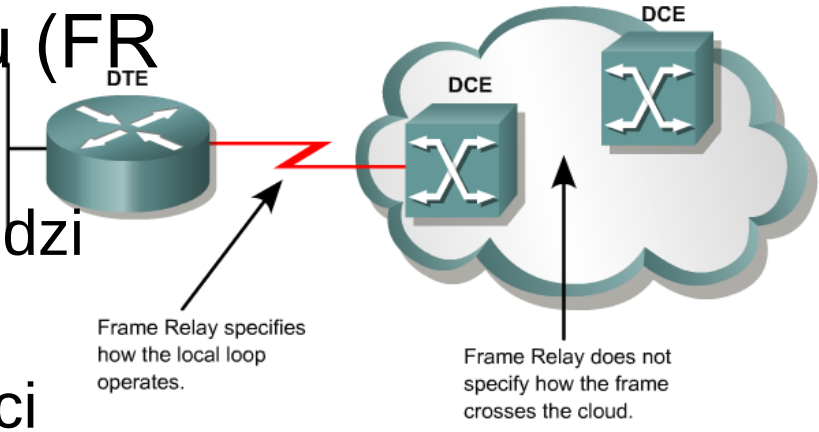
Frame Relay a sieťová bezpečnosť

CCNA Exploration Semester 4 - Kapitoly 3, 4

Čo je Frame Relay?

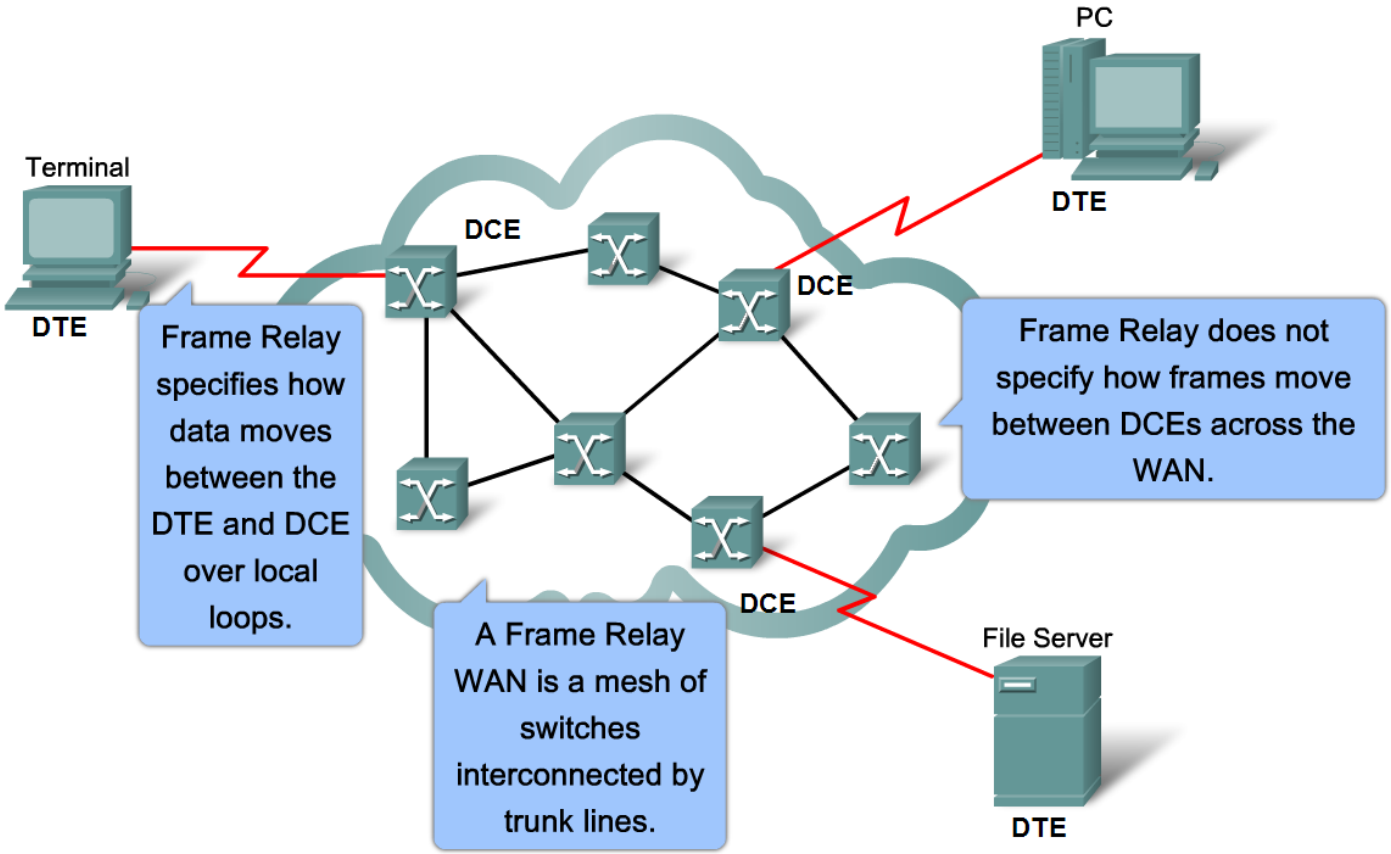
- F.R. je najpoužívanejšia WAN technológia vo svete
  - Pôvodne myslená ako náhrada X.25 protokolu (dáta cez analog. tel. linky) jednoduchším a rýchlejším protokolom
- Definuje rozhranie medzi používateľom a verejnou sieťou (FR mračnom), tzv. UNI
  - Definuje zapuzdrenie rámcov medzi DTE a DCE
  - Nedefinuje prenos rámcov v rámci WAN provider siete



FR vlastnosti

- FR je paketová technológia
  - Založená na Packet switching prepínaní
  - Pôvodne plánovaná ako dátové rozšírenie ISDN
  - Veľkosť rámcov do 4096 bajtov, typicky 1600B
- Pracuje na ISO OSI L2
- Vyžaduje bezporuchovosť prenosových liniek
  - Žiadny mechanizmus riadenia chýb rámcov pri prenose (retransmisia poškodených pri prenose)
    - Detekcia chýb a opravy sú ponechané na protokoly vyšších vrstiev (TCP)
  - Neobsahuje mechanizmus riadenia toku
  - Obsahuje mechanizmus riadenia zahltenia siete (drop)
- Je spojovo orientovaná
  - Medzi používateľmi prepojenými FR existuje virtuálne spojenie
  - Max teoreticky je 1024 na linku
- Ponúka rýchlosti od 64 kbps do približne 45 Mbps
  - Bandwidth je prideľovaný podľa požiadavky (štatistický MUX)
  - Typicky záujem zákazníkov je 1Mbps or 2Mbps
- Najčastejšie nasadenie
  - Bursty prevádzka
    - Prepojenie odľahlých LAN, prístup do Internetu a pod.

Frame Relay WAN

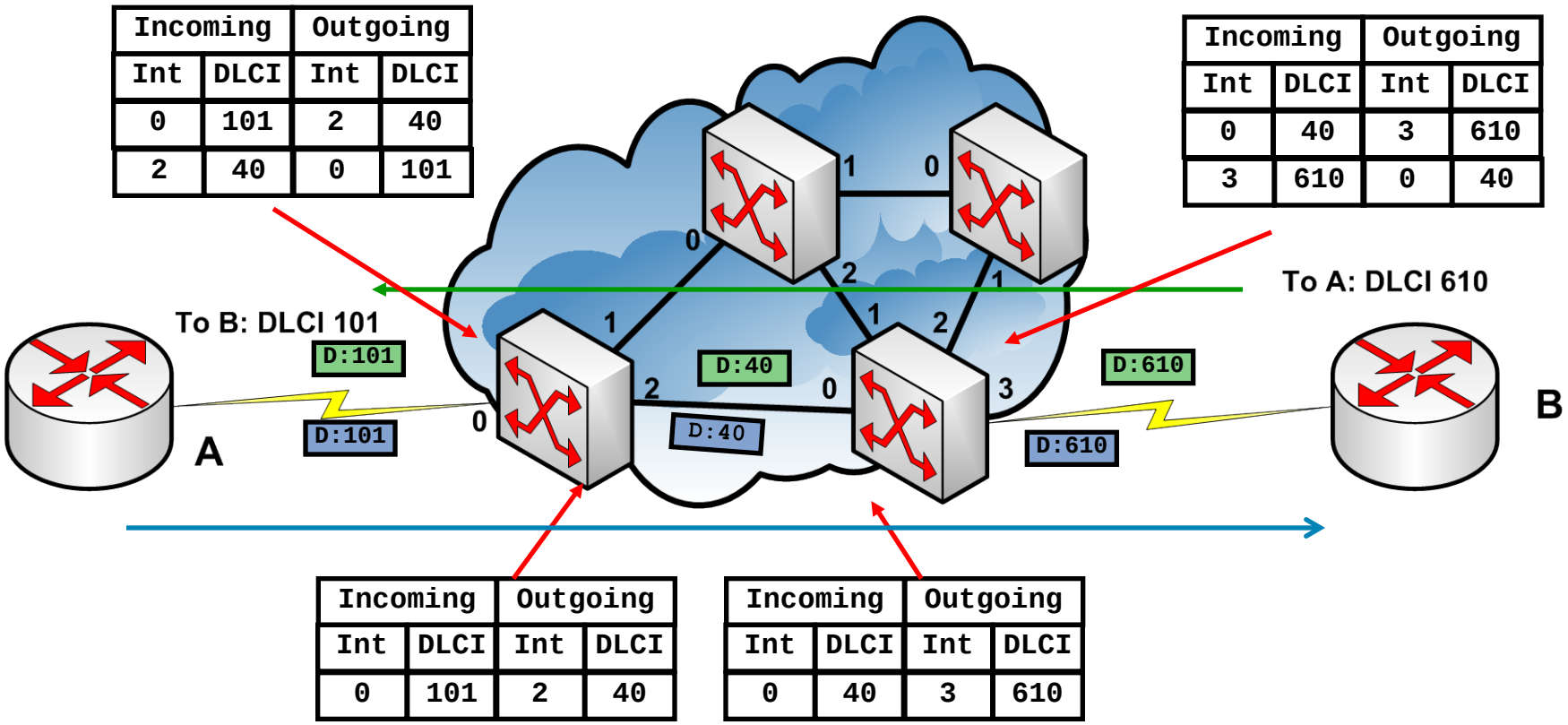


Frame Relay poskytuje:

- prístup do siete
- doručenie rámcov v poradí,
- zabezpečenie chybovosti rámcov Cyclic Redundancy Check

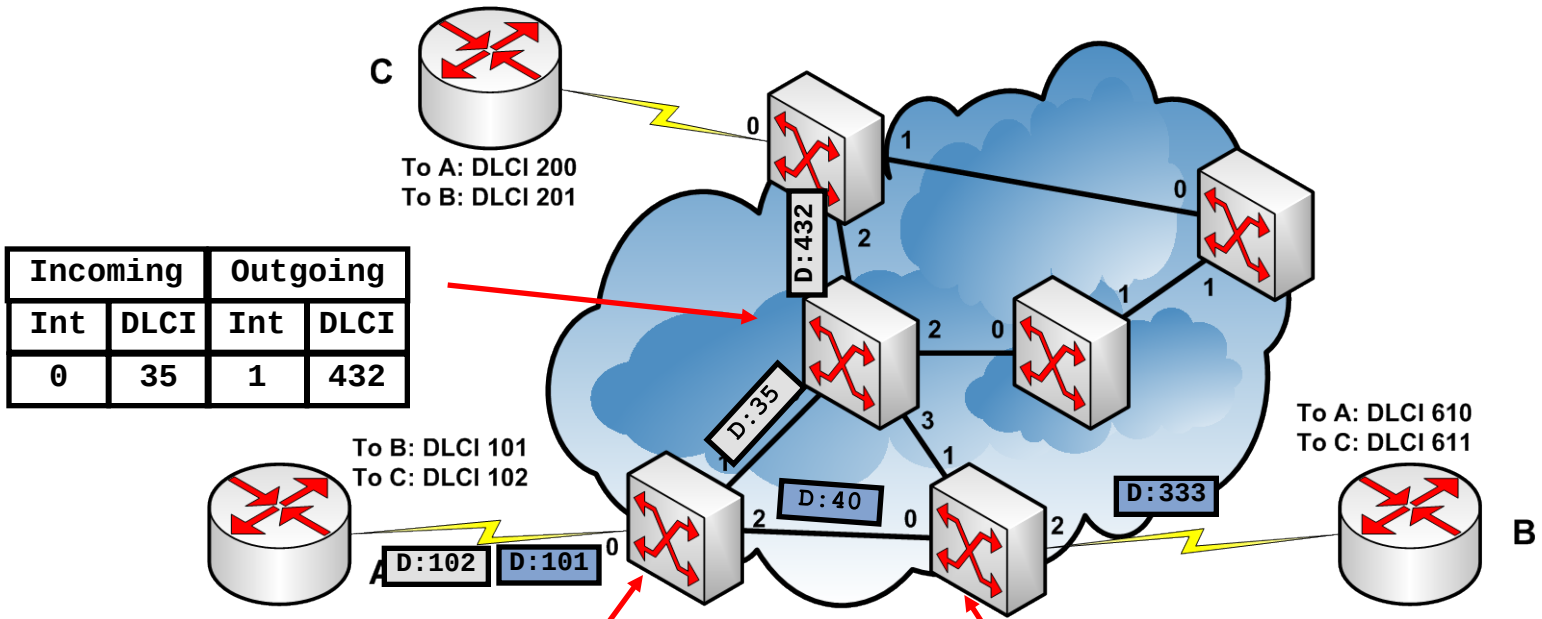
FR – prepojenie – Virtual Connection

- Prepojenie zákazníkov
  - Virtuálne okruhy (logické spojenie)
    - PVC – Permanent Virtual Circuit
    - SVC – Switched Virtual Circuit
      - Zostavené signalizáciou CALL SETUP, DATA TRANSFER, IDLE, CALL TERMINATION
- Identifikátor VC
  - DLCI – Digital Line Connection Identifier
  - Len lokálny význam medzi dvomi FR zariadeniami
  - Pri PVC pridelený providerom



FR – prepojenie zákazníkov - VC

- Multiplexovanie PVC cez prístupovú linku
  - Zdieľanie riešené cez štatistický multiplex
  - Odlíšenie PVC cez DLCI

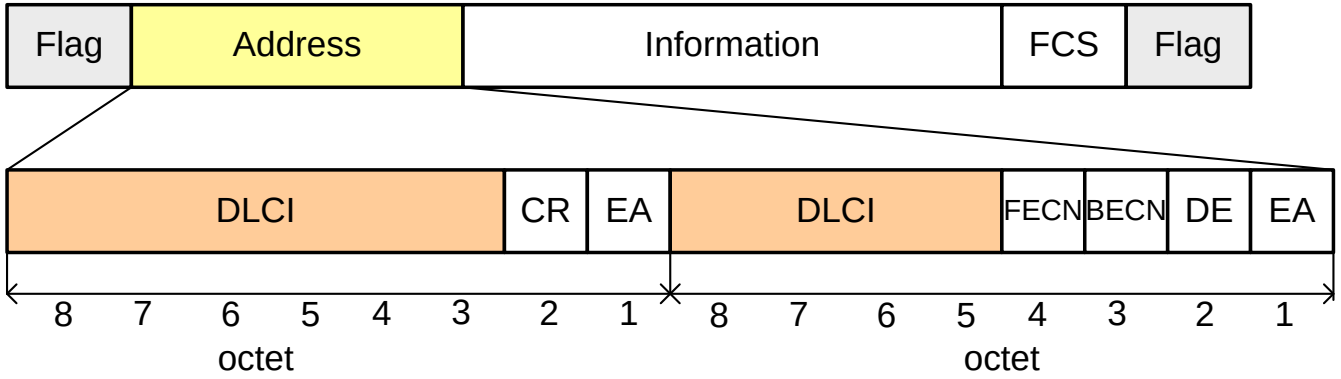


Incoming		Outgoing	
Int	DLCI	Int	DLCI
0	35	1	432

Incoming		Outgoing	
Int	DLCI	Int	DLCI
0	101	2	40
0	102	1	35

Incoming		Outgoing	
Int	DLCI	Int	DLCI
0	40	2	333

FR rámec

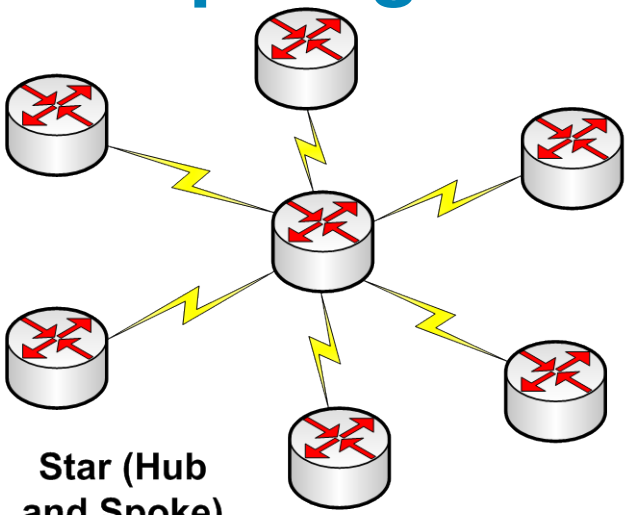


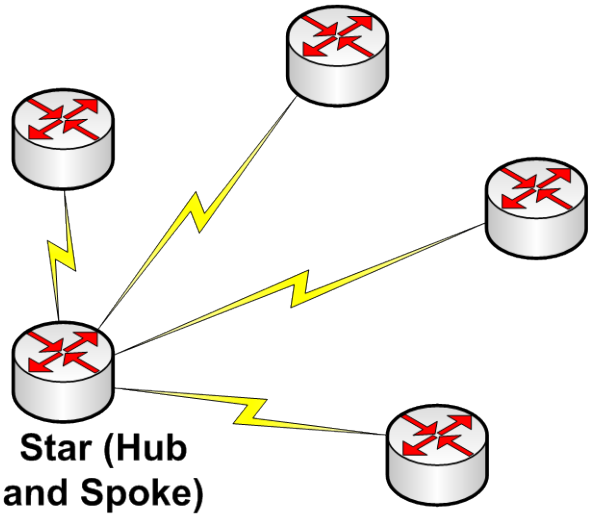
- Flag – 01111110
  - Značka začiatku a konca rámca (1 byte: 01111110)
- Address: 2B
  - DLCI - 10-bit DLCI
  - C/R – command/respond
  - E/A - Extended Address indicator
    - „1“ v rámci nie je ďalší adresný oktet
    - FR môže mať až 4 adresné oktety
  - Riadenie zahltenia
    - FECN: Forward Explicit Congestion Notification
    - BECN: Backward Explicit Congestion Notification
    - DE - Discard Eligibility
- Information: data
- FCS
  - Frame Check Sum, CRC, 2B

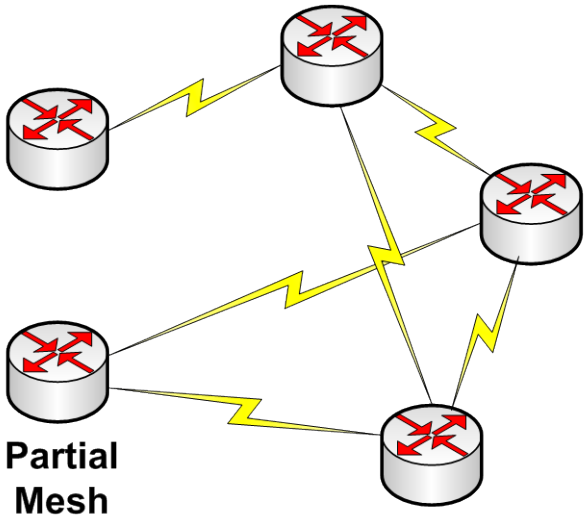
Dva druhy rámcov

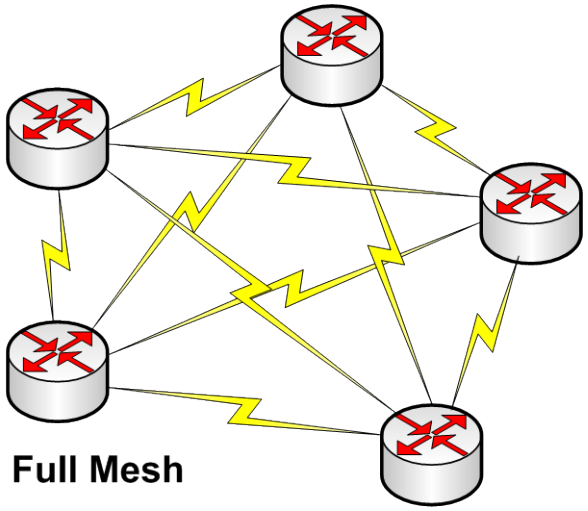
- Cisco: hlavička 4B
- IETF: hlavička 2B

FR topológie









Spôsoby poskytnutia FR prístupu

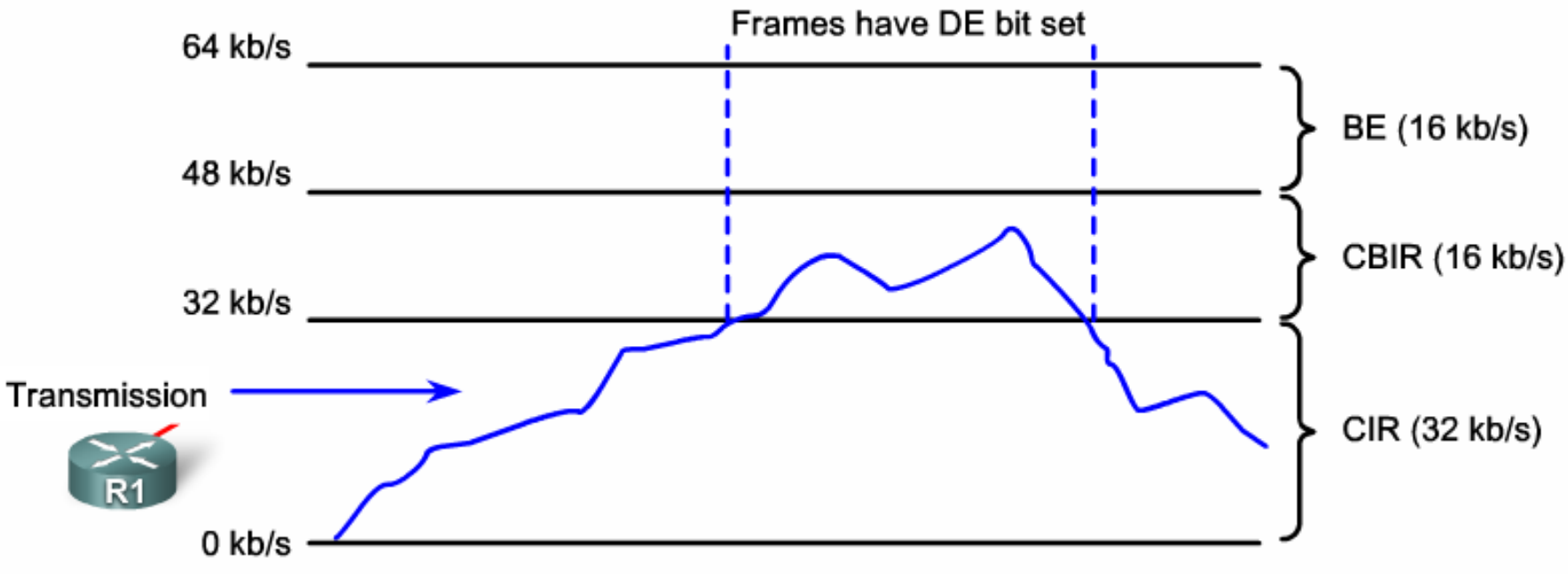
- **Viaceré spôsoby realizácie pripojenia a spoplatnenia**
  - **Access rate or port speed**
    - Provider poskytne prístupovú linku (prenajatý okruh) do POP, ktorej kapacita je dedikovaná zákaznikovi na pripojenie k FR
    - Typicky 56 kb/s, T1 (1.536 Mb/s), or Fractional T1 (násobok 56 kb/s or 64 kb/s).
      - Port speeds má nastavený clock na strane providera
    - Platba za linku podľa rýchlosti, rýchlejšie = drahšie
  - **PVC s Committed Information Rate (CIR)**
    - Vhodné pri Multiplexácií (prepojenie viac pobočiek)
    - Zákazník si dohodne parametre pre každý PVC s providerom, ktoré budú dodržované
    - Prenajatá prístupová linka, musí byť rýchlejšia aby dokázala obslúžiť všetky PVC pri multiplexovaní
      - Príklad: ak multiplexujeme 15 64 kbps PVCs, rýchlosť linky musí byť 960kbps (T1)

FR Oversubscription

- Oversubscription
  - Provider predá často väčšiu kapacitu ako fyzická rýchlosť linky
    - Málokedy pri data komunikácii idú všetci zákazníci naplno v rovnakom čase

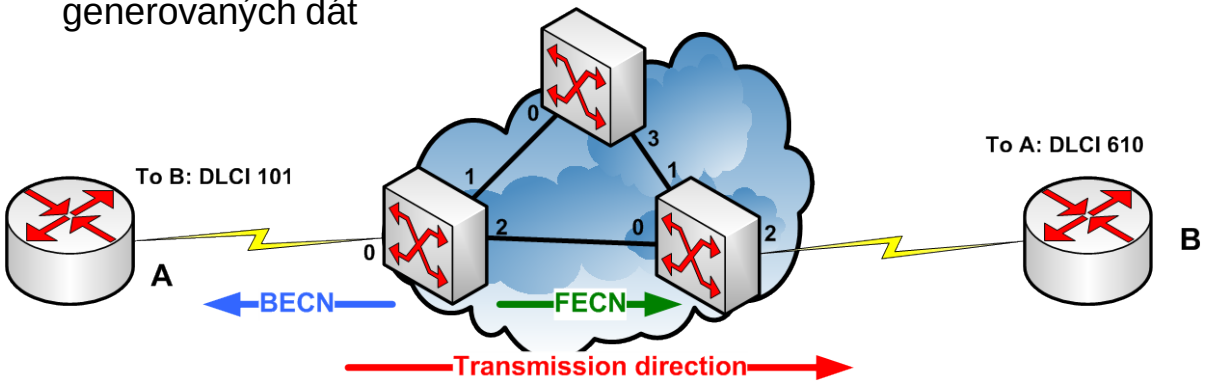
Parametre PVC

- Garantované parametre priepustnosti
  - CIR: Committed Information Rate
    - Garantovaná rýchlosť, počíta sa cez T_c
  - B_C: Committed Burst Size
    - max. počet bitov prenesených počas jednotky času Tc (v rámci CIR)
    - $B_C = T_C * CIR$
- Rozšírené parametre priepustnosti
  - Umožňuje zákaznikovi preniesť určité množstvo dát v špičke navyše nad CIR negarantovane
  - Committed Burst Information Rate (CBIR)
    - Maximálna priepustnosť dostupná zákaznikovi, CIR plus Be .
  - EIR: Extended (Excess) Information Rate
    - Typicky je EIR nastavená na rýchlosť rozhrania.
  - B_E: Extended (Excess) Burst Size
    - max. počet bitov nad Bc, ktoré je sieť schopná preniesť v danom Tc, takéto rámce sú označené DE (Discard Eliglible)
      - Rámce takto označené sieť prenesie ak má kapacitu, ak nemá okamžite ich dropne
    - $B_E = T_C * EIR$
      - Rámce nad CIR plus BE sú pri zahltení hneď dropnuté
- T_C: Measurement Interval


Frames have DE bit set
64 kb/s
48 kb/s
32 kb/s
0 kb/s
BE (16 kb/s)
CBIR (16 kb/s)
CIR (32 kb/s)
Transmission
R1

Riadenie toku a zahltenia

- FR nemá explicitné metódy riadenia toku
  - FR sieť používateľa len informuje o zahltení v sieti (Congestion Avoidance)
- Riadenie zahltenia
  - FR prepínače dropnú pakety zo zahltených zásobníkov
- Informácia o zahltení cez hlavičku:
  - **FECN**
    - Forward Explicit Congestion Notification
    - Informácia prijímateľovi toku, aby informoval komunikačného partnera (odosielateľa), aby znížil množstvo generovaných dát.
  - **BECN**
    - Backward Explicit Congestion Notification
    - BECN bit je nastavený za účelom informovania stanice aby znížila množstvo generovaných dát



Frame Relay (v porovnaní s prenajatými okruhmi)

- Pre firmy s viac pobočkami ponúka výhody
  - Jednoduchosť
    - Jednoduchosť technológie, konfigurácie
  - Flexibilita
    - Väčšia priepustnosť, spoľahlivosť ako prenajaté okruhy
  - Cena
    - Menej zariadení, jednoduchšia implementácia, menej zložitý, platba len za CIR nie za celú linku

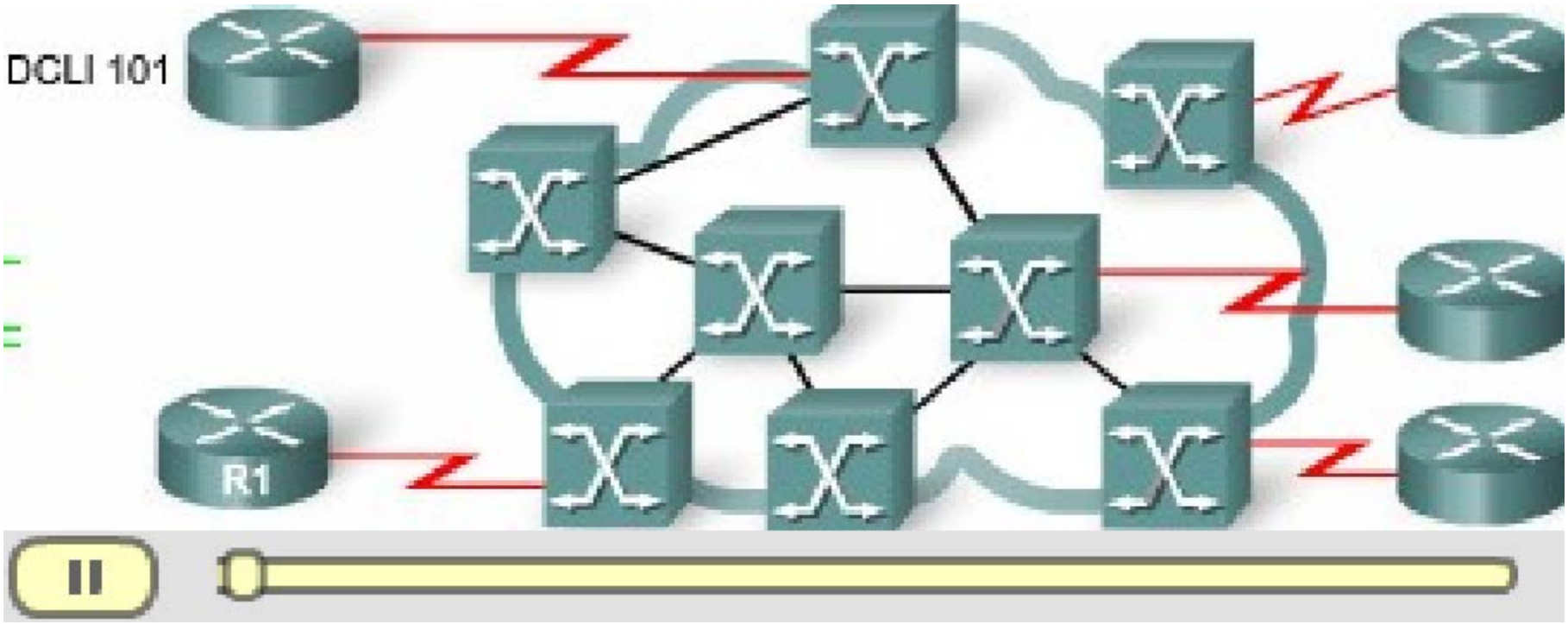
Frame Relay (v porovnaní s prenajatými okruhmi)

- Nevýhody
  - Pozn. mnoho závisí na kontrakte s providerom
  - Nie je vhodný pre časovo citlivé aplikácie
    - VoIP, video
  - Negarantuje doručenie rámcov

Mapovanie adries vo FR

- Ak chce smerovač komunikovať s iným smerovačom cez FR
  - musí vedieť mapovanie lokálnej DLCI (L2 adresa) na L3 IP adresu suseda
- Realizácia
  - Dynamicky
    - inARP (inverse ARP)
      - Smerovač zistí IP adresu suseda z DLCI adresy VC
      - Smerovač posiela cez všetky svoje VC inARP správy
      - Z odpovedí vytvára tabuľku mapovaná L3 IP na L2 DLCI
    - LMI (Local Management Interface)
  - Statické mapovanie
    - Manuálne zadáme aké IP adresy mapovať do akého DLCI VC
    - Použitie:
      - ak smerovač na druhej strane FR mračna nepodporuje inARP
      - Pri topológii Hub and Spoke, kde smerovače nie sú priamo susedia

inARP



LMI (Local Management Interface)

- Signálny štandard medzi DTE a Frame Relay prepínačom (DCE)
  - Doplnený do FR neskôr
  - Slúži na dynamické získavanie informácií o stave siete
- Funkcie poskytované LMI
  - Keepalive mechanizmus
    - Zisťuje stav spojenia medzi DCE a DTE
    - Posielanie dotazov každých 10s
      - Ak nedostanem odpoveď, spojenie je down
  - Používa aj inArp na mapovanie DLCI a IP
- LMI rozšírenia
  - Stavový mechanizmus
    - Aké VC sú k dispozícii
  - Multicast komunikácia pripojených
  - Priradenie globálneho významu pre DLCI
    - Ináč je defaultne lokálne (per hop sa mení)
  - Jednoduché riadenie toku
- Info o LMI **`show frame-relay lmi`**

LMI

- LMI definuje správy na komunikáciu medzi DTE a DCE
- Líšia sa implementácie LMI (druhy)
  - Cisco
  - Ansi
    - ANSI standard T1.617 Annex D
  - Q933a
    - ITU standard Q933 Annex A
- Podľa druhu LMI sa mení využitie niektorých DLCI (max1024)
- Konfigurácia LMI, ak je potrebná

  ```
  frame-relay lmi-type [cisco | ansi | q933a]
  ```
- Konfiguračne musí byť rovnaký typ na oboch stranách spojenia
  - t.j. DTE smerovač a FR prepínač
  - od Cisco IOS v11.2 je druh LMI zistený automaticky

Konfigurácia FR

Konfigurácia FR – nevyhnutné úkony

- Nastavenie enkapsulácie

```
! Nastavenie enkapsulácie
Switch(config)#int serial 0/0/0
Switch(config-if)#encapsulation frame-relay
```

- Konfigurácia dynamického alebo statického mapovania
  - Defaultne je spustené LMI, ktoré využíva inArp
    - Vypnutie LMI – **`no keepalive`**
    - Vypnutie inARP - **`no frame-relay inverse-arp`**

Základná konfigurácia, LMI a inARP podporované

Základné príkazy

```
! Specifikacia rozhrania
Router(config)# interface serial0

! Zadefinovane enkapsulacie
Router(config-if)# encapsulation frame-relay [cisco | ietf]

!zadefinovanie BW pre smerovaci protokol
Router(config-if)# bandwidth value-in-kbps

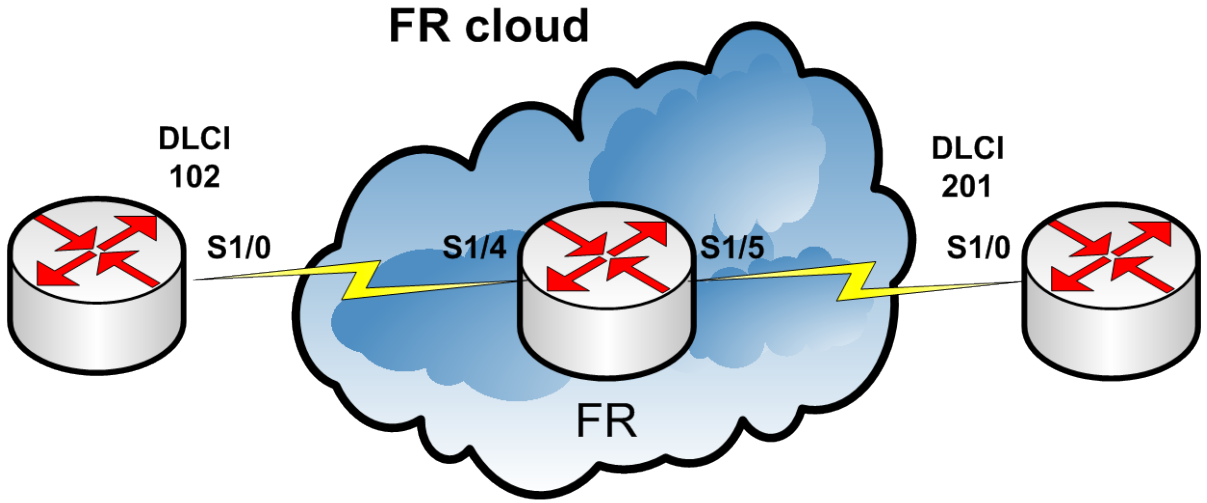
!popis rozhrania
Router(config-if)# description text

!volitelne, od 12.1 autosence
!Zadefinovanie LMI a druhu LMI
Router(config-if)# frame-relay lmi-type [ansi | cisco | q933a]

! Staticke mapovanie IP na DLCI
Router(config-if)# frame-relay map <protocol> <address> <DLCI> [broadcast]

! Nastavenie lokalneho DLCI
Router(config-if)# frame-relay interface-dlci DLCI_num
```

Konfiguráca smerovačov – DTE konce



Incoming int	DLCI	Outgoing int	DLCI
S1/4	102	S1/5	201
S1/5	201	S1/4	102

```
Lavy(config)#interface Serial1/0
Lavy(config-if)# ip address 1.0.0.1 255.255.255.252
Lavy(config-if)# encapsulation frame-relay
Lavy(config-if)#no shut
```

```
Pravy(config)#interface Serial1/0
Pravy(config-if)# ip address 1.0.0.2 255.255.255.252
Pravy(config-if)# encapsulation frame-relay
Pravy(config-if)#no shut
```

Overenie konfigurácie – DTE smerovač

```
Lavy#sh int s 1/0
Serial1/0 is up, line protocol is up
  Hardware is M4T
  Internet address is 1.0.0.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  LMI enq sent  92, LMI stat recvd 92, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  Broadcast queue 0/64, broadcasts sent/dropped 1/0, interface broadcasts 0
  Last input 00:00:07, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:15:27
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     99 packets input, 1928 bytes, 0 no buffer
```

Overenie konfigurácie – DTE smerovač

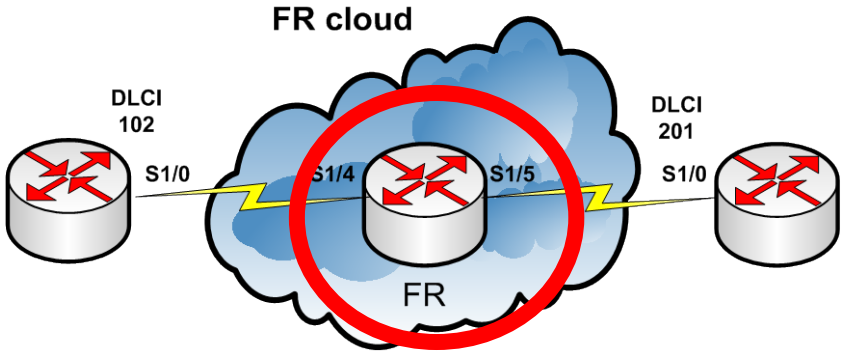
```
Lavy#sh frame-relay map
Serial1/0 (up): ip 1.0.0.2 dlci 102(0x66,0x1860), dynamic,
                broadcast,, status defined, active
```

```
Lavy#sh frame-relay pvc
PVC Statistics for interface Serial1/0 (Frame Relay DTE)
               Active     Inactive      Deleted       Static
  Local           1            0            0            0
  Switched        0            0            0            0
  Unused          0            0            0            0

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial1/0

  input pkts 15            output pkts 18           in bytes 1210
  out bytes 1662           dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                  out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 3         out bcast bytes 102
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:38:46, last time pvc status changed 00:37:46
```

Konfiguráca smerovača ako FR prepínač (DCE)



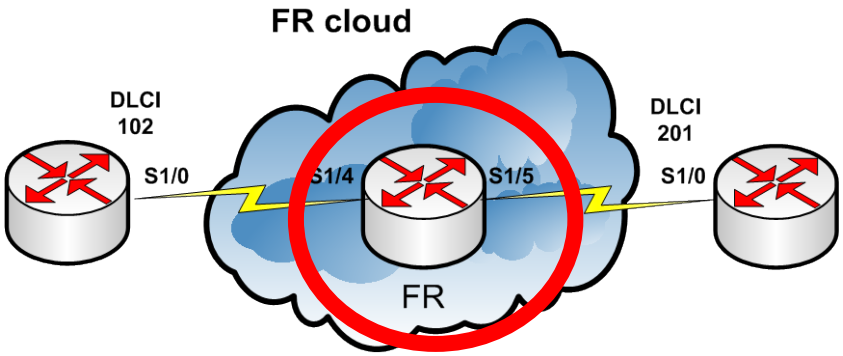
Incoming int	DLCI	Outgoing int	DLCI
S1/4	102	S1/5	201
S1/5	201	S1/4	102

```
!konfiguracia FR prepinania
FR(config)#frame-relay switching

! Konfigurácia rozhraní
FR(config)#int s1/4
FR(config-if)#encapsulation frame-relay
FR(config-if)#frame-relay intf-type dce
FR(config-if)#clock rate 64000
FR(config-if)#no shut
FR(config-if)#int s 1/5
FR(config-if)#encapsulation frame-relay
FR(config-if)#frame-relay intf-type dce
FR(config-if)#clock rate 64000
FR(config-if)#no shut

!Konfigurácia FR prepinacej mapy
FR(config)#int s 1/4
FR(config-if)#frame-relay route 102 int s 1/5 201
FR(config-if)#int s 1/5
FR(config-if)#frame-relay route 201 interface s1/4 102
```

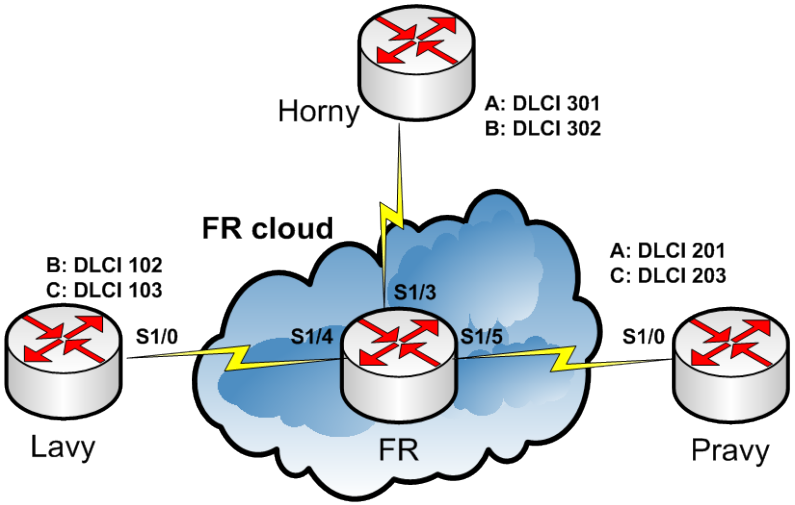
Overenie FR prepínacej mapy



Incoming int	DLCI	Outgoing int	DLCI
S1/4	102	S1/5	201
S1/5	201	S1/4	102

```
FR#sh frame-relay route
Input Intf      Input Dlci      Output Intf     Output Dlci     Status
Serial1/4       102             Serial1/5       201             active
Serial1/5       201             Serial1/4       102             active
```

Príklad 2 – Full mesh



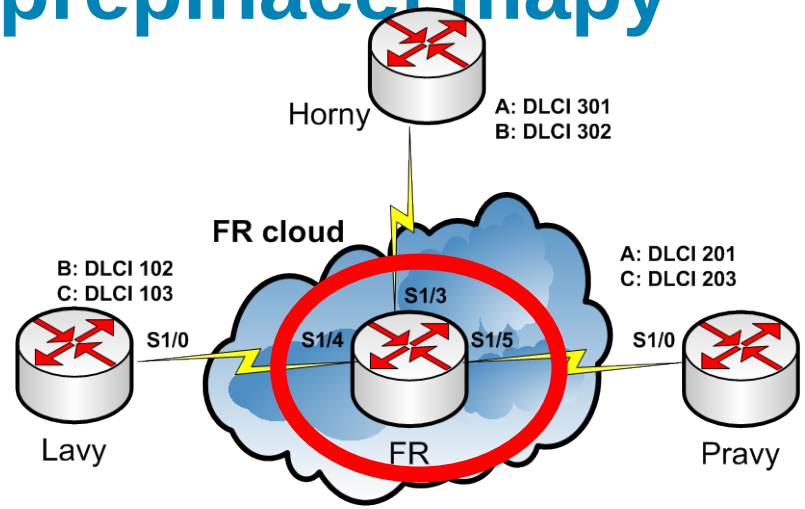
Incoming int	DLCI	Outgoing int	DLCI
S1/4	103	S1/3	301
S1/4	102	S1/5	201
S1/5	201	S1/4	102
S1/5	203	S1/3	302
S1/3	301	S1/4	103
S1/3	302	S1/5	203

```
Lavy(config)#interface Serial1/0
Lavy(config-if)# ip address 1.0.0.1 255.255.255.0
Lavy(config-if)# encapsulation frame-relay
Lavy(config-if)#no shut
```

```
Pravy(config)#interface Serial1/0
Pravy(config-if)# ip address 1.0.0.2 255.255.255.0
Pravy(config-if)# encapsulation frame-relay
Pravy(config-if)#no shut
```

```
Horny(config)#interface Serial1/0
Horny(config-if)# ip address 1.0.0.3 255.255.255.0
Horny(config-if)# encapsulation frame-relay
Horny(config-if)#no shut
```

Overenie prepínacej mapy



Incoming int	DLCI	Outgoing int	DLCI
S1/4	103	S1/3	301
S1/4	102	S1/5	201
S1/5	201	S1/4	102
S1/5	203	S1/3	302
S1/3	301	S1/4	103
S1/3	302	S1/5	203

```
FR#sh frame-relay route
Input Intf      Input Dlci      Output Intf     Output Dlci     Status
Serial1/3       301             Serial1/4       103             active
Serial1/3       302             Serial1/5       203             active
Serial1/4       102             Serial1/5       201             active
Serial1/4       103             Serial1/3       301             active
Serial1/5       201             Serial1/4       102             active
Serial1/5       203             Serial1/3       302             active
```

Overenie konfigurácie – DTE smerovač

```
Lavy# sh frame-relay map
Serial1/0 (up): ip 1.0.0.2 dlci 102(0x66,0x1860), dynamic,
              broadcast,, status defined, active
Serial1/0 (up): ip 1.0.0.3 dlci 103(0x67,0x1870), dynamic,
              broadcast,, status defined, active
```

```
Lavy# sh frame-relay pvc
PVC Statistics for interface Serial1/0 (Frame Relay DTE)
             Active     Inactive      Deleted       Static
  Local          2            0            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0
DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial1/0
  input pkts 15            output pkts 18           in bytes 1210
  out bytes 1662           dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 3         out bcast bytes 102
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:38:46, last time pvc status changed 00:37:46

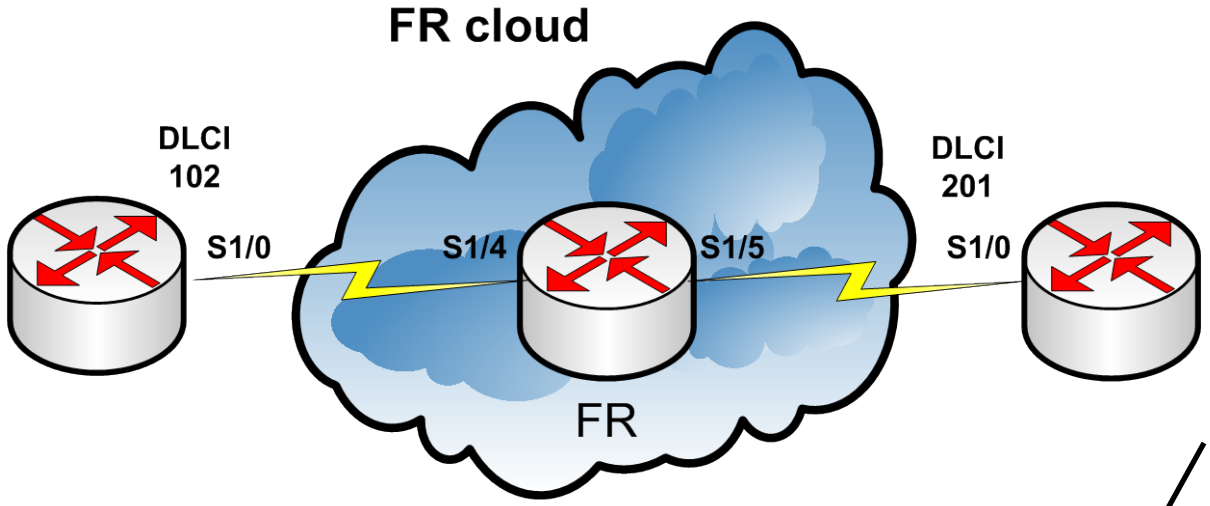
DLCI = 103, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial1/0

  input pkts 6             output pkts 6            in bytes 554
  out bytes 554            dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 1         out bcast bytes 34
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:12:44, last time pvc status changed 00:07:04
```

Konfigurácia statickej FR mapy

Vykonávame v prípade nedostupnosti inARP

Konfiguráca smerovačov – DTE konce



Incoming int	DLCI	Outgoing int	DLCI
S1/4	102	S1/5	201
S1/5	201	S1/4	102

Simulujeme nedostupnosť inARP tak, že ho vypneme

```
Lavy(config)#interface Serial1/0
Lavy(config)#ip address 1.0.0.1 255.255.255.252
Lavy(config)#encapsulation frame-relay
Lavy(config)#no frame-relay inverse-arp
Lavy(config)#no shut
```

```
Pravy(config)#interface Serial1/0
Pravy(config)#ip address 1.0.0.2 255.255.255.252
Pravy(config)#encapsulation frame-relay
Pravy(config)#no frame-relay inverse-arp
Pravy(config)#no shut
```

Overenie konfigurácie – DTE smerovač

```
Lavy#ping 1.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

```
Lavy#sh frame-relay map

Lavy#
```

InARP je vypnutý, nemám ako zistiť adresu suseda

Konfigurácia statickej mapy

```
Router(config-if)# frame-relay map protocol protocol-address dlci [broadcast]
```

Pridáme mapovanie IP na DLCI do oboch DTE smerovačov

```
Lavy(config)#interface Serial1/0
Lavy(config)#frame-relay map ip 1.0.0.2 102 broadcast
Lavy(config)#no shut
```

```
Pravy(config)#interface Serial1/0
Pravy(config)#frame-relay map ip 1.0.0.1 201 broadcast
Pravy(config)#no shut
```

Overenie mapovania

```
Lavy#sh frame-relay map
Serial1/0 (up): ip 1.0.0.2 dlci 102(0x66,0x1860), static,
              broadcast,
               CISCO, status defined, active
```

Overenie dostupnosti

```
Lavy#ping 1.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/20/40 ms
```

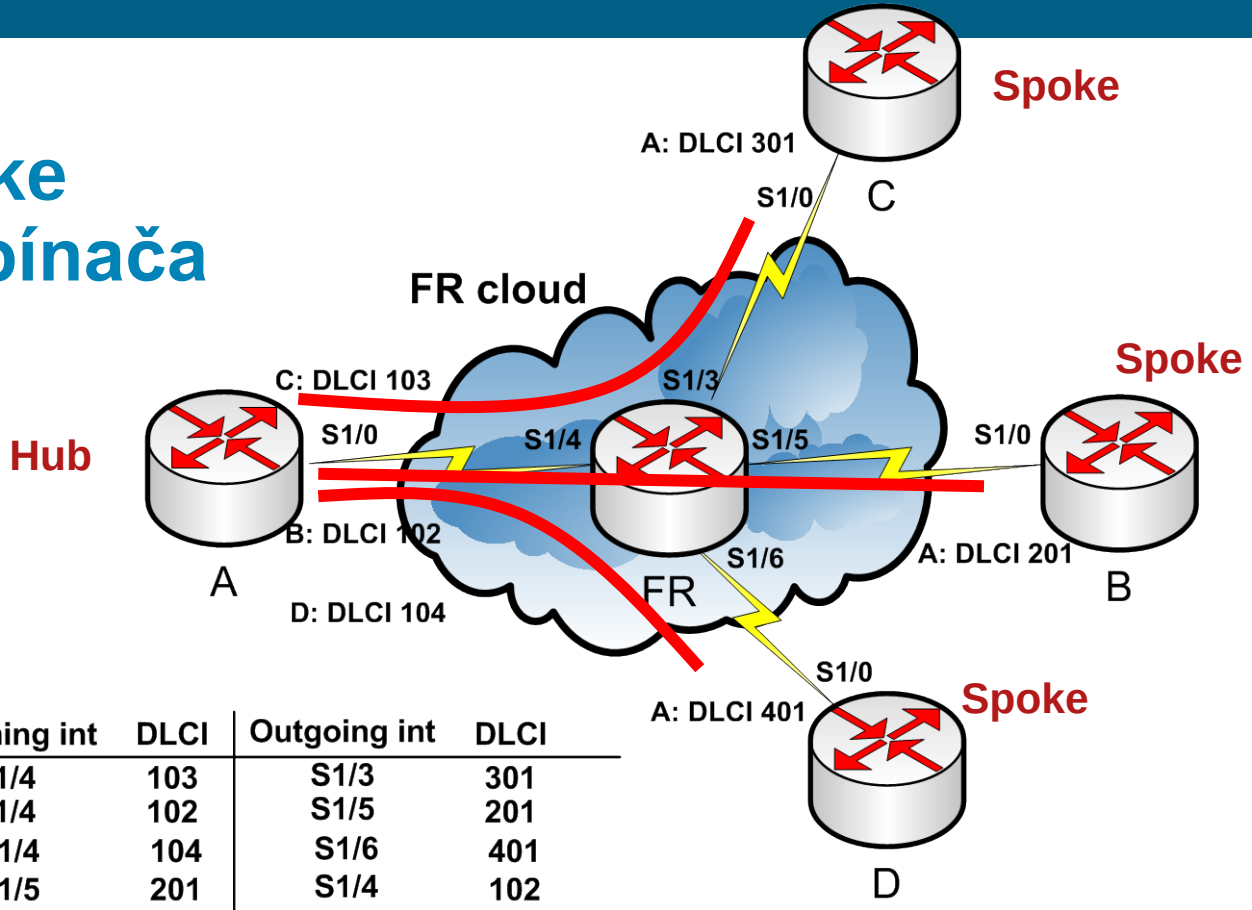
Voľba Broadcast

```
Lavy(config)#interface Serial1/0
Lavy(config)#frame-relay map ip 1.0.0.2 102 broadcast
Lavy(config)#no shut
```

- FR je NBMA sieť a nepodporuje zasielanie broadcastov (aj mcastov) cez PVC
  - Niektoré smerovacie protokoly to k činnosti vyžadujú (RIP. EIGRP, OSPF)
  - Voľba **broadcast** aktivuje zasielanie bcast a mcast paketov cez PVC

Pokročilejšie techniky FR

Príklad 3
– Hub and spoke
- konf. FR prepínača



Incoming int	DLCI	Outgoing int	DLCI
S1/4	103	S1/3	301
S1/4	102	S1/5	201
S1/4	104	S1/6	401
S1/5	201	S1/4	102
S1/3	301	S1/4	103
S1/6	401	S1/4	104

```
FR#sh frame-relay route
Input Intf      Input Dlci      Output Intf     Output Dlci     Status
Serial1/3       301             Serial1/4       103             inactive
Serial1/4       102             Serial1/5       201             inactive
Serial1/4       103             Serial1/3       301             inactive
Serial1/4       104             Serial1/6       401             inactive
Serial1/5       201             Serial1/4       102             inactive
Serial1/6       401             Serial1/4       104             inactive
```

Príklad 3 - Hub and spoke - konf. Spoke smerovačov

```
A(config-if)#int s 1/0
A(config-if)#encapsulation frame-relay
A(config-if)#ip add 1.0.0.1 255.255.255.0
A(config-if)#no shut
```

```
B(config)#int s 1/0
B(config-if)#encapsulation frame-relay
B(config-if)#ip add 1.0.0.2 255.255.255.0
B(config-if)#no shut
```

```
C(config)#int s 1/0
C(config-if)#encapsulation frame-relay
C(config-if)#ip add 1.0.0.3 255.255.255.0
C(config-if)#no shut
```

```
D(config)#int s 1/0
D(config-if)#encap fram
D(config-if)#ip add 1.0.0.4 255.255.255.0
D(config-if)#no shut
```

Akú konektivitu budeme mať?

```
A#ping 1.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/16/44 ms
A#ping 1.0.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/16/36 ms
A#ping 1.0.0.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/15/40 ms
```

Hub

- Konektivita s každým spoke

```
B#ping 1.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/40/72 ms

B#ping 1.0.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
B#ping 1.0.0.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Spoke

- Konektivita len s Hub s inými spoke nie je
- Každý spoke

Kde je problém?

```
A#sh frame-relay map
Serial1/0 (up): ip 1.0.0.2 dlci 102(0x66,0x1860), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 1.0.0.3 dlci 103(0x67,0x1870), dynamic,
                broadcast,, status defined, active
Serial1/0 (up): ip 1.0.0.4 dlci 104(0x68,0x1880), dynamic,
                broadcast,, status defined, active
```

```
B#sh frame-relay map
Serial1/0 (up): ip 1.0.0.1 dlci 201(0xC9,0x3090), dynamic,
                broadcast,, status defined, active
```

```
C#sh frame-relay map
Serial1/0 (up): ip 1.0.0.1 dlci 301(0x12D,0x48D0),dynamic,
                broadcast,, status defined, active
```

```
D#sh frame-relay map
Serial1/0 (up): ip 1.0.0.1 dlci 401(0x191,0x6410),dynamic,
                broadcast,, status defined, active
```

- InARP poskytne mapovanie IP na DLCI medzi susedmi
- Spoke smerovače nie sú susedia
  - Nemám mapovanie ich IP na DLCI

Riešenie – pridať statické mapovanie na spoke smerovače

```
B(config)#int s 1/0
B(config-if)#frame-relay map ip 1.0.0.3 201 broadcast
B(config-if)#frame-relay map ip 1.0.0.4 201 broadcast
```

```
C(config)#int s 1/0
C(config-if)#frame-relay map ip 1.0.0.2 301 broadcast
C(config-if)#frame-relay map ip 1.0.0.4 301 broadcast
```

```
D(config)#int s 1/0
D(config-if)#frame-relay map ip 1.0.0.2 401 broadcast
D(config-if)#frame-relay map ip 1.0.0.3 401 broadcast
```

Overenie – spoke smerovač B

```
B#sh frame-relay map
Serial1/0 (up): ip 1.0.0.1 dlci 201(0xC9,0x3090), dynamic,
              broadcast,, status defined, active
Serial1/0 (up): ip 1.0.0.3 dlci 201(0xC9,0x3090), static,
              broadcast,
              CISCO, status defined, active
Serial1/0 (up): ip 1.0.0.4 dlci 201(0xC9,0x3090), static,
              broadcast,
              CISCO, status defined, active
```

```
B#ping 1.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/26/64 ms
B#ping 1.0.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/32/48 ms
B#ping 1.0.0.4

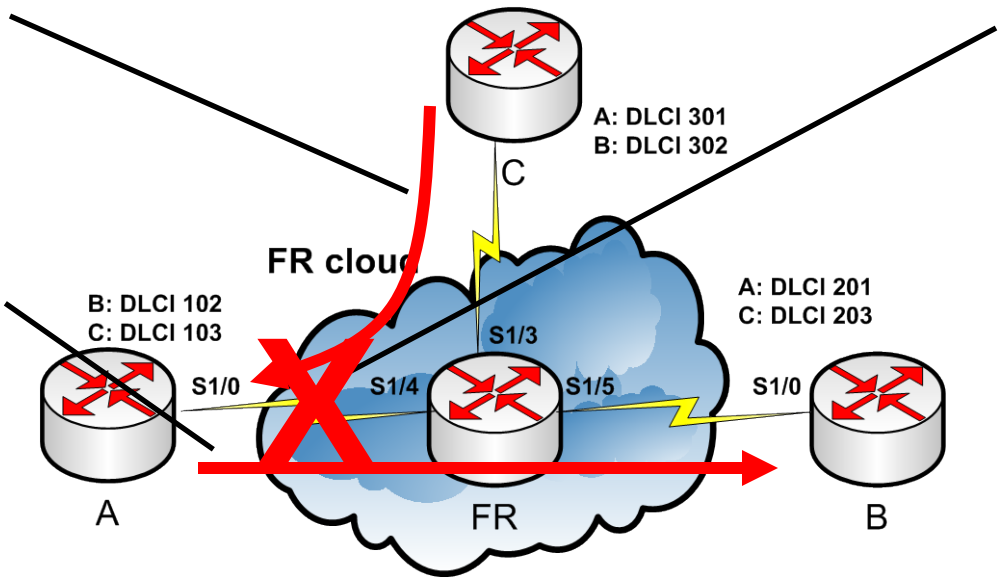
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/30/92 ms
```

FR problémy s dostupnosťou

- FR je NBMA sieť
- Pri nasadení smerovacích protokolov, ktoré pracujú so Split Horizon
  - Môžeme nad FR mať problémy s dostupnosťou (Hub and Spoke topo.).
    - SPLIT zabraňuje posielanie informácií o danej sieti naučených z daného smeru späť cez to isté rozhranie

Ak C pošle routing update A, A ho príjme cez linku a dané PVC

A by malo poslať update svojím susedom cez iné PVC, ale tú istú linku



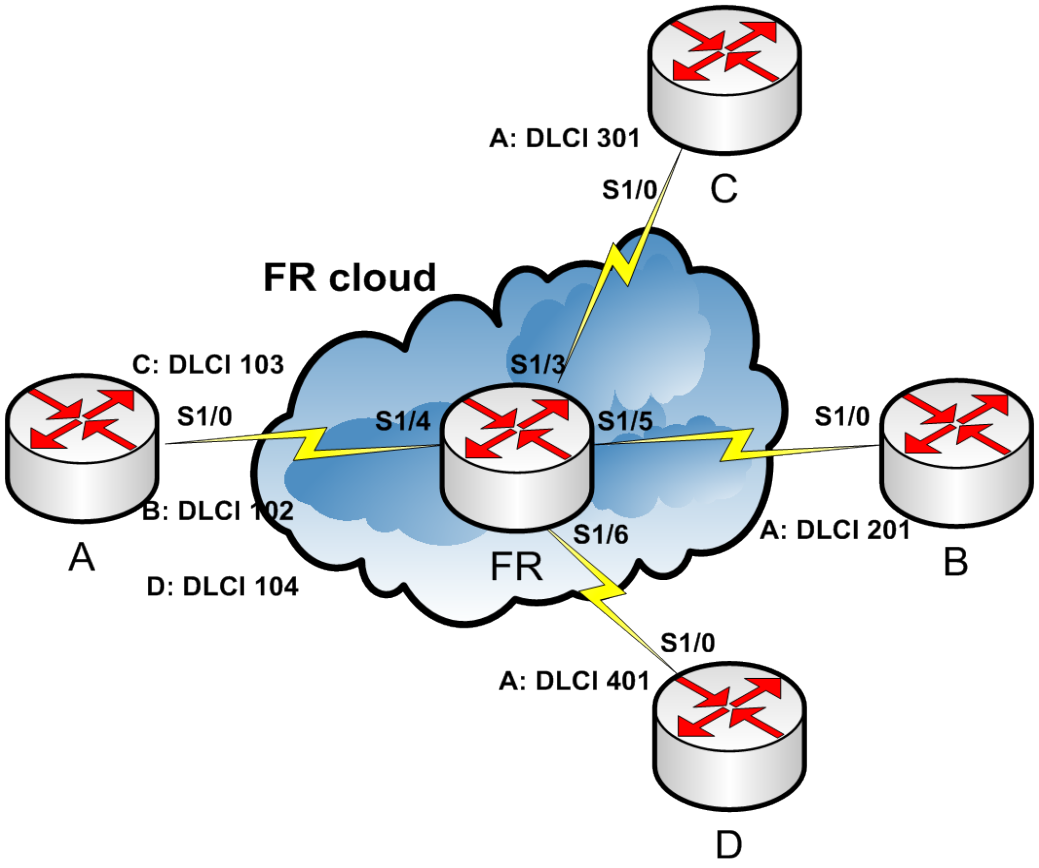
Split horizon zablokuje poslanie update

Riešenie split horizon problému

- Vypnutie split horizon na rozhraní
  - Podporuje len IP protokol
    - IPX a Apple nie
    - Pre RIP je split-horizon automaticky vypnutý
- Iné riešenie
  - Rozdeliť fyzické rozhrania na viac subrozhraní
  - Subrozhrania môžu byť typu
    - **Point-to-point**
      - split hotizon rieší
    - **Point-to-multipoint**
      - split hotizon nerieší

Topo z príkladu 3

- Pridáme LAN siete na každý smerovač a zapneme RIP
  - A:
    - LAN 10.0.0.0/8
    - fa 0/0: 10.0.0.1
  - B:
    - LAN 20.0.0.0/8
    - fa 0/0: 20.0.0.1
  - C:
    - LAN 30.0.0.0/8
    - fa 0/0: 30.0.0.1
  - D:
    - LAN 40.0.0.0/8
    - fa 0/0: 40.0.0.1



RIP nad FR

```
B#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
    inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
    type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 -
    IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-
    user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
C       1.0.0.0 is directly connected, Serial1/0
C    20.0.0.0/8 is directly connected, FastEthernet0/0
R    40.0.0.0/8 [120/1] via 1.0.0.1, 00:00:12, Serial1/0
R    10.0.0.0/8 [120/1] via 1.0.0.1, 00:00:20, Serial1/0
R    30.0.0.0/8 [120/1] via 1.0.0.1, 00:00:20, Serial1/0
```

Routing frčí lebo RIP ma def. Vypnuté split horizon

EIGRP nad FR

```
A#sh ip route                                          Hub - Vypada to OK
     1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       1.0.0.0/24 is directly connected, Serial1/0
D       1.0.0.0/8 is a summary, 00:02:33, Null0
D    20.0.0.0/8 [90/2172416] via 1.0.0.2, 00:02:12, Serial1/0
D    40.0.0.0/8 [90/2172416] via 1.0.0.4, 00:00:36, Serial1/0
C    10.0.0.0/8 is directly connected, FastEthernet0/0
D    30.0.0.0/8 [90/2172416] via 1.0.0.3, 00:01:41, Serial1/0
```

```
B#sh ip route                                  Spoke – problém, siete chýbajú
     1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       1.0.0.0/24 is directly connected, Serial1/0
D       1.0.0.0/8 is a summary, 00:05:58, Null0
C    20.0.0.0/8 is directly connected, FastEthernet0/0
D    10.0.0.0/8 [90/2172416] via 1.0.0.1, 00:05:10, Serial1/0
```

```
C#sh ip route                                  Spoke – problém, siete chýbajú
     1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       1.0.0.0/24 is directly connected, Serial1/0
D       1.0.0.0/8 is a summary, 00:05:56, Null0
D    10.0.0.0/8 [90/2172416] via 1.0.0.1, 00:05:31, Serial1/0
C    30.0.0.0/8 is directly connected, FastEthernet0/0
```

```
D#sh ip route                                  Spoke – problém, siete chýbajú
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       1.0.0.0/24 is directly connected, Serial1/0
D       1.0.0.0/8 is a summary, 00:04:59, Null0
C    40.0.0.0/8 is directly connected, FastEthernet0/0
D    10.0.0.0/8 [90/2172416] via 1.0.0.1, 00:05:04, Serial1/0
```

EIGRP riešenie – zákaz split horizon na spoke smerovači

```
Router(config-if)#no ip split-horizon eigrp AS
```

```
A(config-if)#no ip split-horizon eigrp 1
```

EIGRP nad FR – route tab. je kompletná

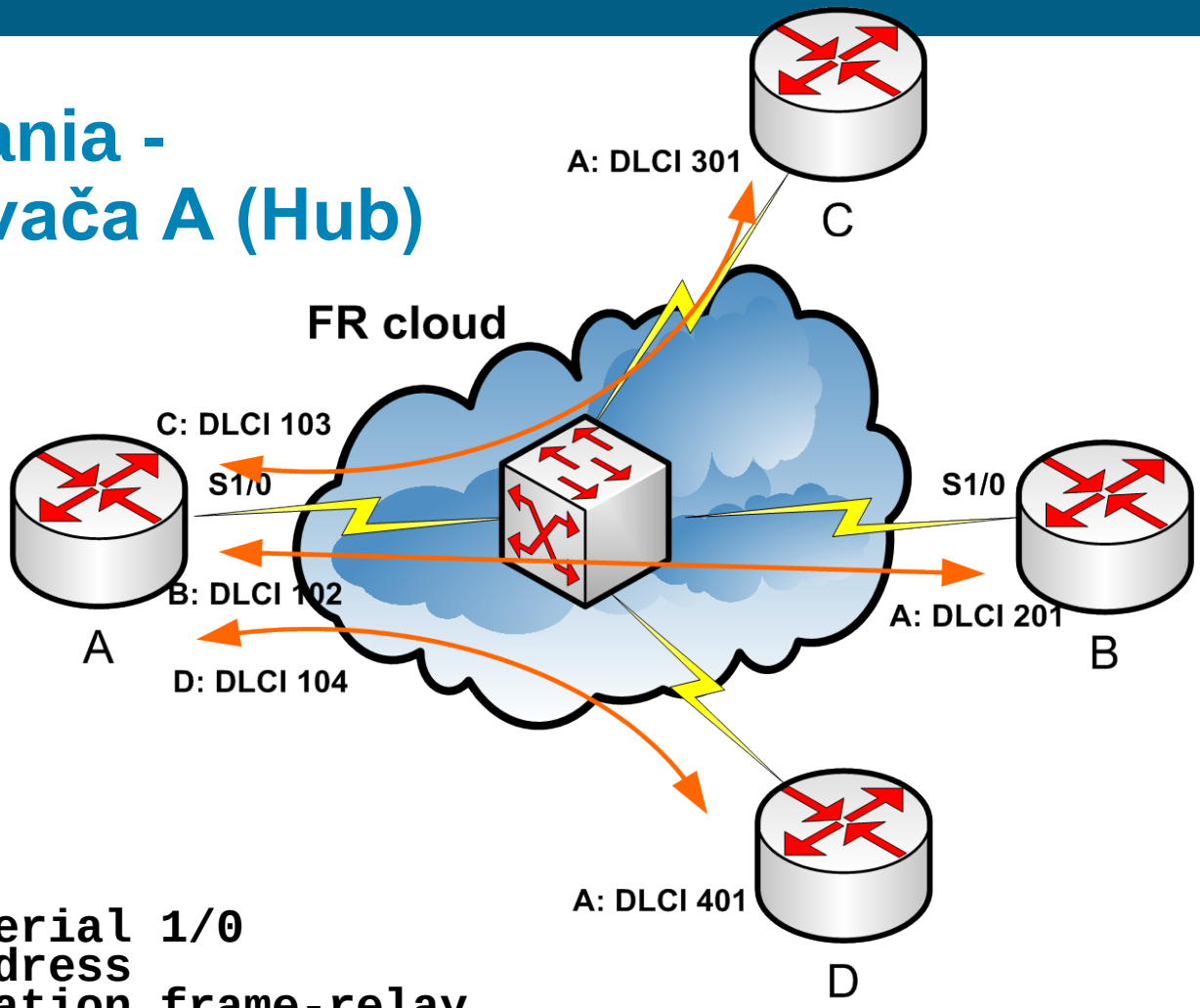
```
B#sh ip route
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.0.0.0/24 is directly connected, Serial1/0
D        1.0.0.0/8 is a summary, 00:10:15, Null0
C     20.0.0.0/8 is directly connected, FastEthernet0/0
D     40.0.0.0/8 [90/2684416] via 1.0.0.1, 00:00:05, Serial1/0
D     10.0.0.0/8 [90/2172416] via 1.0.0.1, 00:00:05, Serial1/0
D     30.0.0.0/8 [90/2684416] via 1.0.0.1, 00:00:05, Serial1/0
```

```
C#sh ip route
 1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.0.0.0/24 is directly connected, Serial1/0
D        1.0.0.0/8 is a summary, 00:09:49, Null0
D     20.0.0.0/8 [90/2684416] via 1.0.0.1, 00:00:39, Serial1/0
D     40.0.0.0/8 [90/2684416] via 1.0.0.1, 00:00:39, Serial1/0
D     10.0.0.0/8 [90/2172416] via 1.0.0.1, 00:00:39, Serial1/0
C     30.0.0.0/8 is directly connected, FastEthernet0/0
```

```
D#sh ip route
       1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.0.0.0/24 is directly connected, Serial1/0
D        1.0.0.0/8 is a summary, 00:08:44, Null0
D     20.0.0.0/8 [90/2684416] via 1.0.0.1, 00:00:59, Serial1/0
C     40.0.0.0/8 is directly connected, FastEthernet0/0
D     10.0.0.0/8 [90/2172416] via 1.0.0.1, 00:00:59, Serial1/0
D     30.0.0.0/8 [90/2684416] via 1.0.0.1, 00:00:59, Serial1/0
```

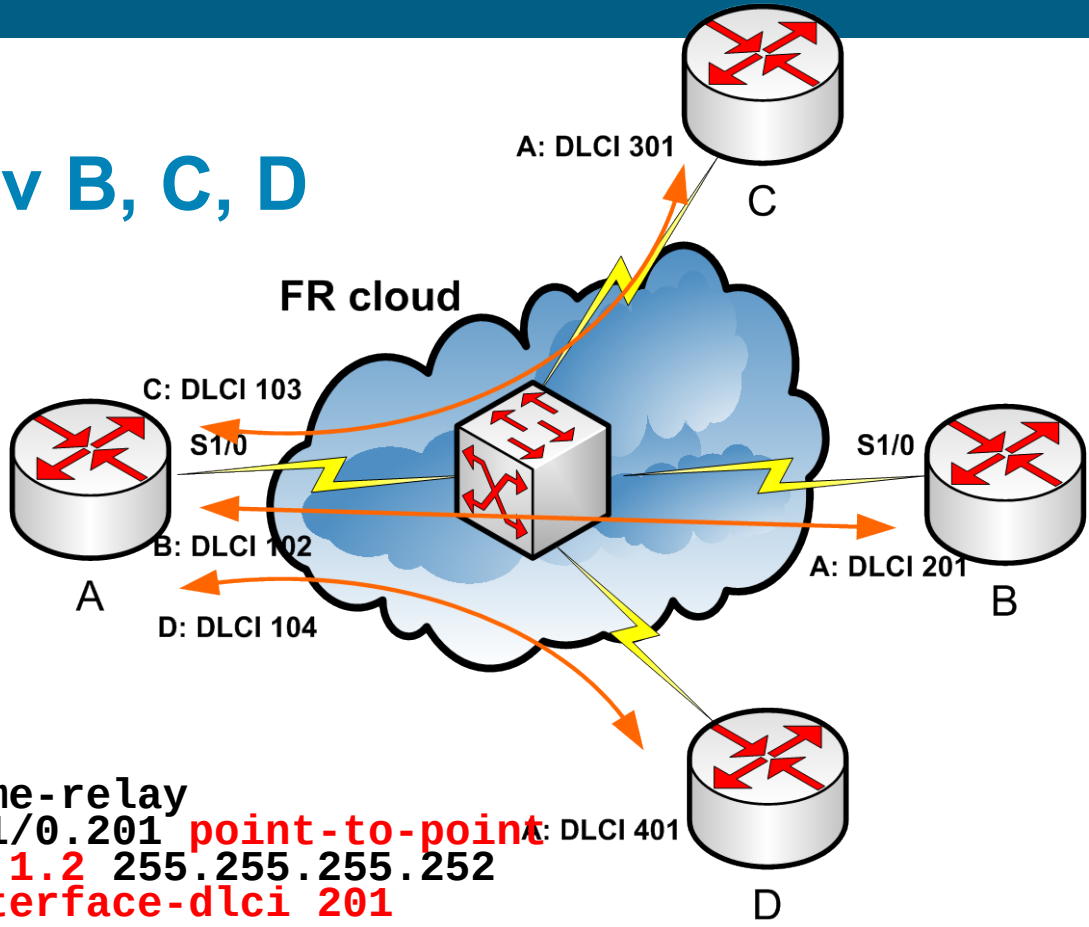
Riešenie cez subinterfaces

FR subrozhrania - Konf. Smerovača A (Hub)




```
A(config)# interface serial 1/0
A(config-if)# no ip address
A(config-if)# encapsulation frame-relay
A(config-if)# interface serial 1/0.102 point-to-point
A(config-subif)# frame-relay interface-dlci 102
A(config-subif)# ip add 192.168.1.1 255.255.255.252
A(config-subif)# interface serial 1/0.103 point-to-point
A(config-subif)# frame-relay interface-dlci 103
A(config-subif)# ip add 192.168.2.1 255.255.255.252
A(config-subif)# interface serial0.104 point-to-point
A(config-subif)# frame-relay interface-dlci 104
A(config-subif)# ip add 192.168.3.1 255.255.255.252
```

FR subrozhrania
Konf. smerovačov B, C, D (Spoke)




```
B(config)# interface serial 1/0
B(config-if)# no ip address
B(config-if)# encapsulation frame-relay
B(config-if)# interface serial 1/0.201 point-to-point
B(config-subif)# ip add 192.168.1.2 255.255.255.252
B(config-subif)# frame-relay interface-dlci 201

C(config)# interface serial 1/0
C(config-if)# no ip address
C(config-if)# encapsulation frame-relay
C(config-if)# interface serial 1/0.301 point-to-point
C(config-subif)# ip add 192.168.2.2 255.255.255.252
C(config-subif)# frame-relay interface-dlci 301

D(config)# interface serial 1/0
D(config-if)# no ip address
D(config-if)# encapsulation frame-relay
D(config-if)# interface serial 1/0.401 point-to-point
D(config-subif)# ip add 192.168.3.2 255.255.255.252
D(config-subif)# frame-relay interface-dlci 401
```

Overenie a diagnostika FR

Príkazy

```
! Info o enkaps a stave rozhrania
sh interface serial 0/0
```

```
! Zobrazi FR mapovanie IP a DLCI - InARP
sh frame-relay map
```

```
! Zobrazi FR mapovanie IP a DLCI
sh frame-relay map
```

```
! Zobrazi info o PVC
sh frame-relay pvc
```

Príkazy

```
! Info o type a stave LMI, DTE, DCE type
A#sh frame-relay lmi

LMI Statistics for interface Serial1/0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0                Invalid Prot Disc 0
  Invalid dummy Call Ref 0                 Invalid Msg Type 0
  Invalid Status Message 0                 Invalid Lock Shift 0
  Invalid Information ID 0                 Invalid Report IE Len 0
  Invalid Report Request 0                 Invalid Keep IE Len 0
  Num Status Enq. Sent 421                 Num Status msgs Rcvd 412
  Num Update Status Rcvd 0                 Num Status Timeouts 9
  Last Full Status Req 00:00:38            Last Full Status Rcvd 00:00:38
```

```
! Info o PVC
A#sh frame-relay pvc

PVC Statistics for interface Serial1/0 (Frame Relay DTE)

                Active     Inactive      Deleted       Static
  Local            3            0            0            0
  Switched         0            0            0            0
  Unused           0            0            0            0

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial1/0

  input pkts 202             output pkts 109           in bytes 15070
  out bytes 8748             dropped pkts 0            in pkts dropped 0
  out pkts dropped 0                     out bytes dropped 0
  in FECN pkts 0             in BECN pkts 0            out FECN pkts 0
  out BECN pkts 0            in DE pkts 0              out DE pkts 0
  out bcast pkts 62          out bcast bytes 4438
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 01:10:02, last time pvc status changed 01:06:52

DLCI = 103, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial1/0
……
```

Príkazy

```
! Info o konketnom PVC

A#sh frame-relay pvc ?
  interface
  <16-1022>  DLCI
  |          Output modifiers
  <cr>

A#sh frame-relay pvc 103

PVC Statistics for interface Serial1/0 (Frame Relay DTE)

DLCI = 103, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial1/0

  input pkts 188           output pkts 107          in bytes 14288
  out bytes 8500           dropped pkts 0           in pkts
dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts
0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 64        out bcast bytes 4566
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 01:12:01, last time pvc status changed 01:06:21
```

Príkazy

```
!debug udalosti

A# debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
A#
*Mar  1 01:29:54.823: Serial1/0(out): StEng, myseq 186, yourseen 185, DTE up
*Mar  1 01:29:54.823: datagramstart = 0x2DB0D74, datagramsize = 13
*Mar  1 01:29:54.827: FR encap = 0xFCF10309
*Mar  1 01:29:54.827: 00 75 01 01 01 03 02 BA B9
*Mar  1 01:29:54.827:
*Mar  1 01:29:54.839: Serial1/0(in): Status, myseq 186, pak size 13
*Mar  1 01:29:54.839: RT IE 1, length 1, type 1
*Mar  1 01:29:54.839: KA IE 3, length 2, yourseq 186, myseq 186
*Mar  1 01:30:04.823: Serial1/0(out): StEng, myseq 187, yourseen 186, DTE up
*Mar  1 01:30:04.823: datagramstart = 0x2DB1274, datagramsize = 13
*Mar  1 01:30:04.823: FR encap = 0xFCF10309
*Mar  1 01:30:04.827: 00 75 01 01 01 03 02 BB BA
*Mar  1 01:30:04.827:
*Mar  1 01:30:04.839: Serial1/0(in): Status, myseq 187, pak size 13
*Mar  1 01:30:04.839: RT IE 1, length 1, type 1
*Mar  1 01:30:04.839: KA IE 3, length 2, yourseq 187, myseq 187

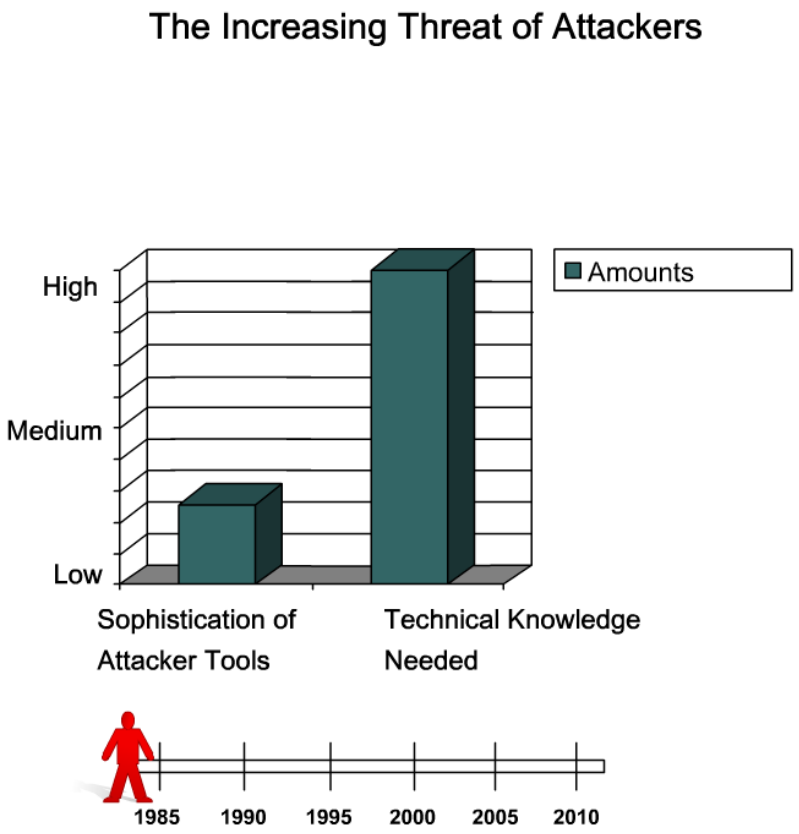
A#undebug all
All possible debugging has been turned off
```

Sieťová bezpečnosť – network security

Kapitola 4

Nárast útokov

- **White hat**
  - Hľadá slabiny, informuje dotyčného, focus na zabezpečenie systému.
- **Hacker**
  - Historicky = programátor expert, súčasnosť = ten čo s snaží získať neautorizovaný prístup k sieť. zdrojom
- **Black hat**
  - Iné pomenovanie osoby, ktorá zneužíva svoje IT vedomosti k prielomu do siete, systému neautorizovane. Cieľom je často osobný alebo finančný zisk
- **Cracker**
  - Vhodnejší názov pre osobu, ktorá sa snaží získať prístup neautorizovane za nevhodným účelom
- **Phreaker**
  - Prielom do telefónnej siete (volanie zadara)
- **Spammer**
- **Phisher**
  - Využíva maškarádu za niekoho za účelom získania citlivých info.



- **Ochrana**
  - **Mysli ako útočník!!**

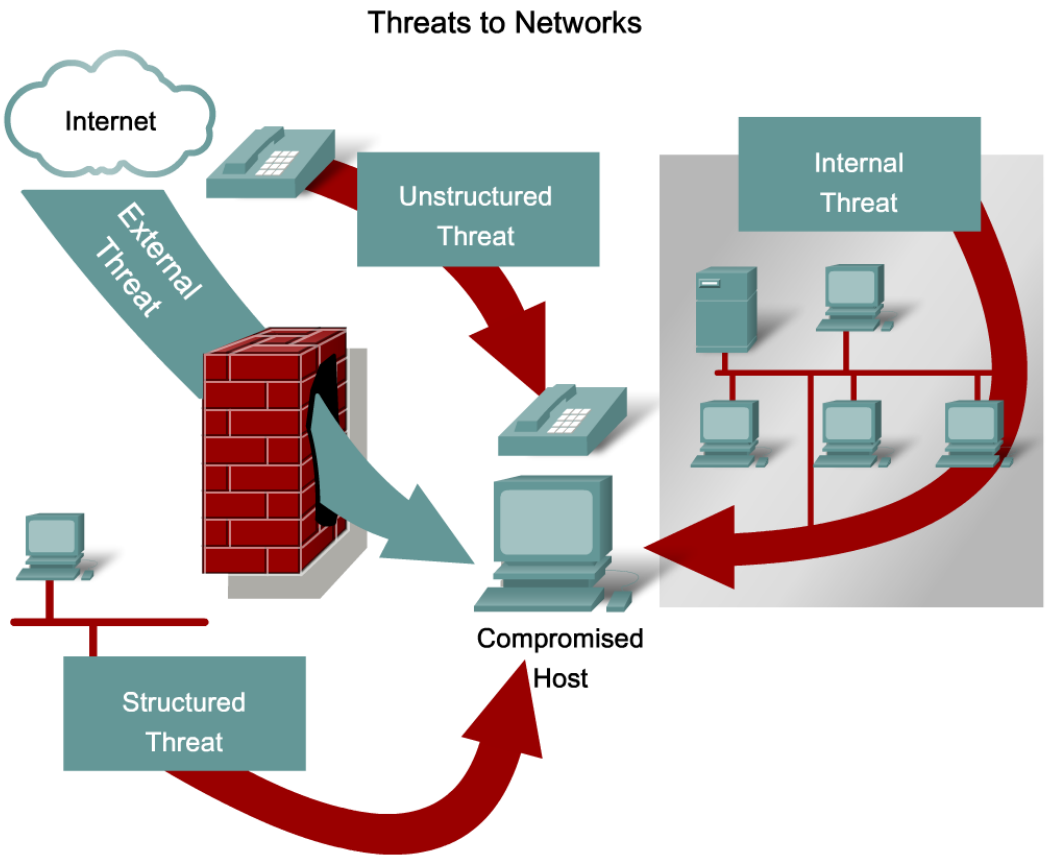
Zraniteľnosť siete

- **Slabé miesta v technológiách**
  - Každá sieťová a počítačová technológia sama o sebe obsahuje určité bezpečnostné problémy.
    - Protokoly, zariadenia, OS, a pod.
- **Slabé miesta v konfigurácii**
  - Veľkú úlohu pri bezpečnosti sietí zohráva ľudský faktor. Pri zlom zaobchádzaní alebo konfigurovaní i tej najbezpečnejšej technológie vzniká veľké riziko ohrozenia bezpečnosti.
    - Nezabezpečené účty, zlé a chybné konfigurácie apod.
- **Slabé miesta v bezpečnostných zásadách**
  - Nedostatočne alebo nejasne definovaná bezpečnostná politika v sieti
    - Nevypracovaná bezpečnostná politika, nespísané pravidlá, scenáre pri nečakaných udalostiach apod.

Hrozby fyzickej infraštruktúry

- Nielen aktívny hacking je problém
- Ale aj riešenie fyzickej bezpečnosti zariadení
  - **Hrozby týkajúce sa hardvéru**
    - Fyzické poškodenie serverov, smerovačov, a sieťových aktív. prvkov
    - **Riešenie**:
      - Zabezpečená uzamknutá miestnosť, jej kontrola a monitoring
  - **Zabezpečenie prevádzkového prostredia, prevádzkové hrozby**
    - Teplota (príliš teplo, zima), vlhkosť, prašnosť
    - **Riešenie**:
      - cez klimatizáciu serverovní a monitoring spomenutých faktorov
  - **Zabezpečenie napájania a z toho vyplývajúce hrozby**
    - Napäťové špičky, prepätia, prepady, šum, rušenie, interferencie, strata napájania
    - **Riešenie**:
      - generátory, UPS, redundacia napájania a pod.
  - **Údržba**
    - Zlé zaobchádzanie so zariadeniami, rozvodmi, zlé uzemnenia, slabé značenie a pod.

Hrozby na sieti



- **Unstructured Threats**
  - Od neskúsených, ktorý skúšajú dostupné nástroje
- **Structured Threats**
  - Útočník je motivovaný a vysoko vyspelý
- **Internal Threats**
  - Útok od niekoho z vnútra siete (má do nej autorizovaný prístup)
- **External Threats**
  - Útok z prostredia mimo firmy

Typy útokov

- **Prieskum (obhliadka, Reconnaissance)**
  - Neoprávnené odhaľovanie, mapovanie a monitorovanie systému, služieb alebo zraniteľných miest v sieti, rozpoznávanie cieľov, odposluch a krádež informácií.
  - Scany (IP, porty), dotazy, sniff (získanie informácií or krádež dát)
    - Nmap, kismet, nagios, wireshark, dig, nslookup, superscan
- **Neoprávnený prístup**
  - Cieľ získať prístup do siete, systému, veľmi často na rootovské (*nix) alebo administrátorské (windows) účty
  - Veľmi časté útoky hrubou silou (brute force), Man in the Middle, port redirect
    - Aircrack, airsort, cain and abel, LC4
- **Odoprenie služieb (Denial of Service, DoS)**
  - Cieľ je zablokovať alebo poškodiť sieť alebo službu.
  - Ping of dead (odstránené), Syn flood, Distribuovaný DoS, Smurf útoky (zahltenie linky množstvom)
- **Trójske kone, vírusy a červy**
  - Umiestnenie záškodníckeho kódu na systém

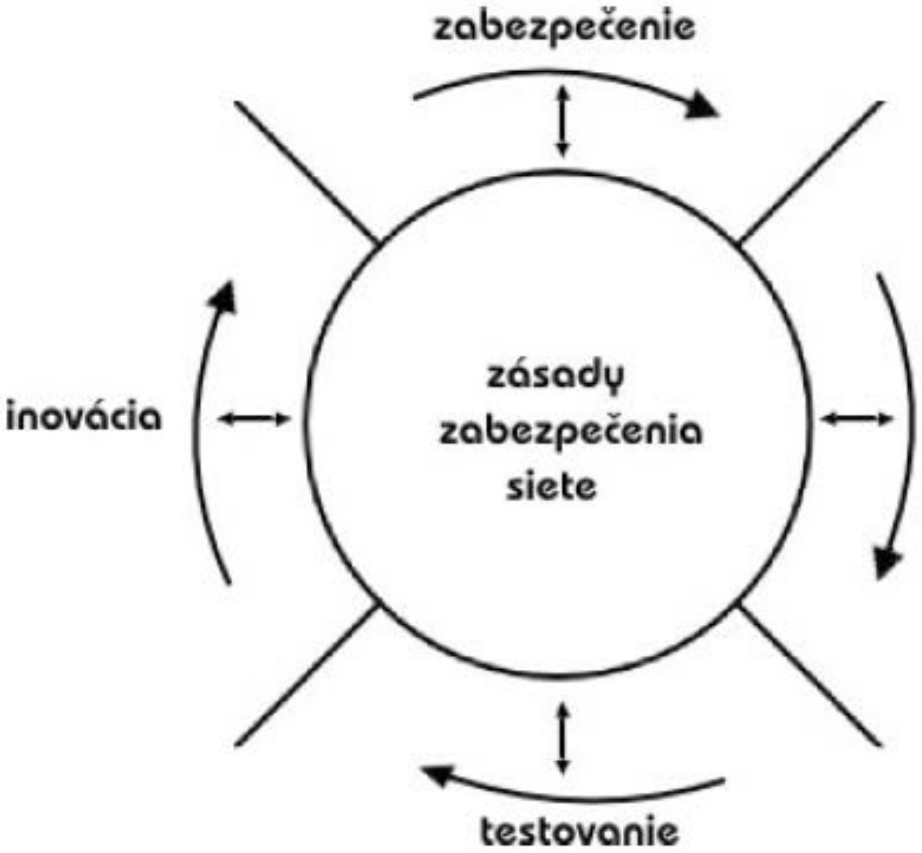
Zmierňujúce techniky

- Device Hardening
  - Odstránenie default nastavení po inštalácií or umiestnení na sieti
- Antivirus
  - A jeho pravidelná aktualizácia
- Osobný firewall
- Aplikácia záplat (Patch)

Zmierňujúce techniky

- Implementácia IDS (Intrusion Detection System)
  - **Sieťovo orientované monitorovanie** (Network based IDS - NIDS)
    - Snort
  - **Monitorovanie na strane hostiteľa** (host based monitoring - HIDS)
    - Snort
- Implementácia IPS (Intrusion Prevention System)
  - Prelude/Prewikka

Vyhodnocovanie bezpečnostných postojov (*Security posture assessment, SPA*)



- **Zabezpečenie (secure)**
  - Inštaluj zariadenia, ktoré zvyšujú úroveň zabezpečenia siete
    - Firewall zo stavovou inšpekciou a filtrami, IDS/IPS, Systém plátania dier
    - Zakáž nechcené služby
  - Zabezpeč konektivitu
    - VPN, web SSL
    - Autorizácia, auntetifikácia, bezpeč. Politiky a vynútenie ich dodržovania
- **Monitorovanie**
  - Pozorovanie a detekcia nechcených aktivít, napr. cez audit logov, trapov apod.
- **Testovanie**
  - Kontrola a testovanie stanovených bezpečnostných opatrní. Napr. penetračné testovanie.
- **Inovácia a zdokonalenie (Improve)**
  - Pridávanie, zdokonaľovanie a aktualizácia bezpečnostných opatrení (podľa potreby).

Definovanie bezpečnostnej politiky

What Is a Security Policy?

"A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide."

(RFC 2196, Site Security Handbook)

Functions of a Security Policy

- Protects people and information
- Sets the rules for expected behavior by users, system administrators, management, and security personnel
- Authorizes security personnel to monitor, probe, and investigate
- Defines and authorizes the consequences of violations

Zásady zabezpečenie siete

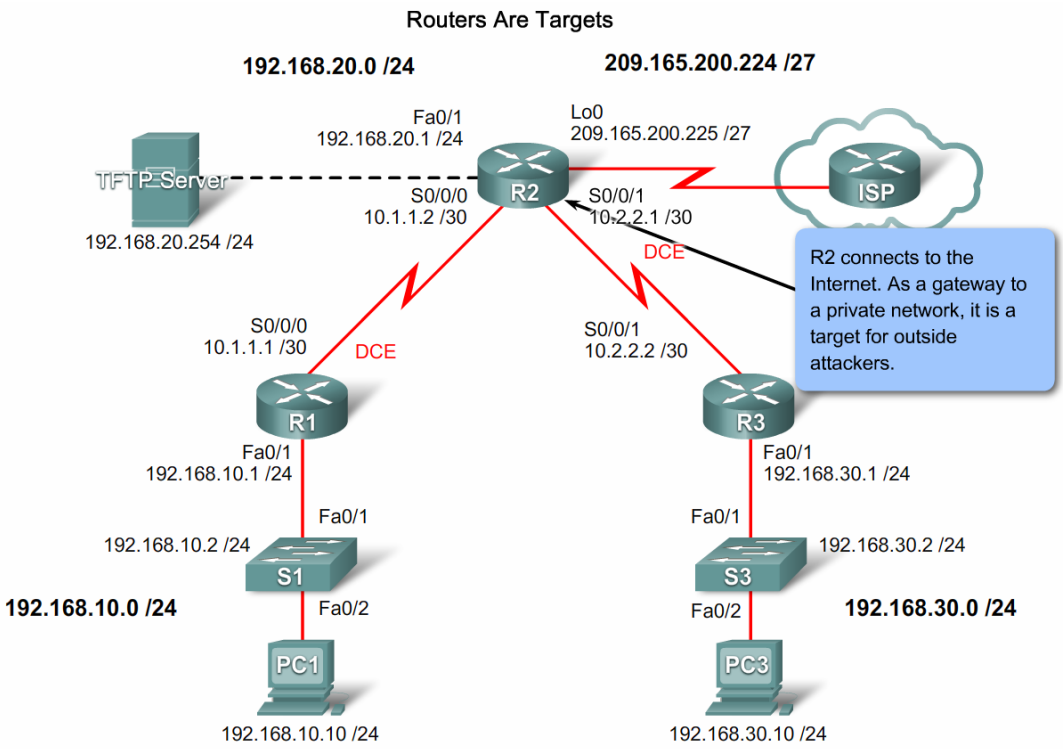
- Podľa SANS Institute (http://www.sans.org)
- Formulácia právomocí a rozsahu pravidiel
  - Definuje garanta bezpečnostných pravidiel a uvádza akých oblastí bezpečnosti siete sa pravidlá týkajú.
- Zásady prístupného chovania
  - Tieto zásady špecifikujú aké chovanie voči internej informačnej infraštruktúre bude povolené alebo zakázané.
- Zásady identifikácie a autentifikácie
  - Definuje mechanizmus (spôsob), ktorý bude zabezpečovať, že k dátam sa dostanú len skutočne oprávnení jednotlivci.
- Zásady prístupu k internetu
  - Definuje, čo je z hľadiska internej siete morálne (etické) a správne použitie internetu.
- Zásady prístupu v internej sieti
  - Spôsob, akým môžu používatelia v internej sieti pracovať s internou dátovou infraštruktúrou.
- Zásady vzdialeného prístupu
  - Spôsob, akým môžu v internej dátovej infraštruktúre pristupovať vzdialení používatelia.
- Postupy pri vzniku bezpečnostného incidentu
  - Popisuje vytvorenie bezpečnostného tímu prie riešenie incidentov a postupy, ktorými sa bude tento tím riadiť behom zisteného incidentu a po ňom.

Úrovne zabezpečenia siete

- Otvorené zásady zabezpečenia
  - Povolené všetko, čo nie je vyslovene zakázané.
  - Jednoduchá konfigurácia i správa.
  - Jednoduchá obsluha pre používateľov siete.
- Reštriktívne zásady zabezpečenia
  - Konfigurácia a správa je komplikovanejšia.
  - Obsluha je ťažšia pre používateľov siete.
  - Vznikajú vyššie náklady na zabezpečenie siete.
- Uzavreté zásady zabezpečenia
  - Najobtiažnejšia konfigurácia i správa.
  - Najobtiažnejšia obsluha pre používateľov siete.
  - Vysoké finančné náklady na zabezpečenie siete.

Zabezpečenie smerovačov

Smerovače sú cieľom útokov



- Smerovače sú cieľom útokov
  - Získanie prístupu a konf. Detailov
  - Kompromitovanie tabuliek
    - Routing, ARP
  - Zmena konfigu
- Preto mysli na:
  - Fyzické zabezpečenie smerovača
  - Update IOS
  - Zálohovanie konf. a IOS
  - Vypnutie služieb a portov ktoré nie sú potrebné

Zabezpečenie smerovačov

Steps to safeguard a router:

Step 1. Manage router security
Step 2. Secure remote administrative access to routers
Step 3. Logging router activity
Step 4. Secure vulnerable router services and interfaces
Step 5. Secure routing protocols
Step 6. Control and filter network traffic

Step 1. Základné zabezpečenie

- Vyber silné heslo
  - Malé a veľké znaky, číslice, špeciálne znaky, dĺžka
- Šifruj heslá
  - **`service password-encryption`**
- Zabezpeč prístup k privilegovanému režimu
  - **`enable secret StrAsn2-dlhE%1_t1ZkE_h2slo`**
- Vynúť minimálnu dĺžku hesla
  - **`security passwords min-length DLZKA`**
- Použi autenfikačnú DB
  - Local
    - **`username Student secret cisco`**
  - TACACS

Step 2. Zabezpečenie prístupu na smerovač

- Vylúč **telnet**, použi SSH
- Zakáž logovanie na AUX

```
R(config)#line aux 0
R(config-line)#no password
%login disabled , until ‘password’ is set
R(config-line)#login
```

- Zabezpeč vty (napr. povoľ len ssh)

```
R(config)#line vty 0 15
R(config-line)#no transport input
R(config-line)#transport input ssh
```

- A aplikuj ACL

```
R(config-line)#ip access class CISLO
```

- A aplikuj dobu neaktivity

```
R(config-line)#exec-timeout min sec
```

- Generuj TCP keepalive na nečinnom vstupujúcom spojení (incoming)

```
R(config)# service tcp-keepalives-in
```

Step 2. Konfigurácia SSH prístupu

```
Switch(config)#username Meno password Heslo
! Domena musi byt zadefinovana
Switch(config)#ip domain-name pepe.sk
Switch(config)#crypto key generate rsa
The name for the keys will be: Switch.pepe.sk
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Switch(config)#ip ssh version 2
*III 1 0:1:9.780:  %SSH-5-ENABLED: SSH 1 has been enabled
Switch(config)#line vty 0 15
Switch(config-line)#transport input ssh
Switch(config-line)#login local
! Ssh timeout v sec (doba neaktivity)
Switch(config)#ip ssh time-out 15
! Ssh login auth retries
Switch(config)#ip ssh authentication-retries 2
```

Step 3. Logovanie aktivít

- Musíme mať sieťovú službu
  - Napr. syslog server

```
Router(config)# logging IP_ADRESA_SERVERA
Router(config)# logging trap SEVERITY_LEVEL
```

Rastie množstvo správ

Severity Level	Keyword	Description
0	emergencies	System unusable
1	alerts	Immediate action required
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant condition
6	informational	Informational messages
7	debugging	Debugging messages

Step 3. Čas (najmä správny) je dôležitý!!!!

```
! Pridaj casovu znacku pre debug spravy
Router(config)# service timestamps debug datetime msec localtime
show-timezone


! Pridaj casovu znacku pre log spravy
Router(config)# service timestamps log datetime msec localtime
show-timezone
```

debug	Indicates that the timestamp should be applied to debugging messages.
log	Indicates that the timestamp should be applied to system logging messages.
uptime	Time stamp with the time since the system was rebooted. The time stamp format for uptime is HHHH:MM:SS.
datetime	Time stamp with the date and time. The time stamp format for datetime is MMM DD HH:MM:SS.
msec	(Optional) Include milliseconds in the time stamp.
localtime	(Optional) Time stamp relative to the local time zone.
year	Include the year in the datetime format.
show-timezone	(Optional) Include the time zone name in the time stamp.

Predpokladá sa správny lokálny čas (NTP?) !!!!

Step4. Spustené služby na smerovačoch ako potencionálne zdroje hrozby

Feature	Description	Default	Recommendation
Cisco Discovery Protocol (CDP)	Proprietary Layer 2 protocol between Cisco devices.	Enabled	CDP is almost never needed; disable it.
TCP small servers	Standard TCP network services: echo, chargen, and so on.	>=11.3: disabled 11.2: enabled	This is a legacy feature; disable it explicitly.
UDP small servers	Standard UDP network services: echo, discard, and so on.	>=11.3: disabled 11.2: enabled	This is a legacy feature; disable it explicitly.
Finger	UNIX user lookup service, allows remote listing of users.	Enabled	Unauthorized persons do not need to know this; disable it.
HTTP server	Some Cisco IOS devices offer web-based configuration.	Varies by device	If not in use, explicitly disable; otherwise, restrict access.
BOOTP server	Service to allow other routers to boot from this one.	Enabled	This is rarely needed and may open a security hole; disable it.
Configuration auto-loading	Router will attempt to load its configuration via TFTP.	Disabled	This is rarely used; disable it if it is not in use.
IP source routing	IP feature that allows packets to specify their own routes.	Enabled	This rarely-used feature can be helpful in attacks; disable it.
Proxy ARP	Router will act as a proxy for Layer 2 address resolution.	Enabled	Disable this service unless the router is serving as a LAN bridge.
IP directed broadcast	Packets can identify a target LAN for broadcasts.	>=11.3: enabled	Directed broadcast can be used for attacks; disable it.
Classless routing behavior	Router will forward packets with no concrete route.	Enabled	Certain attacks can benefit from this; disable it unless your net requires it.
IP unreachable notifications	Router will explicitly notify senders of incorrect IP addresses.	Enabled	Can aid network mapping; disabled on interfaces to untrusted networks.
IP mask reply	Router will send an IP address mask of the interface in response to an ICMP mask request	Disabled	Can aid IP address mapping; explicitly disable on interfaces to untrusted networks.
IP redirects	Router will send an ICMP redirect message in response to certain routed IP packets.	Enabled	Can aid network mapping; disable on interfaces to untrusted networks.
NTP service	Router can act as a time server for other devices and hosts.	Enabled (if NTP is configured)	If not in use, explicitly disable; otherwise, restrict access.
Simple Network Management Protocol	Routers can support SNMP remote query and configuration.	Enabled	If not in use, explicitly disable; otherwise, restrict access.
Domain Name Service	Routers can perform DNS name resolution.	Enabled (broadcast)	Set the DNS server address explicitly, or disable DNS.

Step 4. Príkazy na zákaz niektorých služieb

```
! Small services such as echo, discard, and chargen
Router(config)#no service tcp-small-servers
Router(config)#no service udp-small-servers

!vypni BOOTP
Router(config)#no ip bootp server

!vypni Finger
Router(config)#no service finger

!vypni HTTP
Router(config)#no ip http server

!vypni SNMP
Router(config)#no snmp-server

!vypni CDP
Router(config)#no cdp run

!vypni remote tftp configuration
%Error opening tftp://255.255.255.255/3620.cfg (Socket error)
Router(config)# no service config

!Vypni Source routing
Router(config)#no ip source-route

!vypni Classless routing
Router(config)#no ip classless
```

Step 4. Príkazy na zákaz niektorých služieb

```
!vypni DNS ak nie je potrebny
Router(config)#no ip domain-lookup

! Per interface
!vypni proxy ARP
Router(config-if)#no ip proxy-arp

!vypni smerovy bcast
Router(config-if)#no ip directed-broadcast

!vypni ICMP presmerovanie
Router(config-if)#no ip redirect

!vypni ICMP destination unreachble
Router(config-if)#no ip unreachables
```

http://www.cisco.com/en/US/docs/ios/12_3/ipaddr/command/reference/ipras_r.html

Step 5 . Zabezpečenie smerovacích protokolov

- Dva útoky na smerovanie
  - Disruption of peers
    - Prerušenie komunikácie
  - Falsification of routing information
    - 1. Redirect traffic to create routing loops
    - 2. Redirect traffic so it can be monitored on an insecure link
    - 3. Redirect traffic to discard it
- Použi smerovacie protokoly, ktoré ponúkajú zabezpečenie updatov, napr. cez MD5
  - RIPv2, EIGRP, OSPF, IS-IS, a BGP podporujú MD5 autentifikáciu
  - Ochrana voči odsnifovaniu, a podsunutiu falošných smerovacích informácií
    - Man in the middle, routing loops

Step 5. Kontrola, kam budú posielané updates

- Neposielaj updates do sietí kde nie je treba
  - Nastav passive všetky a potom explicitne povoľuj len tie rozhrania kde treba

```
R(config)#router rip
!napr. Zakaz updates vsade
R(config-router)#passive interface default
! Povoluj per rozhrania
R(config-router)#no passive interface serial 0/0
```

Step 5. Zabezpečene smerovacích protokolov

```
! RIP
! klucenka
Router(config)#key chain RIP_KLUC
Router(config-keychain)#key 1
Router(config-keychain-key)#key-string HESLO

Router(config-if)#int s 1/0
!
Router(config-if)#ip rip authentication mode md5
Router(config-if)#ip rip authentication key-chain RIP_KLUC
```

```
! EIGRP
Router(config)#key chain EIGRP_KLUC
Router(config-keychain)#key 1
Router(config-keychain-key)#key-string HESLO

Router(config-if)#int s 1/0
Router(config-if)#ip authentication mode eigrp AS md5
Router(config-if)#ip authentication key-chain eigrp AS EIGRP_KLUC
```

```
! OSPF
Router(config)#router ospf CISLO_PROCESU
Router(config-router)#area 0 authentication message-digest

Router(config-if)#int s 1/0
Router(config-if)#ip ospf message-digest-key 1 md5 HESLO
Router(config-if)#ip ospf authentication message-digest
```

Auto secure

- Vhodné pre zákazníkov bez hlbších vedomostí o IT bezpečnosti a zabezpečení smerovačov
  - Rozumej nás…zatiaľ
- Slúži na rýchle zabezpečenie smerovača

```
Router# auto secure ?
  firewall      AutoSecure Firewall
  forwarding    Secure Forwarding Plane
  full          Interactive full session of AutoSecure
  login         AutoSecure Login
  management    Secure Management Plane
  no-interact   Non-interactive session of AutoSecure
  ntp           AutoSecure NTP
  ssh           AutoSecure SSH
  <cr>
```

```
Router#auto secure
               --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]:

Interface                  IP-Address      OK? Method Status                Protocol
Serial1/0                  1.0.0.1         YES manual up                    up
Serial1/1                  unassigned      YES unset  administratively down down
Enter the interface name that is facing the internet: Serial 1/0
Invalid interface name
Enter the interface name that is facing the internet: Serial1/0

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

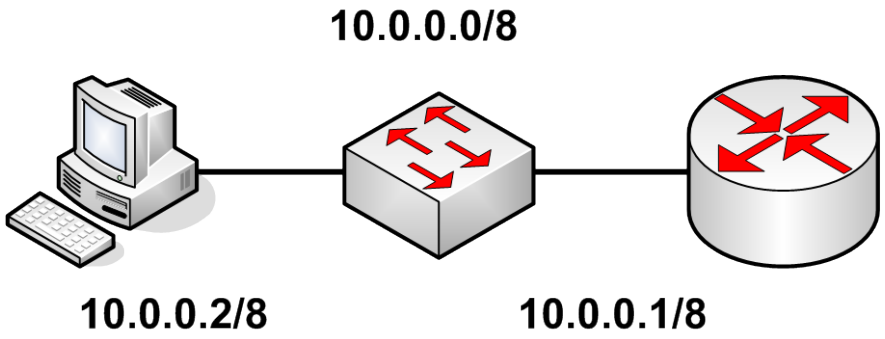
Enter the security banner {Put the banner between
k and k, where k is any character}:
k Access deny! k
Enable secret is either not configured or
... Otput omitted ...
```

SDM – Security device manager

Cisco Router and Security Device Manager (SDM)

- **Zjednodušuje konfiguráciu a manažment smerovačov**
- Je to web GUI nástroj, podporovaný množstvom cisco IOS releases a modelov zariadení
  - od Cisco 830 Series do Cisco 7301
  - Preinštalovaný na nových Cisco 850 Series, Cisco 870 Series, Cisco 1800 Series, Cisco 2800 Series, and Cisco 3800 Series integrated services routers
- Zjednodušená konfigurácia techník ako dynamické smerovanie, WAN access, WLAN, firewall, VPN, SSL VPN, IPS, and QoS
- Musí byť stiahnutý a nainštalovaný
  - Ako? Popis na http://nil.uniza.sk

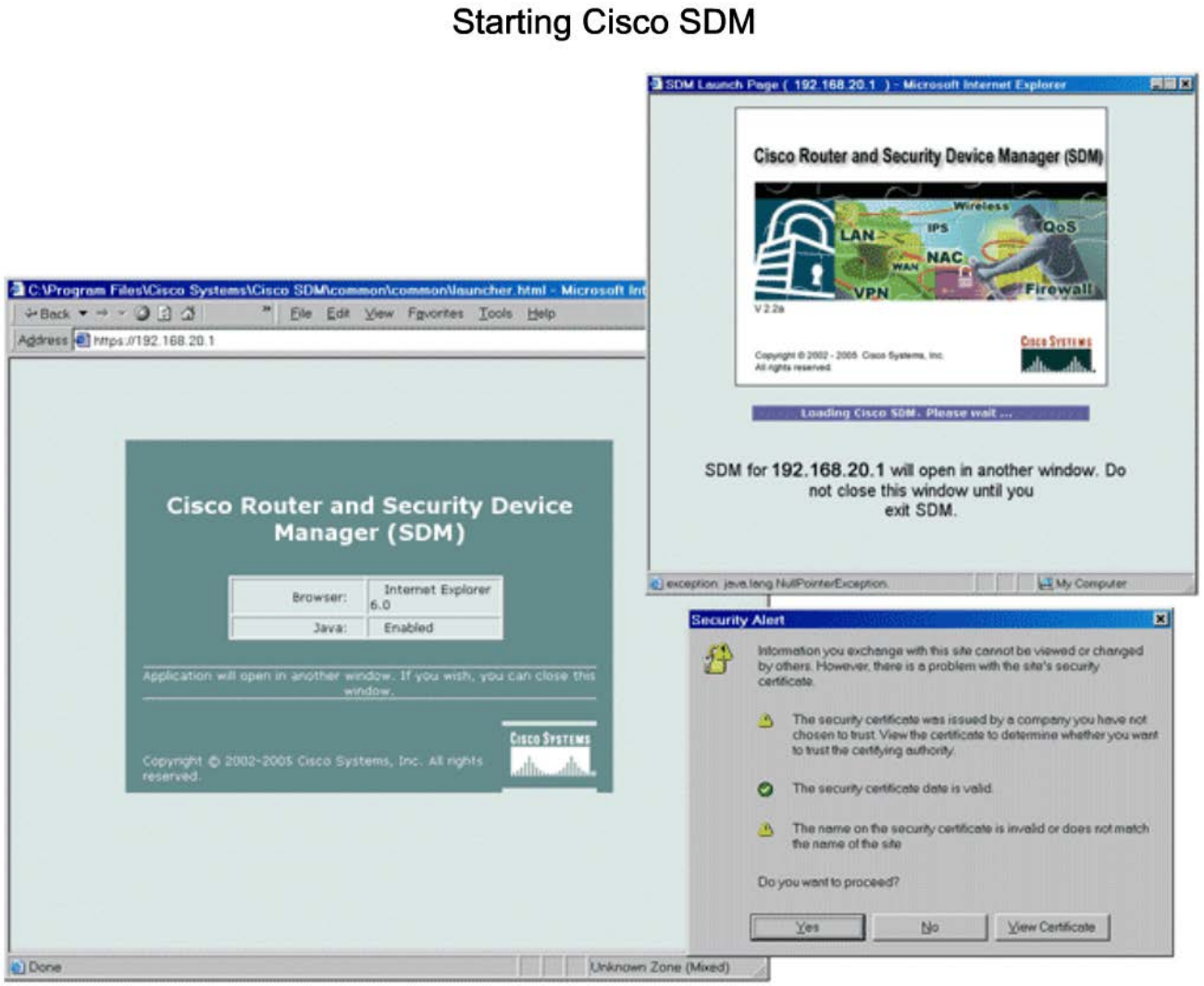
PreKonfigurácia smerovača na použitie SDM

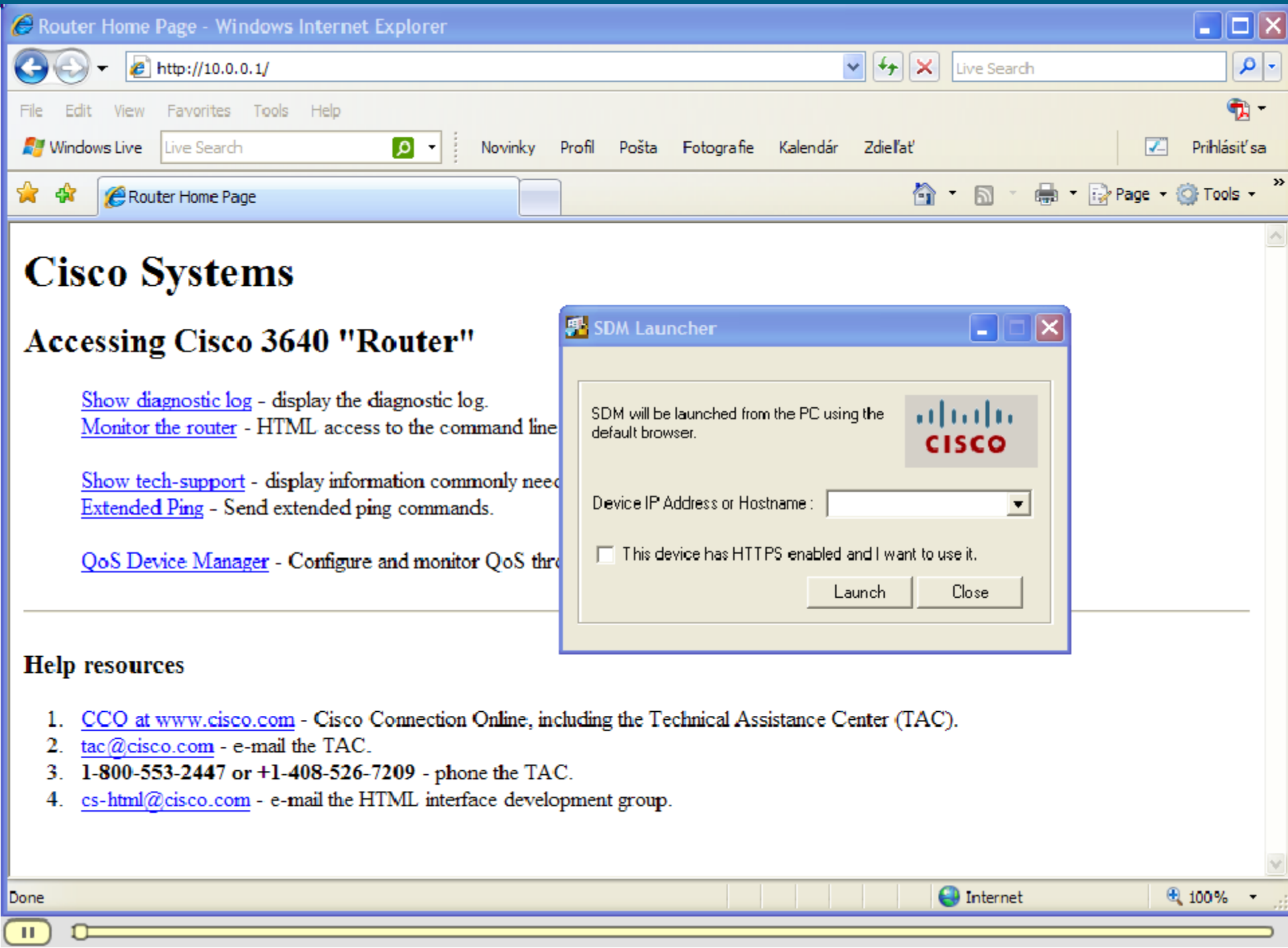



```
! Zabezpec IP konektivitu
! Minimalisticka verzia (len na testovanie)
! V zivych sietach neodporucam
Router(config)#ip http server
Router(config)#enable secret cisco
```

```
! Zabezpec IP konektivitu
! So zabezpecenim autenfikacie na local
Router(config)#ip http server
Router(config)#ip http secure-server
Router(config)#ip http authentication local
Router(config)#username Meno privilege 15 secret HESLO
```

Spustenie SDM



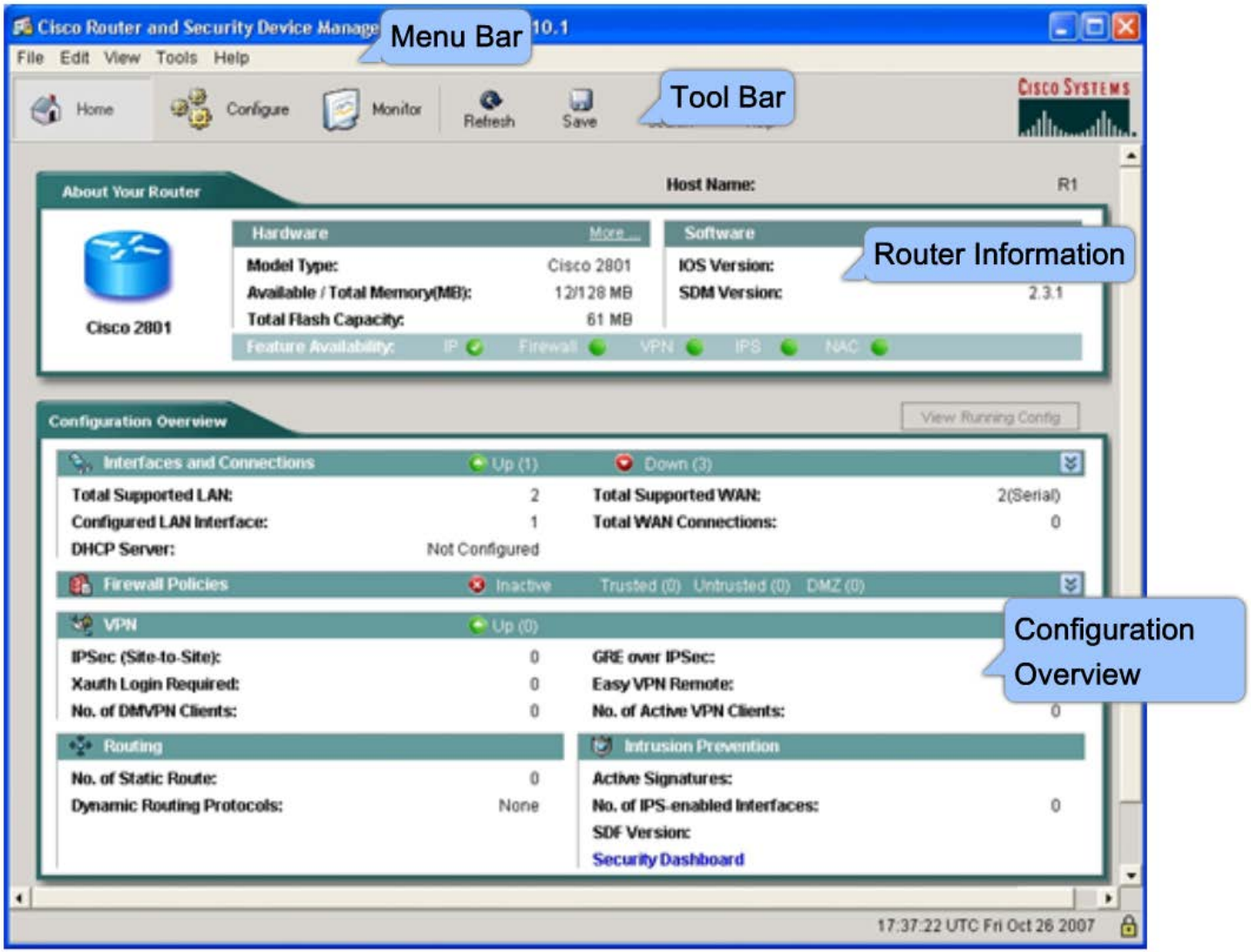

Router Home Page - Windows Internet Explorer
http://10.0.0.1/
Live Search
File Edit View Favorites Tools Help
Windows Live
Live Search
Novinky Profil Pošta Fotografie Kalendár Zdieľať
Prihlásiť sa
Router Home Page
Page
Tools
Cisco Systems
Accessing Cisco 3640 "Router"
Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line
Show tech-support - display information commonly nee
Extended Ping - Send extended ping commands.
QoS Device Manager - Configure and monitor QoS thr
SDM Launcher
SDM will be launched from the PC using the default browser.
CISCO
Device IP Address or Hostname :
This device has HTTPS enabled and I want to use it.
Launch
Close
Help resources
1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.
Done
Internet
100%

Otvor swf

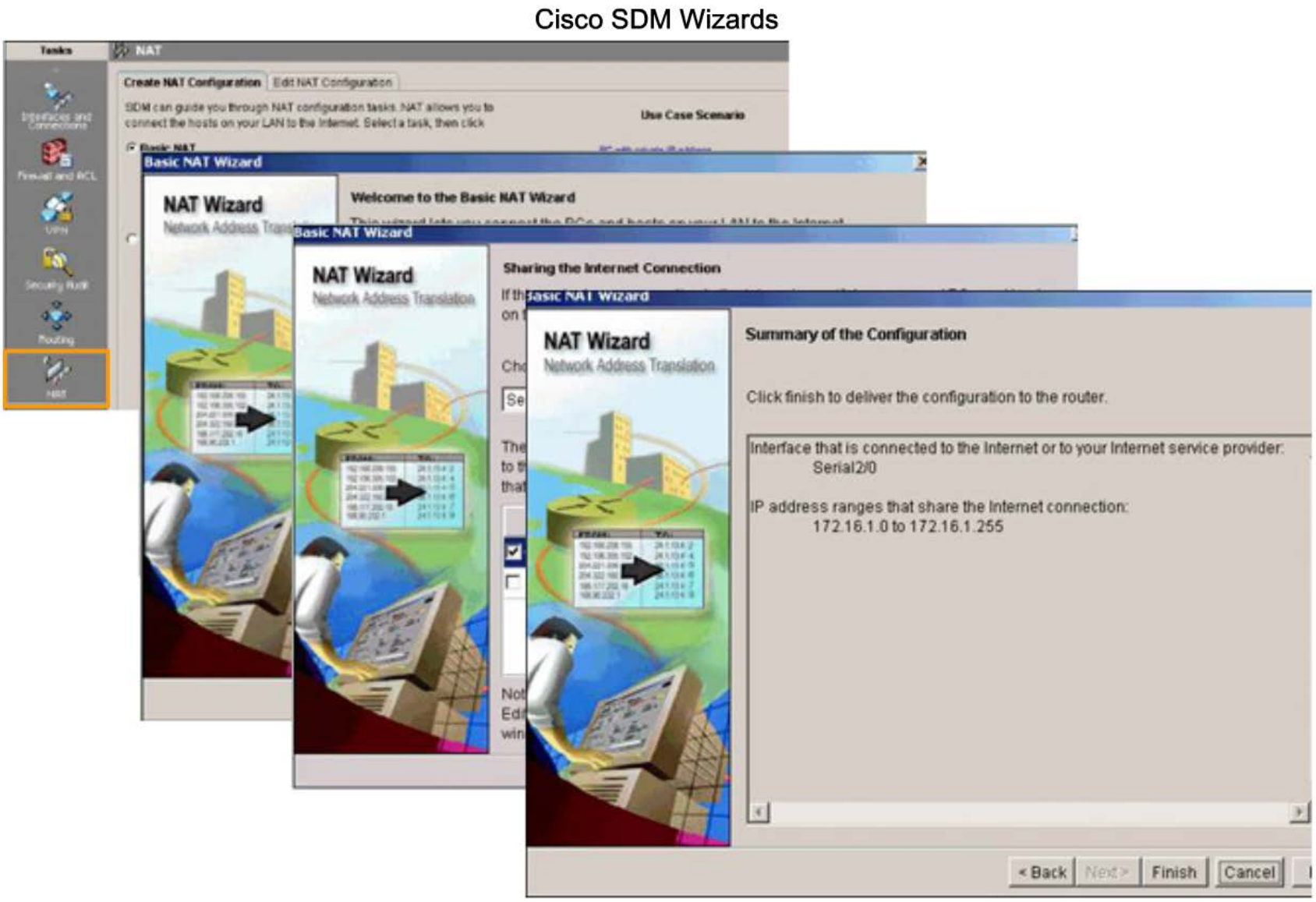
Otvor browser

Orientácia v SDM

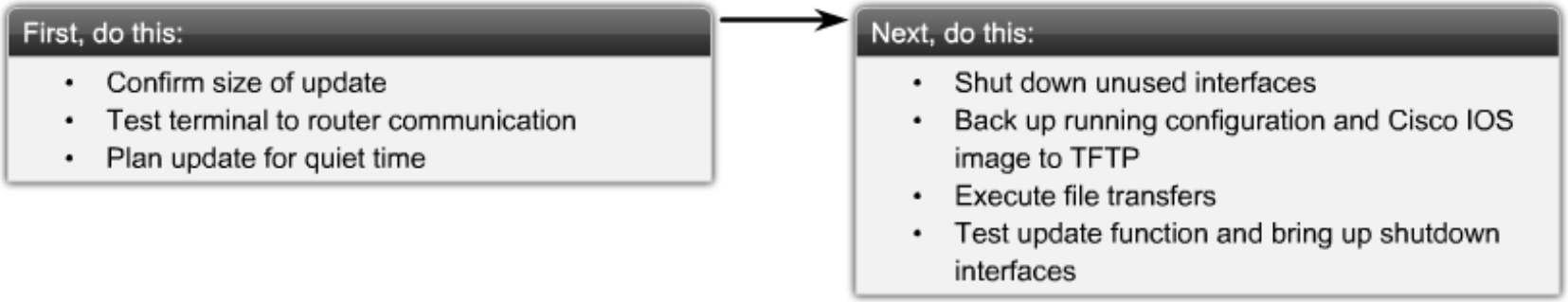
Cisco SDM Home Page Overview



SDM wizards


Cisco SDM Wizards
Tasks
NAT
Create NAT Configuration
Edit NAT Configuration
Use Case Scenario
Basic NAT Wizard
NAT Wizard
Network Address Translation
Welcome to the Basic NAT Wizard
Sharing the Internet Connection
Summary of the Configuration
Click finish to deliver the configuration to the router.
Interface that is connected to the Internet or to your Internet service provider:
Serial2/0
IP address ranges that share the Internet connection:
172.16.1.0 to 172.16.1.255
< Back
Next >
Finish
Cancel

Správa IOS



Cisco IOS Integrated File System (IFS).

```
! Zobrazi podporovane file systemy na smerovaci
Router#sh file systems
File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -    opaque     rw   archive:
           -           -    opaque     rw   system:
       57336       55068     nvram     rw   nvram:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
*   16777212           0     flash     rw   flash:
           -           -     flash     rw   slot0:
           -           -    opaque     wo   syslog:
           -           -    opaque     rw   xmodem:
           -           -    opaque     rw   ymodem:
           -           -   network     rw   rcp:
           -           -   network     rw   pram:
           -           -   network     rw   ftp:
           -           -   network     rw   http:
           -           -   network     rw   scp:
           -           -   network     rw   https:
           -           -    opaque     ro   cns:
```

```
sw_2950T_kis#dir
Directory of flash:/

    2  -rwx     1674921  Mar 01 1993 00:05:59 +00:00  c2950-c3h2s-mz.120-
5.3.WC.1.bin
    3  -rwx         110  Sep 09 1993 14:47:46 +00:00  info
    4  drwx        4160  Sep 09 1993 14:50:56 +00:00  html
   83  -rwx        1048  May 17 1993 03:01:22 +00:00  multiple-fs
  166  -rwx        1411  Mar 15 1993 05:10:11 +00:00  start
  167  -rwx         840  Mar 19 1993 10:20:09 +00:00  vlan.dat
  164  -rwx         110  Sep 09 1993 14:51:40 +00:00  info.ver
    5  -rwx     3117954  Sep 09 1993 14:50:04 +00:00  c2950-i6q4l2-mz.121-
22.EA8a.bin
   84  drwx          64  Mar 01 1993 00:00:16 +00:00  crashinfo
   82  -rwx         301  Sep 09 1993 14:55:09 +00:00  env_vars
  457  -rwx          77  May 17 1993 03:01:22 +00:00  private-config.text
   87  -rwx        3275  May 17 1993 03:01:22 +00:00  config.text

7741440 bytes total (1129984 bytes free)
```

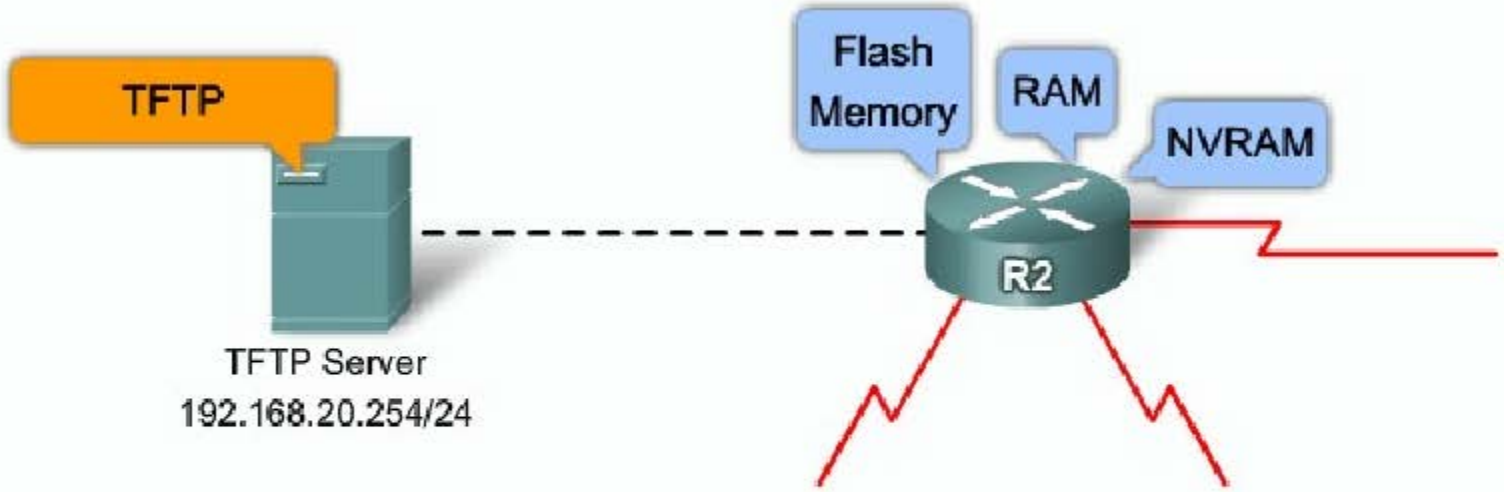
```
sw_2950T_kis#cd nvram:
sw_2950T_kis#pwd
nvram:/
sw_2950T_kis#dir
Directory of nvram:/

   27  -rw-        3275                    <no date>  startup-config
   28  ----          77                    <no date>  private-config
    1  -rw-           0                    <no date>  ifIndex-table

32768 bytes total (28340 bytes free)
```

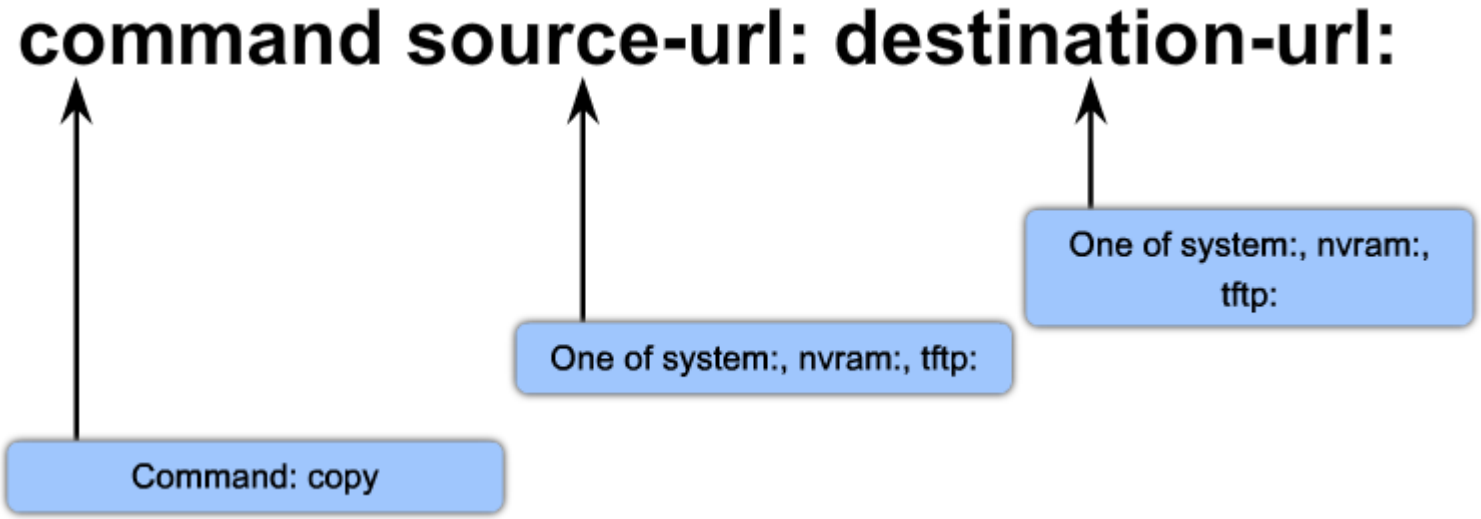
Umiestnenie IOS

- Definované IFS prefixom



Prefix	URL Path
tftp:	[[[//location]/directory]/filename]
tftp://192.168.20.254/configs/backup-config	

Preto zálohovanie a kopírovanie



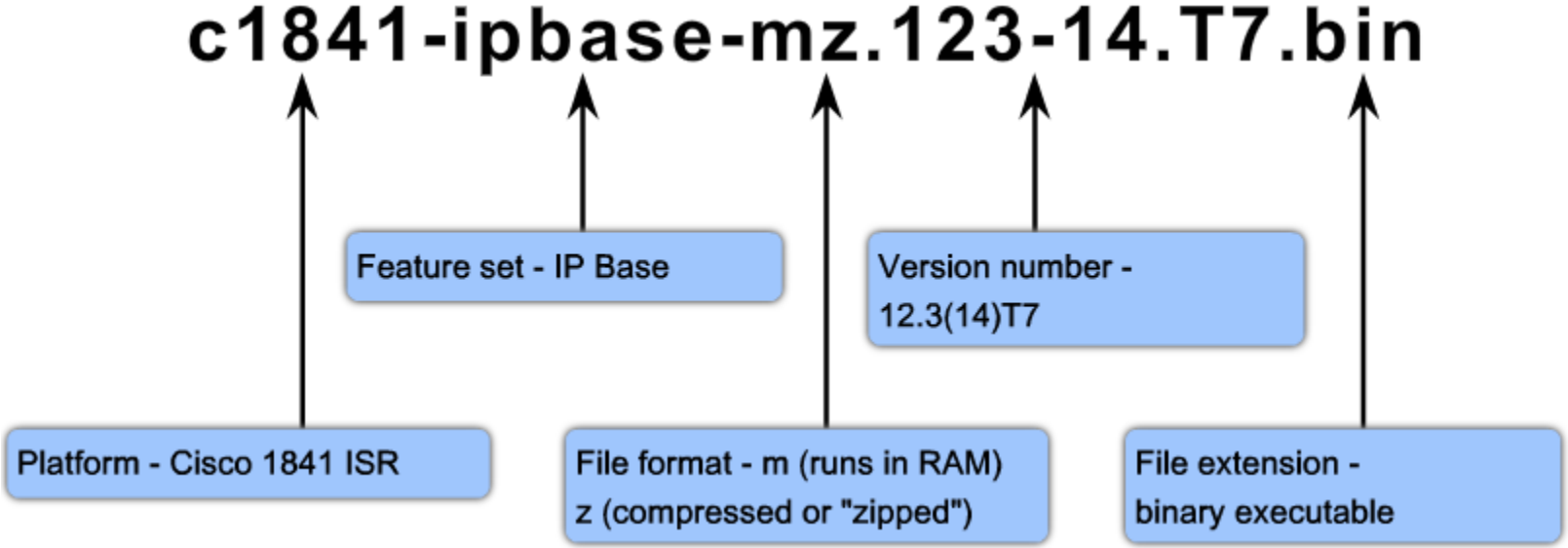

```
Copy the running configuration from RAM to the startup configuration in
NVRAM:
R2# copy running-config startup-config
R2# copy system:running-config nvram:startup-config

Copy the running configuration from RAM to a remote location:
R2# copy running-config tftp:
R2# copy system:running-config tftp:

Copy a configuration from a remote source to the running configuration:
R2# copy tftp: running-config
R2# copy tftp: system:running-config

Copy a configuration from a remote source to the startup configuration:
R2# copy tftp: startup-config
R2# copy tftp: nvram:startup-config
```

Menné konvencie pri IOS



- **C1841** HW platforma
- **Ipbase -** špecifikuje vlastnosti IOS
  - IPbase – základný IP internetworking
  - Iné možnosti
    - **i** - IP feature set
    - **j** - Enterprise feature set (all protocols)
    - **s** - Designates a PLUS feature set (extra queuing, manipulation, or translations)
    - 56i - Designates 56-bit IPsec DES encryption
    - 3 - Designates the firewall/IDS
    - k2 - Designates the 3DES IPsec encryption (168 bit)
- **Mz –** IOS je komprimovaný a beží v RAM
- **12.3-14.T7 –** číslo verzie IOS.
- **Bin –** IOS je binárne vykonávateľný súbor

- **Mz –** IOS je komprimovaný a beží v RAM
- **12.3-14.T7 –** číslo verzie IOS.
- **Bin –** IOS je binárne vykonávateľný súbor

IOS backup na TFTP

- Skontroluj dostupnosť servera

```
Sw#ping 172.16.255.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.255.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/54/132 ms
```

- Skontroluj meno IOS

```
sw#sh flash
Directory of flash:/
2  -rwx     1674921  Mar 01 1993 00:05:59 +00:00  c2950-c3h2s-mz.120-5.3.WC.1.bin
```

- Vykonaj zálohovanie
  - Copy run tftp

Obnova zmazaného IOS

- Cez sieť
  - Tftpdnld
    - ```
      rommon 1 > set
      PS1=rommon ! >
      TFTP_FILE=c2600-jk9o3s-mz.122-29.bin
      BOOT=
      IP_ADDRESS=10.10.104.10
      IP_SUBNET_MASK=255.255.255.0
      DEFAULT_GATEWAY=10.10.104.4
      TFTP_SERVER=10.10.104.4
      ?=1
      RET_2_RTS=
      BSI=0
      RET_2_RCALTS=
      ```
  - Zdroje:
    - Google
    - http://nil.uniza.sk/node/89
- Cez console
  - xmodem
      ```

Obnova strateného hesla

- Smerovač
  - Break
- Prepínač
  - Mode tlačítko
  - http://nil.uniza.sk/practical-cisco/catalyst-2960-password-recovery