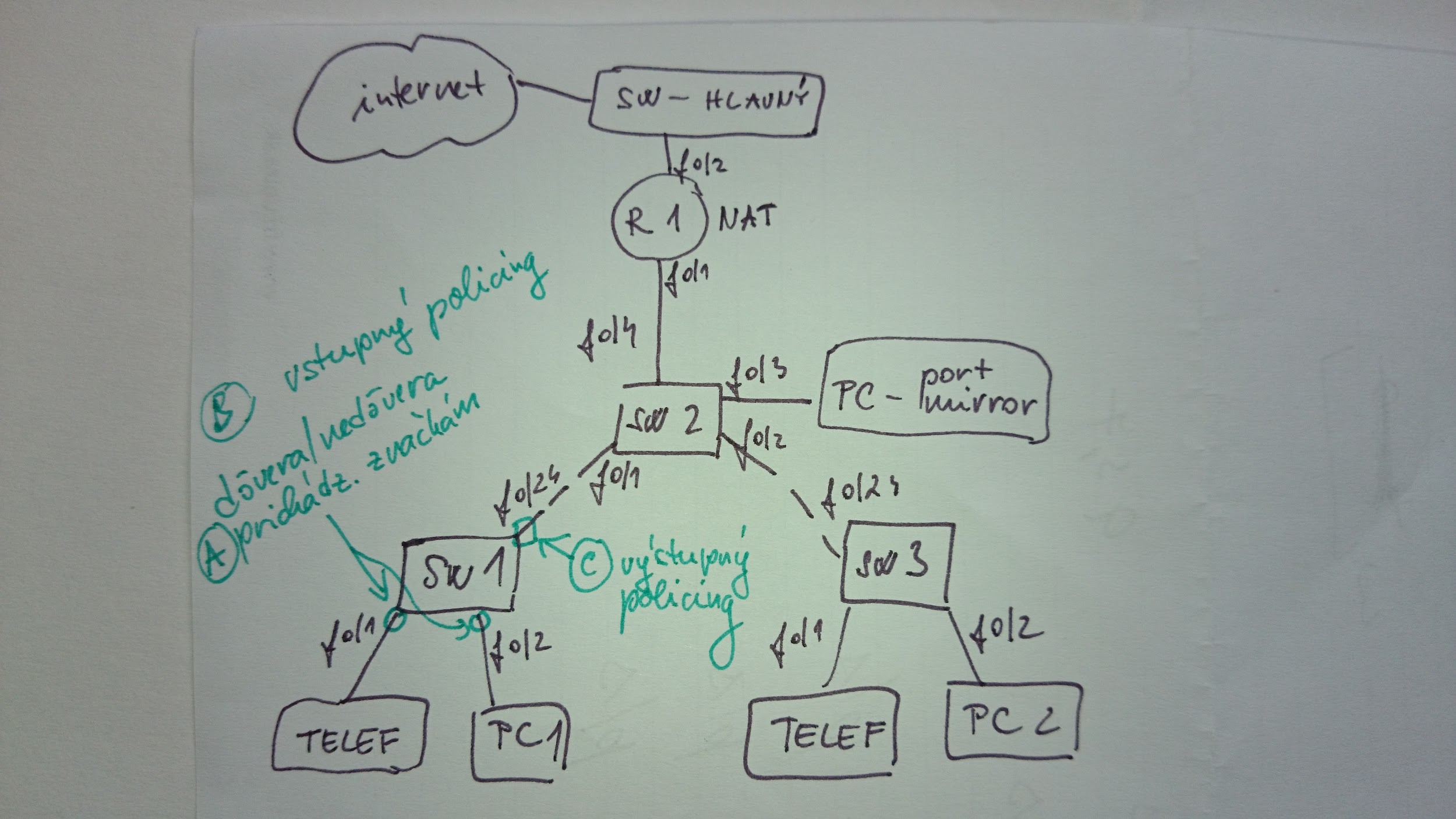
**Lab: QoS na prepínačoch**  
*(Pozri slajdy z predášky 6 - všetky)*

**Graf topológie**

* Ak je nedostatok PoE prepínačov, je možné SW1 a SW3 spojiť do fyzicky jedného prepínača



**Ciele**

* Nastaviť dôveru/nedôveru prichádzajúcim QoS značkám pri vstupe paketov na prepínač
  + dôverujem:
    - CoS (L2)
    - DSCP (L3)
    - ToS (staršia L3, IP precedence)
  + nedôverujem:
    - ACL nepoužijem => DSCP == def.0
    - ACL použijem:
      * nastavím CoS: ACL + class map + policy map - set cos..
      * nastavím DSCP: ACL + class map + policy map - set dscp..
* Nastaviť vstupný policing na prepínači
  + prekračuje daný tok (paket) dohodnutý kontrakt?
    - NIE: prenes paket
    - ÁNO:
      * preznačkuj
      * zahoď
  + vedieť nastaviť prahové hodnoty pre vstupné fronty (2 fronty s WTD, pakety niektorej triedy začnem zahadzovať ešte skôr ako sa front naplní na 100%)
  + vedieť zmeniť parametre pre SRR mechanizmus výberu paketov z front
* Nastaviť výstupný policing na prepínači
  + vedieť nastaviť prahové hodnoty pre výstupné fronty (4 fronty s WTD, pakety niektorej triedy začnem zahadzovať ešte skôr ako sa front naplní na 100%)
  + vedieť zmeniť parametre pre SRR mechanizmus výberu paketov z front

**Príprava**

Pracovať budeme na prepínačoch 2960 a 3560, preto sa nám zíde know-how:  
 [Catalyst **2960**-X Switch **QoS Configuration Guide**, Cisco IOS Release 15.0(2)EX](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/qos/configuration_guide/b_qos_152ex_2960-x_cg/b_qos_152ex_2960-x_cg_chapter_010.html#d3520e2968a1635)

(Configuring Auto-QoS - je iná záložka v ľavom menu )  
[Catalyst **3560** Switch **QoS Configuration Guide**, Release 12.2(55)SE](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_55_se/configuration/guide/3560_scg/swqos.html)

**Generované toky:**

* hlasový tok generovaný Cisco IP telefónom 7970
* dátové toky (multiflow) generované z PC1 D-ITG generátorom:
  + pozor !! musíme pracovať pod OS Debian, lebo Win7 odosiela všetky pakety s DSCP značkou 0
  + vo VirtualBoxe si naklonujte VM Debian
    - nastavte si jej meno na: 2015\_OKS\_Priezvisko\_Meno
    - odimunizujte ho (nastavenia ktoré tam spravíte, vám ostanú aj na nasledujúce cvičenia)
    - doinštalujte D-ITG (ide to pomerne ľahko z repozitárov...)
    - doinštalujte ITG-GUI (zdĺhavejšia úloha, ale dá sa to), fungujúci návod napr. tu:  
      <http://www.cs.uwc.ac.za/~creymoreno/csc730/DITG_Manual_v2.pdf>
  + vygenerujte nejaký tok označkovaný DSCP, pozrite či vám Debian značky nemaže. Ak je to OK, pripravte si nasledovné toky v D-ITG:

|  |  |  |  |
| --- | --- | --- | --- |
| **Typ toku** | **Cieľ port** | **DSCP** |  |
| HTTP | 80 | af21 |  |
| HTTPs | 443 | af31 |  |
| Voice | 9001 | ef |  |
| Data | 9002 | 0 |  |
| Gaming | 9003 | ToS==1 |  |

**Pre nastavenie LinkSys telefónu:**

* jednoducho cez web klikačka

**Pre nastavenie Cisco telefónu je potrebné:**

1. napájanie - prepínač (switch 3560) s podporou PoE, aktuálne (šk.rok 2016/2017) nemáme k dispozícii napájacie adaptéry, preto PoE prepínače
2. Telefóny sú nakonfigurované a pripravené na použitie.
3. Ako vyzerájú konfiguračné súbory si možete pozrieť tu (len informačne):

[www.kis.fri.uniza.sk/~marek/Cisco7970](http://www.kis.fri.uniza.sk/~marek/Cisco7970), potrebné sú všetky 3 súbory:

* 1. SEP000011….. .xml (pozor, tu 000011…. je MAC adresa telefónu, pozrite si od spodu telefónu, alebo v nastaveniach)
  2. XMLDefault… .xml (SIP default)
  3. Dialplan.xml
* v prvých dvoch treba uvidíte výskyty reťazca “2xy”, keďže my budeme používať účty 200 až 220
* na telefóne sa dá nastaviť IP adresa dvojako:
  + staticky
    - \* \* # - odomkneme nastavenia a môžeme niečo zmeniť
      * Ak pýta heslo, je nasledovné: admwt (stačí stláčať číslice 23698)
    - konfigurácia siete -> konfigurácia IPv4 -> IP adresa
  + dynamicky
    - povoliť DHCP v nastaveniach telefónu
* Pokiaľ by sme potrebovali niečo v konfiguračných súboroch zmeniť, môžeme, a následne treba nahrať všetky 3 súbory na telefón cez TFTP server, na ploche svojho PC máte TFTPd32 server, použili by ste ten, alebo čokoľvek iné. Pár hintov ako povoliť na telefóne TFTP:

|  |
| --- |
| \* \* \*  settings  2  1  16 → áno  17 → IP |

1. použiť katedrové účty 200 až 220 (meno = heslo = 2xy)
2. registrovať sa voči serveru: 158.193.152.2

**Základná konfigurácia**

* Nakonfigurujte topológiu podľa hore uvedeného grafu topológie, na smerovači treba nastaviť NAT preklad privátnych adries z našej LAN, a DHCP server pre prideľovanie adries pre PC a telefóny. Budeme využívať katedrový server pre možnosť telefonovania cez Cisco telefóny.
* Port mirror

**Otestujte:**

1. viete sa dovolať susedovi
2. odsledujte na PC1, PC2 aj PC3 (tam kde je port mirror) značenie DSCP, ktoré pridáva váš Cisco telefón pre hlasové pakety
   1. aká je default hodnota? Je to EF?
   2. kde v konfiguračných súboroch telefónu je miesto pre výber značky pre hlasové pakety (..DSCPvoice..)? je možné to zmeniť? dá sa zmenť aj CoS, alebo len DSCP?
3. zapojte PC1 (podobne aj PC2) do voľného portu na Cisco telefóne a skúste či sa PC1, aj PC2 dostane do internetu (ping, web...). Odsledujte značku pre tieto pakety.
4. vygenerujte toky cez D-ITG z PC1 na PC2, odsledutje či sa značkujú ako majú Podobne to otestujte aj v opačnom smere.

**Ingress dôvera/nedôvera prichádzajúcim QoS značkám**

Najprv zistite, či je QoS zapnuté  
R1# show mls qos

Ak nie, QoS zapneme:  
R1(config)#mls qos  
Príkazy na overenie nastavení - v tejto chvíly si pozrite každé z nich, výstupy si odpožte do svojho reportu (posledné 3 netreba ukladať do reportu, ešte nemáte nič nastavené) :

R1# show mls qos

R1# show mls qos interface f0/1

R1# show mls qos maps dscp-output-q

R1# show ip access-list

R1# show class-map

R1# show policy-map

Aj v scenároch nižšie si zaznamenávajte výstupy zo show príkazov, na ktoré vás upozorníme v zadaní, a vyznačte (farebne) podstatné časti.

**1. Krok: nastav dôverovanie Cisco telefónu**

Dôveru môžeme nastaviť viacerými spôsobmi, vyskúšame si dva z nich, najprv zapojíme telefón do f0/1, otestujeme čo sa deje, potom do f0/2, otestujeme čo sa deje (cdp musí byť zapnuté, defaultne aj je, cdp run globálne, cdp enable na rozhraní):

1. pre f0/1 nastavte:  
   R1(config-if)# mls qos trust dscp  
   R1(config-if)# mls qos trust device cisco-phone  
     
   R1# show mls qos interface f0/1  
   R1# show run
2. pre f0/2 nastavte:  
    R1(config)# auto qos voip cisco-phone   
    ! zapne funkciu trusted boundary  
    ! využije CDP protokol na zistenie, či je na porte zapojený telefón:  
    ! ak ÁNO: ingress classification == trust QoS label (očakáva DSCP 24, 26, alebo 42)  
    ! ak NIE: ingress classification == don’t trust QoS label

**2. Krok: nastav dôveru/nedôveru na portoch:**

1. pre f0/3 nastavte, že **veríte DSCP**:

R1(config-if)# mls qos trust dscp

zapoj PC1 do tohto portu, pusti cez D-ITG multiflow do cieľa na PC2 a pozri cez Wireshark či videť značky (ak používate oddelené prepínače pre koncové LAN, odsledujte značkovanie aj na PC kde je port mirror), aj výstupy:

R1# show mls qos

R1# show mls qos interface f0/1

R1# show mls map

pozri tam dscp-mutation mapu

1. pre f0/4 nastavte, že **veríte DSCP, ale...** zmeníme si DSCP značku na inú:

pre HTTP (dscp 18) a HTTPS (dscp 26) zmeníme značky na dscp 28.. zisti aké je to afxy?

R1(config-if)# mls qos trust dscp

R1# show mls qos

R1# show mls qos interface f0/1

R1# show mls qos map

R1(config-if)# mls qos map dscp-mutation MENO\_MAPY DSCP\_STARA to DSCP\_NOVA  
 R1# show mls qos map

zapoj PC1 do tohto portu, pusti cez D-ITG multiflow do cieľa na PC2 a pozri výsledok vo Wiresharku, či vidieť značky a aké, zdokumentujte - toto zopakujte aj pre nasledujúce 3 body.

1. pre f0/5 nastavte, že **veríte ToS:**  
   R1(config-if)# mls qos trust ip-precedence   
   R1# show mls qos interface f0/1  
   R1# show mls qos map
2. pre f0/6 nastavte, že neveríte ničomu (nenastavím trust), a označkujeme si prichádzajúce pakety po svojom (viď tabuľka toky v D-ITG):
   1. ACL
   2. class map
   3. policy map
3. pre f0/7 nastavte, že neveríte ničomu (nenastavím trust), a nerobím nič

**3. Krok: nastavte vstupný policing na prepínači pre f0/3:**

* policy mapa pre HTTP a HTTPs
* police [..bps] [veľkosť zhluku]
  + bps - prispôsobte na 80% z cekového toku, ktorý generujete v D-ITG (aby sme videli dôsledok, 20% prevádzky nad rámec kontraktu bude odmietnutej)
  + veľkosť zhluku v B, nastavte aspoň 2 rôzne hodnoty (spravte 2 experimenty) a odsedujte výsledok v grafe vo Wiresharku - IO graphs
* odsledujte výsledok policingu vo Wiresharku na vhodnom mieste v topológií - porovnajte graf s grafom pre scenár, kde nebol nastavený policing.
* Nastaviť prahové hodnoty pre vstupné fronty
  + Najrpv zistite aké sú defaultné prahové hodnoty pre WDT pre 2 vstupné fronty
  + A zsitite, ktoré DSCP značky defaultne radí do fronty 1 a ktoré do fronty 2

**4. Krok: nastavte výstupný policing na prepínači:**

* nastaviť výstupný policing
  + Pre HTTP a HTTPS:
    - police [..bps] [veľkosť zhluku]
      * bps - prispôsobte na 80% z celkového toku, ktorý bude vychádzať von týmto rozhraním
        + Tu stanovujeme hornú hranicu pre súčtový tok, ktorý príde z ktoréhokoľvek PC v danej LAN
      * veľkosť zhluku zvoľte rozumne a odsledujte výstup v IO graphs, resp. sh...
* nastaviť prahové hodnoty pre výstupné fronty (4 fronty s WTD, pakety niektorej triedy začnem zahadzovať ešte skôr ako sa front naplní na 100%)
* zmeniť parametre pre SRR mechanizmus výberu paketov z front
  + Najprv zistite do akej