**Cv. 03 - Buček, Juriš**

Pred začatím práce na úlohách ,ktoré nám boli zadané na cvičení sme museli najprv spraviť niekoľko nasledujúcich krokov:

1) Zapojiť malú sieť (2 Smerovače, 2 PC)

2) Zapojenú sieť nakonfigurovať podľa zadania:

- IP adresy na rozhrania fa0/0 a s0/0/0

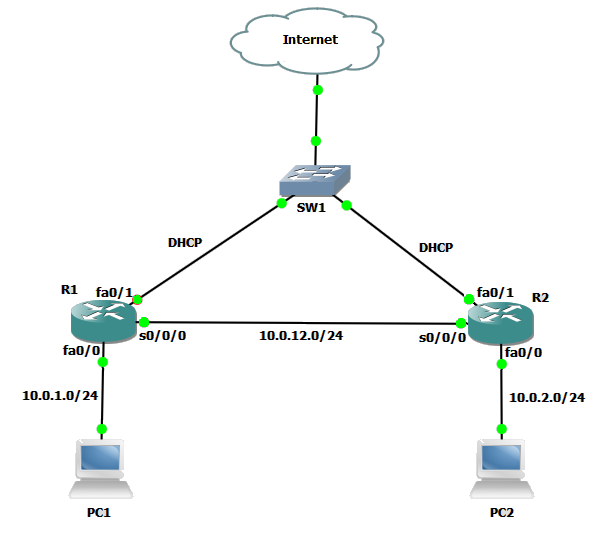
- clock-rate 128000, bandwidth 128

- statické smerovanie

3) Overiť plnú konektivitu (Trebalo vypnuť Windows Firewall)

Následne ,keď boli tieto prvotné úkony hotové prešli sme k úlohám ktoré nám boli zadané ,a v ktorých šlo o nastavenie QoS na CISCO Smerovačoch (Class-mapy, Policy-Mapy, …), Značkovanie paketov na vstupnom rozhraní a.i.

**Topológia:**



**Úloha 1 – Cisco AutoQoS**

* Verzia IOS na smerovačoch: 15.5
* AutoQoS je potrebné spustiť na požadovaných rozhraniach (s0/0/0)

Na sériovom rozhraní odosielateľa sme zapli AutoQoS príkazmi:  
*auto discovery qos*

*auto qos*

auto qos voip

\* Príkaz na spustenie: #R1(config-if)#auto qos voip

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

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

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

ip access-list extended AutoQoS-VoIP-RTCP

permit udp any any range 16384 32767

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

Ako prvé bolo treba nakonfigurovať NAT a aplikovať ho ,čo sme spravili príkazmi:

*access-list 100 permit ip 10.0.0.0 0.255.255.255 any*

*ip nat inside source list 100 int fa0/1 overload*

*int fa0/0*

*ip nat inside*

*int fa0/1*

*ip add dhcp*

*ip nat outside*

Následne po týchto krokoch sme vytvorili class-mapy a policy-mapy ktoré mali slúžiť na značkovanie paketov, vytvorili sme ich následovne:

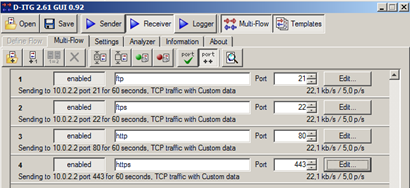
*Class-mapy:*

* HTTP - match protocop http, secure-http
* FTP - match protocol ftp, secure-ftp

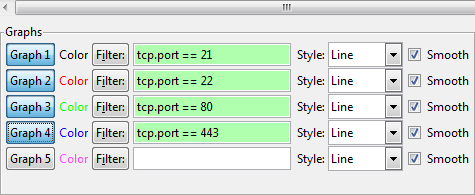
*Policy-mapy:*

* DSCP = 1 pre HTTP a HTTPS
* DSCP = 2 pre FTP a SFTP

Pomocou programu D-ITG sme si následne vygenerovali 4 rôzne prevádzky cez protokol TCP (FTP, SFTP, HTTP, HTTPS) Vo Wiresharku sme si následne odsledovali a analyzovali vygenerovanú prevádzku.



Obrázok 1 - Vygenerovaná prevádzka



Obrázok 2 - Nastavenie v IO Grafe vo WireSharku

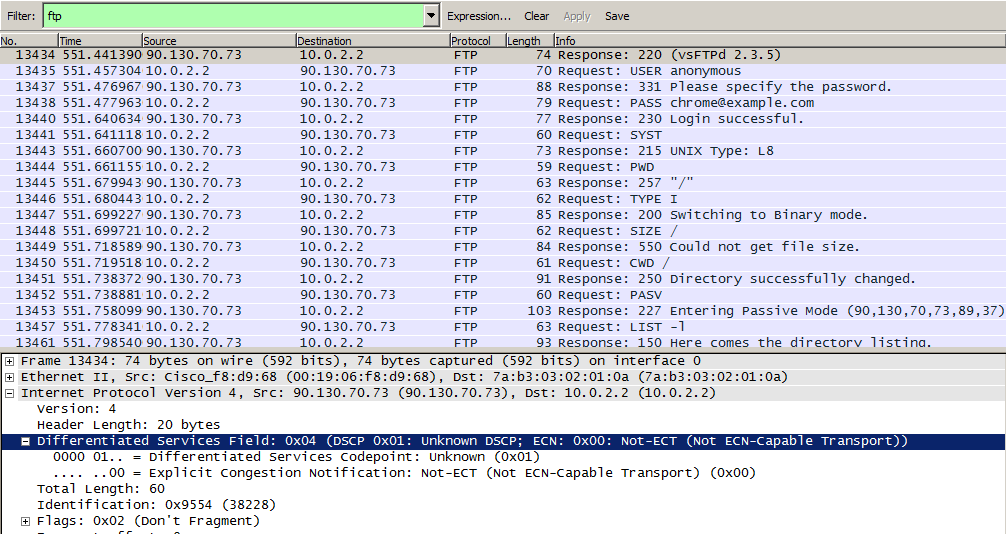
Pomocou príkazu *"show nbar port-map"* sme zistili ,že sú podporované protokoly FTP, HTTP a HTTPS, bohužiaľ protokol SFTP nebol podporovaný a teda nebol ani značkovaný v našom prípade tak ako sme chceli.

Konfigurácia:

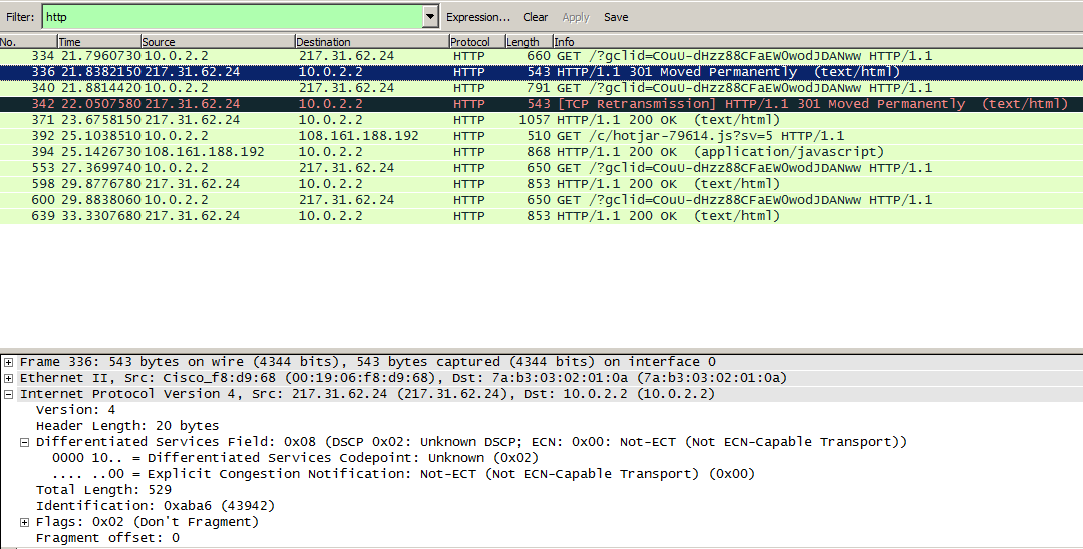
*class-map match-any mojaTriedaHTTP  
 match protocol http*

*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  
  
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*

Následne po tejto konfigurácii bolo možné vidieť značkované pakety ako na smerovači tak aj vo WireSharku.



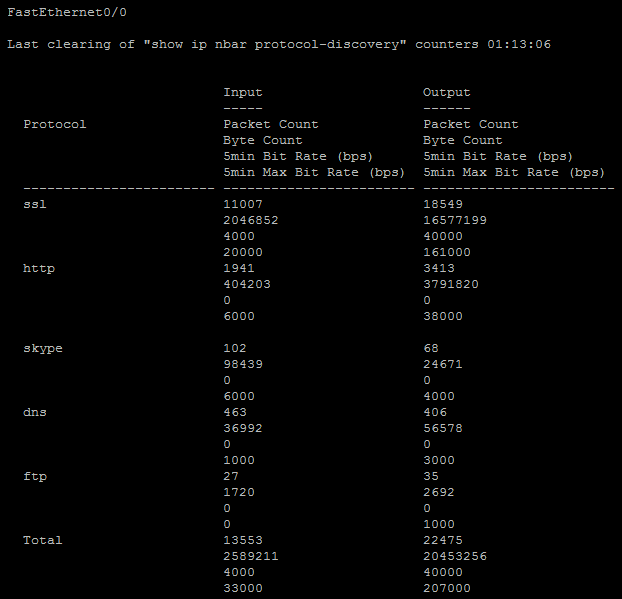
Obrázok 3 - Značkované FTP pakety



Obrázok 4 - Značkované HTTP pakety

**Úloha 3 – Sledovanie štatistík NBAR**

Následne po dokončení predchádzajucich úloh sme našu topológiu pripojili do internetu, aby sme mohli vygenerovať čo najväčší počet protokolov a sledovať štatistiky NBAR. Štatistiku sme odsledovali pomocou príkazu:  
*show ip nbar protocol-discovery*



**Bonusová Úloha:**

Pomocou príkazu "*show ip nbar port-map"* sme zistili ,že z predvolených TCP pozná NBAR iba DNS avšak nie TELNET. Pri UDP pozná taktiež DNS.

Parametre daných tokov:

* Pri každom z prípadov sa jedná o konštatný tok
* TCP – Telnet:
  + intenzita toku = 90p/s,
  + veľkosť paketu = 42B
* TCP – DNS
  + intenzita toku = 1p/s,
  + veľkosť paketu = 222B
* UDP – DNS
  + intenzita toku = 1p/s,
  + veľkosť paketu = 210B
* UDP – Gaming
  + intenzita toku = 24p/s,
  + veľkosť paketu = 71B
* UDP – Voice
  + intenzita toku = 26p/s,
  + veľkosť paketu = 70B