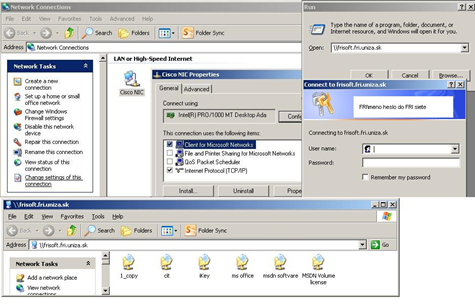
**Topológia:**

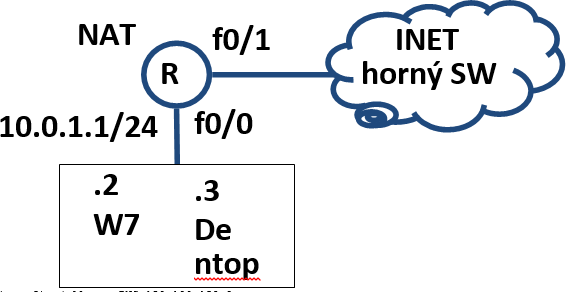
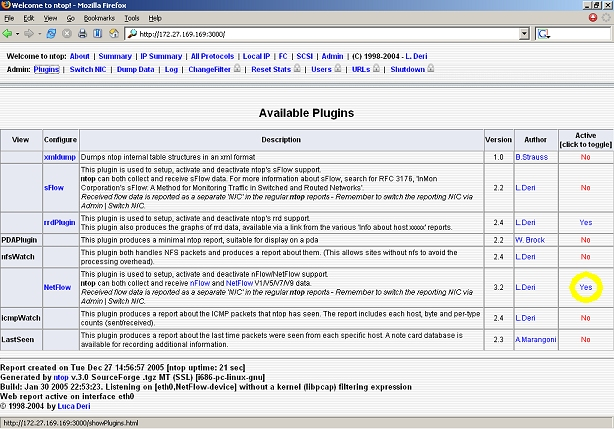
PC1 (Wireshark +I/O graphs,statistics, D-ITG+logger) --- R1 --- R2 --- PC2 (Wireshark +I/O graphs,statistics, D-ITG+logger)

Poznámka: Ak sa bije telnetové pripojenie z VM Debian s pripojením telnet vo Windowse cez PuTTy, treba zadať vo VM Debian > Machine > Stop.

1. **Cisco autoQoS**
   1. Otestovať na danej verzii IOSu
   2. Zistiť ako a v akom režime sa spúšťa, zistiť čo všetko daná funkcionalita nastaví a kde všade (aké QoS pravidlá aktivuje)
      1. Spraviť si zálohu running-config pred a po a porovnať (resp. show class-map, sh policy-map, sh policy-map int XY)
      2. Záloha pred je dôležitá, aby sme sa vedeli vrátiť do pôvodného stavu, keďže budeme chcieť nastaviť QoS aj svojou cestou, bez automatiky, viď nasledujúce body 2-4.
2. **Značkovanie paketov na vstupnom rozhraní smerovača** (distribution layer)  
   (*Do DSCP v hlavičke paketu zapíšeme príslušnosť k triedam, pre FTP dáme DSCP=1, pre HTTP značku 2, pre HTTPS značku 3*)
   1. Cez D-ITG vygeneruj 3 rôzne typy prevádzky (intenzita tokov tak, aby linka stíhala):
      1. FTP + secureFTP
      2. HTTP
      3. HTTPs
   2. Odchyť dáta Wiresharkom na cieľovej stanici a analyzuj či D-ITG generuje vhodné dáta, pozri aj IO graphs
   3. Nastavte značkovanie paketov, ktoré prislúchajú protolom: FTP a secure-FTP => DSCP=1, HTTP => DSCP = 2, HTTPS
      1. Príslušnosť určí NBAR pre podporované a definované protokoly
         1. Ktoré sú to over cez show ip nbar port-map.
         2. Ako tam vidieť identifikáciu protokolov FTP a secureFTP? Ako HTTP? Ako HTTPs? (pozri transp. protokol aj č. portu)
      2. Vytvor novú triedu prevádzky (využi na to konštrukt class-map):
         1. Meno: mojaTriedaFTP (pozor zváž či match any alebo match all)
         2. Klasifikačné kritérium (2x match): FTP aj secure-FTP
      3. Následne vytvor QoS politiku, ktorá bude značkovať takto identifikované pakety
         1. Meno: znackujFTP-in
         2. Odkaz na vašu triedu mojaTriedaFTP
         3. QoS pravidlo: set dscp 1
      4. Podobne vytvor triedu prevádzky pre HTTP a HTTPs a doplň QoS politiku pre značkovanie paketov z takýchto tried
         1. Pozor, max. jedna QoS politika na jednom rozhraní v jednom smere, takže všetko bude v jednej policy-map
      5. Aktivuj danú QoS politiku na vstupnom rozhraní R1
         1. Over jej funkčnosť
            1. Zaznamenaj do reportu výstupy: sh run, sh class-map – pribudla aj default-class?, sh policy-map, sh policy-map int XY – ako tu vyzerajú počty paketov? Resp. over keď vygeneruješ príslušné dáta cez D-ITG:
            2. Generuj príslušné toky, skontroluj značkovanie cez Wireshark u príjemcu (aj zdroji, ak je problém)
   4. Preskúmaj parametre príkazov:
      1. R1(config-cmap)#?
      2. R1(config-cmap)# match ip ?
      3. R1(config-cmap)# match protocol ?
3. **Sledovanie štatistík NBAR**
   1. Zapnite sledovanie pre rozhranie na vašom smerovači vedúce k LAN (ip nbar protocol discovery)
   2. Vygenerujte čo najväčcší objem dát
      1. Browsovanie na internete, rôzne protokoly – hamachi, torrent, zdieľanie priečinkov napr. [\\frisoft.uniza.sk](file:///\\frisoft.uniza.sk), ...

V nastaveniach Cisco NIC treba povoliť Client for Microsoft Networks  
  


* + 1. Zobrazte si štatistiky o typoch prevádzky:  
       show ip nbar protocol-discovery  
       show ip nbar protocol-discovery top-n 5  
       show ip nbar protocol-discovery int f0/x

1. **Zbieranie štatistík protokolom NetFlow na kolektor Ntop**  
   Cisco zariadenia vedia zbierať štatistiky o prevádzke a posielať ich protokolom NetFlow v pravidelných intervaloch na tzv. “kolektor”. Neposielajú sa detailné údaje o paketoch, ale štatistiky pre rôzne toky. Je vecou kolektora, resp. analyzátora zozbieraných dát (NetFlow Analyzers), ako ďalej takéto štatistiky spracuje a graficky zobrazí pre používateľa. Nástrojov je pomerne veľa (PRTG Network Monitor www.prtg.cz, Scrutinizer, Syslog-ng www.syslog-ng.org, Ntop... ), my použijeme Ntop, ktorý je aj kolektorom aj analyzátorom zároveň, a má aj webové rozhranie.
   1. Topológiu si rozšírime iba tým, že využijeme aj VM Debian, kde nainštalujeme Ntop  
      
   2. Stiahnite a nainštalujte Ntop
      1. apt-get update, apt-get install ntop
         1. Rozhrania eth0,eht1 (bez medzery)
         2. Používateľ: ntop
         3. Admin heslo pre web: ….
   3. Spustite Ntop
      1. V prehliadači otvoriť: localhost: 3000 (zistiť číslo portu možno cez: netstat -apn)
         1. Následne sa otvorí GUI Ntop-u
      2. Vytvoriť formálnu sieťovú kartu "Net device ...2"  
         Plugin – NetFlow – Activate – Flow (Plugin – NetFlow –Configure/Edit)  
         “Net device…2”, Set … - treba vždy tlačidlo vpravo!  
         Port: 2055, Set port  
         Adddress: 10.0.1.0 255.255.255.0, Set … - lokálna sieť, kde sa nachádza ntop  
         
2. **Bonusová úloha**  
   Preskúmajte toky, ktoré generuje D-ITG pre predvolené scenáre - vpravo hore "Application Layer Data".
   1. Pre TCP má predpripravenú šablónu pre aplikačné protokoly Telenet a DNS, pre UDP aplikačné protokoly Voice, DNS a Gaming
      1. Zisitte ktoré z nich pozná NBAR (show ip nbar port-map) a aj ich korektne rozpozná.
      2. Aké parametre majú dané toky:
         1. Intenzita toku, s akým rozdelením? Konštatný tok?
         2. Veľkosť paketu?
         3. Čo obsahuje telo TCP, resp. UDP segmentu?