysokom zaťažení
Vplyv na sieť	Žiadny, transparentný, neovplyvňuje prevádzku	Minimálne, ale pri veľkom množstve prevádzky môže spomaliť
Presnosť dát	Maximálna, vhodné pre forenznú analýzu a monitoring L7	Menej presná, nie vždy zachytí všetky pakety
Cena a implementácia	Vyššia, vyžaduje hardvérové zariadenie TAP	Lacnejšie, využíva existujúci prepínač


Workstation
Filter
User Interface
Aggregate
Config Files
Flow Consumer Applications
Storage

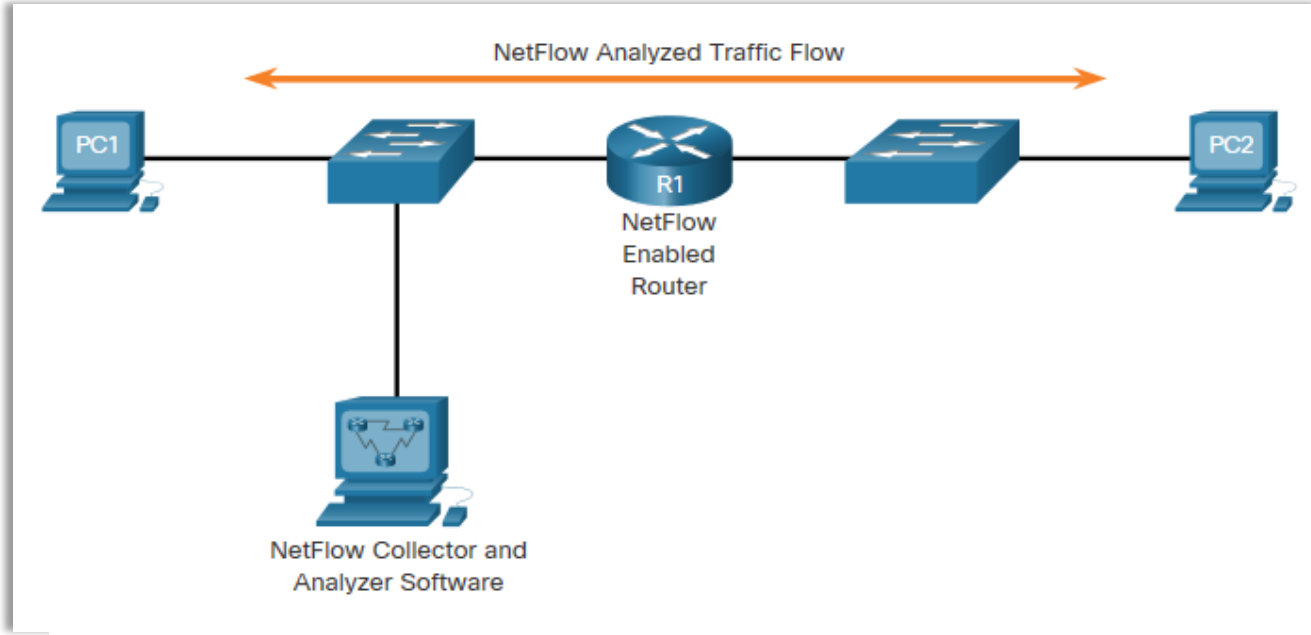
NetFlow

Bezpečnostné služby

NetFlow



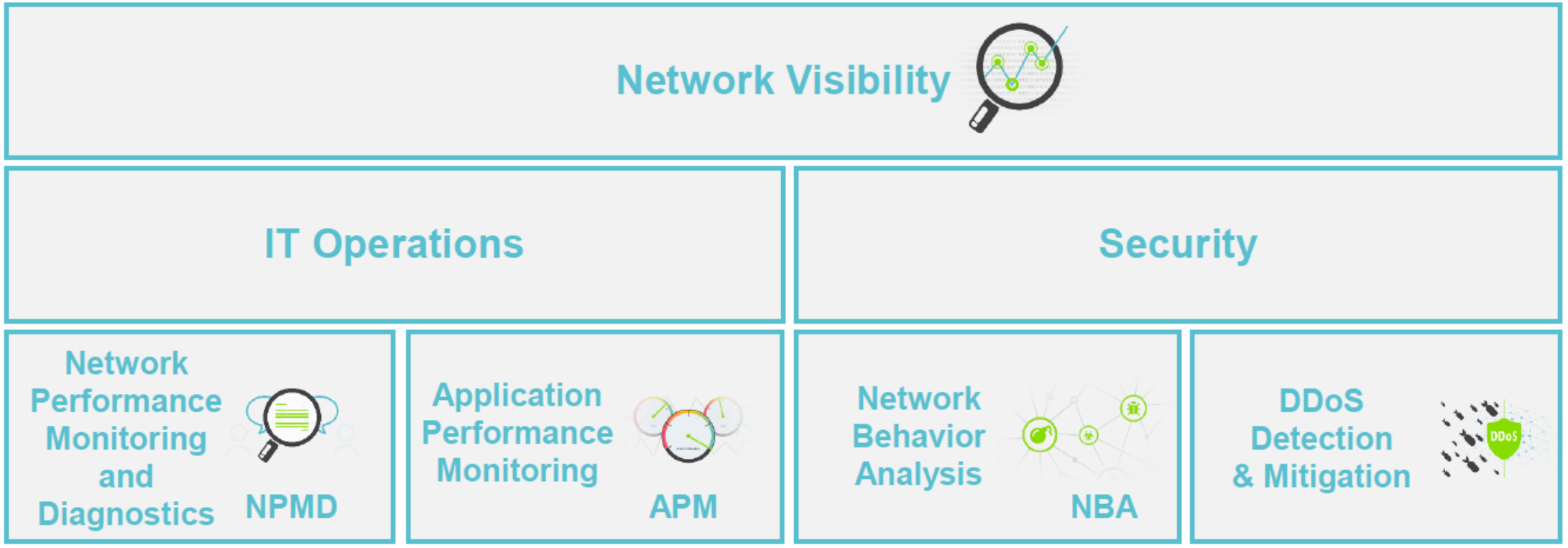
- NetFlow je funkcia, ktorá bola zavedená na Cisco smerovačoch okolo roku 1996 a ktorá poskytuje schopnosť odchytávať sieťovú prevádzku pri vstupe alebo výstupe z rozhrania.
- NetFlow poskytuje dáta, ktoré umožňujú:
  - Monitorovanie siete a jej bezpečnosti,
    - Monitorovanie a diagnostika výkonu siete NPMD (Network Performance Monitoring and Diagnostics)
    - Viditeľnosť a zabezpečenie siete
      - Bezpečnosť na perimetri
      - Bezpečnosť koncových staníc
  - Plánovanie siete
    - aby alokácia zdrojov bola podľa zákazníkových požiadaviek
  - Analýza prevádzky, ktorá má zahŕňať identifikáciu úzkych hrdiel siete
  - IP accounting na účely účtovania poplatkov



PC 1 sa pripája na PC 2 pomocou HTTPS

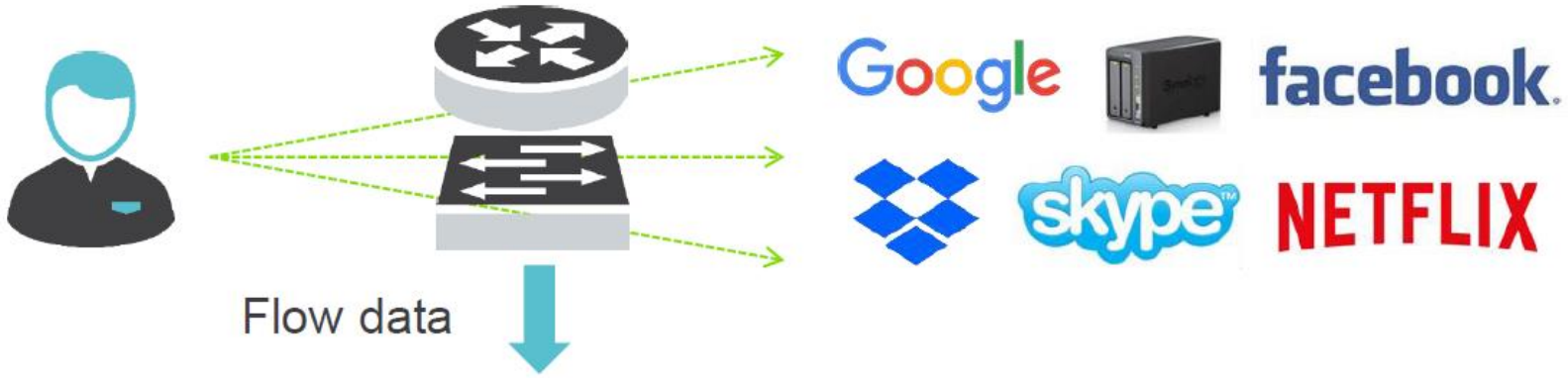
NetFlow

- NetFlow môže monitorovať aplikačné pripojenia, počet prenesených bajtov a počet paketov pre tento individuálny aplikačný tok.
- Potom posiela štatistiky na externý server nazývaný NetFlow collector.
- Nabaliť sa môžu ďalšie iné funkcionality



Čo je Flow Data?

- Moderná metóda monitorovania siete – meranie toku
- Štandard Cisco NetFlow v5 / v9, norma IETF IPFIX
- Zameriava sa na informácie L3 / L4 a objemové parametre
- Pomer reálnej prevádzky k štatistickému toku je 500:1

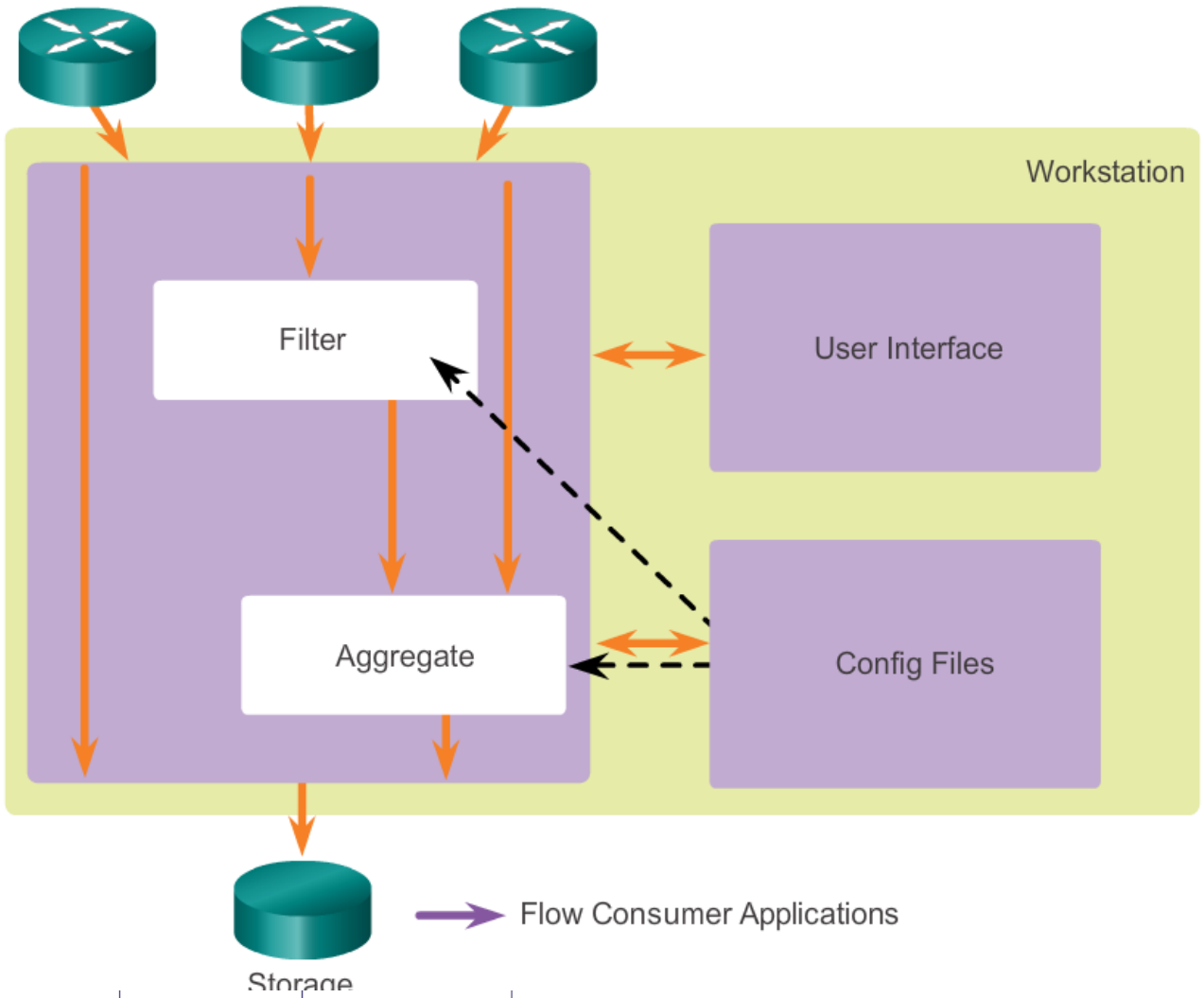


Network Flows

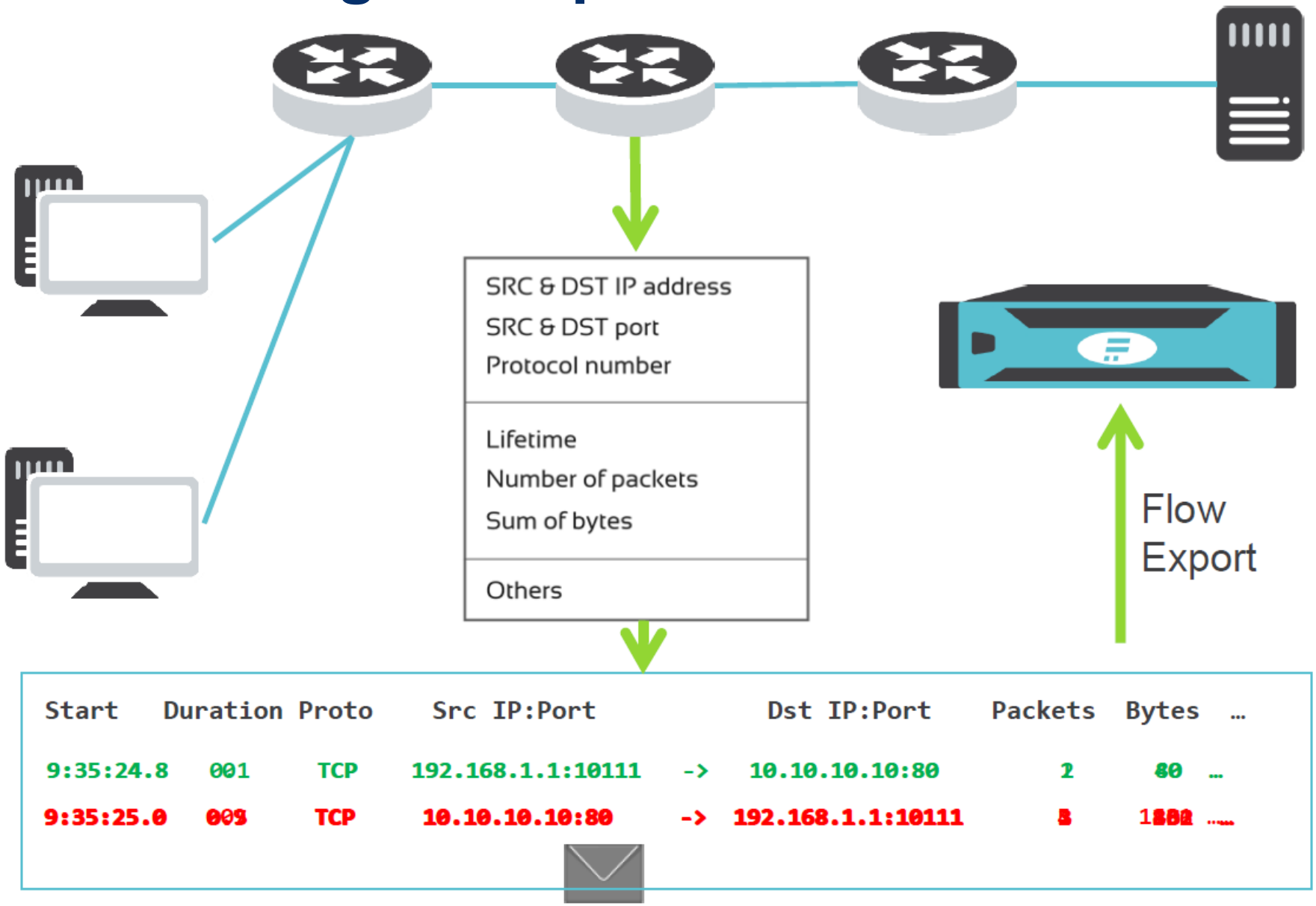
Súčasná NetFlow technológia má za sebou už niekoľko generácií, pričom každá poskytovala sofistikovanejšie definovanie internetovej prevádzky. “Originálny NetFlow“ rozlišoval typ prevádzky pomocou kombinácie siedmych faktorov.

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

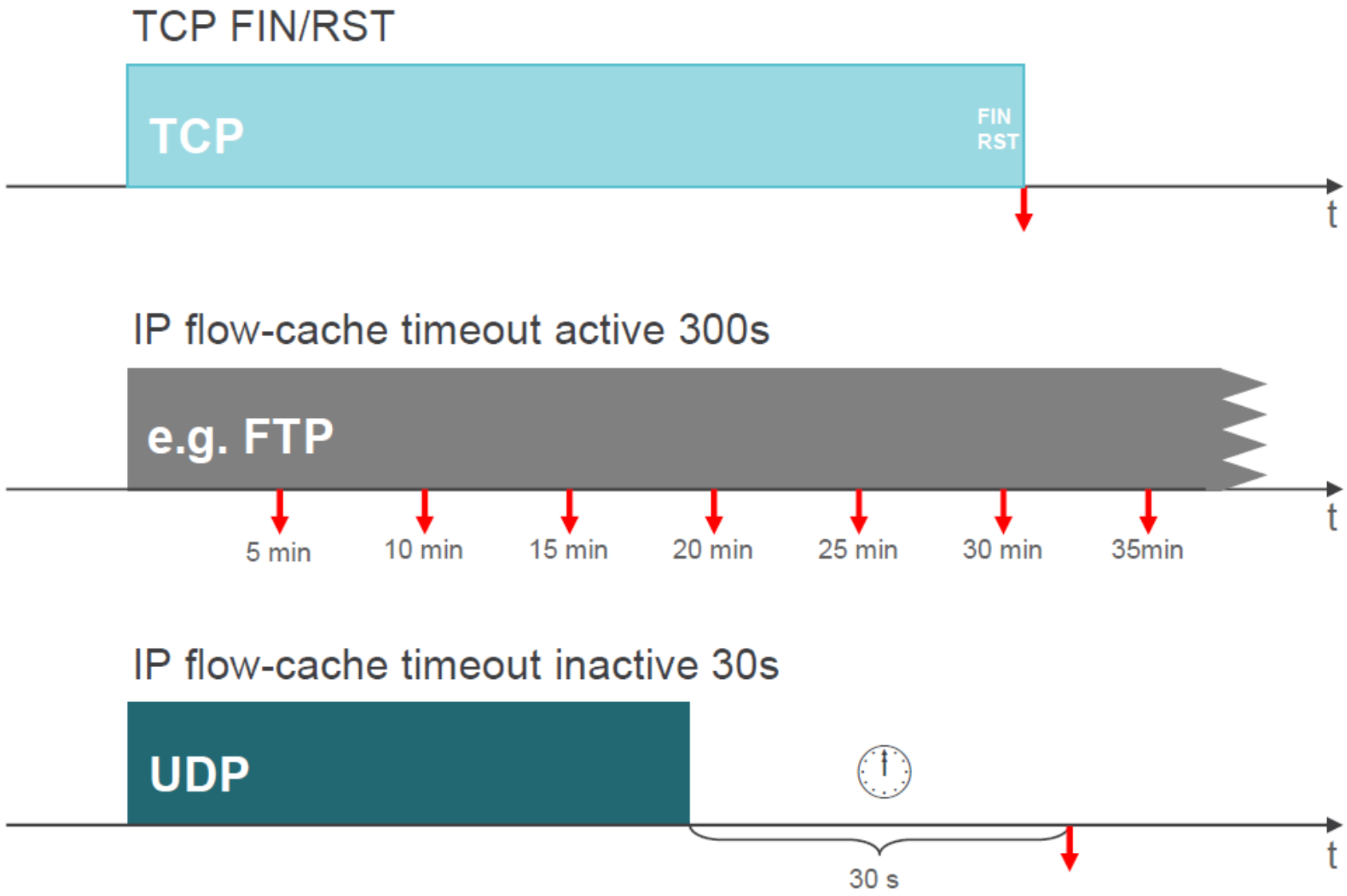
Examining Traffic Patterns
NetFlow Collector Funkcie



Flow Monitoring Principle



Flow Export Principle



Flow Key vs. Non-Key Fields

Flow Key	vs. Non-Key Field
• Packet count • Byte count	• Zdrojová IP adresa • Cieľová IP adresa
• Start sysUpTime • End sysUpTime	• Zdrojový TCP/UDP port • Cieľový TCP/UDP port
• Input ifIndex	• Next hop adresa • Číslo zdrojového AS • Číslo cieľového AS • Zdrojová maska • Cieľová maska • …
• Output ifIndex	
• Type of service	
• TCP flags	
• Protocol	

Flow Standards

Cisco standard	**NetFlow v5**	• fixný formát • dostupné iba základné položky • bez IPv6, MAC, VLANs...
	NetFlow v9 (Flexible NetFlow)	• flexibilný formát pomocou šablón • potrebný pre súčasné požiadavky • podporuje IPv6, MAC, VLANs...
Independent IETF standard	**IPFIX (“NetFlow v10”)**	• budúcnosť monitorovania tokov • viac flexibilný ako NetFlow v9
Huawei	**NetStream**	• rovnaký ako pôvodný Cisco štandard • NetFlow v9
Juniper	**jFlow**	• podobný ako NetFlow v9 • problémy s časovými pečiatkami • obmedzená použiteľnosť

Flow Standards

Related standards	**Cisco – NEL, NSEL**	• používa NetFlow protokol na export firewall alebo NAT udalostí a logov, podobný formát ale odlišná interpretácia a prípady použitia
	sFlow	• funguje na základe vzorkovania paketov • nie je to naozajstný tok, obmedzené použitie • nie je možné použiť na bezpečnostné účely

- **Trendy**
  - Nové monitorované položky (informácie o L7 dátach)
    - NBAR2 (detekcia aplikácií L7), HTTP, …
  - Počet zariadení s využitím tokov stúpa
    - Firewall, UTM, virtualizácia, sieťové zariadenie SMB, …

Netflow versions

Version	Comment
v1	Prvá implementácia, teraz už zastaralá, a obmedzená na IPv4 (bez IP masky and čísiel AS).
v2	Cisco interná verzia, nebola nikdy vydaná.
v3	Cisco interná verzia, nebola nikdy vydaná.
v4	Cisco interná verzia, nebola nikdy vydaná.
v5	Najbežnejšia verzia, dostupná (v roku 2009) na mnohých smerovačoch rôznych výrobcov, ale obmedzená na IPv4 toky.
v6	Už nie je podporovaná spoločnosťou Cisco. Informácie o zapúzdrení (?).
v7	Ako verzia 5 ale s dodatočným poľom o zdrojovom smerovači. Používaná (iba?) na Cisco Catalyst prepínačoch.
v8	Niekoľko agregačných formátov, ale len pre informácie, ktoré sa už nachádzajú v záznamoch verzie 5
v9	Postavená na šablónach, dostupná (v roku 2009) na niektorých nových smerovačoch. Väčšinou sa používa na hlásenie tokov ako IPv6, MPLS, alebo dokonca obyčajný IPv4 s BGP nexthop-om.
v10	Používa sa na identifikáciu IPFIX. Hoci je IPFIX do veľkej miery založený na NetFlow, verzia 10 nemá s NetFlow nič spoločné.

Netflow support by vendors

Vendor and type	Models	NetFlow Version
Cisco IOS-XR routers	CRS, ASR9000 old 12000	v5, v8, v9
Cisco IOS routers	10000, 7200, old 7500	v5, v8, v9
Cisco Catalyst switches	7600, 6500, 4500	v5, v8, v9
Cisco Nexus switches	5600, 7000, 7700	v5, v9
Juniper legacy routers	M-series, T-series, MX-series with DPC	v5, v8
Juniper legacy routers	M-series, T-series, MX-series with DPC	v5, v8, v9
Juniper routers	MX-series with MPC-3D, FPC5 for T4000	v5, IPFIX
Nokia routers	7750SR	v5, v8, v9, v10 IPFIX
Huawei routers	NE5000E NE40E/X NE80E	v5, v9
Enterasys Switches	S-Serie[9] and N-Serie[10]	v5, v9
Flowmon Probes	Flowmon Probe 1000, 2000, 4000, 6000, 10000, 20000, 40000, 80000, 100000	v5, v9, IPFIX
Nortel Switches	Ethernet Routing Switch 5500 Series (ERS5510, 5520 and 5530) and 8600 (Chassis-based)	v5, v9, IPFIX
PC and Servers	Linux FreeBSD NetBSD OpenBSD	v5, v9, IPFIX
VMware servers	vSphere 5.x[16]	v5, IPFIX (>5.1)[17]
Mikrotik RouterOS	RouterOS 3.x, 4.x, 5.x, 6.x [18]	v1, v5, v9, IPFIX (>6.36RC3)

NetFlow - Trendy

NetFlow už nie je len o L3/L4 dátach, ale je kľúčovým nástrojom **pre viditeľnosť L7 aplikácií**, detekciu hrozieb a monitoring **heterogénnych moderných sietí**, vrátane virtualizácie a cloud prostredí.

Trendy v monitoringu sieťových tokov (NetFlow)

1. **Rozšírené monitorované položky**
   - Moderné NetFlow a alternatívy (IPFIX, sFlow) už dokážu zachytiť **informácie až do vrstvy 7 (L7)**:
     - typ aplikácie, URL, metódy HTTP, DNS dotazy, atď.
   - Ide o **deep flow inspection** bez nutnosti full packet capture.
2. **Detekcia aplikácií – NBAR2 a alternatívy**
   - **NBAR2** (Cisco) umožňuje klasifikáciu L7 aplikácií aj pri použití nekonvenčných portov alebo tunelov.
   - Podobné funkcie majú aj moderné firewally a UTM zariadenia pre presnú identifikáciu aplikácií.
3. **Rozširovanie typu monitorovaných zariadení**
   - NetFlow tokmi sa dnes monitorujú nielen tradičné smerovače a prepínače, ale aj:
     - **Firewally a UTM** (kontrola bezpečnosti a aplikácií)
     - **Virtualizované zariadenia a cloud sieťové prvky** (napr. VMware NSX, AWS VPC Flow Logs)
     - **SMB / SOHO / edge zariadenia** s podporou NetFlow/IPFIX
4. **Škálovanie a automatizácia**
   - Počet zariadení a tokov stúpa, preto moderné SIEM a monitoring riešenia využívajú:
     - **Streamovanie dát do centralizovaných platforiem**
     - **Big Data a ElasticSearch backend** pre analýzu miliónov tokov za sekundu
     - **Automatickú detekciu anomálií** na základe NetFlow vzorcov
5. **Integrácia s bezpečnostnými nástrojmi**
   - NetFlow tokmi sa dnes obohacuje **IDS/IPS a UEBA analytika**, umožňujúca detekciu lateral movement, DDoS a ďalších útokov.

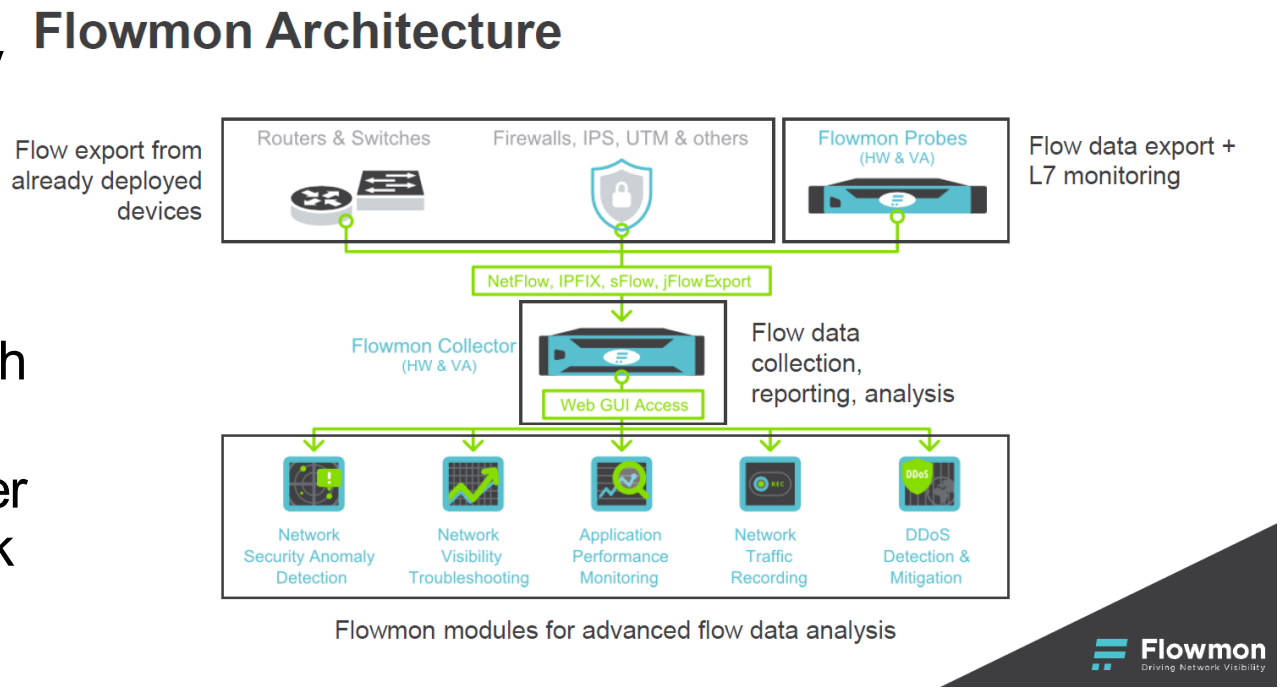
Nové alebo navrhované rozšírenia IPFIX (po roku 2023)

IE = Information Element - jednotlivá dátová položka, ktorá opisuje určitý atribút sieťového toku

- RFC 9487 (november 2023): pridáva IPFIX IEs pre **Segment Routing over IPv6** (SRv6), vrátane informácií zo Segment Routing Headeru.
- RFC 9740 (marec 2025): zavádza nové IEs **pre TCP Options** (tcpOptionsFull) a **IPv6 rozšírené hlavičky** (IPv6 extension headers), nahrádza staré IEs tcpOptions a ipv6ExtensionHeaders.
- RFC 9870 (september 2025): nové IPFIX IEs pre **UDP options**, čo umožňuje exportovať voliteľné polia UDP paketov.
- RFC 9565 (marec 2024): aktualizuje IE tcpControlBits (napr. **zmeny TCP flagov**) pre lepšiu interoperabilitu.
- Návrh (draft) IPFIX – Forwarding Exceptions (2023): predkladá nové IEs, ktoré umožňujú sledovať **chyby smerovania** (napr. packet drops kvôli control-plane entitám).

Príklad jedného nástroja založeného na NetFlow dátach

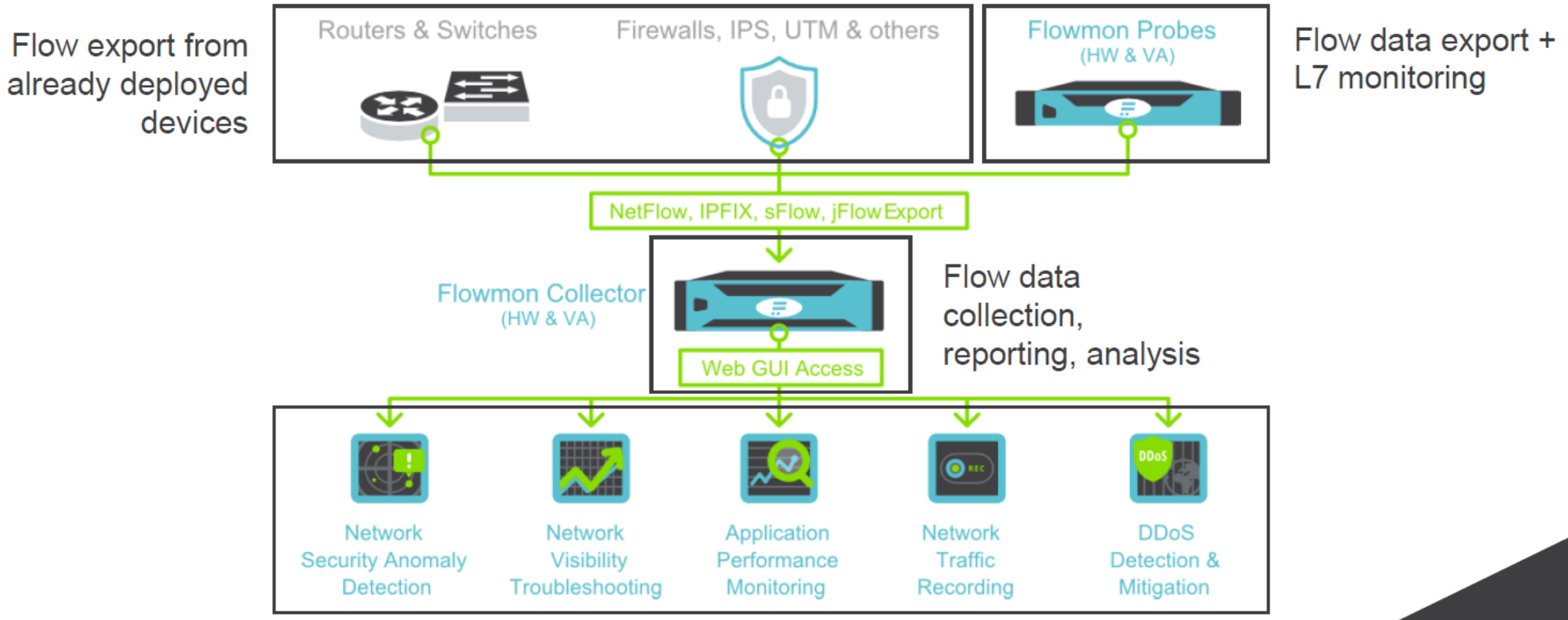
- Skupina vedcov združenia CESNET v ČR v roku 2002 začala projekt Liberouter, z ktorého vzišiel prototyp sieťovej monitorovacej sondy „**FlowMon**“.
- Počas projektu GEANT2 vyvinuli tento prototyp, ktorý sa stal základom komerčných riešení.
- V roku 2012 sa Flowmon umiestnil v Gartner Magic Quadrant v kategórii NPMD (Network Performance Monitoring & Diagnostics).



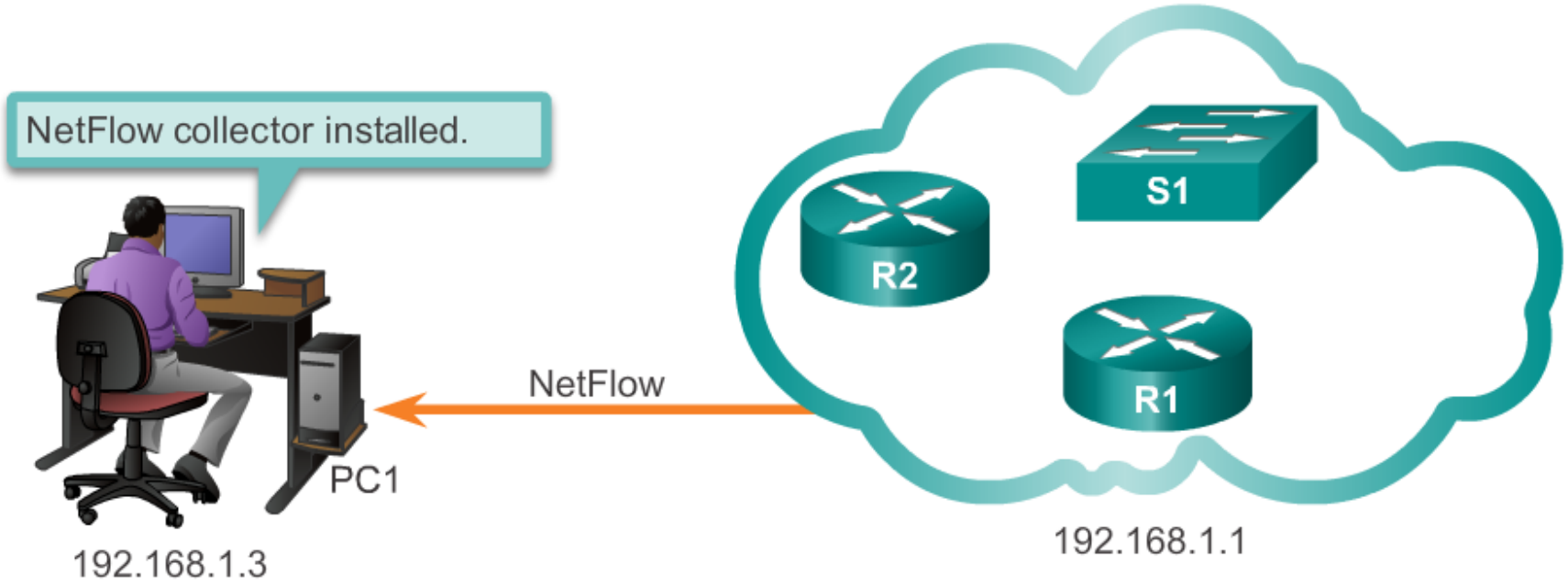
- V novembri 2020 Flowmon Networks získala spoločnosť Kemp Technologies, čím sa spojila expertíza pre load-balancing a bezpečnosť so sieťovou viditeľnosťou.
- V septembri 2021 bol Kemp vrátane Flowmonu prevzatý spoločnosťou **Progress Software**, takže Flowmon je teraz súčasťou portfólia Progressu.
- Dnes sa Flowmon marketingovo označuje ako **Progress Flowmon**, a ich riešenia pokrývajú NPMD, NDR (Network Detection & Response), analýzu anomálií a Flow kolektory.

Príklad jedného nástroja založeného na NetFlow dátach

Flowmon Architecture



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
```

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 analýza s NetFlow Collector

Chart

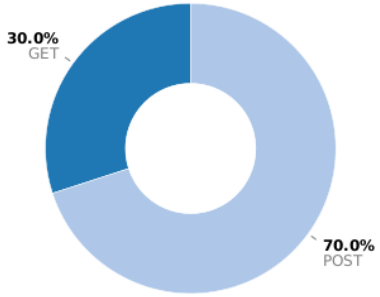
Timeseries

Traffic (Rc
Traffic (Se

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

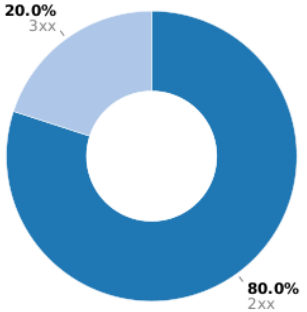
HTTP Queries	Method	Requests
	GET	3
	POST	7
	HEAD	0
	PUT	0
	Other Method	0

Distribution



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

Distribution



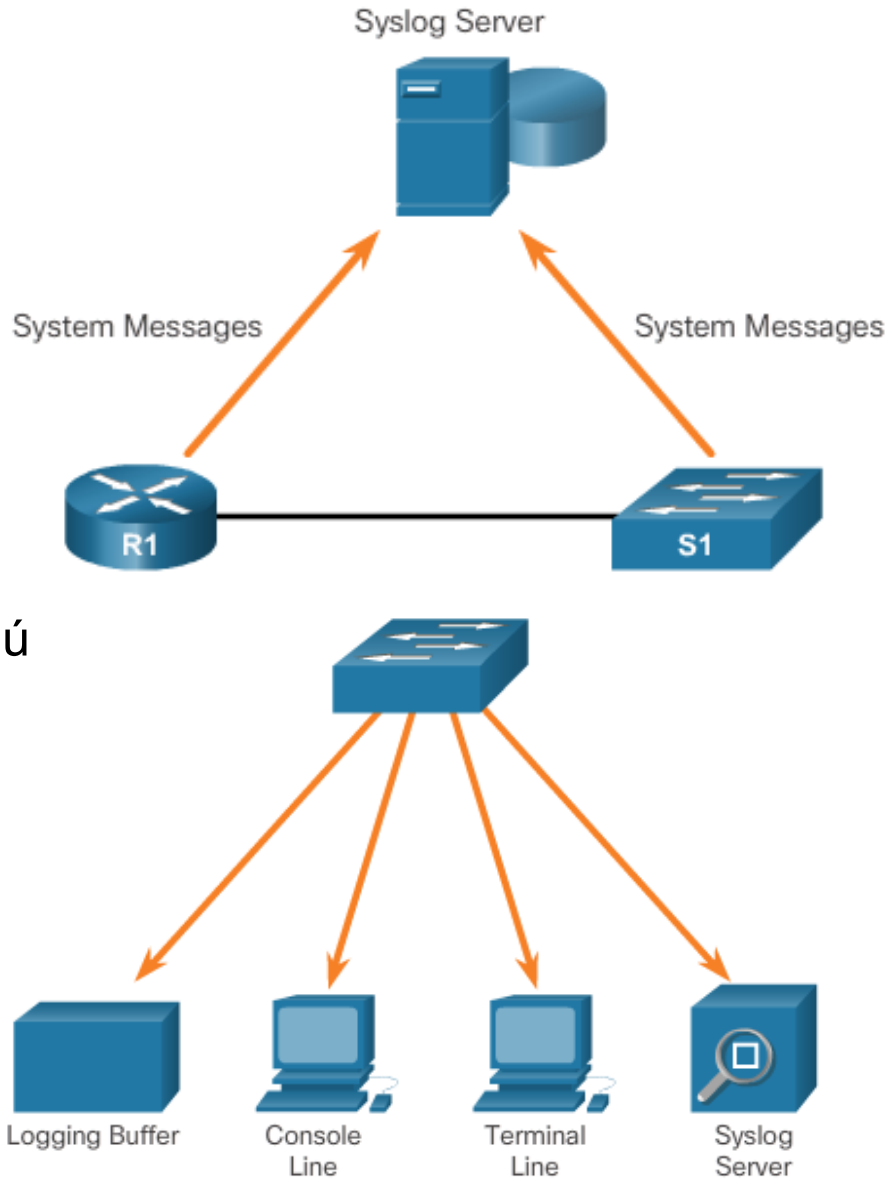
104.27.136.1
104.27.136.111 SSL 3.12 KB

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

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.

Syslog Severity Level

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

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

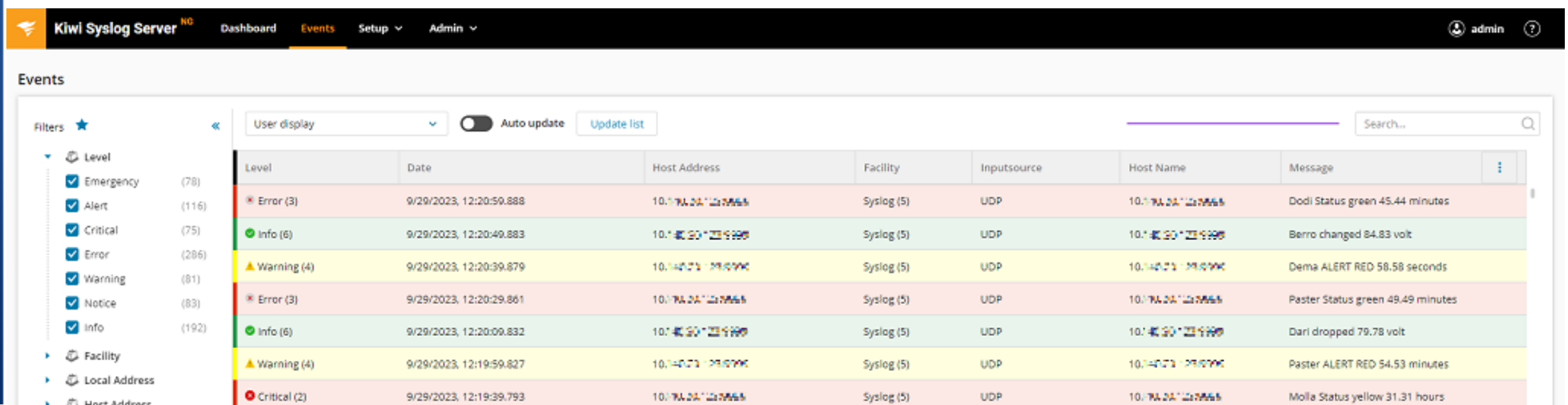
Príkazy smerovačov a prepínačov pre Syslog klientov

```
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#
```

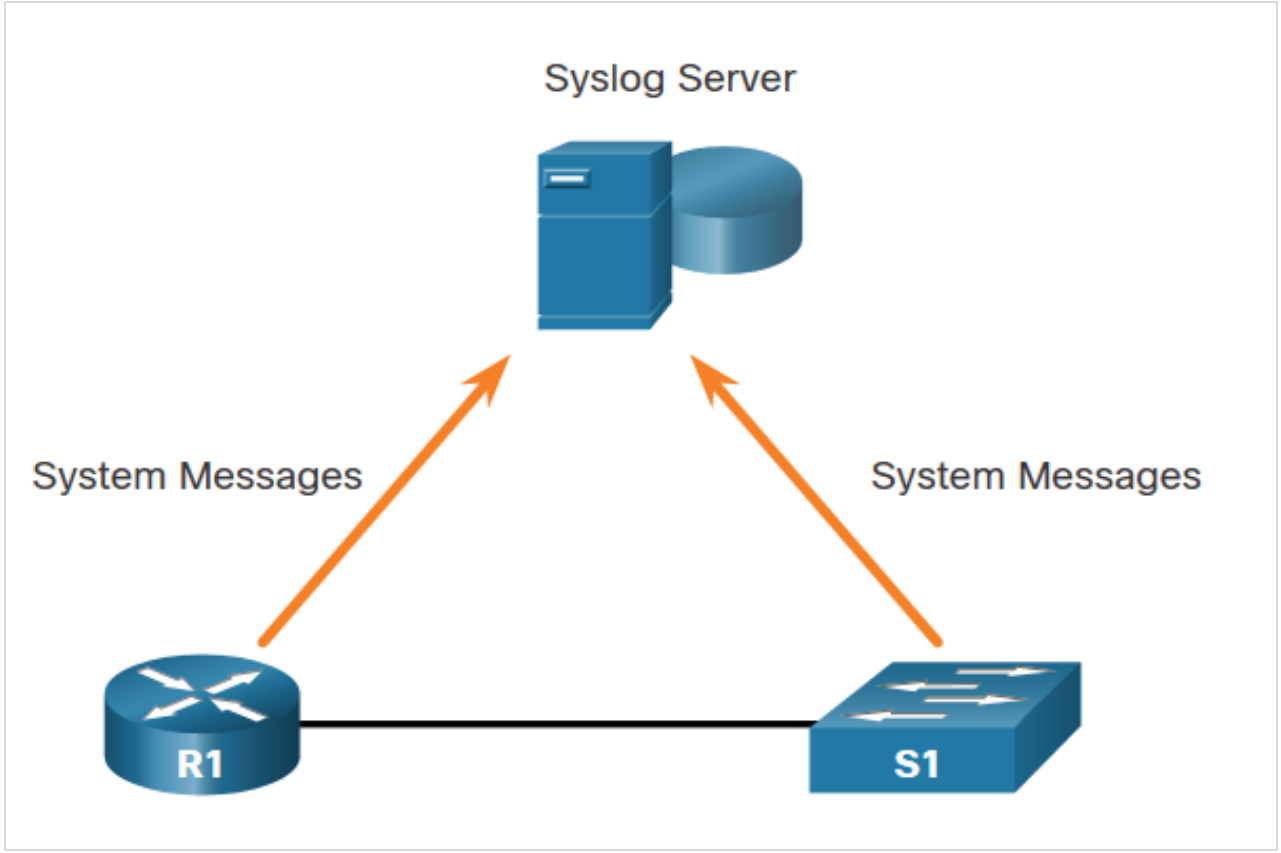
Rôzne projekty: syslog, rsyslog, syslog-ng

- 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

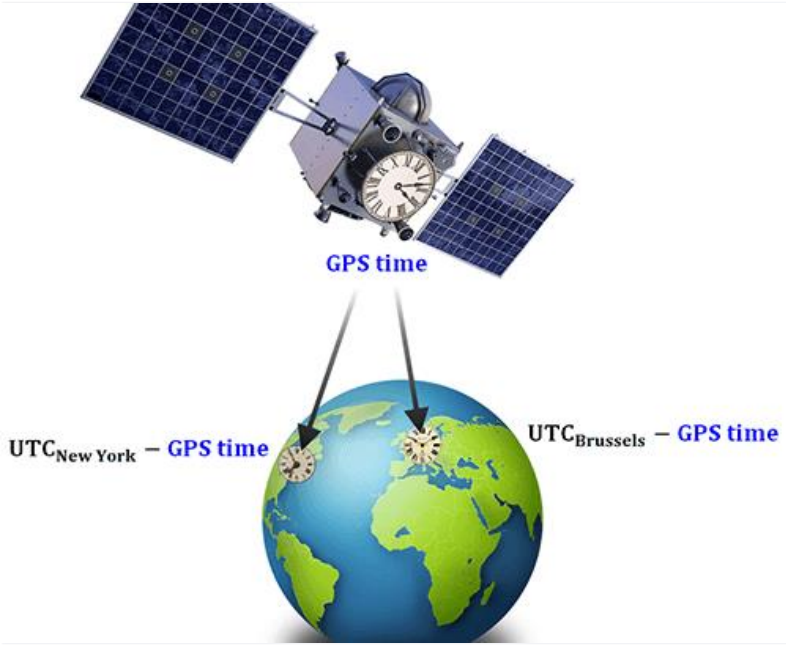
- **Rsyslog**
  - 2004, rozšíril syslog o nové funkcie:
    - Podpora protokolu RELP (application-level ACK)
    - Podpora prevádzky vo vyrovnávacej pamäti

Syslogové servery – sumár funkcií

- Najbežnejšou metódou prístupu k systémovým správam je použitie protokolu syslog
- Protokol syslog umožňuje sieťovým zariadeniam posielať systémové správy cez sieť na syslogové servery
- Zabezpečuje tri hlavné funkcie:
  - Schopnosť zhromažďovať logovacie informácie na účely monitorovania a riešenia problémov
  - Schopnosť vybrať typ zaznamenaných informácií
  - Schopnosť určiť miesto, na ktoré sa systémové správy majú odosielať

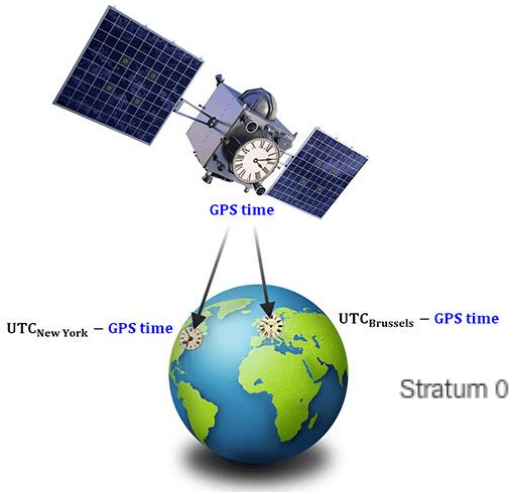


Syslog

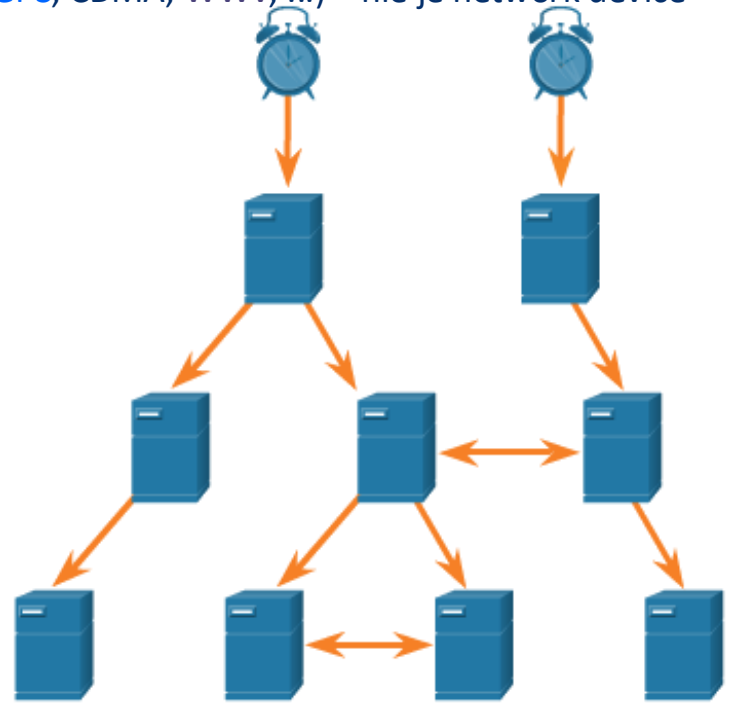


NTP

NTP koncept



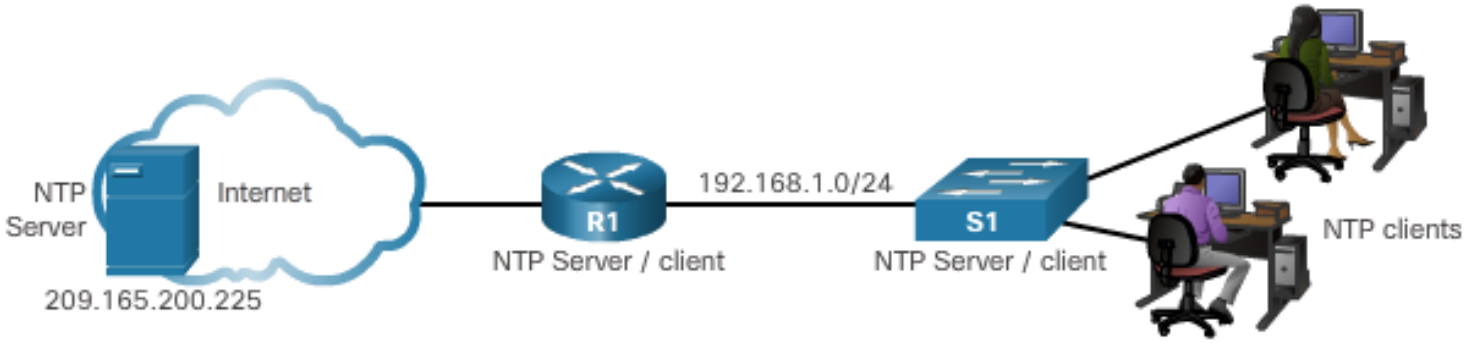
Reference clock (malé, alebo žiadne oneskorenie – GPS, CDMA, WWV, ...) – nie je network device



- Reference clock = stratum 0
  - Spoľahlivý zdroj času UTC
  - Malý alebo žiadny delay
  - Nie sú to zriadenia v sieti
    - ale na ne sa napájajú stratum 1 servery
  - Používa
    - GPS
    - CDMA (Code Division Multiple Access)
    - WWV (broadcasting of time signals, Washington, 50W transmission, 500 m wavelength, dnes v: Fort Collins, Colorado)
      - A iné:Irig-B, DCF77, ..
- Stratum 1
  - Server, ktorý je priamo prepojený na stratum 0 zariadenie – nie cez sieťovú linku!
    - Buď má v sebe stratum 0 zariadenie (EndRun time servers)
    - Ale priamu linku – RS 232 prepoj, alebo cez IRIG-B časové kódovanie
  - je základným štandardom sieťového času
  - Presnosť: 10 mikrosekúnd voči UTC
- Stratum 2
  - Pripojený k stratum 1 cez sieťovú linku (čas dostane cez NTP pakety)
  - Presnosť: 0,5 - 100 ms
- Stratum 3...

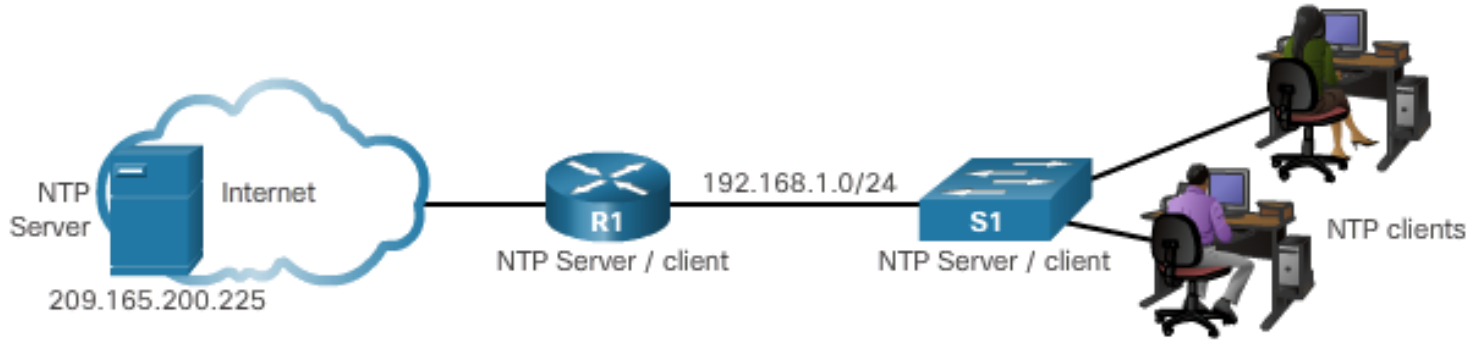
Implementácia NTP

```
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.
```

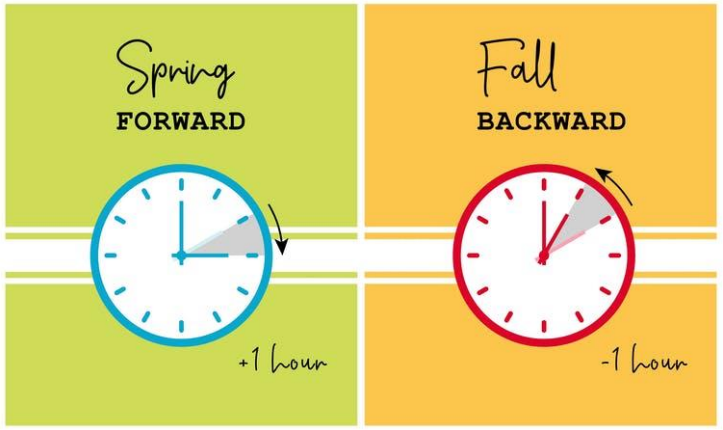
Implementácia NTP

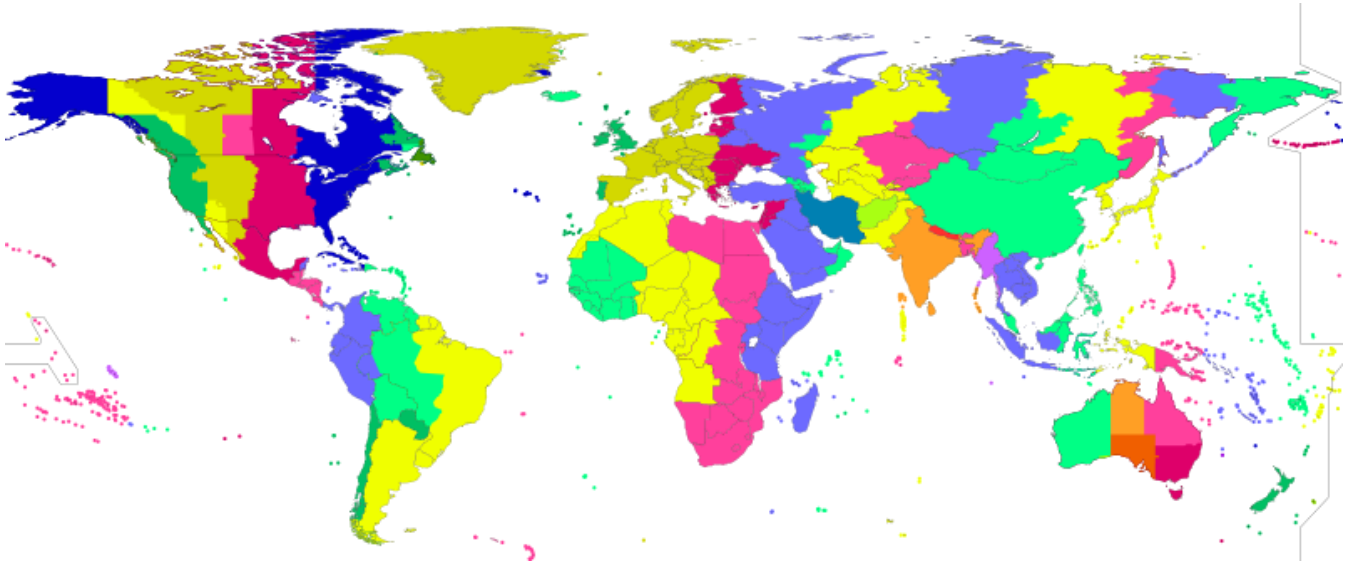



```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations

  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)?

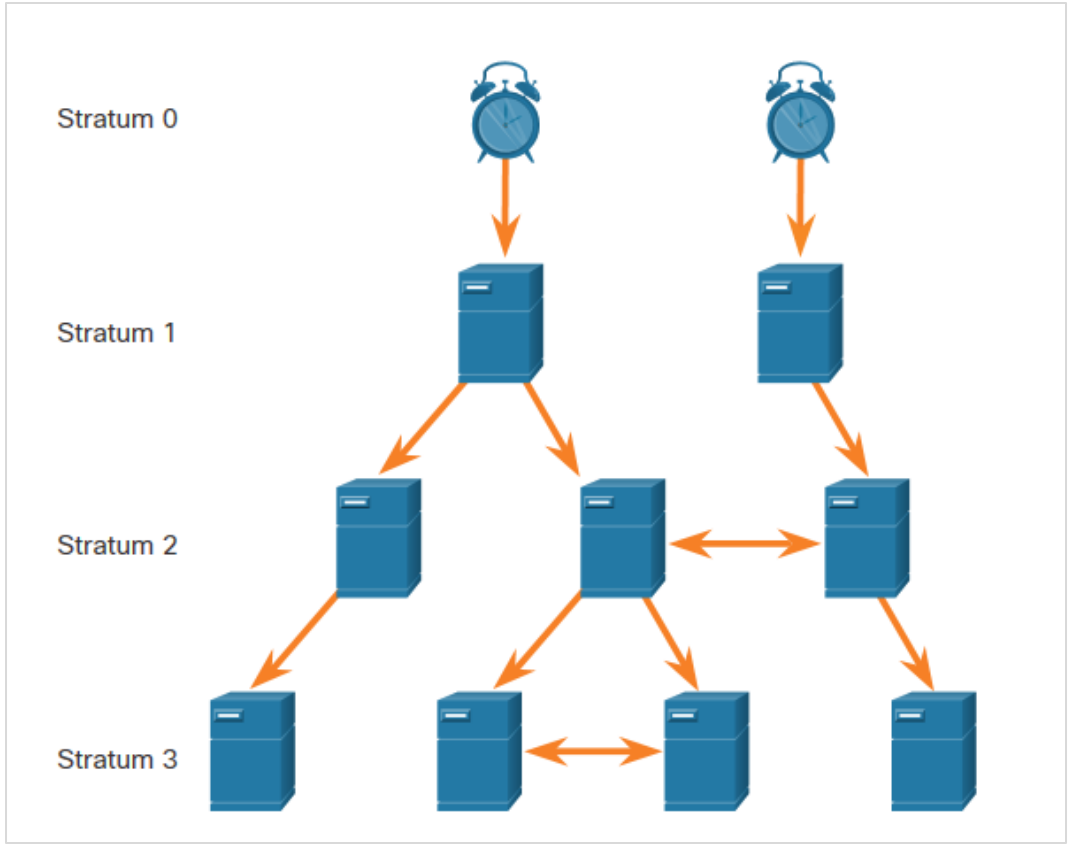
- Daylight saving time (DST)
- Pri NTP nie je potrebné:
  - prepínanie na letný čas
  - nerozlišuje ani časové pásma
- Dôvod:
  - NTP je založený na UTC
  - UTC nemá prechod na letný čas
  - za prechod z/do DST sú výhradne zodpovedné OS serverov a klientov
  - aj za manipuláciu s časovými pásmami





NTP – súhrn vlastností

- Je dôležité synchronizovať čas všetkých zariadení v sieti. Nastavenie dátumu a času na sieťovom zariadení možno vykonať jednou z dvoch metód:
  - Manuálna konfigurácia dátumu a času
  - Konfigurácia pomocou Network Time Protocol (NTP)
- NTP siete používajú hierarchický systém zdrojov času, kde sa každá úroveň v tomto systéme nazýva stratum. Servery NTP sú usporiadané na troch úrovniach známych ako stratum:
  - **Stratum 0**: Sieť NTP získava čas z autoritatívnych zdrojov času.
  - **Stratum 1**: Zariadenia sú priamo pripojené k autoritatívnym časovým zdrojom.
  - **Stratum 2 a vyššie**: Zariadenia stratum 2, ako sú NTP klienti, synchronizujú svoj čas pomocou NTP paketov zo stratum 1 serverov.



NTP Stratum Levels

Otvorená reflexia

Ktorý protokol sa najčastejšie používa na zber metrických údajov o zariadeniach (CPU, RAM, počítadlá na rozhraní)?

- A) Syslog
  B) SNMP
  C) NTP
  D) Port mirroring

Čo je hlavným účelom NetFlow/IPFIX?

- A) Synchronizácia času
  B) Záznam detailov o sieťových komunikáciách
  C) Šifrovanie sieťovej komunikácie
  D) Správa konfigurácie prepínačov

Čo robí Port Mirroring (SPAN)?

- A) Duplikuje vybrané sieťové rámce na monitorovací port
  B) Synchronizuje čas na prepínači
  C) Vytvára záznamy o tokoch paketov
  D) Ukladá logy do centrálneho servera

Ktorá technológia poskytuje najpresnejšie a „bezstratové" odpočúvanie siete?

- A) Port Mirroring
  B) TAP (Test Access Point)
  C) Syslog server
  D) SNMP polling

Na čo slúži protokol NTP?

- A) Zber logov zo zariadení
  B) Synchronizáciu času medzi systémami
  C) Monitorovanie QoS
  D) Zachytávanie paketov

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Koncept funkčného monitorovania

Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza (Blok VI)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk