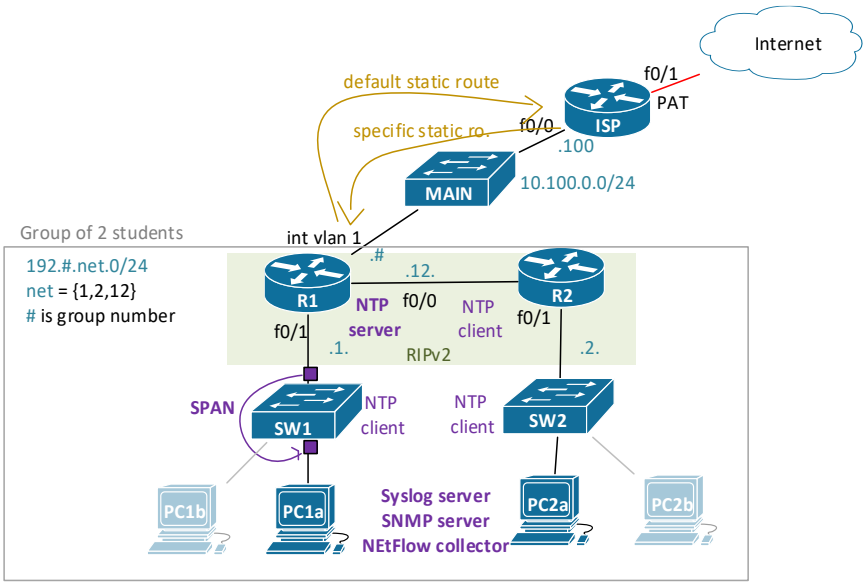
PS1 / Cvičenie 11 / CDP_LLDP_ Syslog_NTP_PasswRecovery_SPAN_SNMP_NetFLow

Topológia



Pozn.: Topológiu rieši dvojica, prípadne trojica, potom pridať jeden R a jeden SW, za R2.

Postup

1. **Základná konfigurácia:**
   a. **Rozdeľte si pridelený IPv4 rozsah** 192.#.net.0/24, kde net je {1, 2, 12} viď obrázok s topológiou, a # je číslo vašej skupiny (dvojica).
   b. **Na prepínačoch**:
      i. Overte či nie je uložený config (`show startup`), a či je prázdna VLAN databáza, ak nie dorieš (`delete vlan.dat, erase startup`)
      ii. Nastavte hostnames SW#1, SW#2
      iii. Zabráňte na prepínačoch výpis hlášok do písaného textu na konzole (zmiešavanie vstupu a výstupu CMD) (line console 0, logging synchronous)
      iv. Vypnite prekladanie doménových mien na IP adresy (no ip domain-lookup)
      v. Zapni RSTP na svojom prepínači
      vi. Skupina, ktorá bude popredu, overí konfiguráciu prepínača MAIN - či je vlan.dat prázdna, či nie je prítomný startup-config, nastaví hostname MAIN-SW a zapne RSTP.
      vii. Kvôli vzdialenému prístupu prideľte prepínaču najvyššiu IPv4 adresu (.254) z danej LAN, nastavte default GW IP, nastavte vty a overte funkčnosť

c. **Na smerovačoch**:
   i. Nastavte hostnames R#1, R#2
   ii. Nastavte IP adresy pre všetky rozhrania
      - Overte stav rozhraní `sh ip int br`, pozrite čo vidieť v smerovacej tabuľke `sh ip route`
   iii. Nakonfigurujte RIPv2 iba vo svojej topológii, nie smerom k hlavnému prepínaču!
      - Over konektivitu medzi PCs
   iv. Na **R1** nastavte default route cez ISP (10.100.0.100)
   v. Na **R1** oznamujte default static route v RIPv2 updatoch (`default-information originate`)
      - Na R2 overte, či v smerovacej tabuľke vidíte redistribuovanú default static route z R1 (riadok **R***)
   vi. Skupina, ktorá je popredu dokonfiguruje ISP smerovač:
      - Neukladajte konfiguráciu! len tam doplňte:
      - PAT na IP výstupného rozhrania f0/1.
         - Pozor červený kábel, ktorý vedie do internetu musí byť na ISP smerovači v f0/1
         - PAT premysli ako, aby išli pingy do inetu aj z R1! nielen z PCs a R2, over či funguje
      - Statické cesty do topológií jednotlivých skupín (192.#.0.0/16), toľko, koľko je skupín
   vii. Skontrolujte obsah smerovacích tabuliek a otestujte konektivitu do internetu z PCs

2. CDP, LLDP (LLDP nemusí byť podporované na všetkých zariadeniach)
   a. Najprv na smerovačoch:
   b. Over či beží CDP (`show cdp`) a zisti ako často sa posielajú CDP pakety.
   c. Vypni CDP (`no cdp run`), a pozri výpis show cdp
   d. Následne CDP znova zapni (`cdp run`)
   e. Pozri na ktorých rozhraniach CDP beží (`show cdp interfaces`)
   f. Preskúmaj okolité zariadenia pomocou informácií získaných z CDP správ (`show cdp neighbors`)
      i. Zisti hostname a platformy daných zariadení
      ii. Čo sa stane keď hodnota v sĺpci Holdtime (timer) klesne na 0 pre nejakého suseda?
      iii. Vieš zistiť aj IP adresy daných susedov?
   g. Zisti detailné info o susedoch cez cdp (`show cdp neighbors detail`)
      i. Vieš zistiť aj IP adresy daných susedov?
      ii. Vieš zistiť verziu IOSu susedov?
      iii. Ukazuje ti aj IP adresy prepínačov?
   h. Na R1 vypnite cdp na rozhraní vedúce k MAIN prepínaču (int f0/), over funkčnosť (`show cdp neighbors, show cdp interface`)
   i. Preskúmaj na svojom PC vo Wiresharku CDP správy
      i. V čom sú enkapsupované?
      ii. Kam sa posielajú?
      iii. Aké info nesú?
      iv. Ako často chodia?

j. Ďalej na prepínačoch:
k. Z bezpečnostných dôvodov vypnite CDP na všetkých rozhraniach okrem rozhrania vedúceho k smerovaču. (`int range ..., no cdp enable`)
   i. Over znova na PC vo Wiresharku, že CDP už prestali chodiť
l. Zisti aký je rozdiel medzi `clear cdp counters`, a `clear cdp table`
   i. Najprv si over, čo vidíš, až potom rob clear..
m. Zopakuj celý postup a. až k. pre LLDP protokol. LLDP je vendor-neutral, CDP je Cisco-proprietary.
   i. Niekde nemusí byť LLDP podporované na Cisco zariadeniach, over.
   ii. Použi `show lldp, lldp run, lldp transmit, lldp receive, show lldp neighbors`

3. NTP

a. Na R1 aj R2 over aký máš nastavený dátum a čas (`show clock`).
   i. Je aktuálny?
   ii. Je správne nastavená časová zóna?
b. Nastav na R1 správny dátum a čas (`clock set ...`), na R2 sa schválne pomýľ a posuň rok na 2000. Ak je potrebné, dá sa zmeniť aj časová zóna (`clock timezone ..`)
   i. Over zmenený čas (`show clock`)
c. Over na oboch smerovačoch či beží NTP služba (`show ntp status`)
   i. Over že kvôli tomu ani nemáš s nikým zatiaľ vytvorené žiadne NTP spojenia, so žiadnym NTP serverom (`show ntp associations`)
d. Nastav aby R1 bol NTP server, nešpecifikuj stratum
   i. Najprv zisti voliteľné parametre príkazu: `ntp master ?`
   ii. Potom nastav R1 ako NTP server: `ntp master` (bez voľby len enter))
   iii. Over nastavenia na R1 (`show ntp status`)
      - Toto bude zaujímavé pozrieť neskôr na R2, ktorý bude NTP clientom, ale aby sme videli rozdiel, čo vidieť vo výpise z pohľadu servera, pozri na R1: `show ntp status, show ntp associations`
        - Aká je stratum na serveri? Čo to znamená?
e. Nastav, aby R2 bol NTP client a čas si nastavil z NTP servera na R2
   i. Na R2: `ntp server 192.#.12.1` (IP adresa NTP servera)
   ii. Over a porovnaj časy na oboch smerovačoch (`show clock`)
   iii. Over a porovnaj na oboch smerovačoch výpisy pre NTP službu a NTP spojenia (`show ntp status, show ntp assoc`)

4. Syslog (robia obaja z dvojice na svojom smerovači a svojom PC)

a. Console logging
   i. Over a uvedom si zobrazovanie Syslog správ v CLI console:
      - Na smerovači (R1 aj R2) vytvor Loopback rozhranie (`int lo 0`), znova ho zruš (`no int lo 0`), odsleduj výpisy – Syslog správy.
      - Na R1 vypni rozhranie k MAIN prepínaču, a znova ho zapni, odsleduj Syslog správy.
   ii. Syslog správa môže obsahovať aj pečiatku s dátumom a časom, čo je aj vhodné, keď neskôr budeme chcieť Syslog správy posielať niekam na Syslog server (bod c.), alebo ukladať do lokálneho buffra na zariadení (bod b.)
      - Overte, že aktuálne používanie časových pečiatok nie je aktivované (`show run`, hľadaj na začiatku výpisu: `no service timestamps log datetime msec`)

Komentár od [JU1]: Syslog messages that are generated by the network devices can be collected and archived on a syslog server. The information can be used for monitoring, debugging, and troubleshooting purposes. The administrator can control where the messages are stored and displayed. Syslog messages can be time-stamped for analysis of the sequence of network events; therefore, it is important to synchronize the clock across the network devices with a Network Time Protocol (NTP) server.

- Over default nastavenia pre Syslog, cez `show logging`, zatiaľ pozri len časť `Console logging`, a pozri, či: `Count and timestamp logging messages: disabled`
- Nastavte používanie časových pečiatok pre Syslog správy
  - Odporúčame si pozrieť na mieste `log, datetime` a `msec` najprv overiť možnosti cez `?` a následne vybrať finálne túto voľbu: `service timestamps log datetime msec`
  - over v konfigurácií (`show run | include timestamp`)
- Na smerovači (R1 aj R2) vytvor Loopback rozhranie (`int lo 1`), znova ho zruš (`no int lo 1`), odsleduj výpisy – Syslog správy na console.
  - Obsahuje už teraz syslog správa aj čas a je aktuálny?

b. Buffer logging
   i. Over nastavenia a Syslog správy uložené v lokálnej databáze na zariadení (buffer): `show logging`, a zameraj sa na `Buffer Logging: ...` vo výpise
      - Vidíš tam aj tie syslog správy (na konci výpisu za `Log Buffer (4096 bytes): ...`), ktoré boli výsledkom tvojej akcie v bode 4.a.i.?
        - Ak nie, aktivuj ukladanie syslog správ do lokálneho buffra (`R(config)#logging buffer`)
        - Over zmeny nastavení, a zopakuj bod 4.a.i, a opätovne pozri na koniec výpisu (`show logging`)
        - Over čo všetko sa dá ešte nastaviť príkazom logging (`R(config)#logging ?`)

c. Monitor logging
   i. Pozri ešte raz výpis `show logging`, ale teraz sa zameraj na `Monitor Logging: ...` vo výpise, pre pohľad na default nastavenia
   ii. Prihláste sa vzdialene na smerovač (alebo prepínač)
   iii. Zopakujte krok a.i. (ale zmeň číslo rozhrania na `int lo 3`, alebo zapni a vypni akékoľvek iné rozhranie)
      - Prečo nevidieť žiadne Syslog správy?
      - Zapni aj napr. debugovanie RIP updatov (`debug ip rip`). Rovnako nebudeš zatiaľ nič vidieť.
   iv. Zabezpečte zobrazovanie Syslog správ aj cez telnet
      - Musíš sa vzdialene prihlásiť na smerovač co svojho PC (ak si sa medzi tým odhlásil/a) a použiť príkaz (R#`terminal monitor`)
      - over, že teraz syslog správy budú viditeľné – mal/a by si vidieť RIP updates, následne môžeš debug vypnúť (`undebug all`) a over aj Syslog UPDOWN správy - vypni/zapni rozhranie `loopback 4`, ...
   v. Over správy aj cez `show logging`, pokús sa špecifikovať napr:
      - `show logging | include changed state to up`
      - `show logging | include RIP`
      - `show logging | begin RIP`

d. Syslog server logging
   i. Nájdite a spustite TFTPd utilitu na ploche (ak nemáš, zisti či nemá spolužiak z dvojice, ak ani ten, doinštaluj s pomocou učiteľa), prepnite záložku na Syslog server (na minulých cvičeniach sme používali TFTP server).
      - Nastav `Server interfaces` na IP adresu tvojho PC (Cisco NIC)
      - `Current Directory` zmeň na niečo v .. Student\Documents

Komentár od [JU2]: R1#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 9 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 9 messages logged, xml disabled,
filtering disabled
Buffer logging: disabled, xml disabled,
filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
Trap logging: level informational, 9 message lines logged

Komentár od [JU3]: Schválne je tu 1, a nie 0 ako sme robili vyššie

Komentár od [JU4]: R1(config)#logging ?

A.B.C.D IP address of the logging host
Buffered Set buffered logging parameters
console Set console logging parameters
host Set syslog server IP address and parameters
on Enable logging to all enabled destinations
trap Set syslog server logging level
userinfo Enable logging of user info on privileged mode enabling

ii. Aktuálne máš zapnuté služby časových pečiatok, takže Syslog správy, ktoré budeš posielať, budú obsahovať info o dátume a čase. (`show run | include timestamp`)
iii. Nakonfiguruj svoj smerovač, aby posielal syslog správy na Syslog server, ktorý ti beží na PC v TFTPd utilite
- Nastav cieľ, t.j. kde bude smerovač posielať syslog správy (`logging host IP_adresa_PC`)
- Over nastavenie (`show logging`, hľadaj `Trap logging:` .. a `Logging to`..)
  - Je tam viditeľná IP adresa syslog servera?
  - Aká protokol a port používa syslog?
  - Pre aký severity level je aktuálne zapnuté posielanie syslog trap správ?
- Overte aké možnosti máte pri výbere severity levelu (`R(config)# logging trap ?`)

iv. Zmeňte severity level na 4=warnings (`R(config)# logging trap 4` alebo `R(config)# logging trap warrnings`)
- Zopakujte krok 4.a.i. (ale zmeň číslo rozhrania na `int lo 4`, alebo zapni a vypni akékoľvek iné rozhranie)
- Prečo nevidieť žiadne Syslog správy?
- Zapni aj napr. debugovanie RIP updatov (`debug ip rip`). Rovnako nebudeš nič vidieť.
- Na záver zmeň severity level na 6 (debugging správy nebudeme posielať na syslog server)

e. pridajte aj prepínač pre posielanie syslog správ na Syslog server (na svoje PC)
   i. over funkčnosť

5. Password recovery
   a. lab 10.3.1.11
   b. zrealizuj to na smerovači aj prepínači - návod je aj na nástenke v B303 (nakoniec vráť späť hodnotu konfiguračného registra - 0x2102)

6. SPAN (Port Mirroring)
   a. lab 5.3.2.3
   b. monitoruj port idúci zo svojho prepínača na smerovač, a všetku prevádzku posielaj cez jeden port k PC (pozor, daný port na PC už nebude štandardne funkčný, bude fungovať iba pre SPAN, nebudete vedieť pingnúť PC od nikadiaľ)
   c. na záver (t.j. keď pôjdeš na bod 7) sa prepni (PC) do iného portu na prepínači, takého kde nemáš nastavený SPAN port, aby si mal/a zase konektivitu do topológie

7. SNMP
   a. lab 5.2.2.6
   b. použi iReasoning MibBrowser na ploche (alebo dohľadaj v programoch) a ďalšie info k nemu:
      i. stačí keď použijete SNMP ver. 1, Windows Firewall vyššie verzie blokuje, a bolo by ho potom treba vypnúť (s pomocou učiteľa, ale na konci cvičenia nezabudnúť znova zapnúť !!)
      ii. vytvorte si aj read aj write community
      iii. pre čítanie (GET) objektov zo smerovača:
      `MIB > iso > interface > ifTable > TableView`
      iv. pre zapisovanie (SET) do objektov na smerovači: zober ako index číslo riadku
      - objekt, ktorý sa dá prepisovať, má na začiatku ikonku pera

Komentár od [JU5]: Syslog Severity

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

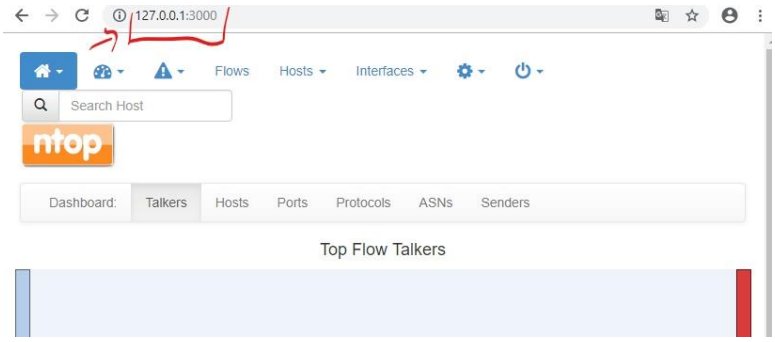
- napr. Stav rozhrania vieme prepísať
  - over po SET, priamo na smerovači

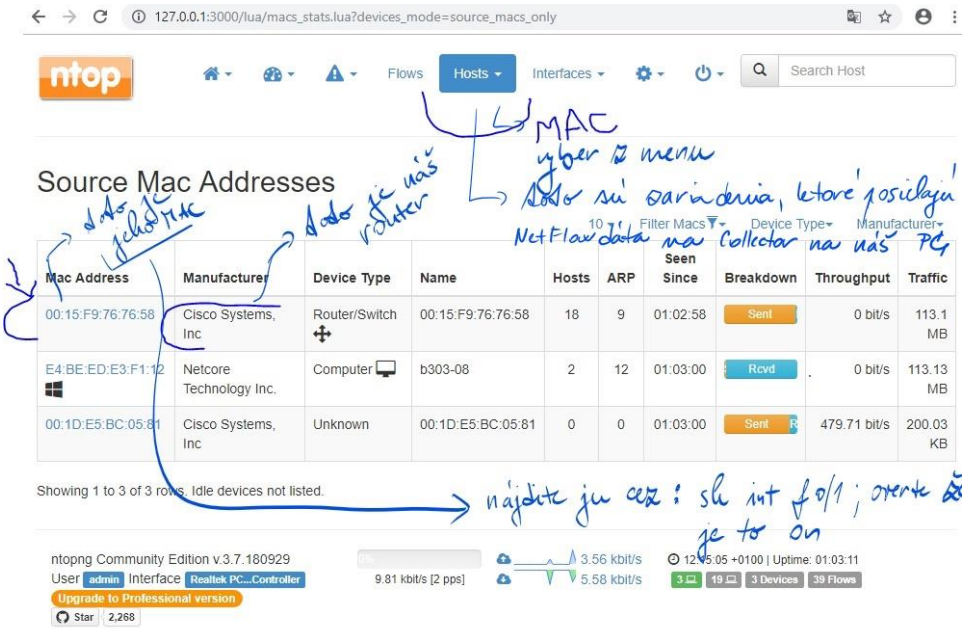
8. NetFlow

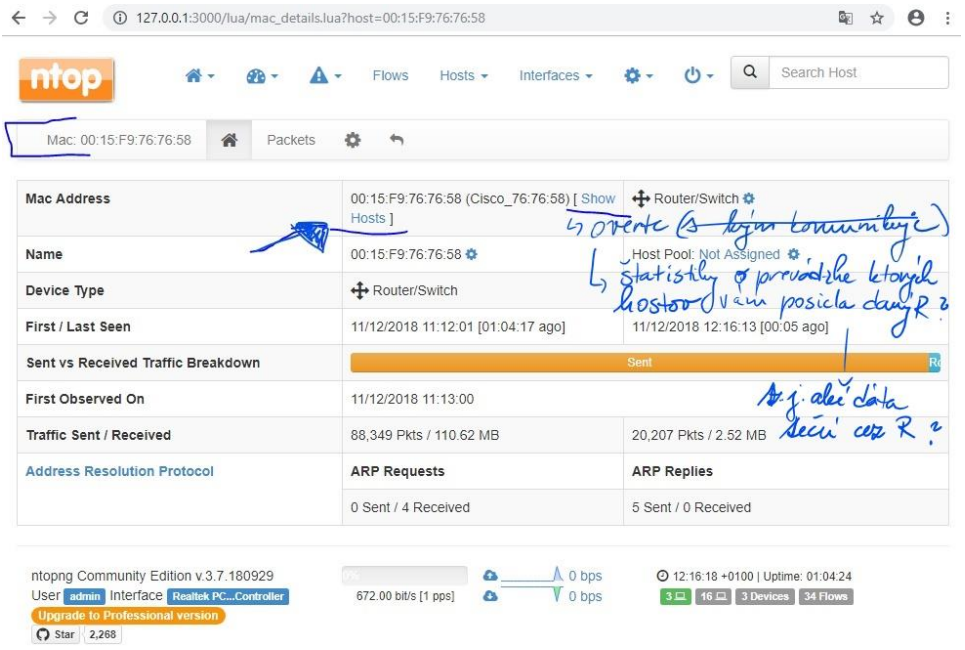
a. Použi návod: Configuring NetFlow.pdf, ale s touto zmenou:

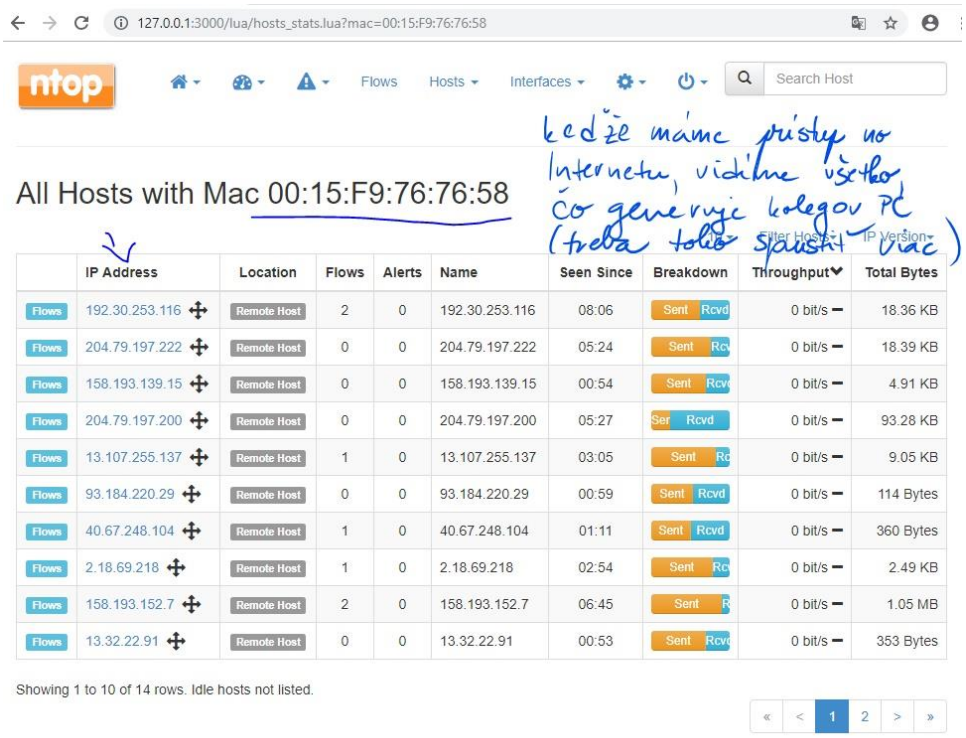
b. Part 4 - Freeware NetFlow software available: na PC by mal byť nainštalovaný NTOP, stačí jeden v dvojici (ak nie je, doinštaluj s pomocou učiteľa). Následne viete zrealizovať min. tieto kroky:

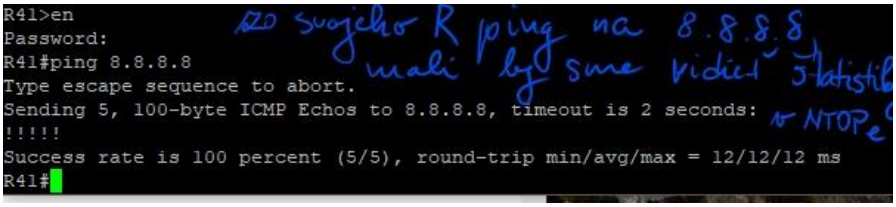
Do prehliadača zadajte:

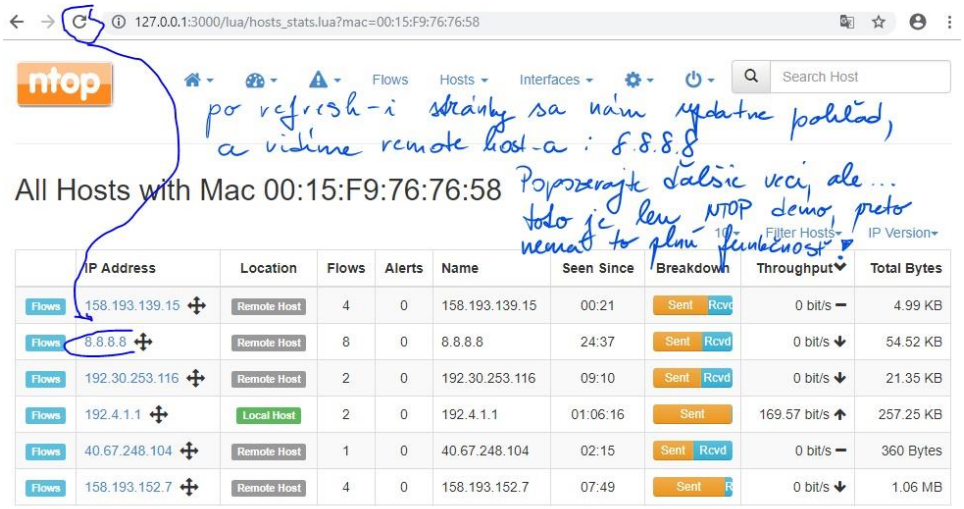





127.0.0.1:3000/lua/mac_details.lua?host=00:15:F9:76:76:58
ntop
Flows
Hosts
Interfaces
Search Host
Mac: 00:15:F9:76:76:58
Packets
Mac Address
00:15:F9:76:76:58 (Cisco_76:76:58) [Show Hosts]
Router/Switch
Name
00:15:F9:76:76:58
Host Pool: Not Assigned
Device Type
Router/Switch
First / Last Seen
11/12/2018 11:12:01 [01:04:17 ago]
11/12/2018 12:16:13 [00:05 ago]
Sent vs Received Traffic Breakdown
Sent
First Observed On
11/12/2018 11:13:00
Traffic Sent / Received
88,349 Pkts / 110.62 MB
20,207 Pkts / 2.52 MB
Address Resolution Protocol
ARP Requests
ARP Replies
0 Sent / 4 Received
5 Sent / 0 Received
ntopng Community Edition v.3.7.180929
User admin Interface Realtek PC...Controller
Upgrade to Professional version
Star 2,268
672.00 bit/s [1 pps]
0 bps
0 bps
12:16:18 +0100 | Uptime: 01:04:24
3 16 3 Devices 34 Flows


127.0.0.1:3000/lua/hosts_stats.lua?mac=00:15:F9:76:76:58
ntop
Flows
Hosts
Interfaces
Search Host
keďže máme prístup na Internetu, vidíme všetko čo generuje kolegov PC (treba tolko spustit viac)
All Hosts with Mac 00:15:F9:76:76:58
Filter Hosts
IP Version
IP Address | Location | Flows | Alerts | Name | Seen Since | Breakdown | Throughput | Total Bytes
Flows | 192.30.253.116 | Remote Host | 2 | 0 | 192.30.253.116 | 08:06 | Sent Rcvd | 0 bit/s | 18.36 KB
Flows | 204.79.197.222 | Remote Host | 0 | 0 | 204.79.197.222 | 05:24 | Sent Rcvd | 0 bit/s | 18.39 KB
Flows | 158.193.139.15 | Remote Host | 0 | 0 | 158.193.139.15 | 00:54 | Sent Rcvd | 0 bit/s | 4.91 KB
Flows | 204.79.197.200 | Remote Host | 0 | 0 | 204.79.197.200 | 05:27 | Rcvd | 0 bit/s | 93.28 KB
Flows | 13.107.255.137 | Remote Host | 1 | 0 | 13.107.255.137 | 03:05 | Sent Rcvd | 0 bit/s | 9.05 KB
Flows | 93.184.220.29 | Remote Host | 0 | 0 | 93.184.220.29 | 00:59 | Sent Rcvd | 0 bit/s | 114 Bytes
Flows | 40.67.248.104 | Remote Host | 1 | 0 | 40.67.248.104 | 01:11 | Sent Rcvd | 0 bit/s | 360 Bytes
Flows | 2.18.69.218 | Remote Host | 1 | 0 | 2.18.69.218 | 02:54 | Sent Rcvd | 0 bit/s | 2.49 KB
Flows | 158.193.152.7 | Remote Host | 2 | 0 | 158.193.152.7 | 06:45 | Sent Rcvd | 0 bit/s | 1.05 MB
Flows | 13.32.22.91 | Remote Host | 0 | 0 | 13.32.22.91 | 00:53 | Sent Rcvd | 0 bit/s | 353 Bytes
Showing 1 to 10 of 14 rows. Idle hosts not listed.
« < 1 2 > »


R41>en
Password:
R41#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/12 ms
R41#
z PC svojeho R ping na 8.8.8.8 mali by sme vidiet v NTOPe



	IP Address	Location	Flows	Alerts	Name	Seen Since	Breakdown	Throughput	Total Bytes
Flows	158.193.139.15	Remote Host	4	0	158.193.139.15	00:21	Sent Rcvd	0 bit/s	4.99 KB
Flows	8.8.8.8	Remote Host	8	0	8.8.8.8	24:37	Sent Rcvd	0 bit/s	54.52 KB
Flows	192.30.253.116	Remote Host	2	0	192.30.253.116	09:10	Sent Rcvd	0 bit/s	21.35 KB
Flows	192.4.1.1	Local Host	2	0	192.4.1.1	01:06:16	Sent	169.57 bit/s	257.25 KB
Flows	40.67.248.104	Remote Host	1	0	40.67.248.104	02:15	Sent Rcvd	0 bit/s	360 Bytes
Flows	158.193.152.7	Remote Host	4	0	158.193.152.7	07:49	Sent	0 bit/s	1.06 MB

Zo študentského emailu viete požiadať o licenciu aj na NTOPng enterprise, a nainštalovať si ho doma, pre obzeranie tokov a štatistík z/do vášho PC.