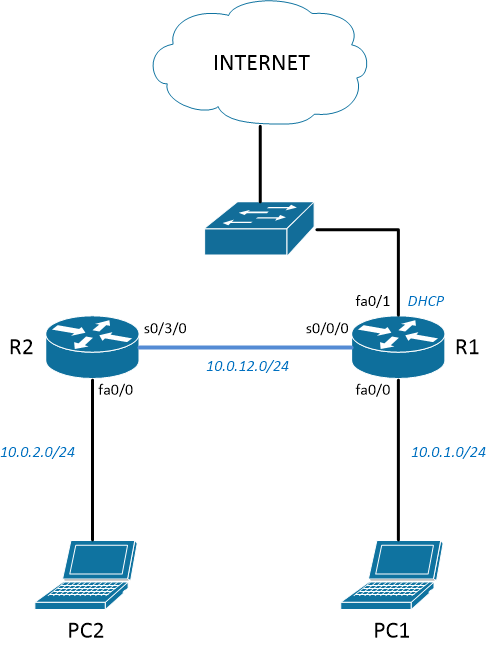
**Topológia**

****

**Úloha 1 – Cisco AutoQoS**

Verzia:

Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 15.3(3)XB12, RELEASE SOFTWARE (fc2)

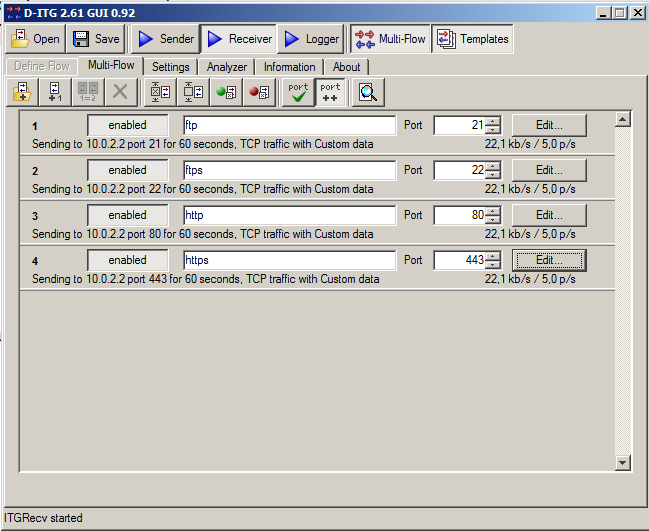
R2(config-if)# *auto discovery qos*

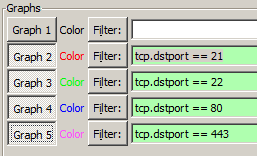
R2(config-if)# *auto qos voip*

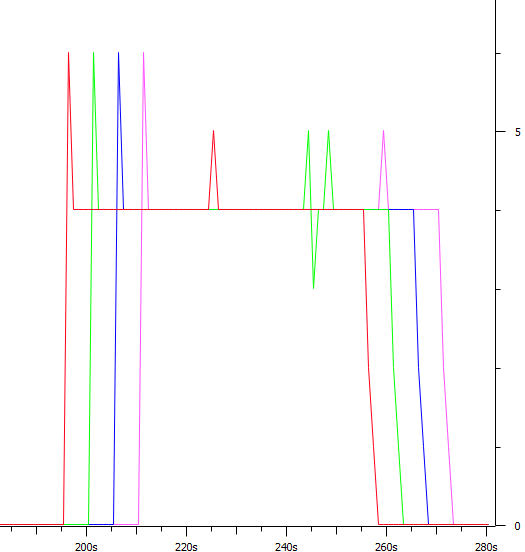
R2(config-if)# *do sh auto qos*  
 !  
 policy-map AutoQoS-Policy-UnTrust  
 class AutoQoS-VoIP-RTP-UnTrust  
 priority percent 70  
 set dscp ef  
 class AutoQoS-VoIP-Control-UnTrust  
 bandwidth percent 5  
 set dscp af31  
 class AutoQoS-VoIP-Remark  
 set dscp default  
 class class-default  
 fair-queue  
 !  
 class-map match-any AutoQoS-VoIP-Remark  
 match ip dscp ef  
 match ip dscp cs3  
 match ip dscp af31  
 !  
 class-map match-any AutoQoS-VoIP-Control-UnTrust  
 match access-group name AutoQoS-VoIP-Control  
 !  
 class-map match-any AutoQoS-VoIP-RTP-UnTrust  
 match protocol rtp audio  
 match access-group name AutoQoS-VoIP-RTCP  
 !  
 ip access-list extended AutoQoS-VoIP-RTCP  
 permit udp any any range 16384 32767  
 !  
 ip access-list extended AutoQoS-VoIP-Control  
 permit tcp any any eq 1720  
 permit tcp any any range 11000 11999  
 permit udp any any eq 2427  
 permit tcp any any eq 2428  
 permit tcp any any range 2000 2002  
 permit udp any any eq 1719  
 permit udp any any eq 5060  
 !  
 rmon event 33333 log trap AutoQoS description "AutoQoS SNMP traps for Voice Drops" owner AutoQoS  
  
Serial0/3/0 -  
 !  
 interface Serial0/3/0  
 no ip address  
 encapsulation ppp  
 ppp multilink  
 ppp multilink group 8  
 !  
 interface Multilink8  
 bandwidth 128  
 ip address 10.0.12.2 255.255.255.0  
 ppp multilink  
 ppp multilink interleave  
 ppp multilink group 8  
 ppp multilink fragment delay 10  
 service-policy output AutoQoS-Policy-UnTrust  
 ip rtp header-compression iphc-format

**Úloha 2 - Značkovanie paketov na vstupnom rozhraní smerovača (distribution layer)**

Cez D-ITG sme vygenerovali 4 rôzne prevádzky cez TCP (FTP, sFTP, HTTP, HTTPs). Vo wiresharku sme overili a odchytili vygenerovanú prevádzku.

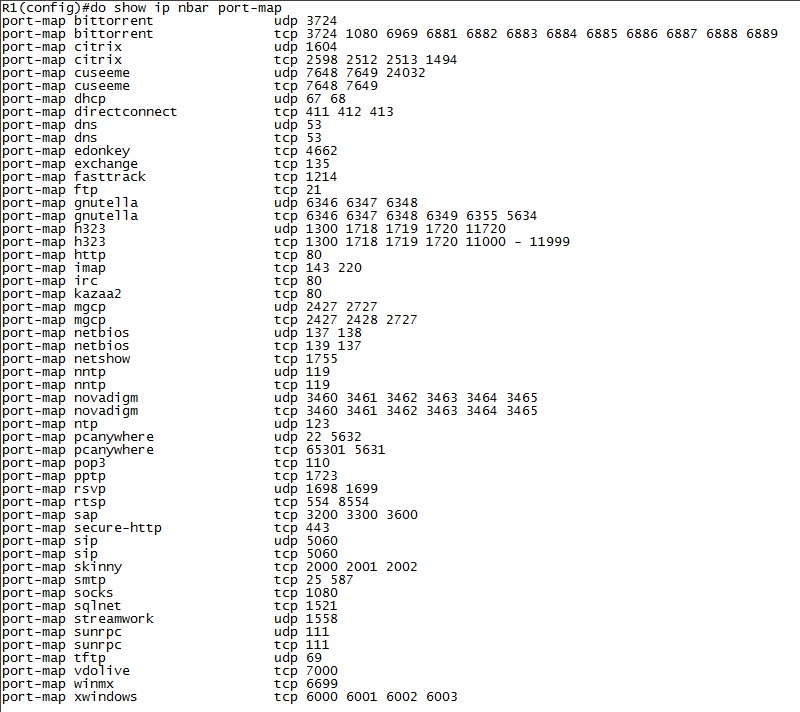






Následne sme nastavili značkovanie paketov (*pre FTP a sFTP DSCP=1, pre HTTP 2, pre HTTPS 3*) na smerovači R1 (a aplikovali policy na vstupnom rozhraní FastEthernet0/0).

Najskôr sme si zistili ktoré protokoly sú podporované cez nasledovný príkaz:

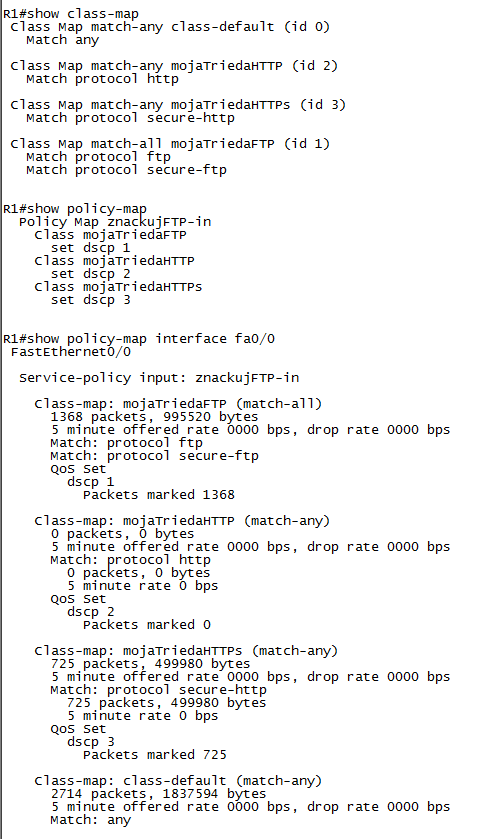


Z toho vidíme že protokoly ktoré potrebujeme sú FTP(21), HTTP(80), secure-HTTP(443),vidíme že secure-FTP sa nenachádza v zozname.

Následne sme spravili nasledovnú konfiguráciu na smerovači R1:

*class-map match-any mojaTriedaHTTP*  
 *match protocol http*  
*class-map match-any mojaTriedaHTTPs*  
 *match protocol secure-http*  
*class-map match-all mojaTriedaFTP*  
 *match protocol ftp*  
 *match protocol secure-ftp*  
  
*policy-map znackujFTP-in*  
 *class mojaTriedaFTP*  
 *set dscp 1*  
 *class mojaTriedaHTTP*  
 *set dscp 2*  
 *class mojaTriedaHTTPs*  
 *set dscp 3*  
  
*interface FastEthernet0/0*  
 *ip address 10.0.1.1 255.255.255.0*  
 *ip nbar protocol-discovery*  
 *duplex auto*  
 *speed auto*  
 *service-policy input znackujFTP-in*

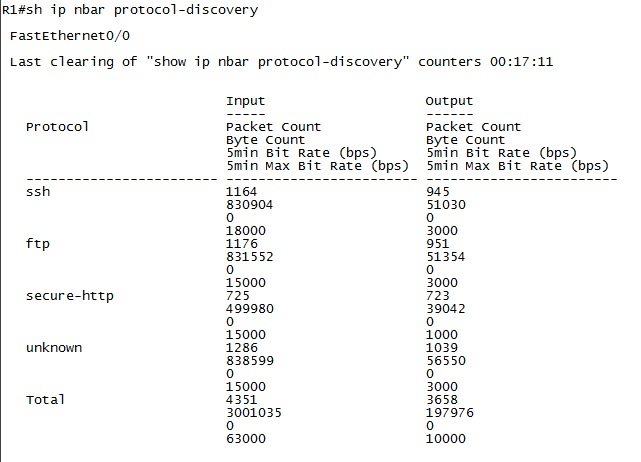
Overenie nastavených policy na smerovači:

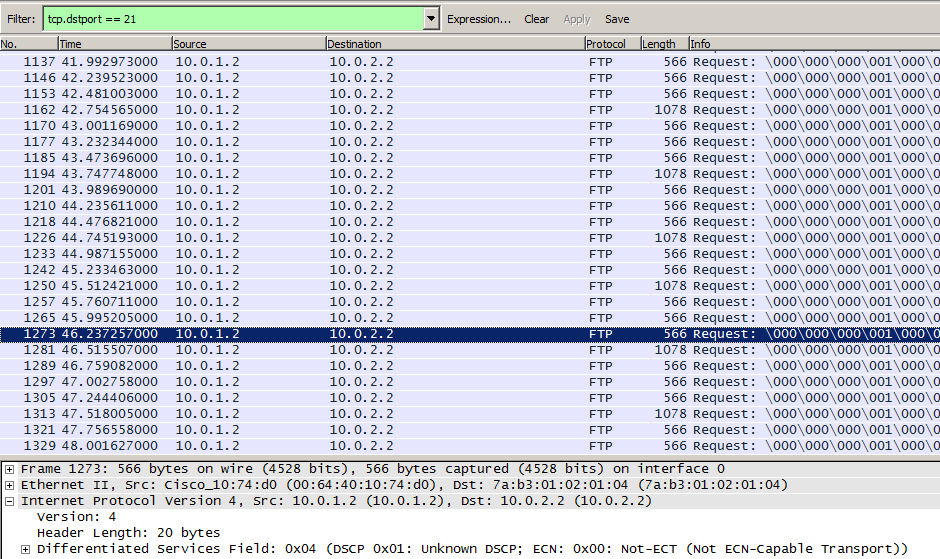


Pri nastavovaní už bol k dispozícií aj protokol secure-FTP, lenže ako vidíme neskôr, nepodarilo sa nám ho značkovať, keďže ho smerovač prijíma ako SSH nie ako secure-FTP.

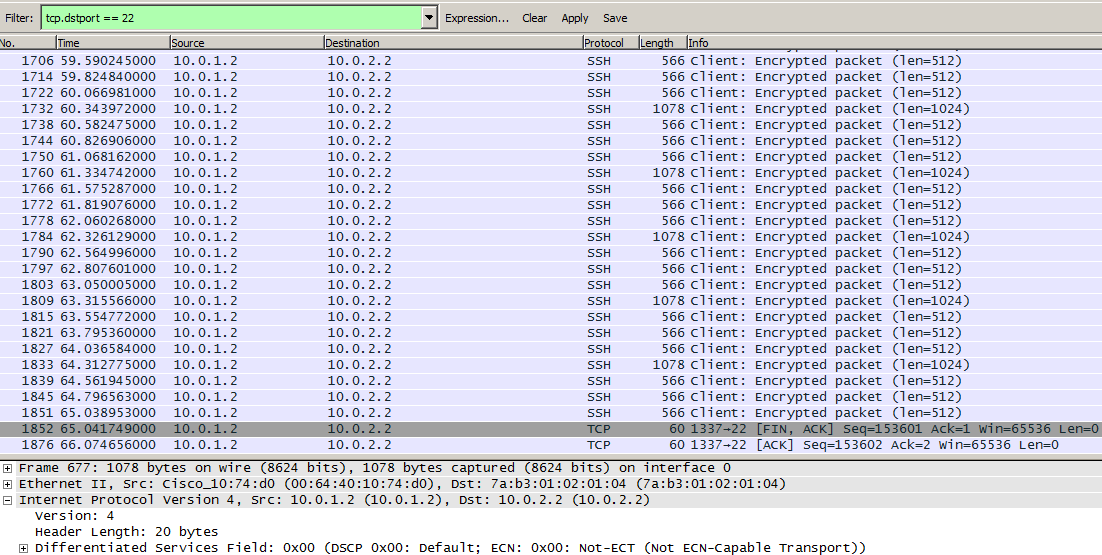
Rovnako sa nám nepodarilo značkovať ani HTTP protokol.

Môžeme vidieť značkované pakety ako na smerovači, tak aj vo Wiresharku.

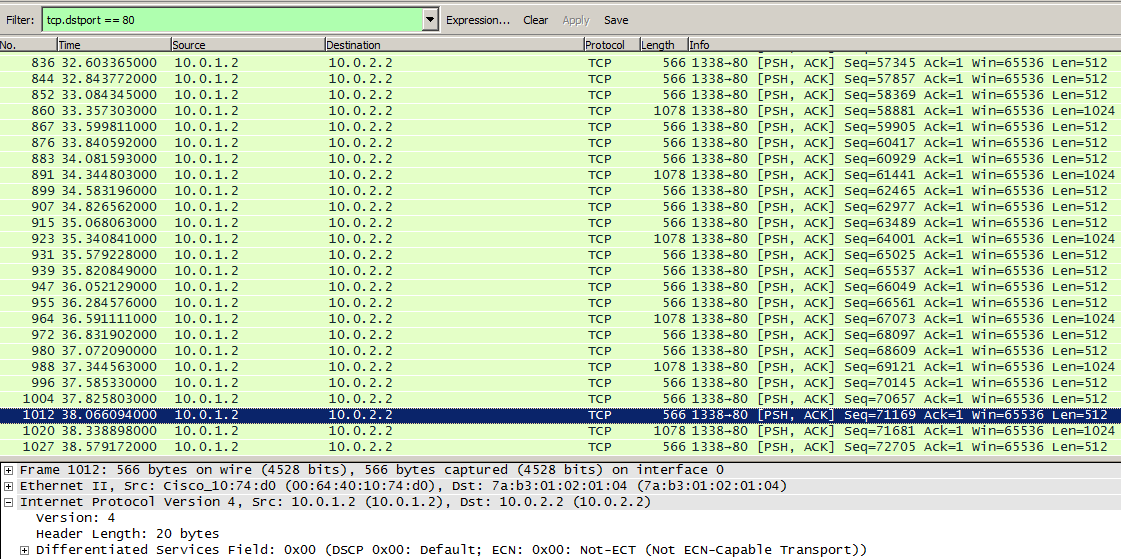




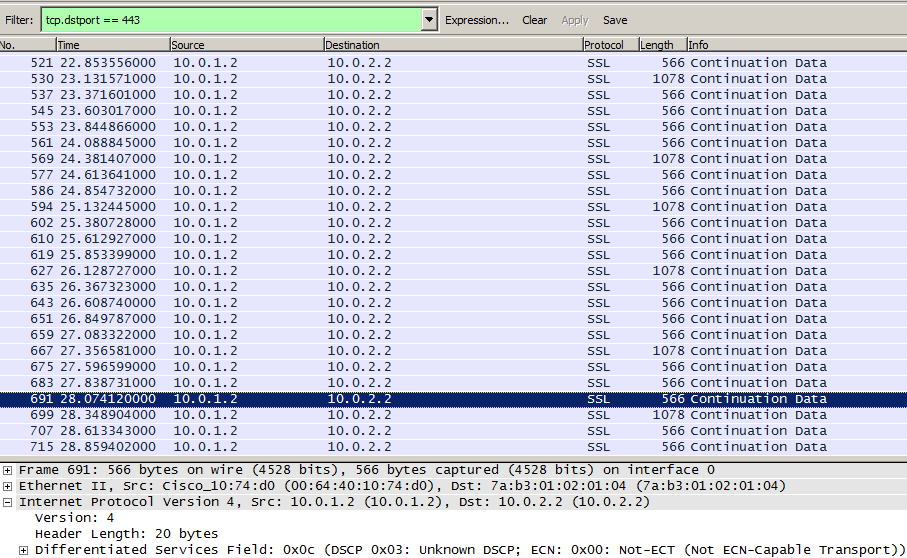
Obrázok FTP – 21 port (značkuje)



Obrázok sFTP – 22 port (neznačkuje)



Obrázok HTTP – 80 port (neznačkuje)



Obrázok HTTPS – 443 port (značkuje)

**Úloha 3 – Sledovanie štatistík NBAR**

Následne sme našu topológiu pripojili do internetu, aby sme mohli vygenerovať čo najviac protokolov a sledovať štatistiky NBAR.

