# Skalovanie IP adries

**Network Address Translation (NAT)** pomáha riešiť nedostatok IP adresného priestoru, veľa privátnych adries klientskych staníc prekladá na niekoľko verejných. **Port Address Translation (PAT)** je podobný NAT, ale umožňuje preložiť veľa privátnych adries len na jednu verejnú. **Dynamic Host Configuration Protocol (DHCP)** bol navrhnutý na dynamické prideľovanie IP adries a onych dôležitých sieťových konfiguračných informácií.

Routre, servery a iné kľúčové zariadenia na sieti obyčajne vyžadujú statickú IP konfiguráciu. Klientske stanice nevyžadujú špecifickú adresu, ale jednu z rozsahu, zatiaľ čo iné hodnoty sú statické (SM, Default Gateway, DNS server).

### 1.1.1. Privátne adresovanie

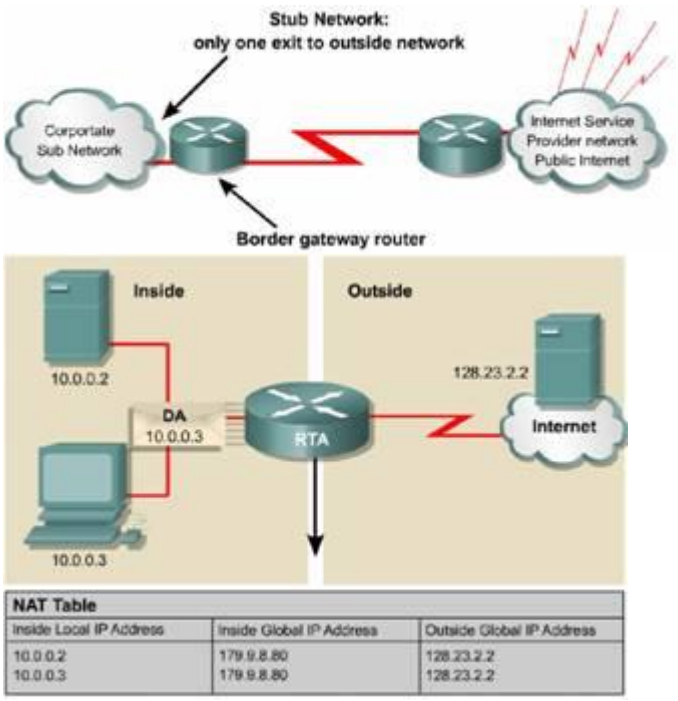
Adresy pre privátne siete, použiteľné len pre vnútorné siete:

| Class | RFC 1918 Internal Address Rango | CIDR Prefix |
|---|---|---|
| A | 10,0.0.0-10,255.255,255 | 10.0.0 Ľ'S |
| B | 172.16.0.0-172.31.255.255 | 172.16.0.0/12 |
| C | 192.168.0.0 -192.168.255.255 | 192.i6e.00ne |

je nevyhnutný NAT.

### 1.1.2. Úvod do NAT a PAT

Nie sú smerované cez internet. Nevyžadujú registráciu. Aby spoločnosti mohli zrealizovať prístup svojich klientov s privátnou adresou na internet, NAT je určený na udržiavanie privátnych adries v privátnej sieti a ich preklad na smerované verejné adresy, čím sa zvyšuje sieťová bezpečnosť ukrytím privátnych adries.




NAT pracuje na hranici netranzitnej siete. Netranzitná sieť má priame pripojenie na susednú sieť. Keď host v netranzitnej sieti chce komunikovať s hostom vonkajšej siete, pošle paket na router, ten ju preloží cez NAT na vonkajšiu smerovatelnú adresu.

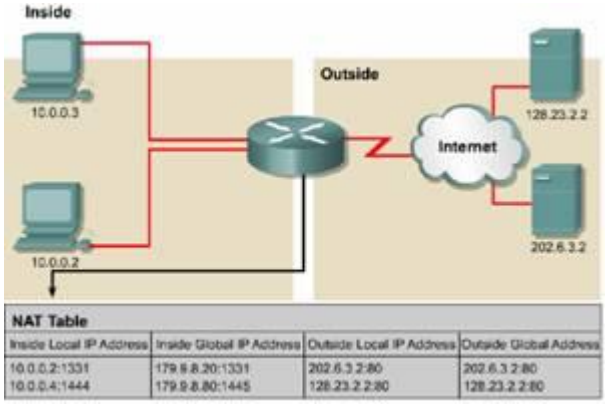
**NAT termíny:**

- **Inside local address -** IP adresy vo vnútornej siete, privátne IP adresy

- **Inside global address** - IP adresy pridelené poskytovateľom služby, predstavujú jednu alebo niekoľko lokálnych adries vo svete
- **Outside local address** - IP adresa vonkajšieho hosta, predstavuje hosta vnútornej siete
- **Outside global address** - IP adresa pridelená hostovi vo vonkajšej sieti, jedinečná v rámci internetu

### 1.1.3. Vlastnosti NAT a PAT

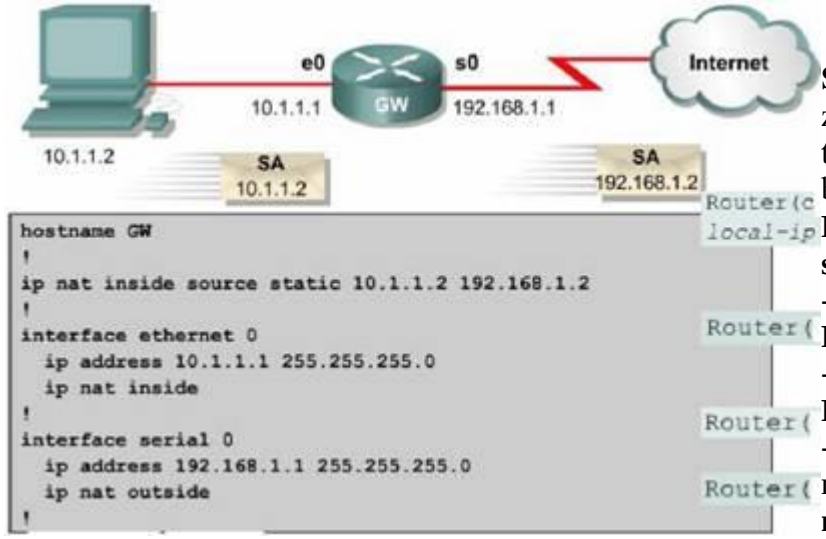
**NAT: statický**, jednoduché mapovanie lokálnych a globálnych adries. Vhodné pri hostoch, kde musí byť rovnaká adresa, kvôli prístupu z internetu, ako podnikové servery a sieťové zariadenia dynamický, dynamické mapovanie privátnych adries na verejné adresy. Hocijaká adresa z rozsahu verejných IP adries je pridelená hostovi.




**Port Address Translation (PAT)**: viacnásobné mapovanie privátnych IP adries na jednu verejnú IP adresu. Rozlišuje sa podľa čísla portu, je 16 bitový. Teoretický počet interných adries, ktoré môžu byť preložené na vonkajšie je 65535, prakticky je to okolo 4000.

**Výhody NAT:**
eliminuje nutnosť prideľovania novej adresy každému hostovi pri zmene ISP.
šetrí adresy, z PAT vnútorný hosti môžu zdieľať jedny verejnú IP adresu.
zvyšuje sieťovú bezpečnosť, nie sú zverejnené vnútorné IP adresy

### 1.1.4. Konfigurovanie NAT a PAT




**Statický preklad**:
zabezpečiť statický preklad medzi vnútornou lokálnou adresou a vnútornou globálnou adresou
**Router(config) #ip nat inside source static global-ip**
- špecifikovať vnútorné rozhranie
**Router(conf ig) interface type number**
- označiť rozhranie za vnútorné
**Router(config) #ip nat inside**
- špecifikovať vonkajšie rozhranie **Router(config) interface type number**
- označiť rozhranie za vonkaj šie
**Router(config) #ip nat outside**

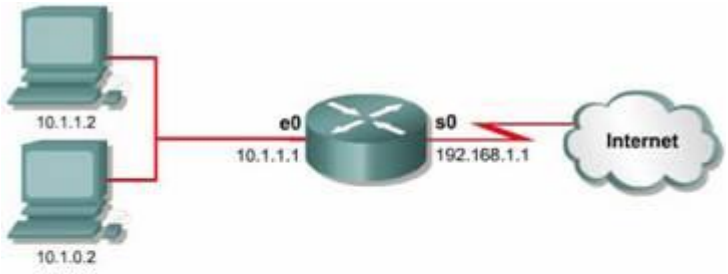
**Dynamický překlad:**

1. Do **ip nat pool** name start IP end IP **netmask** net mask - zadefinujem rozsah globálnych adries
2. Do access listu zadáme adresy, ktoré budú překládané

   **Router(config) #access-list 1 permit 10.0.0.0  0.0.255.255**

   zavedenie dynamického prekladu na základe access listu a rozsahu globálnych adries

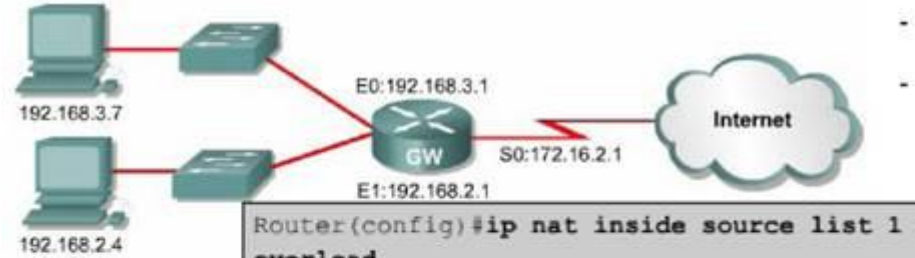
   **Router(config) #ip nat inside source list 1 pool nat-pool**




```
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1
!
interface ethernet 0
  ip address 10.1.1.1 255.255.0.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
access-list 1 permit 10.1.0.0 0.0.0.255
```

Preklad zdrojových adries podľa AL1 v rozsahu 10.1.0.0/24 na adresy z rozsahu 179.9.8.80/24 - 179.9.8.95/24 10.1.1.2 – pre túto adresu nebude povolený preklad, nie je v AL.

**Overloading – PAT**




```
Router(config)#ip nat inside source list 1 interface serial0/0
overload
```

```
interface ethernet 0
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
!
interface ethernet 1
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
!
ip nat inside source list 1 interface serial 0 overload
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
```

- do access listu zadáme adresy, ktoré budú prekladané

```
Router(config)#access-list 1 permit 10.0.0.0 0.0.255.255
```

špecifikujeme vnútorné a vonkajšie rozhranie vytvoríme dynamický preklad zdrojových adries špecifikovaný AL

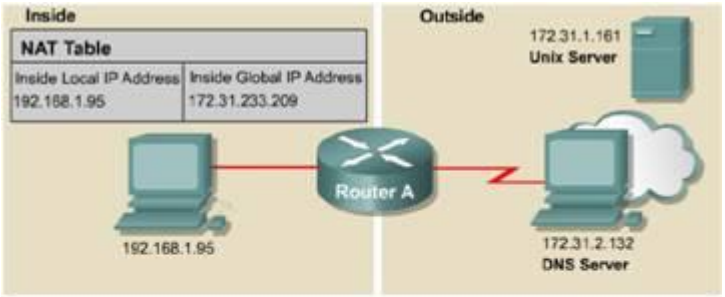
### 1.1.5. Overovanie PAT konfigurácie

Príkazy pre overovanie: **clear a show**
**clear ip nat translation** – zmaže všetky záznamy z NAT translation tabuľky, umožní zmenu konfigurácie NAT
**show ip nat translation** – zobrazí aktívny preklad
**show ip nat statistics** – zobrazí prekladovú štatistiku

### 1.1.6. Riešenie problémov v NAT a PAT konfigurácii

Kroky pre určenie správnej funkčnosti NAT:
- v závislosti na konfigurácii, jasne definujme, či sa NAT uskuteční
- overiť, či je správny preklad podľa záznamov v tabuľke prekladov
- pomocou príkazov show a debug overiť, či nastáva preklad
- overiť, či router má správne smerovacie informácie, na presun paketu

**debug ip nat** – zobrazenie informácií o všetkých paketoch, ktoré sú prekladané routrom
**debug ip nat detailed** - generuje výpis každého prekladaného paketu , generuje tiež všetky chyby a výnimky




```
RouterA#debug ip nat
NAT:  s= 192.168.1.95   --> 172.31.233.209,        d=172.31.2.132 [6825]
NAT:  s= 172.31.2.132,     d=172.31.233.209,    --> 192.168.1.95 [21852]
NAT:  s= 192.168.1.95   --> 172.31.233.209,        d=172.31.1.161 [6826]
NAT*: s= 172.31.1.161,     d=172.31.233.209,    --> 192.168.1.95 [23311]
NAT*: s= 192.168.1.95   --> 172.31.233.209,        d=172.31.1.161 [6827]
NAT*: s= 192.168.1.95   --> 172.31.233.209,        d=172.31.1.161 [6828]
NAT*: s= 172.31.1.161      d=172.31.233.209,    --> 192.168.1.95 [23313]
NAT*: s= 172.31.1.161,     d=172.31.233.209,    --> 192.168.1.95 [23313]
```

V prvých 2 riadkoch je DNS požiadavka a odpoveď. V ostatných riadkoch je telnetové pripojenie hosta z vnútornej siete na hosta vo vonkajšej sieti Popis debug:
* za NAT indikuje, že preklad nastal v rýchlej prepínanej časti. 1 paket vždy ide cez pomalú cestu, je postupne prepínaný. Ostatné pakety idú cez rýchlu cestu ak existujú záznamy v CACHE
s= a.b.c.d je zdrojová adresa, zdrojová adresa je preložená na w.x.y.z.
d=e.f.g.h je cieľová adresa
hodnota v [] je IP identifikačné číslo

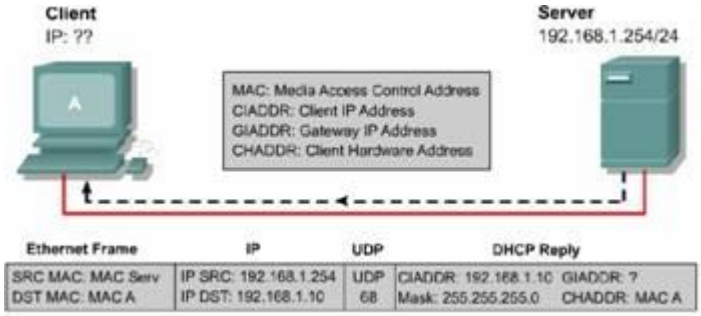
### 1.1.7. Otázky s NAT

Výhody NAT:
NAT šetrí registrované IP adresy privatizáciou intranetu, zvyšuje flexibilitu pri pripojení na verejné siete, vnútorná adresná schéma je stála, pri zmene verejnej IP nie je potrebné prečíslovanie hostov
Nevýhody:
pri použití NAT nebudú pracovať niektoré protokoly alebo aplikácie, sú skryté end to end adresy, niekedy sa dá tento problém vyriešiť statickým mapovaním, NAT zvyšuje oneskorenie
- zaťaženie procesora, zariadenie kontroluje každú hlavičku paketu a rozhoduje, či bude prekladaný

Cisco IOS umožňuje nasledujúce typy komunikácie: Cisco IOS nepodporuje nasledovnú komunikáciu:

| | |
|---|---|
| ICMP | - aktualizácie smerovacích tabuliek |
| File Transfer Protocol (FTP) | - prenos DNS oblasti |
| NetBIOS cez TCP/IP | - BOOTP |
| RealNetworks' RealAudio | - protokoly talk a ntalk |
| Xing Technologies' StreamWorks | - Simple Network Management Protocol (SNMP) |

DNS "A" a "PTR" požiadavky
H.323/Microsoft NetMeeting, IOS verzia 12.0(1)/12.0(1)T a neskoršia
VDOnet's VDOLive, IOS verzia 11.3(4)11.3(4)T a neskoršia
VXtreme's Web Theater, IOS verzia 11.3(4)11.3(4)T a neskoršia
IP Multicast, IOS verzia 12.0(1)T len preklad zdrojových adries
1.2.1. Úvod do DHCP
Dynamic Host Configuration Protocol (DHCP) pracuje v móde klient – server podľa RFC 2131. DHCP Klient
získa IP konfiguráciu z DHCP servera, čím sa ušetrí práca pri konfigurovaní klientov.
DHCP klienta obsahuje veľa rôznych OS: Windows operating systems, Novell Netware, Sun Solaris, Linux a MAC OS




Klient požaduje adresné hodnoty od DHCP servera. Server odpovie klientovi podľa konfigurácie a podľa prideleného adresného priestoru, prenajatie adresy je vymedzený na určitú periódu, po jej vypršaní klient musí požiadať o novú adresu. DHCP nie je určené: routre, prepínače, servery – vyžaduje sa statická konfigurácia
DHCP umožňuje poskytnutie ďalších informácií, ako adresu WINS servera, doménové meno, rezervovanie určitej adresy na základe MAC adresy.
DHCP využíva na komunikáciu transportný protokol, klienti posielajú požiadavky na porte 67 a server posiela správy na porte 68.
1.2.2. Rozdiely medzi BOOTP a DHCP
BOOTP bol vyvinutý v roku 1985, je definovaný RFC 951. Bol predchodca DHCP a tiež používal porty 67 a 68. Základné IP parametre:
IP adresa
adresa východzej brány
maska siete
adresa DNS servera
BOOTP nepodporoval dynamické prideľovanie adries, na BOOTP servery boli predom nadefinované IP adresy a k nim MAC adresy, na základe tejto väzby bola klientovi pridelená IP, vždy mal tú istú IP adresu.


Rozdiely medzi BOOTP a DHCP:
pri DHCP je pridelenie adresy na určité obdobie, po ktorom musí požiadať o novú adresu, klient si môže prenajať adresu
DHCP poskytuje klientovi aj iné informácie ako WINS a doménové meno
1.2.3. Hlavné výhody DHCP
Mechanizmy na prideľovanie IP adries:
automatické pridelenie, DHCP prideľuje trvalú IP adresu
manuálne pridelenie, IP adresa pre klienta je pridelená administrátorom, DHCP pridelí IP klientovi
- dynamické pridelenie, automatické pridelenie na určité obdobie

Niektoré konfiguračné parametre podľa IETF RFC 1533:
sieťová maska
Router
meno domény

Domain Name Server
- WINS Server

Na sieti môže byť viac DHCP serverov, klient si môže vybrať len jeden.

1.2.4. Fungovanie DHCP

Postup konfigurácie klienta:

klient musí mať nakonfigurovaný DHCP pri spustení siete. Klient posiela požiadavku na server o IP konfiguráciu cez broadcast nazývaný DHCPDISCOVER. Niekedy môže klient navrhnúť IP, napr. pri požiadavke na predĺženie prenájmu.

pri príjme požiadavky serverom sa určuje, či je možné spracovať túto žiadosť podľa jeho databázy. Ak nemôže, môže presmerovať požiadavku na iný server. Ak môže, pridelí klientovi konfiguračné informácie cez unicast DHCPOFFER. V informácii je navrhnutá IP adresa, adresa DNS servera a čas prenájmu.

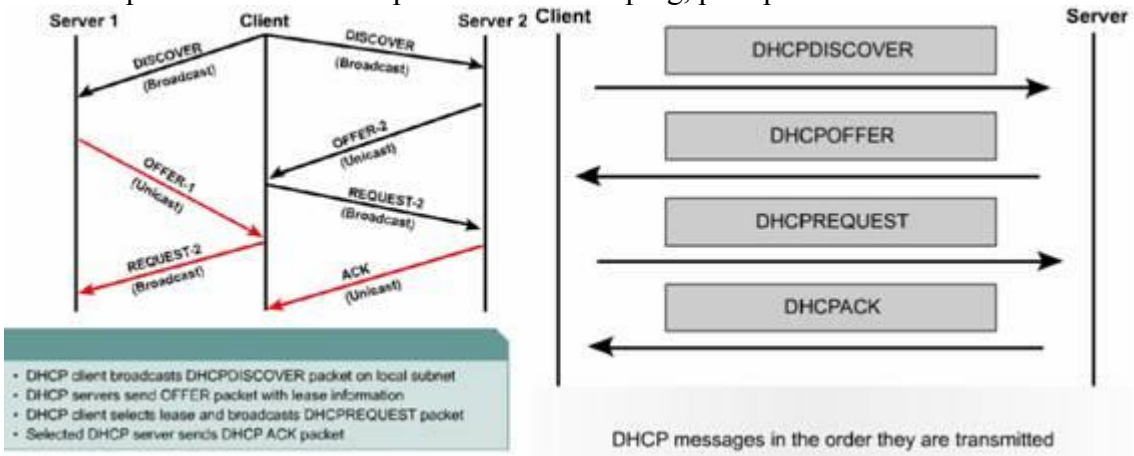
pri príjme ponuky klient posiela broadcast DHCPREQUEST, aby aj ostatné servery vedeli o akceptovanej ponuke.

server, ktorý prijal DHCPREQUEST, potvrdí konfiguráciu cez unicast DHCPACK. Toto potvrdenie oprávňuje klienta používať pridelenú IP adresu.

ak klient zdeteguje, že adresa je už používaná, pošle DHCPDECLINE a proces začne od znova. Ak klient prijme DHCPNACK od serveru po poslaní DHCPREQUEST, proces sa naštartuje od znova.

- ak klient nepotrebuje IP, pošle na server DHCPRELEASE

Cisco IOS DHCP server vždy pred pridelením IP adresy klientovi kontroluje, či adresa už nie je používaná. Bude posielať ICMP echo požiadavku alebo ping, pred poslaním DHCPOFFER.




5

1.2.5. Konfigurovanie DHCP

ip dhcp pool – vytvára blok so špecifickým menom a prepína router do DHCP konfiguračného módu.
network IP rozsah SN – zadáva sa v DHCP konfiguračnom móde, definuje rozsah adries ip dhcp excluded-address IP – rezervuje individuálnu adresu alebo rozsah adries pre klienta default-router IP – nastavuje východziu bránu dns-server IP– adresa DNS servera netbios-name-server IP - WINS server

```
Router(config)#ip dhcp excluded-address ip-address [end-ip-address]
```

```
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10
Router(config)#ip dhcp excluded-address 172.16.1.254
```

```
Router(config)#ip dhcp pool subnet12
Router(dhcp-config)#network 172.16.12.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.12.254
Router(dhcp-config)#dns-server 172.16.1.2
Router(dhcp-config)#netbios-name-server 172.16.1.3
Router(dhcp-config)#domain-name foo.com
```

domain-name – špecifikuje doménové meno pre klienta lease – doba prenájmu, default je jeden deň

1.2.6. Overovanie funkčnosti DHCP

show ip dhcp binding – zobrazí všetky pridelené adresy DHCP serverom show ip dhcp server statistics – zobrazí množstvo poslaných a prijatých správ

1.2.7. Riešenie problémov DHCP

debug ip dhcp server events – príkaz bude zobrazovať periodické kontroly servera, či niektoré prenajatie nevypršalo.

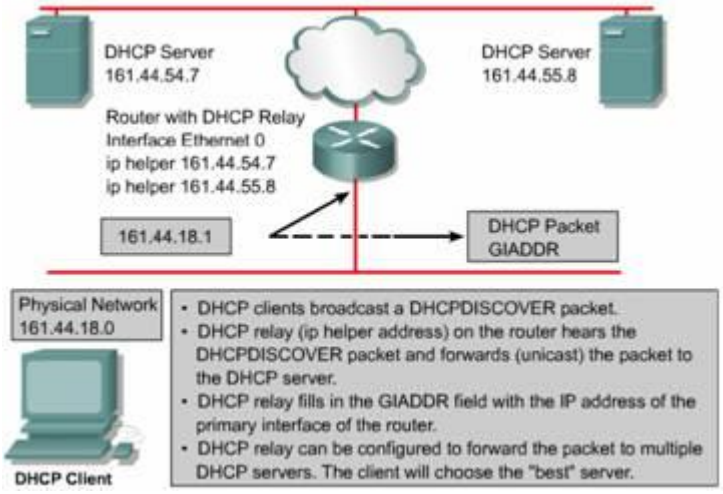
1.2.8. Zmena DHCP

DHCP klient využíva broadcast na nájdenie DHCP servera, ak sa server nachádza za routrom, server nebude nájdený, pretože router neprepúšťa broadcast. Broadcast sa taktiež využíva pri hľadaní TFTP a TACACS (security server) servera. Riešením je umiestniť DHCP server na všetky podsiete alebo využiť Cisco IOS helper address feature. Druhá je praktickejšia.

ip helper-address – spustí prenos broadcastových požiadaviek pre kľúčové UDP služby podporované

UDP služby pri ip helper-address:

Time - BOOTP/DHCP Server - NetBIOS Name Service
TACACS - BOOTP/DHCP Client - NetBIOS datagram
DNS - TFTP Service




Pri vyslaní DHCPDISCOVER broadcastového paketu klientom a nakonfigurovanej helper-address na routri je paket východzou bránou na špecifickú adresu. Pred presunom paketu router vyplní GIADDR pole IP adresou routra pre tento segment. Táto adresa potom bude východzou bránou pre DHCP klienta.

WAN technologie

**2.1.1. WAN technológie**

WAN je dátová komunikačná sieť, ktorá prepája geograficky oddelené LAN. WAN služby sa prenajímajú od

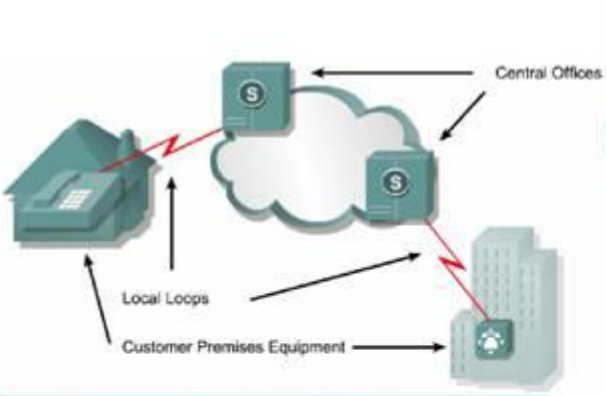
vonkajšieho **WAN poskytovateľa služby**. Využívajú sa na vzájomné prepojenie organizácií, pripojenie k vonkajším službám a vzdialených používateľov. Vo WAN sú rôzne dátové typy, ako hlas, dáta a video.

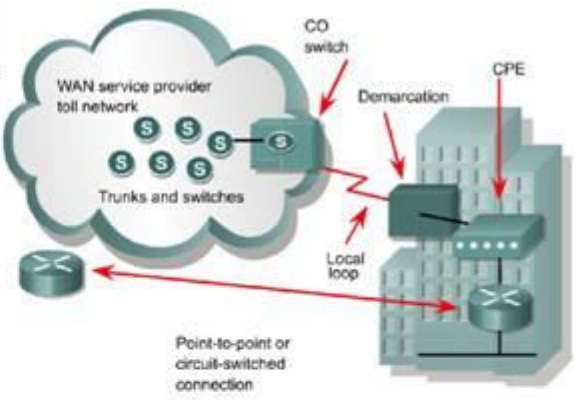
**customer premises equipment** (CPE) – zariadenia u zákazníka, ktoré si kúpi alebo prenajme od poskytovateľa

služby.

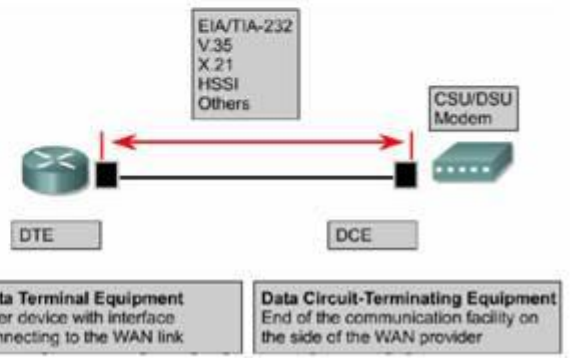
**central office (CO) -** miesto u poskytovateľa, kam vedú medené alebo optické káble od zákazníka

**miestna slučka (posledná míľa)** – káble medené alebo optické k CO




| Line Type | Signal Standard | Bit Rate Capacity |
|---|---|---|
| 56 | DS0 | 56 Kbps |
| 64 | DS0 | 64 Kbps |
| T1 | DS1 | 1.544 Mbps |
| E1 | ZM | 2.048 Mbps |
| E3 | M3 | 34.064 Mbps |
| J1 | Y1 | 2.048 Mbps |
| T3 | DS3 | 44.736 Mbps |
| OC-1 | SONET | 51.84 Mbps |
| OC-3 | SONET | 155.54 Mbps |
| OC-9 | SONET | 466.56 Mbps |
| OC-12 | SONET | 622.08 Mbps |
| OC-18 | SONET | 933.12 Mbps |
| OC-24 | SONET | 1244.16 Mbps |
| OC-36 | SONET | 1866.24 Mbps |
| OC-48 | SONET | 2488.32 Mbps |



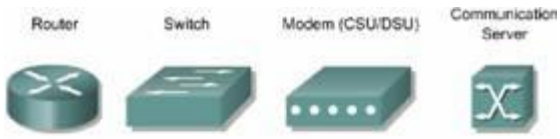

**data communications equipment (DCE)** – zariadenie, ktoré prekladá dáta na lokálnu slučku u poskytovateľa

**data terminal equipment (DTE)** – koncové dátové zariadenie u zákazníka

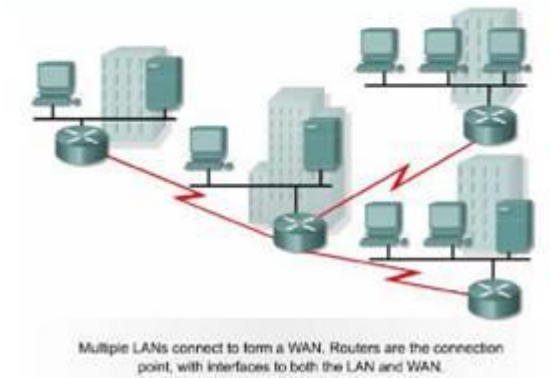
DTE/DCE – využíva protokoly fyzickej vrstvy

WAN linky sú poskytované s rôznou rýchlosťou od bps po Mbps v plnom duplexe.

### 2.1.2. Zariadenia WAN



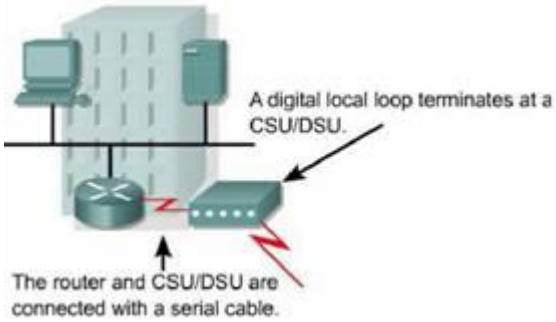




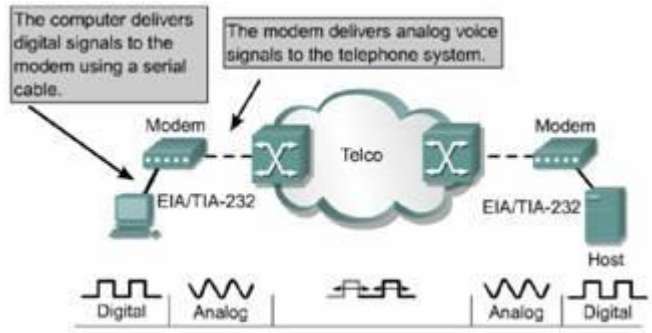
Multiple LANs connect to form a WAN. Routers are the connection point, with interfaces to both the LAN and WAN.

WAN je zoskupenie sietí LAN cez linky od poskytovateľa služieb. Tieto linky musia byť pripojené do LAN cez rôzne zariadenia. Komunikácia na LAN je posielaná na router, ktorý obsahuje LAN aj WAN rozhranie. channel service unit (CSU) a data service unit (DSU) – prevádzajú signál do zrozumiteľnej

podoby pre komunikačné linky, môžu byť zabudované rovno v rozhraní routra.




1




**Modem** – využíva sa na prevod digitálneho signálu na analógový a naopak.

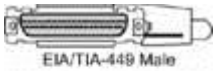
### 2.1.3. WAN štandardy

WAN štandardy sú spravované množstvom úradov:

| Acronym | Organization |
|---|---|
| iTU-T(wasCCnT) | lriteriiatiun.nl Telecommunication Union Telecommunicatíor Standardization Sector, formerly the Consultative Committee for Intemational Tetegraph and Telephone |
| ISO | Intemational Organization for Standardization |
| IETF | Intemet Engineering Task Foroe |
| EIA | Electronic Ind u strieš Association |
| **TIA** | TelecLnnmijnic:atians ln:Juslrieří Asodíätion |

**Eä^**

Fyzická vrstva protokolu popisuje, ako sú poskytnuté elektrické, mechanické a funkčné pripojenia na poskytovateľa služieb. Niektoré štandardy fyzickej vrstvy:

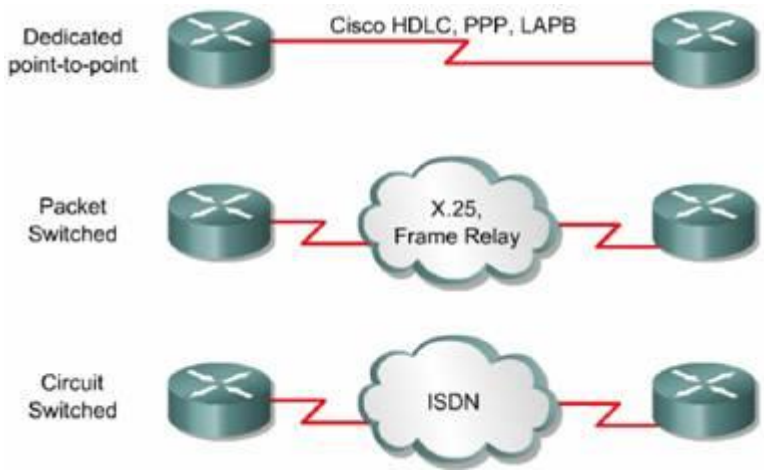




EIA/TIA-232 Malé
EIA/TIA-232 Female
**£^^S>**
X.21 Female
EIA-530 Malé

| **Štandard** | " |
|---|---|
| **Descríption** | |
| EIA/TIA-232 | Allows signál speeds of up to 64 Kbps on a 25 pin D connector over short distances lt was formeriy known as R 5-232, The **ITU-T** V.24- specificatirjn is eľfectively the jame |
| EIA/TIA-449/530 | A tester (up Lo 2 Mbps) version of EIA/TIA-232. \l uses a 35 pin D conneclor and is capable of longer cable runs. There are several versions. Also known as RS-422 and RS-423. |
| EIA/TIA-612/613 | The Higľi Speed Seriál Interface (HS5I}, which provides access to services- at up to 52 Mbps on a 60 pin D connector |
| V.35 | Ari ITU-T štandard fof synchrofious commuinicatiaris between a network access device and a packet nelworti gt speeds up lo 48 Kbps. II uses a 34 pin rectangular conneclor. |
| X.21 | An **ITU-T** štandard for synchronous digilal communicalions. II uses a 15pin D connector. |

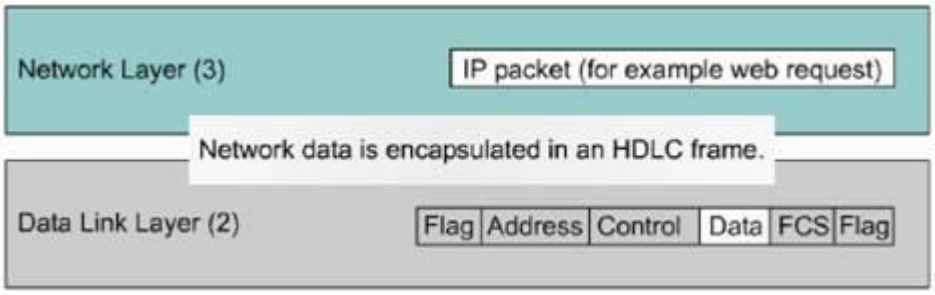
V.35 Malé
>
V.35 Female
EIA-613HSSIMale



Linková vrstva definuje, ako sú dáta zapuzdrené pre prenos. Sú využívané rôzne technológie, ako ISDN, Frame Relay alebo Asynchronous Transfer Mode (ATM).

### 2.1.4. WAN zapuzdrenie

Dáta zo sieťovej vrstvy prechádzajú na linkovú vrstvu a na fyzickú vrstvu. Linková vrstva pridá dáta pre kontrolu, zapuzdruje dáta sieťovej vrstvy. Na zapuzdrenia sa využívajú rôzne štandardy, napr. HDLC. Na zabezpečenie správnej komunikácie, musí byť na oboch routroch správne nakonfigurované zapuzdrenie. HDLC poskytuje spoľahlivé doručovanie dát na nespoľahlivej linke, zabezpečuje kontrolu toku a kontrolu chýb. Rámec vždy štartuje na oboch koncoch s 8 bitovým poľom: 0111 1110. Pretože dáta by mohli obsahovať tento prefix, vkladá HDLC po každých 5 jednotkách 0 bit, tak zabezpečí, že prefix je len na koncoch rámca. Prijímací systém odstráni vkladané bity.
2

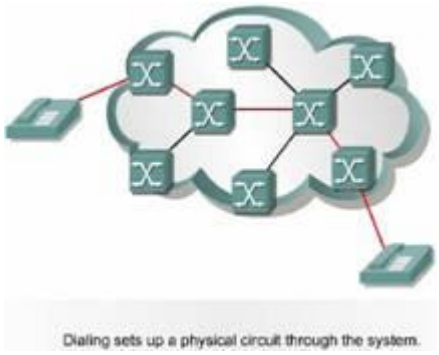



Pri WAN linkách nie je potrebné adresné pole, pretože je tu vždy spojenie bod – bod. Je však stále prítomné
a môže byť 1 -2 byty dlhé.
Kontrolné pole indikuje typ rámca, veľkosť 1 byt:
nečíslovaný, nesú nastavovacie správy
informačné, nesú dáta sieťovej vrstvy
Supervisory (kontrolné), kontrolujú tok informačných správ a požiadavky pre preposlanie pri chybe Hlavička rámca: adresa a kontrolné pole Za hlavičkou nasledujú zapuzdrené dáta a kontrolný súčet. Protokoly pre linkovú vrstvu:

| Protocol | Usage |
|---|---|
| Link Access Procedure Balanced (LAPB) | X.25 |
| Link Access Procedure D Channel (LAPD) | ISDN D channel |
| Link Access Procedure Frame (LAPF) | Frame Relay |
| High-Level Data Link Control (HDLC) | Cisco default |
| Point-to-Point Protocol (PPP) | Dialup connections |

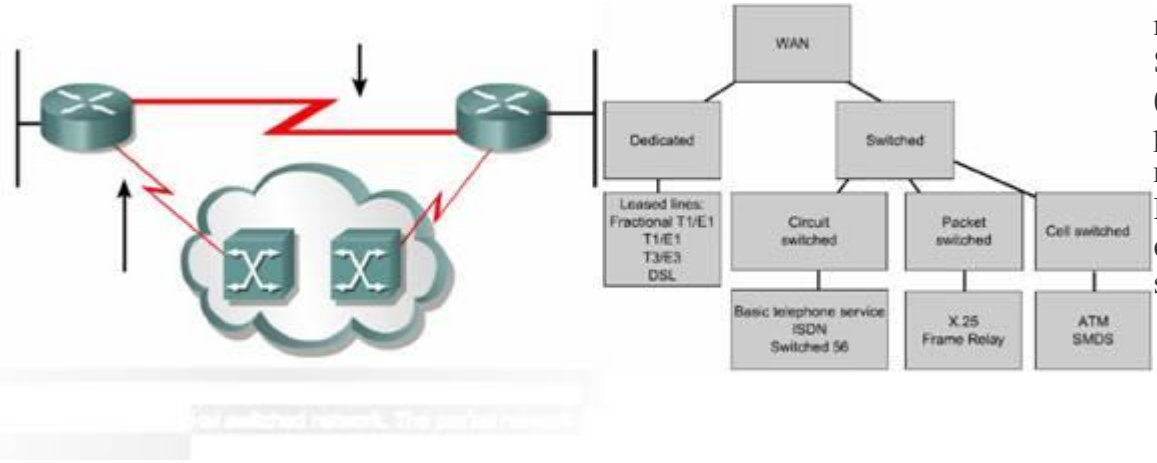
### 2.1.5. Paketové a okruhové prepínanie

Paketová prepínaná sieť prekonáva okruhové siete a je efektívnejšia vo WAN technológii.



**Kruhová prepínaná sieť**: na prepínacie operácie je využitý okruh. Pri vytočení telefónneho čísla, je číslo použité na nastavenie prepínačov v súvislom okruhu od volajúceho k volanému. **Time division multiplexing (TDM)**: cesta medzi ústredňami je zdieľaná, je dostupná pevná kapacita pripojenia pre účastníka. Pri prenose počítačových dát je neefektívne využitie pevnej kapacity. Tento spôsob prenosu je drahý.

**Paketovo prepínaná sieť:** paket prechádza od ústredne k ústredni. Pri zdieľanom okruhu je nevyhnutné označovať pakety, aby systém vedel, kam ich má doručiť. Kapacita dopravy je využitá, len keď je potrebná,
dostupná kapacita linky je zdieľaná medzi veľa používateľmi, čím sa dosahuje nižšej ceny. Pri tomto spôsobe
komunikácie vznikajú oneskorenia.
Spojenie môže byť spojito alebo bez spojito orientované. Bezspojité sú napr. internet, pri tomto spôsobe musí
prepínač určiť, či paket bude poslaný ďalej.
V spojito orientovaných systémoch je vopred určené smerovanie pre paket a každý paket potrebuje niesť len
identifikátor, vo Frame Relay je to Data Link Control Identifiers (DLCI). Prepínač sa rozhoduje na základe
identifikátora v tabuľke.
Virtual Circuit (VC) – záznamy v tabuľke len po dobu prechodu paketu cez prepínač, tabuľka je zostavená na




základe zaslania connection request cez sieť.
Switched Virtual Circuit (SVC) – výsledný okruh po zaslaní connection request.
Permanent Virtual Circuit (PVC) – trvale dostupný okruh

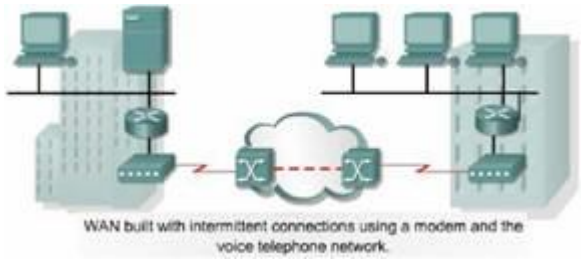


### 2.1.6. Voľby WAN liniek

LANs can be **corinected** with **a long** leased **lirie or with shorter**
leased lines to a packet switched network. The packet network (LANs môžu byť prepojené cez dlhé, prenajaté linky
does the long haul alebo cez krátke linky v paketovo prepínanej sieti.)
Kruhové prepínanie zabezpečuje fyzické prepojenie medzi odosielateľom a prijímateľom pre hlas alebo dáta. Pred komunikáciou musí zabezpečiť nastavenie prepínačov, v telefónnom systéme sa to realizuje vytočením čísla.
Trvalý okruh - odstraňuje oneskorenie spojené s vytočením linky, tieto prenajaté linky majú vyššiu rýchlosť a býva medzi prepínanými okruhmi. Príklad pre kruhové prepínanie:
starý telefónny systém
ISDN
**Cena** pri paketovom prepínaní je nižšia, než pri okruhovom, pretože linky sú zdieľané veľa užívateľmi.
**Oneskorenie** pri paketovom je vyššie, než pri okruhovom, je to z dôvodu zdieľania linky a paket musí byť prijatý celý, pred poslaním na ďalší prepínač. Hoci je premenlivé oneskorenie, táto technológia sa

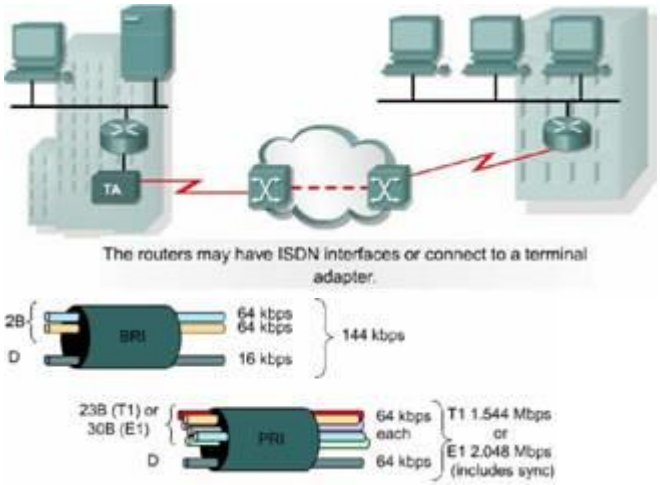
používa na prenos hlasu a dokonca videa.
point-of-presence (POP) - miesto u poskytovateľa, kde sa užívateľ pripája na paketovo prepínanú sieť.
Bunkovo alebo paketovo prepínané spojenie:
Frame Relay
X.25
ATM

### 2.2.1. Analógové spojenie




Na prenos sa využíva analógová telefónna linka a modem, je vhodné pre malý prenos dát. Pripojenie je realizované po medenom vedení nazývané miestna slučka. Pretože lokálna slučka nie je určená na digitálnu komunikáciu, používa sa modem na prevod digitálneho signálu na analógový (modulácia). V cieľovej stanici je opäť demodulovaný na digitálny signál. Maximálna rýchlosť je 56kbps. Tarifa je odvodená od vzdialenosti medzi koncovými bodmi, hodiny a doby trvania pripojenia. Výhodou je jednoduchosť, dostupnosť a nízka cena. Nevýhodou je nízka rýchlosť a dlhé pripájanie.

### 2.2.2. ISDN




Lokálna slučka nesie digitálny signál, vyššia kapacita prepínaného pripojenia.



**Integrated Services Digital Network (ISDN)** – zmena lokálnej slučky na TDM pripojenie. Využíva sa 64kbps
nosný kanálový pár (B) na dáta alebo hlas a delta (D) kanál pre servisné služby.
**Basic Rate Interface (BRI) ISDN** – je určený pre domácnosti a malé podniky, poskytuje 2 64kbps B kanály
a jede D 16kbps kanál.
**Primary Rate Interface (PRI) ISDN** – 23 x 64kbps B kanálov a jeden 64kbps D servisný kanál v severnej
Amerike. Maximálna rýchlosť je 1.544 Mbps = T1.
V Európe, Austrálii a iných častiach sveta je to 30 x 64 kbps B kanálov a jeden D kanál z maximálnou

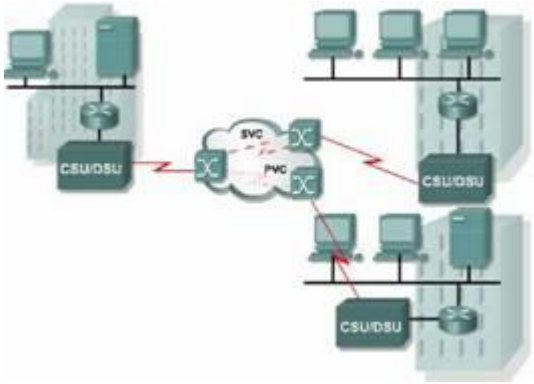
rýchlosťou do 2.048 Mbps = E1
Pri BRI nie je D kanál využitý na maximum, niektorí poskytovatelia služieb sprístupnia prenos aj na tom-
to
kanály, ale nižšou rýchlosťou ako X.25 na 9,6kbps.
Pri požiadavke na vyššiu rýchlosť ako 64kbps je možné využiť druhý B kanál, čím sa dosiahne rýchlosť 128kbps. Možné využitie je pre prenos video konferencií, nie je premenlivé oneskorenie.

**2.2.3. Prenajaté linky**

| **Line Type** | **Signál Štan-dard** | **Bit Rate Capacity** |
|---|---|---|
| 56 | DSC | SSkbps |
| Bi | DSC | 64kbps |
| T1 | DS1 | 1 544 Mbps |
| E1 | ZM | 2 048 Mbps |
| E3 | M3 | 34.064 Mbps |
| J1 | Y1 | 2 048 Mbps |
| T3 | DS3 | 44.736 Mbps |
| OC-1 | SONET | 51 84 Mbps |
| OC-3 | SONET | 155.54 Mbps |
| OC-B | SONET | 406.56 Mbps |
| OC-12 | SONET | 622 0B Mbps |
| OC-18 | SONET | 833.12 Mbps |
| DC-24 | SONET | 1244.16 Mbps |
| OC-36 | SONET | 1866.24 Mbps |
| OC-48 | SONET | 2488.32 Mbps |

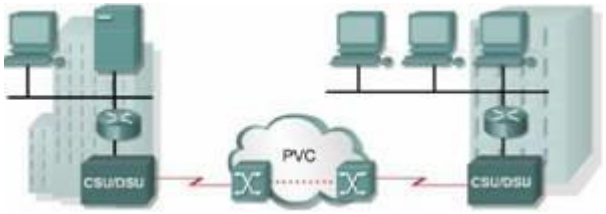

Používa sa pri požiadavke na trvalé pripojenie do 2.5
Gbps.
Tieto linky sú spoplatnené na základe požadovanej šírky
pásma a vzdialenosti medzi dvoma prípojnými bodmi,
prenajatie linky musí byť vyvážená výhodami.
Sú vyžadované sériové porty na routroch CSU/DSU. Využívajú sa pre výstavbu WANs.
Medzi nevýhody patrí premenlivé využitie linky a má fixnú kapacitu.
Cez prenajatú linku môže byť multiplexované viacero prepojení, výsledkom je menej rozhraní.

**2.2.4. X.25**




Protokol pre paketovo prepínanú sieť, poskytuje nízku bitovú rýchlosť zdieľanej premenlivej kapacity maximálne do 48 kbps, ktorá môže byť trvalá alebo prepínaná. Je poskytovaný so sieťovou adresou. Prejavuje sa oneskorenie. Je cenove výhodný, spoplatňuje sa na základe množstva prenesených dát.

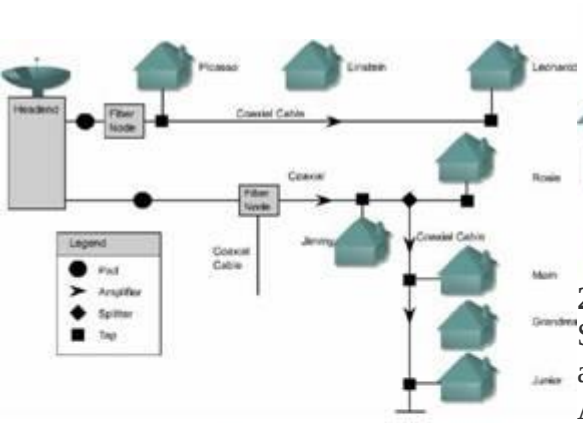
### 2.2.5. Frame Relay

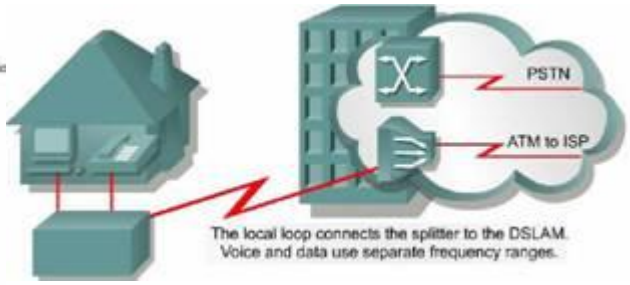


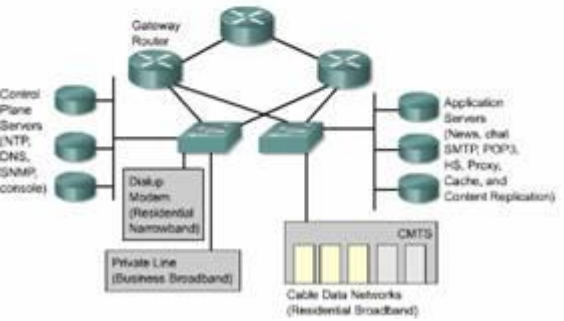

Vyznačuje sa vyššou šírkou pásma a menším
oneskorením paketového prepínania. Podobný X.25
ale prenosová rýchlosť je 4 Mbps.
Nemá implementovanú detekciu chýb a kontrolu toku.
Jednoduché narábanie s rámcami redukuje
oneskorenie.
PVC pripojení vo Frame Relay je viac než SVC. Tarifa je založená na kapacite prípojných portov k sieťovému okraju. FR poskytuje trvalú strednú zdieľanú šírku pásma prepojenia, slúži na prenos hlasu aj dát. Ideálne na prepojenie podnikových LANs. Router potrebuje len samostatné rozhranie, dokonca aj pri viacerých použitých VC.



### 2.2.6 ATM




**2.2.7 DSL**

| Service | Downlo-ad Upload | |
|---|---|---|
| ADSL | 94kbps-e 192Mbps | lekbps-WJkbps |
| 3DSL | 1 544 MbfS • 2.043 Mbps | 1 .544 Mbps - 2.048 MbpS |
| HDSL | 1.344 Mbps - 2.043 Mbps | 1.544 Mbps - 2.048 Mbps |
| IDSL | 144kbps | 144kbps |
| CDSL | 1 Mbps | i6kbps-iepkbps |

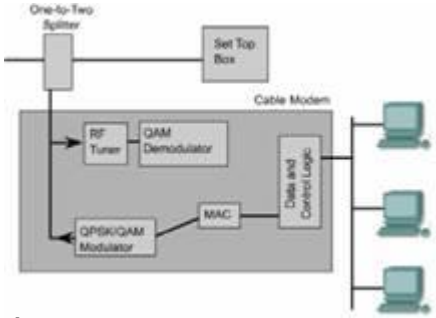
**Asynchronous Transfer Mode (ATM)** – dátová rýchlosť nad 155 Mbps. Je schopná prenášať dáta a video cez privátne siete. Je založená na rámcovej architektúre. Bunky majú fixnú dĺžky 53 bitov. Ponúkajú PVC aj SVC. PCV je viac používané. Umožňuje viaceré VC na jednej prenajatej linke.

**Digital Subscriber Line (DSL)** – je širokopásmová technológia využívajúca na prenos existujúcou krútenou telefónnu dvojlinku. Maximálna rýchlosť do 8.192 Mbps. Využíva sa technológia viacnásobných frekvencií na jednom fyzickom médiu. Používajú sa už nainštalovaná telefónne vedenia. DSL technológie:
Asymmetric DSL (ADSL)
Symmetric DSL (SDSL)
High Bit Rate DSL (HDSL)
ISDN (like) DSL (IDSL)
Consumer DSL (CDSL), prezývaná DSL-lite alebo G.lite DSL umožňuje normálne telefónne pripojenie a trvalé pripojenie do siete.
DSL Access Multiplexer (**DSLAM**) – multiplexuje samostatné účastnícke linky do jednej, vysokokapacitnej linky poskytovateľa.
Telefónna linka poskytuje frekvencie od 330 Hz do 3.3 KHz. Pre jeden hovor sa používa len 4KHz. DSL technológia využíva na upload (upstream) a download (downstream) zvyšné frekvencie nad 4KHz okno. Čím sa zabezpečí súčasné prenos dát aj hlasu. Najpoužívanejšie služby:
ADSL, vyšší download než upload
SDSL, rovnaká kapacita pre download a upload, na prenos hlasu je potrebná ďalšia linka Prenosová rýchlosť závisí na dĺžke poslednej míle a stave vedenia, maximálna dĺžka je do 5,5 km.

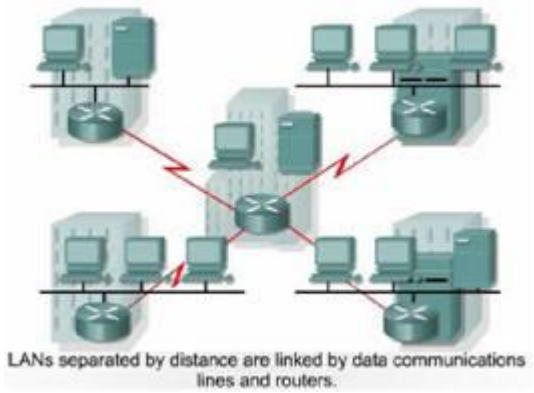
**2.2.8. Káblový modem**

Sieťový prístup je dostupný v niektorých káblových televíznych sieťach. Je tu lepšia šírka pásma, ako pri telefónnych linkách. Káblový modem umožňuje vysokorýchlostný prenos dát po tom istom kábli, po ktorom je vedené káblová TV.

Je možné dosiahnuť rýchlosť do T1, potom je linka vhodná na prenos video, audio súborov a prenos veľkého množstva dát.
Káblový modem je schopný doručovať 30- 40 Mbps dát na jednom 6MHz káblovom kanále. To je skoro 500x rýchlejšie než na 56kbps modeme.



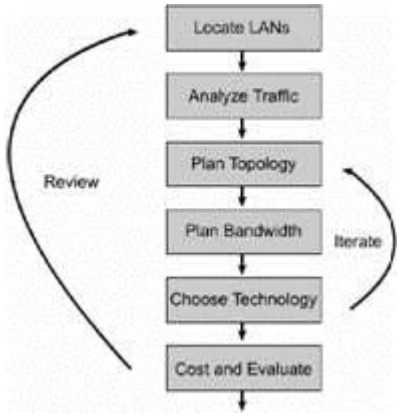

Účastník môže súčasne prijímať dáte pre TV aj PC, zabezpečuje to **one-to-two splitter**.
6


LANs separated by distance are linked by data communications lines and routers.

### 2.3.1. WAN komunikácia

WAN sú považované za dátové linky, ktoré pripájajú routre na oddelených LANs. Linky sa prenajímajú za od poskytovateľov, sú značne pomalšie ako 100Mbps na LAN. Koncové stanice, servery a routre komunikujú cez LAN a WAN dátové linky ukončujú lokálne smerovače. WAN technológie pracujú na spodných 3 vrstvách OSI modelu.

### 2.3.2. Kroky vo WAN dizajne



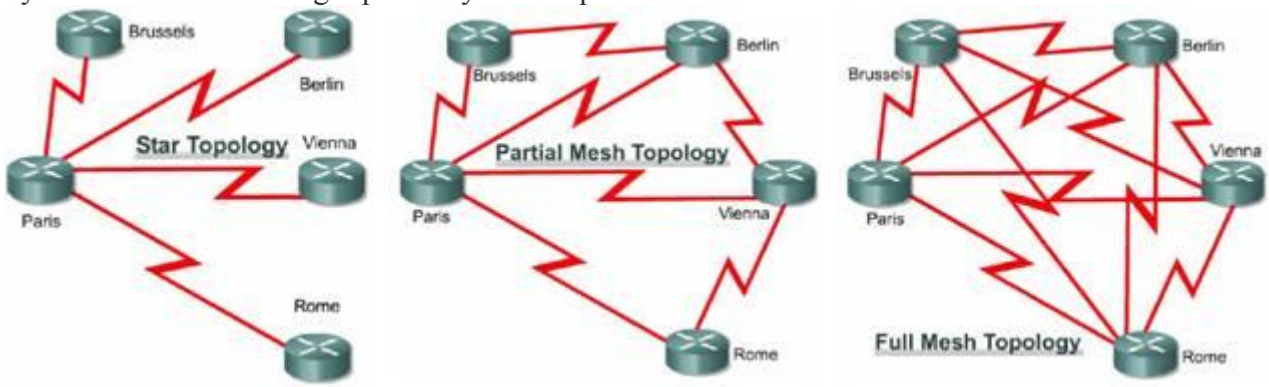
| Traffic | Latency | Jitter | Bandwidth |
|---|---|---|---|
| Voice | Low | Low | Medium |
| Transaction data (for example, SNA) | Medium | Medium | Medium |
| Messaging (e-mail) | High | High | High |
| File transfer | High | High | High |
| Batch data | High | High | High |
| Network management | High | High | Low |
| Videoconferencing | Low | Low | High |

Some WAN traffic types wilh tolerance to latency and jitter, along with bandwidth requirennents

Návrh WAN môže byť náročný, ale systematickým návrhom môže byť dosiahnutý lepší výkon za nižšiu cenu. Väčšina sa však vyvíja priebežne v čase.
Ako prvé je treba vedieť, aké dáta budú prenášané.
V závislosti na geografickom hľadisku by sa menila topológia.

### 2.3.3. Ako identifikovať a vybrať sieťovú kapacitu

Dizajn WAN pozostáva:
výberom rôzneho typu liniek medzi lokalitami
vybrať vhodnú technológiu pre linky za akceptovateľnú cenu




Faktory vybranej schémy:
viac liniek bude zvyšovať cenu sieťovej služby, ale viacnásobné cesty zvýšia spoľahlivosť
pridaním viacerých zariadení na ceste sa bude zvyšovať oneskorenie a znižovať spoľahlivosť Pre siete, kde sa vyžaduje rýchla odozva a malé oneskorenie nie sú vhodné dialup služby. ATM, Frame Relay a X.25 nesú dopravu niekoľkých zákazníkov, vyskytuje sa tu oneskorenie, preto nie sú vhodné pre niektoré aplikácie, ale výhodou je cena.

### 2.3.4. Trojvrstvový návrhový model

Výhody pri 3-vrstvovom riešení:
**škálovatelnosť**, sieť môže rásť bez obmedzení kontroly alebo správy, pretože funkcionalita je sústredená a problém je možné nájsť jednoduchšie
**jednoduchá implementácia**, hierarchický dizajn priradí funkcionalitu každej vrstve

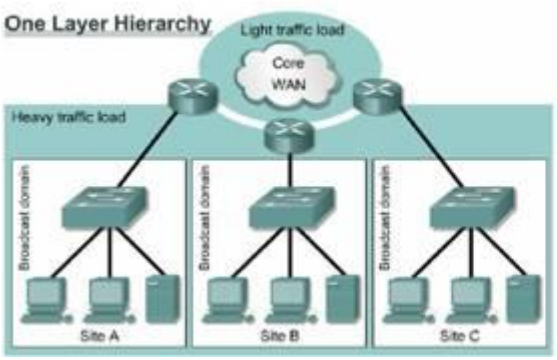


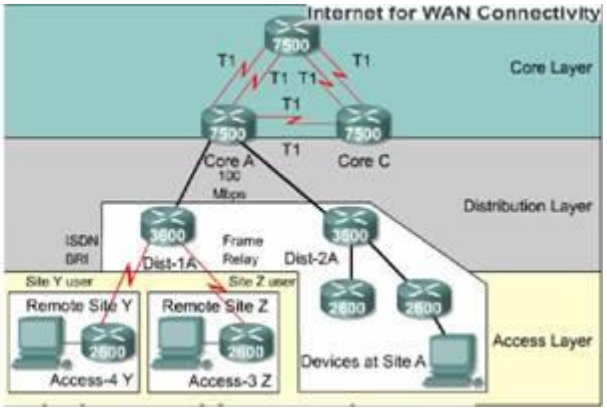
**jednoduché odstraňovanie problémov**, funkcionalita každej vrstvy je dobre definovaná, izolovanie problému v sieti je menej komplikované
**predictability**, správanie siete je použitím funkčných vrstiev je do značnej miery predpovedateľné
**podpora protokolov**, miešanie terajších a budúcich protokolov je jednoduchšie, pretože základná infraštruktúra je logicky organizovaná

- **manažovatelnosť**

Trojvrstvový hierarchický model využívajú telefónne systémy. Rozdelenie je medzi regióny, oblasti a odbory. **access links** alebo prístupová vrstva na WAN, pripájajú rôzne miesta v oblasti na podnikovú sieť
**distribution links** – prepájajú dopravu medzi oblasťami, presun dát medzi regiónmi

### 2.3.5. Iné vrstvovo orientované modely




Veľa sietí nepotrebuje komplexnosť plnej 3-vrstvovej siete. Pri podnikoch z niekoľkými pobočkami a minimálnymi požiadavkami na vzájomnú komunikáciu môžme zvoliť 1-vrstvový model, na prepojenie je
vhodné použiť Frame Relay.

### 2.3.6. Iné WAN dizajnové hľadiská

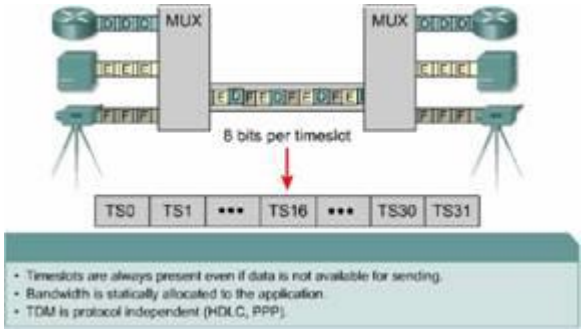
Veľa podnikových sietí je pripojených do internetu, cez ktorý je možné zrealizovať vnútropodnikové prepojenie. Každá LAN je pripojená na miestneho ISP. Bezpečnosť rôznych LAN je sporná.
PPP

### 3.1.1. Úvod do sériovej komunikácie

WAN technológie sú založená na sériovom prenose po fyzickej vrstve. Bity, ktoré tvoria rámce 2 vrstvy, sú jeden po druhom prenášané po fyzickom médiu. Príklady komunikačných štandardov:
RS-232-E
V.35
High Speed Serial Interface (HSSI)

### 3.1.2. Časový multiplex

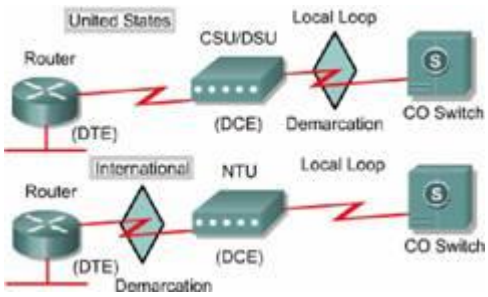
Time-division multiplexing (**TDM**) je prenos niekoľkých zdrojových informácií, použitím jedného kanálu a následne rekonštruovaný na pôvodný prúd na vzdialenom konci. Pracuje na fyzickej vrstve.

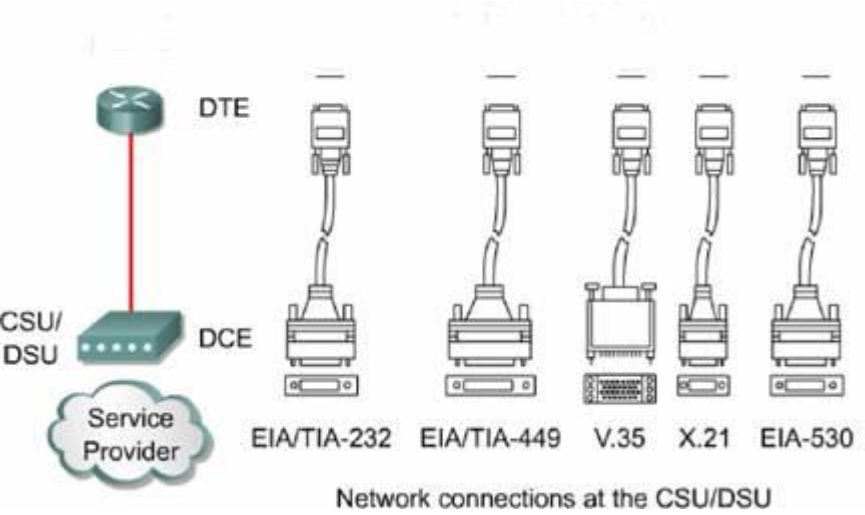



V tomto prípade sú 3 zdrojové informácie zahrnuté do výstupného kanálu. Veľkosť tejto informácie môže byť rôzna, ale typicky býva 8 bitov alebo bajtov, v závislosti na bitoch alebo bajtoch ide o preklad **bitový** alebo **bajtový.**
Súčet kapacity všetkých kanálov musí byť menší, než kapacita výstupného kanálu. Časové sloty sú prideľované, aj keď nie sú dáta pre daný kanál. Príkladom využitia časových slotov je ISDN, pri BRI sú 2 64 kbps B kanály a jeden 16kbps kanál. TDM má 9 časových slotov, ktoré sú opakované.

### 3.1.3. Demarcation (hraničný) bod

- je bod v sieti, kde končí zodpovednosť servisného poskytovateľa (telco) za službu.



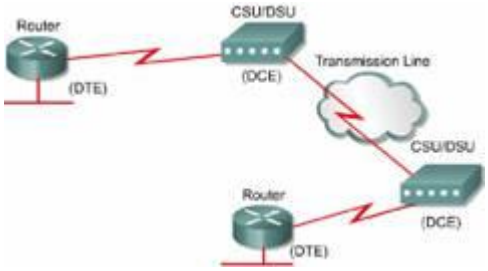


Network connections at the CSU/DSU

**USA** je tento bod až pri CSU/DSU, na ktorom je ukončená lokálna slučka. Toto ukončenie spravuje zákazník.
**iných krajinách** je ukončenie (network terminating unit (NTU)) spravované telco. To umožňuje spravovať lokálne slučky. Zákazník pripája customer premises equipment (**CPE**) zariadenie na NTU cez V.35 alebo RS-232 sériové rozhranie.

### 3.1.4. DTE/DCE

Sériové pripojenie má na jednej strane data terminal equipment (**DTE**) a na druhej data communications equipment (**DCE**).
Prepojenie medzi dvoma DCE zariadeniami je WAN sieť




servisného poskytovateľa.
CPE je hlavný router a je DTE zariadením. Iné DTE zariadenia môžu byť terminál, tlačiareň, počítač alebo fax.
**DCE,** obyčajne modem alebo CSU/DSU, je zariadenie, ktoré prevádza užívateľské dáta z DTE na akceptovateľnú formu pre transportnú linku WAN servisného poskytovateľa.

Špecifikácie pre rozhranie DTE/DCE:
**mechanické / fyzické**, typ konektoru a počet pinov
**elektrické**, napäťové úrovne pre 0 a 1
**funkčné**, špecifikuje funkcie priradené každej signálnej linke v rozhraní
**procedurálne**, špecifikuje poradie udalostí pre prenášané dáta

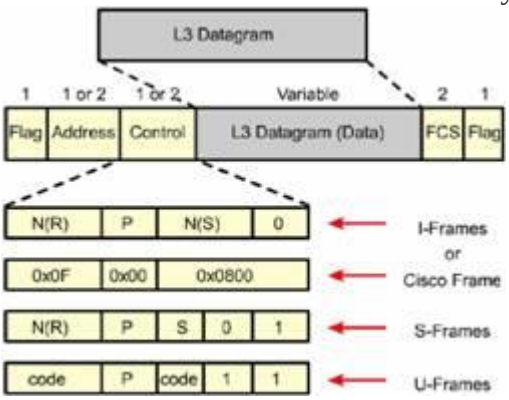
1

**Nulový modem** - kábel na prepojenie 2 DTE zariadení.
Na prepojenie 2 zariadení DTE a DCE sa používa tienený sériový kábel. DCE musí poskytovať hodinový signál. WAN poskytovatelia diktujú typ kábla. CISCO zariadenia podporujú EIA/TIA-232, EIA/TIA-449, V.35, X.21, a EIA/TIA-530 sériový štandard.
End-User Router Connections
Device
[S] [S] [S] [S] [S]

### 3.1.5 HDLC zapuzdrenie

Bitovo orientovaný dátový linkový protokol nahradil znakovo orientovaný protokol. Zapuzdruje dáta na synchrónnej sériovej linke. Linkové protokoly odvodené od HDLC:
Link Access Procedure , Balanced (LAPB) pre X.25

Link Access Procedure on the D channel (LAPD) pre ISDN
Link Access Procedure for Modems (LAPM), PPP pre modemy
Link Access Procedure for Frame Relay (LAPF) pre Frame Relay




HDLC využíva synchrónny sériový prenos poskytujúci bezchybnú komunikáciu medzi 2 bodmi. Definuje štruktúru 2 vrstvy, ktorá umožňuje kontrolu prúdu a kontrolu chýb využitím potvrdení a oknovej schémy. Všetky rámce majú rovnaký formát. Typy rámcov s rôznym formátom kontrolného poľa:
*Information frames* **(I-frames**), informačný rámec, nesené dáta budú prenášané pre stanicu. Podporuje kontrolu prúdu a chýb, dáta sú prepravované v informačnom rámci
*Supervisory frames* (**S-frames**), kontrolný rámec, poskytujú mechanizmus požiadavka/odpoveď
*Unnumbered frames* (**U-frames**), nečíslované rámce, poskytujú doplnkové linkové kontrolné funkcie
Prvé 1 alebo 2 bity rámca slúžia na identifikáciu typu rámca.

### 3.1.6 Konfigurovanie HDLC zapuzdrenia

Prednastavená zapuzdrovania metóda na synchrónnych sériových linkách CISCO zariadení je HDLC.
**encapsulation hdlc** – na rozhraní nastaví zapuzdrenie HDLC.
HDLC sa využíva na prepojenie 2 CISCO zariadení. PPP je použitý, ak sa pripája na nie CISCO zariadenie.

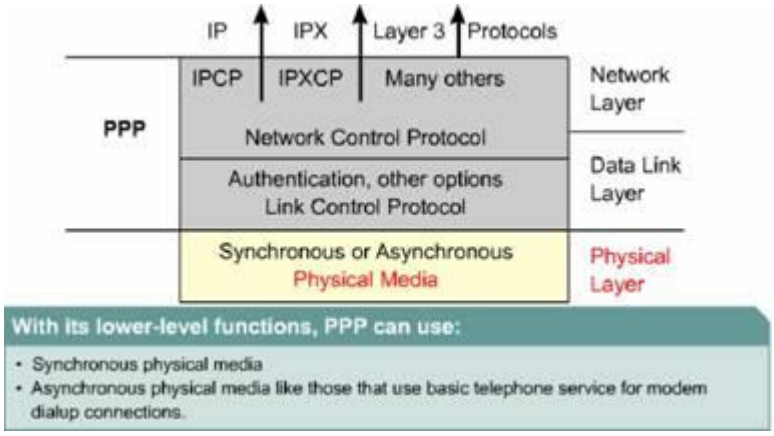
### 3.1.7. Riešenie problémov na sériovom rozhraní

**show interfaces serial** – zobrazí informácie na špecifickom rozhraní, pri nakonfigurovanom HDLC sa vo výpise zobrazí *"Encapsulation HDLC"*, pri nakonfigurovanom PPP je vo výpise *"Encapsulation PPP"*.
Zo stavu rozhrania môžu byť identifikované nasledujúce možné problémy:
**Serial x is down, line protocol is down**, zlyhanie hardwaru, zlý kábel,
**Serial x is up, line protocol is down**, lokálny alebo vzdialený smerovač je nenakonfigurovaný, zle nastavené časovanie,
**Serial x is up, line protocol is up**, správny stav linky
2

- **Serial x is administratively down, line protocol is down**, rozhranie je vypnuté, alebo je nastavená duplicitná adresa

**show controllers** – zobrazuje stav rozhrania a či je kábel pripojený na rozhranie *Ladiace príkazy*:
**debug serial interface** – treba overiť, či HDLC keepalive packets je zvyšovaný, ak nie, treba skontrolovať časovanie
**debug arp** – overenie, či router posiela ARP pakety (o naučených routroch) do WAN
**debug frame-relay lmi** – určenie, či router posiela alebo prijíma Local Management Interface (LMI) informácie
**debug frame-relay events** – overenie, či je výmena medzi routrom a Frame Relay prepínačom
**debug ppp negotiation** – zobrazí PPP pakety počas vyjednávania
**debug ppp packet** – zobrazí, či PPP pakety sú prijímané a posielané
**debug ppp** – zobrazuje PPP chyby
**debug ppp authentication** – výmena medzi Challenge Handshake Authentication Protocol (**CHAP**) aPassword Authentication Protocol (**PAP**)

### 3.2.1. PPP vrstvová architektúra




PPP využíva vrstvovú architektúru. Poskytuje metódu pre zapuzdrenie viacerých protokolových datagramov, využíva linkovú vrstvu na testovanie spojenia. Subprotokoly PPP:
**Link Control Protocol**, slúži na zabezpečenie linky bod- bod
**Network Control Protocol**, využíva sa na konfigurovanie rôznych sieťových protokolov
PPP sa využíva na rozhraniach:
synchrónnych a asynchrónnych sériových
vysokorýchlostných sériových rozhraniach (**HSSI**)
Integrated Services Digital Network (**ISDN**)

PPP využíva Link Control Protocol (**LCP**) na zapuzdrenie a dojednanie volieb pre viacnásobné sieťové vrstvové
protokoly.
Využitie PPP na automatické dohodnutie volieb ako:
**autentifikácia**, využíva sa na overenie, že volajúci má právo vytvoriť volanie. Voľby pre autentifikáciu sú *Password Authentication Protocol* (**PAP**) a *Challenge Handshake Authentication Protocol* (**CHAP**).
**kompresia**, kompresná voľba zvyšuje efektívnosť priepustnosti redukovaním množstva dátových rámcov, ktoré musia prejsť cez linku. Sú dva pre CISCO zariadenia: *Stacker* a *Predictor*.
**detekcia chýb**, detekuje zlyhanie , voľby na zabezpečenie spoľahlivosti: *Quality* a *Magic Number*
**multilink**, od CISCO 11.1. Slúži na rozdelenie výkonu.
**PPP Callback**, na ďalšie rozšírenie bezpečnosti, podporované od CISCO 11.1. Routre môžu pracovať ako klient alebo server pre volanie späť.
LCP zabezpečuje:
spracovanie paketových limitov v paketoch
detekovanie chýb zlou konfiguráciu
ukončenie linky
- určenie funkčnosti linky OK/zlyhanie

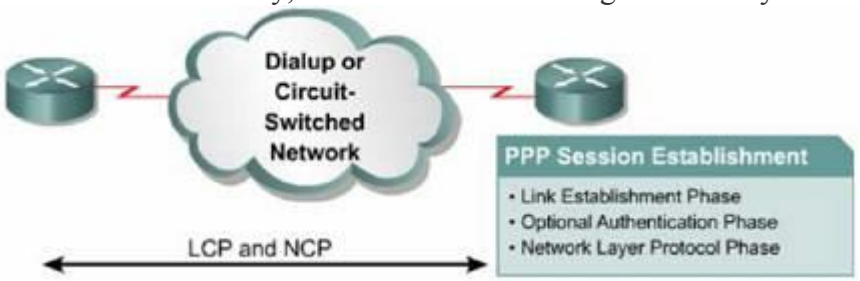
PPP rámce sú delené na oblasti:

| Value (in hex) | Protocol Name |
|---|---|
| 8021 | Internet Protocol Control Protocol |
| 8023 | OSI Network Layer Control Protocol |
| 8029 | Appletalk Control Protocol |
| 802b | Novell IPX Control Protocol |
| c021 | Link Control Protocol |
| c023 | Password Authentication Protocol |
| c223 | Challenge Handshake Authentication Protocol |

**Flag** (vlajka), indikuje koniec a začiatok rámca: 01111110
**Adresa,** štandardná broadcastová 255,
**Kontrolná,** 1 byte pozostávajúci z 00000011
**Protokol**, 2 bajty, typ zapuzdrenia rámca
**dáta,** maximálna veľkosť dát je 1500 bajtov
**FCS,** 2 bajty pre kontrolný súčet

### 3.2.2. Zabezpečenie PPP spojenia

Spojenie prechádza zriadením linky, autentifikáciou a fázou sieťového protokolu. Tieto 3 fázy zabezpečujú LCP
rámce.
Využitie LCP rámcov v PPP spojení:
rámce zabezpečenia linky, zabezpečenie a konfigurovanie linky
rámce ukončenia linky, na ukončenie linky
rámce udržiavania linky, na manažovanie a debagovanie linky



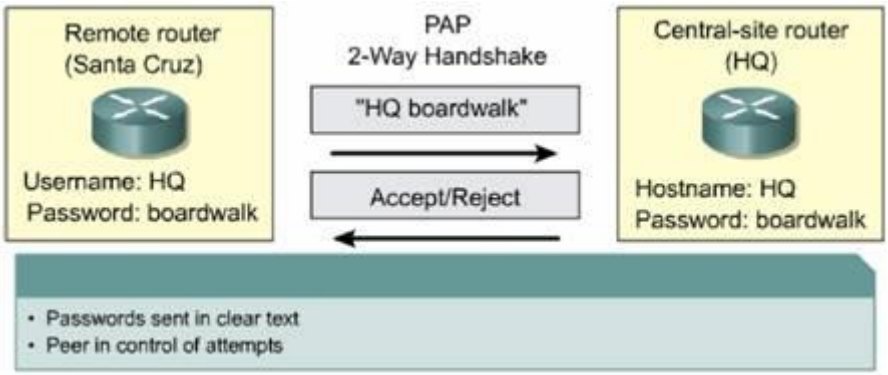

Fázy zabezpečenie PPP spojenia:
**Link-establishment phase**, každé zariadenie pošle rámec na konfigurovanie a testovanie dátovej linky. LCP obsahu voľby na dohodnutie maximálnej rýchlosti (MTU), kompresie a autentifikačný protokol. Ak v LCP pakete nie sú konfiguračné údaje, sú použité default. Pred poslaním sieťových paketov, LCP musí otvoriť spojenie a dohodnúť konfiguračné parametre, fáza je dokončená po poslaní potvrdzovacieho rámca.
**Authentication phase**, voliteľná, prebieha pred fázou sieťového vrstvového protokolu. Otestuje, či linka je dosť dobrá na zavedenie sieťového linkového protokolu.
**Network layer protocol phase**, v tejto fáze PPP zariadenia posielajú NCP paket na výber a konfigurovanie jedného alebo viacerých sieťových vrstvových protokolov.
PPP linka zostáva nakonfigurovaná pre komunikáciu až kým:
LCP alebo NCP rámce neuzavrú linku
kým neuplynie neaktívny časovač
na zásah užívateľa

### 3.2.3. PPP autentifikačný protokol

Táto fáza PPP spojenia je voliteľná. Po vytvorení linky je vybratý autentifikačný protokol, spúšťa sa pred sieťovým vrstvovým protokolom.
Volajúca strana na linke vloží autentifikačné informácie, vymenia si autentifikačné správy, tým je zabezpečené, že užívateľ má prístup na sieť. Na autentifikáciu sa využíva *Password Authentication Protocol* (**PAP**) alebo *Challenge Handshake Authentication* protokol (**CHAP**).

### 3.2.4 Password Authentication protokol (PAP)

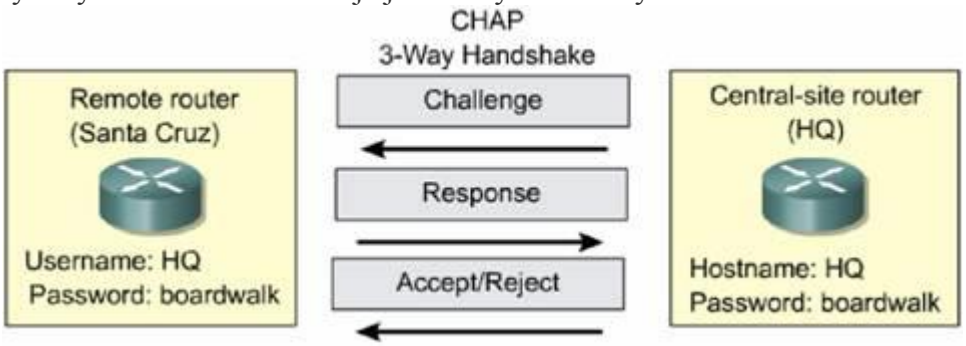
Jednoduchá metóda pre overenie identity vzdialeného bodu, využíva 2-cestné nadviazanie spojenia. Po zabezpečení PPP linky je poslané meno/heslo vzdialeným bodom, pri správnom je poslané potvrdenie, pri chybnom je spojenie ukončené. Tento algoritmus posiela heslo nezakriptované, je napadnuteľný.




4

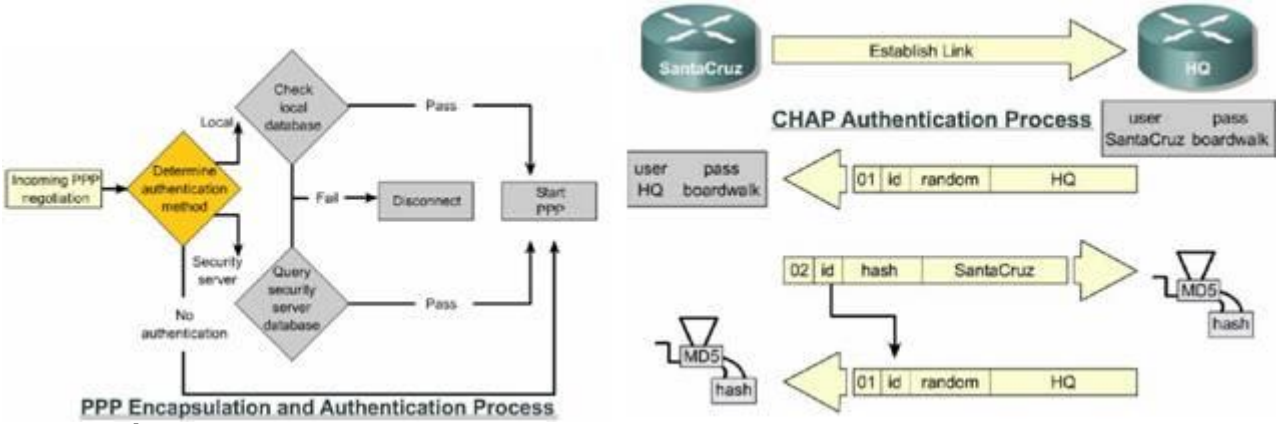
### 3.2.5 Challenge Handshake Authentication Protocol (CHAP)

CHAP sa prevádza nielen pri spustení, ale aj periodicky počas prevádzky. Využíva sa 3-cestné overovanie. Po zabezpečení PPP linky, lokálny router pošle správu s výzvou na vzdialený bod. Vzdialený bod odpovie s hodnotou vypočítanou hash funkciou, ktorá je typicky Message Digest 5 (MD5). Táto hodnota závisí od výzvovej správy a od hesla. Lokálny router porovná túto hodnotu s jeho vlastnou kalkuláciou, ak súhlasí, autentifikácia je potvrdená, pri nezhode dôjde k ukončeniu spojenia.
Spojenie realizované CHAP protokolom je odolné proti útokom, výzva v správe je jedinečné a náhodná, tým výsledok hash funkcie je jedinečný a náhodný.




### 3.2.6. PPP zapuzdrenie a autentifikačný proces

**encapsulation ppp** – príkaz na nastavenie zapuzdrenia Postupnosť pri autentifikácii:
určená metóda autentifikácie
je porovnané meno a heslo s lokálnou databázou na zhodu
pri zhode hesla je spojenie nadviazané, pri nezhode je ukončené




### 3.3.1. Úvod do konfigurovania PPP

V PPP je možné konfigurovať metódu autentifikácie, kompresie, detekciu chýb a podporu viacnásobných liniek.

### 3.3.2. Konfigurovanie PPP

Príklad zapuzdrenia sériovej linky:
Router#**configure terminal**
Router(config)#**interface serial 0/0**

Router(config-if)#**encapsulation ppp** Kompresia môže významne pôsobiť na výkon, nie je doporučená pri veľkom množstve prenášaných súborov. Príklad konfigurovania kompresie:
Router(config)#**interface serial 0/0**
Router(config-if)#**encapsulation ppp**
Router(config-if)#**compress [predictor | stac] -** predictor / stac kompresné algoritmy
5

Monitorovanie dát na linke:
Router(config)#**interface serial 0/0**
Router(config-if)#**encapsulation ppp**
Router(config-if)#**ppp quality percentage** Zabezpečenie vyrovnávania záťaže na viaceré linky:
Router(config)#**interface serial 0/0**

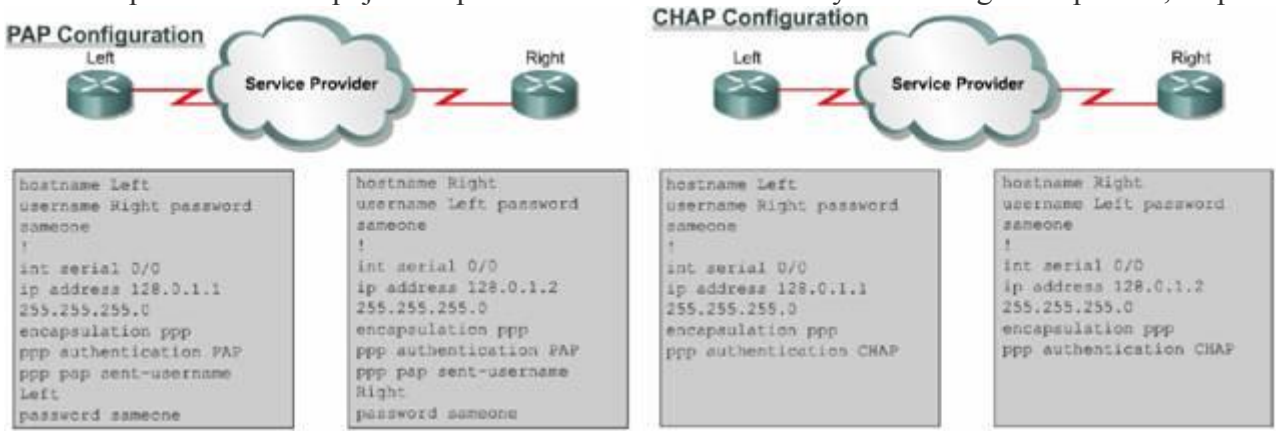
| Step | Description |
|---|---|
| Step 1 | On each router, define the username and password to expect from the remote router:<br>`Router(config)#username name password secret`<br>The arguments are described as follows:<br>• *name*–This is the host name of the remote router.<br>Note: The host name is case sensitive.<br>• *secret*–On Cisco routers, the secret password must be the same for both routers. |
| Step 2 | Enter interface configuration mode for the desired interface. |
| Step 3 | Configure the interface for PPP encapsulation:<br>`Router(config-if)#encapsulation ppp` |
| Step 4 | Configure PPP authentication:<br>`Router(config-if)#ppp authentication {chap \| chap pap \| pap chap \| pap}` |
| Step 5 | If CHAP and PAP are enabled, then the first method specified is requested during the link negotiation phase. If the peer suggests using the second method or simply refuses the first method, then the second method is tried. |
| Step 6 | In Cisco IOS Releases 11.1 or later, PAP must be enabled on the interface, as it is disabled by default.<br>`Router(config-if)#ppp pap sent-username username password password` |

Router(config-if)#**encapsulation ppp**
Router(config-if)#**ppp multilink**


### 3.3.3. Konfigurovania PPP autentifikácie

**PAP**
**username** *name* **password** *password* – meno / heslo druhého routra
**hostname** na jednom routri musí súhlasiť s **username** na druhom routri. Heslo sa musí zhodovať.
Overovanie len pri nadviazaní spojenia
**CHAP**

Overenie pri nadviazaní spojenia a periodické overovanie identity. Pri konfigurácii platí to, čo pri PAP.




**Overovanie konfigurácie sériového zapuzdrenia PPP show interfaces serial** – príkaz na overenie správnej konfigurácie HDLC alebo PPP zapuzdrenia.
**Riešenie problémov v sériovom zapuzdrení a konfigurácii**
**debug ppp authentication** – zobrazuje sekvenciu autentifikácie **debug ppp** – zobrazenie informácií o operáciách PPP

ISDN a DDR

### 4.1.1. Úvod do ISDN

ISDN je jedna z WAN technológií, ktoré poskytujú sieťový prístup zo vzdialeného miesta. Je vhodná pri nižších nárokoch na šírku pásma, ako zmena za vytáčané pripojenie.
Pri analógovom okruhu bola limitácia šírky pásma na lokálnej slučke, frekvencia sa pohybovala do 3kHz. ISDN umožňujú využitie digitálneho okruhu pre lokálnu slučku, poskytujú lepšiu prístupovú rýchlosť pre vzdialených používateľov. Bola navrhnutá ako plne digitálna sieť. Výhody ISDN:
nesú premenlivé dáta, ako dáta, hlas, video.
rýchlejšie nadviazanie spojenia, ako pri modemovom pripojení
B kanály poskytujú väčšiu rýchlosť ako pri modemovom pripojení
- B kanály vhodné pre dohodnutie Point-to-Point Protocol (PPP) linky

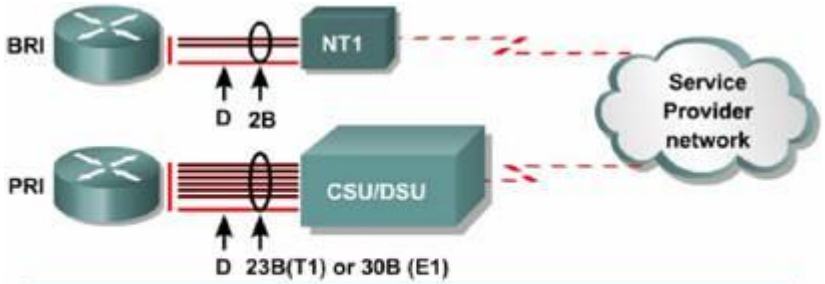
ISDN je schopné využiť viacnásobné kanály na prenos rôznych dát po jednom vedení.
D – kanál je pre nadviazanie spojenia a pre signalizáciu hovoru.
B – kanály sú nosné kanály, doprava je čisto digitálna. Každý B kanál poskytuje 64 kbps, využíva sa PPP zapuzdrenie.

### 4.1.2. ISDN štandardy a prístupové metódy

ISDN štandardy sú sada protokolov, ktoré zahŕňajú digitálne telefóny a dátovú komunikáciu. Delenie ISDN protokolov:
**E protokoly**, doporučený sieťový štandard pre ISDN.
**I protokoly**, časť s konceptmi, terminológiou a hlavnými metódami.
- **Q protokol**, spôsob zabezpečovania ISDN hovoru.

Kanálové typy podľa ISDN štandardu:
- B kanál, definovaný ako čiste digitálny cesta 64 kbps.
- D kanál, 16 kbps pre BRI a 64 kbps PRI, využíva sa na prenos kontrolných informácií B kanálu

**connection setup** – výmena informácií pri nadviazaní spojenia
**in-band signaling –** vnútrokanálová signalizácia, rovnaká cesta je použitá pre prenos dát a kontrolných informácií **out-of-band signaling** – prenos signálnych informácií po samostatnom kanále D **BRI** (2B+D) - na prenos sa používajú 2 B 64 kbps kanály a jeden 16 kbps D kanál na signalizáciu.




| Channel | Capacity | Mostly Used for |
|---|---|---|
| B | 64 kbps | Circuit-switched data (HDLC, PPP) |
| D | 16/64 kbps | Signaling information (LAPD) |

**PRI:**
v Severne Amerike a Japonsku sa na prenos sa používa 23 B 64 kbps kanálov a jeden 64kbps D kanál na signalizáciu, T1.
v Európe sa na prenos sa používa 30 B 64 kbps kanálov a jeden 64kbps D kanál na signalizáciu, E1.

### 4.1.3. ISDN 3-vrstvový model a protokoly

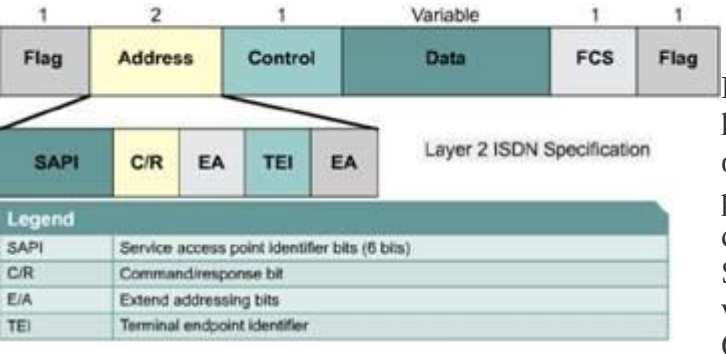
| OSI Layer | D-Channel | B-Channel |
|---|---|---|
| 3 | Q.931 - ISDN Network Layer between Terminal and Switch | IP |
| 2 | Q.921 – LAPD (Link Access Procedure on the D channel) | PPP HDLC |
| 1 | I.430/I.431 – ISDN physical-layer interface: • I.430 for the basic interface • I.431 for the primary interface | |

ISDN využíva vrstvy OSI modelu:
fyzickú, BRI a PRI sú definované v ITU-T I.430 a I.431
dátovú, špecifikovaná ITU-T Q.920, Q.921, Q.922, Q.923
sieťovú, je definovaná ITU-T Q.930, tiež známa ako I.450 a ITU-T Q.931, špecifikujú užívateľ – užívateľ, kruhovo a paketovo prepínané spojenie

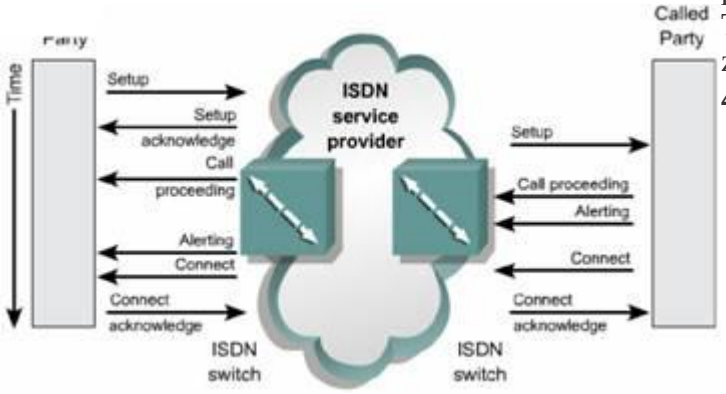
1

BRI služba je poskytovaná cez miestne medené vedenie, pri jednej fyzickej ceste sú tu 3 separátne informačné cesty. Informácie pre 3 kanály je multiplexovaná na jednu fyzickú cestu. Delenie rámcov na fyzickej vrstve:
- prichádzajúce, sú posielané zo siete na terminál, majú NT rámcový formát.
- odchádzajúce, sú posielané z terminálu do siete, majú TE formát

Rámec obsahuje:
8 bity z B1 kanálu
8 bity z B2 kanálu
4 bity z D kanálu
6 bitov prídavných
ISDN rámec obsahuje 48 bitov. 4000 je ich prenesených za sekundu. Každý kanál má kapacitu 2*(8*4000) = **64 kbps**. D kanál má kapacitu 4*4000 = **16 kbps**. Dohromady je **144 kbps**, ale celkovo sa prenáša **192 kbps**. Ostatné sú použité ako prídavné. Využitie prídavných bitov:
*rámcový bit*, poskytujú synchronizáciu
*bit pre rozdelenie výkonu*
*Echo D kanálového bitu*, používaný pri riešení kolízie, ak niekoľko zariadení súťaží o kanál
*aktivačný bit*, aktivuje zariadenie
*Spare bit*, nepoužitý




PAPD – signalizačná 2 vrstva na ISDN kanále, používaný cez D kanál na overenie a kontrolu, že informácia je prijatá správne. Adresné pole je 2 bajty dlhé
SAPI – LDAP brána pre služby 3. vrstvy
C/R – indikuje, čí rámec obsahuje príkazy alebo odpoveď.
TEI – jedinečný identifikátor zákazníckeho zariadenia



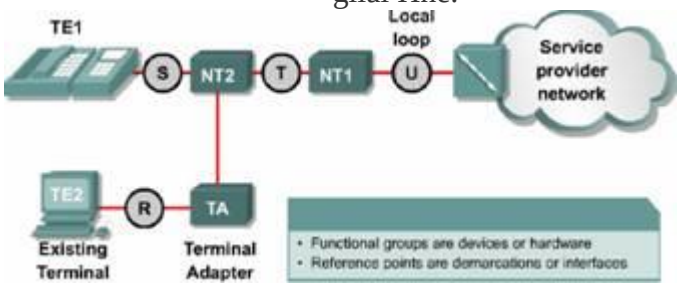

### 4.1.4. Funkcie ISDN

2
Na zabezpečenia ISDN hovoru je využitý D kanál medzi routrom a ISDN prepínačom, kanál je vždy up. D kanál je používaný pre *kontrolné volacie funkcie* ako nadviazanie *spojenia, signalizovanie a ukončenie*. Tieto funkcie sú implementované v protokole **Q.931**.
Q931 pracuje na 3. vrstve OSI modelu.
Sekvencia udalostí počas zabezpečenia BRI alebo PRI hovoru:
D kanál je použitý na poslanie volaného čísla na ISDN prepínač
lokálny prepínač využije SS7 signálny protokol na nastavenie cesty a prejdenie na volaného čísla na vzdialený ISDN prepínač
vzdialený prepínač spojí cieľ cez D kanál
vzdialený ISDN zariadenie pošle vzdialenému ISDN prepínaču *call-connect message*
vzdialený ISDN prepínač využije SS7 na poslanie *call-connect message* na lokálny prepínač lokálny ISDN prepínač pripojí jeden B kanál bod – bod, druhý kanál ponechá pre nový hovor alebo dátový prenos

### 5.1.4. Referenčné body

| Device | Device Type | Device Function |
|---|---|---|
| TE1 | **Terminál Equipmenl 1** | Design g les *3* device wllh a nallve ISDN inlerface, šuch as an ISDN router or ISDN Lelephone. |
| TE2 | Terminál Equipment 2 | Designates a noci-ISDN device, šuch as a workstalion or router, thal requires a TA to connect to a n ISDN service provider. |
| TA | Terminál Ad a pier | Converts EIA/TIA-232, V.35, and othersignals inloERI signals. |
| NT2 | Nelwortí Termiration *2* | The point at which all ISDN Unes at a custoroer site are aggregated and switched using a cuslomer swit- |

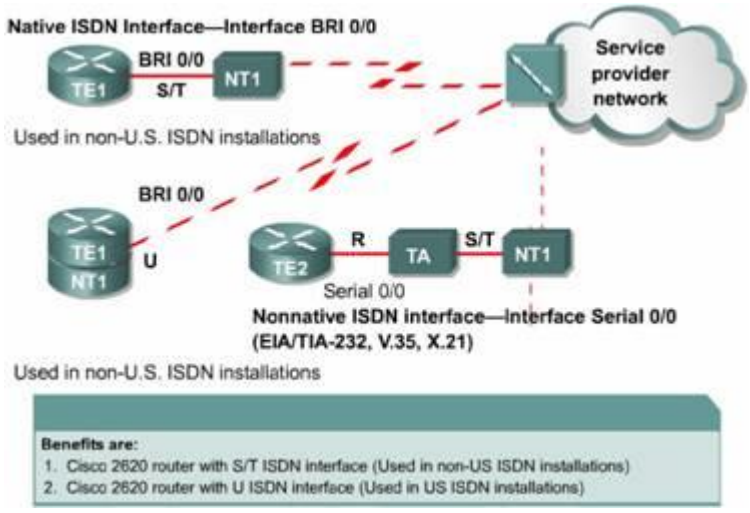
| | | |
|---|---|---|
| | | ching device. |
| NT1 | Networtí Termi-nation 1 | Controls the physical and electrical termination of the ISDN al the cjstomeŕs premi-ses. Converts the four-wire BRI signals into Iwo-wire signals u$ed by the ISDN di-gilal Hne. |




ISDN špecifikácia definuje 4 referenčné body, ktoré pripájajú jedno ISDN zariadenie na druhé. Každé ISDN zariadenie na ceste vykonáva špecifickú otázku na umožnenie bod – bod spojenia.

Referenčné body: rozhrania medzi dvoma zariadeniami. Rozdelenie referenčných bodov:
**R**, odporučenie na prepojenie medzi nekompatibilným ISDN zariadením *Terminal Equipment type 2* (**TE2**) a *Terminal Adapter* (**TA**), napr. RS232 sériové rozhranie
**S**, odporučenie na body, ktoré pripájame na zákaznícke prepínacie zariadenie *Network Termination type 2* (**NT2**) a umožňuje volanie medzi rôznymi typmi zákazníckych zariadení
**T**, elektricky zhodné s S rozhraním, odkazuje sa na odchádzajúce spojenie z NT2 na ISDN sieť alebo *Network Termination type 1* (NT1).
- **U**, odkazuje sa na prepojenie medzi NT1 a ISDN sieťou cez telefónnu spoločnosť

Pretože S a T rozhrania sú elektricky podobné, niektoré rozhrania sú označované ako S/T.




### 4.1.5. Určenie rozhrania pre ISDN router

spojených štátoch NT1 poskytuje zákazník.
Európe a iných krajinách NT1 poskytujú telefónne spoločnosti a predstavujú S/T zariadenie pre zákazní-ka. Zariadenie ako router s ISDN modulom musí mať preto správne rozhranie. Výber CISCO routra so správnym rozhraním:
Určiť, či router podporuje ISDN BRI.
Určiť poskytovateľa NT1.
Ak NT1 je zabudované v CPE, router by mal U rozhranie.
Ak router má S/T rozhranie, potom budeme potrebovať externé NT1.
Ak router má rozhranie označené ako BRI, potom je už ISDN povolené, pri zabudovanom ISDN rozhra-

ní, router je TE1 a bude potrebovať pripojenie na NT1. Ak router má U rozhranie, už má zabudované NT1.

| Country | Switch Type |
|---|---|
| United States and Canada | AT&T 5ESS and 4ESS; Northern Telecom DMS-100 |
| France | VN2, VN3 |
| Japan | NTT |
| United Kingdom | Net3 and Net5 |
| Europe | Net3 |

### 4.1.6. ISDN prepínacie typy

Routre musia byť nakonfigurované na typ prepínača, s ktorým budú komunikovať. Treba vedieť, aký typ prepínania využíva servisný provajder, to je nevyhnutné na



určenie *service profile identifiers* (**SPIDs**). SPIDs umožňuje viacerým zariadeniam zdieľať tú istú linku, sú používané len v Severnej Amerike a Japonsku.

### 4.2.1. Konfigurovania ISDN BRI

**isdn switch-type** *switch-type* – zadáva sa v globálnom konfiguračnom móde, alebo v móde rozhrania na určenie ISDN prepínača poskytovateľa. Pri GKM sa nastavenia uplatnia na všetkých ISDN rozhraniach.
Po nainštalovaní ISDN služby vydá poskytovateľ informácie o type prepínača a SPIDs.
**SPIDs** sú využívané na definovanie dostupných služieb pre jednotlivých ISDN účastníkov.
**isdn spid1** a **isdn spid2** slúžia na špecifikovanie SPID, je potrebný pre sieť pri inicializovaní volania
**isdn switch-type none** – zakázanie prepínača na ISDN rozhraní
Konfigurovanie ISDN BRI:
v GKM: Router(config)#**isdn switch-type** *switch-type, switch-type* indikuje typ prepínača poskytovateľa.
Príklad: Router(config)#**isdn switch-type basic-ni**
v konfiguračnom móde rozhrania definujem SPID číslo pridelené B kanálu: **isdn spid#**, príklad: Router(config-if)#**isdn spid1** spid-number [ldn ], kde *ldn* definuje lokálne telefónne číslo

Cisco

```
isdn switch-type basic-ni
!
<Output Omitted>
!
interface BRI0/0
 isdn switch-type basic-ni
 isdn spid1 51055540000001 5554000
 isdn spid2 51055540010001 5554001
!
```

**interface bri** – vstup do konfiguračného módu rozhrania

### 4.2.2. Konfigurovanie ISDN PRI

ISDB PRI sú dodávané cez prenajatú T1 alebo E1 linku. Konfiguračné otázky:
určiť správny typ PRI prepínača
špecifikovať T1/E1 kontrolér, typ rámcovania a kódovanie linky pre zariadenie ISDN poskytovateľa
- nastaviť PRI skupine časový slot pre T1/E1 zariadenie a uviesť použitú rýchlosť

**interface serial** - ISDN PRI D a PRI B kanály sa konfigurujú oddelene v móde rozhrania
**isdn switch-type** – špecifikuje ISDN prepínač, použitý poskytovateľom, na ktorý sa PRI pripája, môže

byť použitý v GKM alebo v konfiguračnom móde rozhrania.
Tabuľka typov prepínačov pre ISDN PRI konfiguráciu:
Príklad: Router(config)**#isdn switch-type primary-net5**

| Switch Type | Description |
|---|---|
| primary-5ess | AT&T basic rate swittiies (USA} |
| primary-dmsICO | Norttiem Telecom DMS-100 (North America) |
| primary-ni | Natieral ISDN {North America] |
| príma ry-net5 | Switch type fór Net5 in United Kingdom, Európe, and Austrália |
| primary-ntt | NTT ISDN switch (Japan) |

Konfigurovanie T1 alebo E1 kontroléra: 1.1. V GKM špecifikujeme kontrolér a slot/port v routri, kde je PRI karta umiestnená:
Router(config)#**controller** {**t1** | **e1**} {*slot*/*port*}
Router(config-controller)#



**T1 Sample Configuration**

```
Router(config)#controller t1 1/0
Router(config-controller)#framing esf
Router(config-controller)#linecode b8zs
Router(config-controller)#pri-group timeslots 1-24

Router(config-controller)#interface serial3/0:23
Router(config-if)#isdn switch-type primary-5ess
Router(config-if)#no cdp enable
```

**E1 Sample Configuration**

```
Router(config)#controller e1 1/0
Router(config-controller)#framing crc4
Router(config-controller)#linecode hdb3
Router(config-controller)#pri-group timeslots 1-31

Router(config-controller)#interface serial3/0:15
Router(config-if)#isdn switch-type primary-net5
Router(config-if)#no cdp enable
```

### 4.2.3. Overovanie ISDN konfigurácie

Konfigurovanie rámcov, konfigurácia linky a časovanie **framing** – na výber rámcového typu použitého PRI poskytovateľom Príklad pre T1: Router(config-controller)#**framing** {**sf** | **esf**} Príklad pre E1: Router(config-controller)#**framing** {**crc4** | **no-crc4**} [australia] **linecode** – na identifikovanie signálnej metódy na fyzickej vrstve od poskytovateľa Príklad: Router(config-controller)#**linecode** {**ami** | **b8zs**| **hdb3**} Pre **Severnú Ameriku** na T1 je použitá *B8ZS*, pre **Európu** *HDB3*.
Konfigurovať špecifické rozhranie pre PRI a počet pridelených timeslotov Príklad: Router(config-controller)#**pri-group** [**timeslots** range] Pre T1 sú timeslot 1 – 24, pre E1 1 – 31
Špecifikovať rozhranie pre PRI D kanál, je to sériové rozhranie na T1/E1 routri Príklad: Router(config)#**interface serial**{slot/port: | unit:}{**23** | **15**} V Cisco zariadeniach sa začína číslovať od 0, preto *interface serial 0/0:23* Subrozhrania sú oddeľované bodkou: *0/0.16* Označenie pre kanály: *S0/0:23*

Na overenie správnej ISDN konfigurácie sa používa niekoľko **show** príkazov.
**show isdn status** – zobrazí BRI operácie na rozhraniach. Používa sa po konfigurácii, či komunikuje správne s ISDN prepínačom. Treba overiť:
- Layer 1 Status: je ACTIVE
- Layer 2 Status: je v stave MULTIPLE_FRAME_ESTABLISHED

**show isdn active –** zobrazí aktuálne volacie informácie, obsahuje:
volané číslo
čas až do odpojenia
Advice of charge (AOC)
zaťaženie použitých jednotiek počas volania
- či informácia o AOC je poskytnutá počas hovoru alebo na konci volania

**show dialer** – zobrazí informáciu o vytočenom rozhraní:
stav aktuálneho volania
hodnotu časovača Dialup

dôvod vytočenia
- vzdialené pripojené zariadenie

**show interface bri0/0** – zobrazí štatistiku pre rozhranie BRI
- **show interface bri0/0:1** – špecifické informácie o kanály

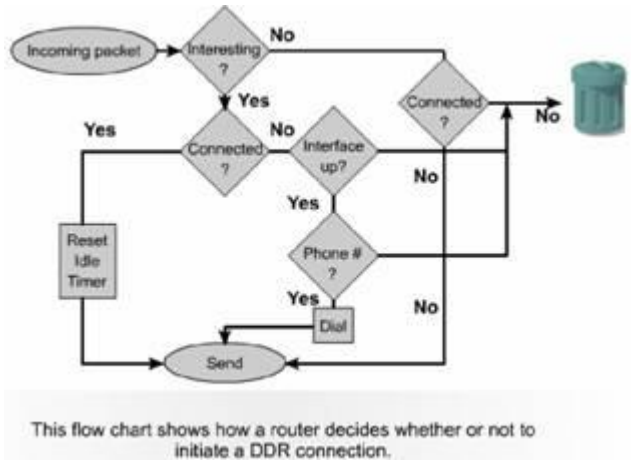
### 4.2.4. Riešenie problémov v ISDN konfigurácii

Na riešenie problémov sa používajú debugovacie príkazy:
**debug isdn q921** – zobrazuje dáta na 2 (linkovej) vrstve na D kanále medzi ISDN prepínačom a routrom, využíva sa ak LAYER nie je v stave ACTIVE
**debug isdn q931** – zobrazí výmenu pri nadväzovaní spojenia, zobrazuje dáta na 3 (sieťovej) vrstve
**debug ppp authentication** – zobrazí správy PPP autentifikačného protokolu, obsahujúce PAP alebo CHAP pakety
**debug ppp negotiation** - zobrazí informácie o PPP pri dojednávaní, obsahujú LCP, autentifikáciu a NCP výmenu



- **debug ppp error** – zobrazí chybový protokol a chybovú štatistiku spojenú s PPP **4.3.1. Funkcia DDR**

*Dial-on-demand routing* (**DDR**) {vytočené na žiadosť smerovania} rozhranie je vytočené, keď sú splnené preddefinované pravidlá. Doprava je označená za zaujímavú, pri takomto stave je ukončený hovor.
**dialer-list** – na nadefinovanie zaujímavej dopravy, podľa tohto listu môže všetka doprava so špecifickým protokolom vytočiť DDR linku, alebo podľa definovaného access listu určiť, či pre danú komunikáciu bude linka vytočená. Pokiaľ je linka vytočená, môže byť dokonca prenášaná aj doprava, ktorá nevyhovuje AC.
Realizácia DDR v Cisco smerovačoch:



This flow chart shows how a router decides whether or not to initiate a DDR connection.

smerovač prijme dopravu, porovná so smerovacími tabuľkami či nastane smerovanie a určí odchádzajúce rozhranie
ak je rozhranie nakonfigurované pre DDR určí, či je doprava zaujímavá
router identifikuje volanú informáciu nevyhnutnú na vytvorenie hovoru použitím volacej mapy k ďalšiemu hopu smerovania
Router skontroluje, či sa používa vytáčaná mapa. Ak už existuje spojenie do cieľa, doprava je poslaná. Ak rozhranie ešte nie je vytočené, pošle požiadavku na spojenie cez D kanál
Po zapnutej linke sa prenáša zaujímavá aj nezaujímavá doprava
Linka je vytočená, pokiaľ neuplynie časovač nečinnosti pre zaujímavé dáta, nezaujímavé dáta neresetujú časovač.

### 4.3.2. Konfigurácia legacy DDR

*Legacy DDR* je termín používaný pre základnú konfiguráciu DDR, v ktorom vytáčacie parametre sú apli-

kované na rozhranie. Ak na jedno rozhranie bude použitých viacero jedinečných konfigurácií, bude potrebné použiť vytáčaňcí profil. Konfigurovanie DDR:
definovať statické smerovanie
určiť zaujímavú dopravu
nakonfigurovať vytáčacie informácie

### 4.3.3. Definovanie statického smerovanie pre DDR

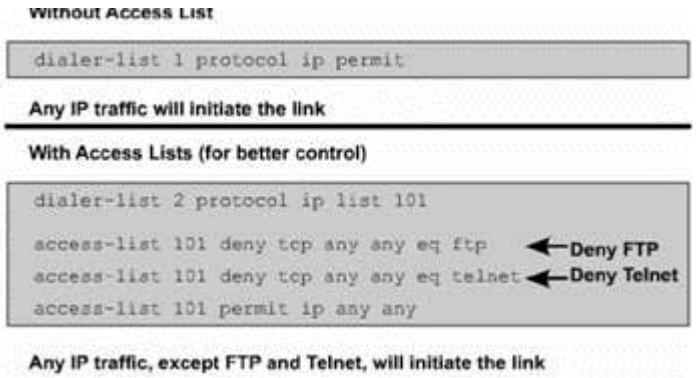
Na presun dopravy router potrebuje vedieť aké smerovanie použije pre daný cieľ. Pri dynamickom smerovaní bude DDR rozhranie vytáčané pri každej smerovacej aktualizácii alebo hello správe, ak sú definované ako zaujímavé.
Ako **prevenciu** ne neustále sa vytáčanú alebo trvale vytočenú linku definujeme **statické** smerovanie.
Definovanie statického smerovania:
Router(config)#**ip route** *net-prefix mask {address | interface }* [distance ] [**permanent**]
Podmienky pre statické smerovanie:
*statické bude mať prednosť* pred dynamickým, pretože má menšiu administratívnu vzdialenosť
na limitovanie záznamov v smerovacej tabuľke sa definuje *default* statické smerovanie



### 4.3.4. Určenie zaujímavej dopravy pre DDR

DDR volania sú spúšťané pre zaujímavú dopravu. Je definovaná:
IP dopravou príslušného typu protokolu
paketami s určitou zdrojovou alebo cieľovou adresou
- inými kritériami definovanými administrátorom

**dialer-list** – príkaz pre zaujímavú dopravu. Syntax:
Router(config)#**dialer-list** dialer-group-num **protocol** *protocol-name {permit | deny |* **list** *access-list-number } dialer-group-num* – je číslo od 1 – 10, identifikuje vytáčací list na smerovači




**dialer-list 1 protocol ip permit** – umožní všetkej doprave vytočiť linku. Miesto povolenia všetkej dopravy je lepšie určiť v **AL**, ktorá doprava vyvolá vytočenie linky. V 2. vytáčacom list je zabránené FTP a Telnetu vytočiť linku.

### 4.3.5. Konfigurovanie DDR vytáčacích informácií

Pri ISDN rozhraniach Cisco je používané HDLC zapuzdrenie, ale veľa sieťových služieb využíva PPP zapuzdrenie, preto pre B kanál je používané PPP zapuzdrenie. Konfigurovanie PPP na DDR rozhraní:
Home(config)#**username Centrál password cisco**
Home(config)#**interface briO/0**
Home(config-if)#**encapsulation ppp**
Home(config-if)#**ppp authentication chap**
Home(config-if)#**ip address 10.1.0.1 255.255.255.0**

Treba spojiť vytáčací list určujúci zaujímavú dopravu pre DDR z daným rozhraním:
**dialer-group** *group-number,* kde *group-number* - špecifikuje vytáčanú skupinu od 1 - 10. Toto číslo musí sedieť s **dialer-list** *group-number.* Pre každé rozhranie sa definuje len jedna vytáčacia skupina, ale rovnaký vytáčací list môže byť priradený viacerým rozhraniam.
Príklad: Home(config-if)#**dialer-group 1**
**dialer map** - vytáčacie informácie pre špecifikujúce pre DDR rozhranie, je zadávaný protokol, adresa a telefónne číslo.
syntax: Router(config-if)#**dialer map** *protocol next-hop-address* [**name** *hostname* ] [**speed 56** | **64**] [**broadcast**] *dial-string*
**dialer idle-timeout** *seconds* - určuje počet sekúnd do odpojenia od poslania posledného zaujímavého

10.1.0.1 .^-^
***Y*** **5551000**


**10! 0 -, _____ _____ 101 0 2** paketu, prednastavené je

**Subnets**
101000
10.20.0.0
**Subnet** <~ ^JlA **Subnets** 12*0.*
10.400.0
**brlO 5552000**

useiname Centrál pňsswcrd cisco interface ERIO
ÍP adldress 10.1.0.1 255,255.255.0

**f**
encap-sulation ppp
dialer idle-timeout 160
dialer inap ip 10.1,0,2 fiame Centrál 5552000
dialer-group 1 A
*no* feir-queue *_____
ppp autllenticätton ch^p

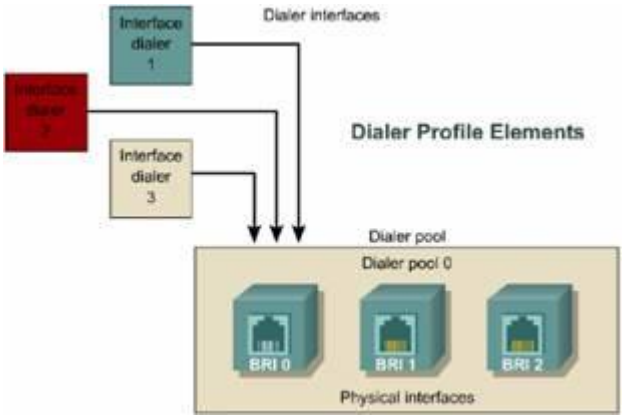
**Remote host name ' Used for PPP CHAP**
**------ Number to dial**
Remote **IP address**

Tne name parameter in the **dialer map** command enables tľie router to track ISDN calls by the hostname **or** the remote router.

### 4.3.6. Vytáčacie profily

Dynamické profily umožňujú fyzickým rozhraniam dynamicky prideľovať rôzne charakteristiky v závislosti od prichádzajúceho alebo odchádzajúceho volania. Volacie profily umožňujú:
definovať zapuzdrenie a prístupové kontrolné listy
určiť minimálny a maximálny počet hovorov
- vzťahy zapínať a vypínať

Oddeľujú logické porty DDR od fyzických rozhraní
Požiadavky pre vytáčané profily:




nakonfigurovať ISDN B kanály s rôznou IP adresou
použiť rôzne zapuzdrenie na ISDN B kanáloch
nastaviť rôzne DDR parametre pre B kanály ISDN rozhrania
- eliminovať plytvanie ISDN B kanálmi

Vytáčaný profil pozostáva z nasledujúcich prvkov:
**Dialer interface** - logická jednotka vytáčaného profilu
**Dialer pool** – jedno alebo viacero rozhraní združených vo vytáčacom profile
**Physical interfaces** – na fyzickom rozhraní sa konfiguruje PPP autentifikácia, typ zapuzdrenia a PPP multilink
Vytáčané profily sú aktívne, keď zaujímavá doprava bude posielaná na DDR rozhranie. Postup:
zaujímavý paket je smerovaný na vzdialenú DDR IP adresu
router skontroluje konfigurované vytáčané rozhranie, ktoré zdieľa rovnakú podsieť, ako vzdialená DDR adresa. Ak existuje, router nájde fyzické DDR rozhranie vo vytáčanom poli.
konfigurácia z konfiguračného poľa je aplikovaná na rozhranie a router sa pokúsi vytvoriť spojenie
po ukončení spojenia je rozhranie vrátené vytáčanému poľu pre nasledujúce volanie

### 4.3.7. Konfigurovanie vytáčaných profilov

**interface dialer** – vytvorí dialer rozhranie a vstúpi do konfiguračného módu rozhrania Požiadavky pri konfigurovaní rozhrania:
1. Nakonfigurovať jedno alebo viac vytáčaných rozhraní
IP adresa
typ zapuzdrenia a autentifikácia
časovač nečinnosti
vytáčaná skupina pre zaujímavú dopravu
Nakonfigurovať **dialer string** a **dialer remote-name,** meno vzdialeného routra a telefónne číslo na vytáčanie. **dialer pool** – spojiť toto logické rozhranie s poľom fyzických rozhraní
Konfigurovať fyzické rozhranie. **dialer pool-member** – asociovanie fyzického rozhrania s vytáčaným poľom.
**dialer pool-member** – asociácia rozhrania s viacnásobným poľom, ak existuje viac než jedno



rozhranie v poli, je možné prideľovať prioritu cez voľbu

Kombináciou rozhraní môže byť použitá s vytáčanými poľami:

| | |
|---|---|
| Synchronous Serial | - BRI |
| Asynchronous Serial | - PRI |

### 4.3.8. Overovanie DDR konfigurácie

**show dialer interface [BRI]** – zobrazí informácie o štatistike DDR prichádzajúcich a odchádzajúcich hovorov.

**show isdn active** – zobrazí informácie o aktuálnom ISDN hovore

**show isdn status** – zobrazí informácie o 3 vrstvách na BRI rozhraní, výstup obsahuje:

ISDN Layer 1 is active

ISDN Layer 2 is established with SPID1 and SPID2 validated

aktívne spojenie na 3 vrstve

### 4.3.9. Riešenie problémov v DDR konfigurácii

Problémy:

- nevytáča, keď by mal
- neustále vytáča

Správy od **dubug isdn q921**:

0x05, indikuje správu pre nadviazania spojenia
0x02, indikuje správy vykonávania spojenia
0x07, indikuje správu pre spojenie

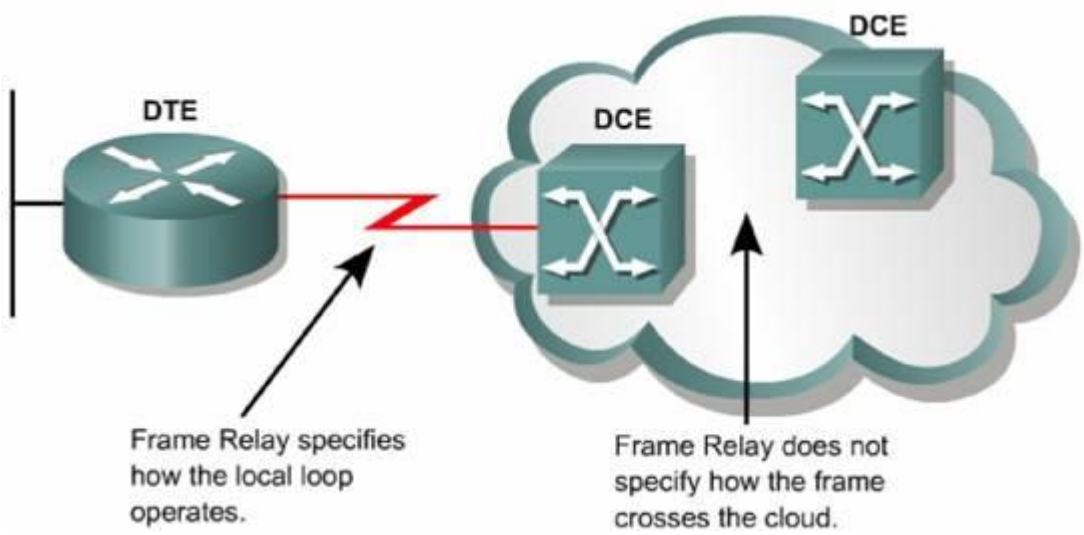
- 0x0F, správa pre potvrdenie spojenia ack

**debug isdn q931** - zobrazuje správy počas nadviazania spojenia
**debug dialer events** – zobrazuje, keď DDR linka sa pripojí, pri zlej konfigurácii nie sú vypisované žiadne správy
**debug dialer packet** – poslané hlásenie na konzolu, keď paket opustí DDR rozhranie **isdn call interface** – príkaz na donútenie lokálneho routra vytočiť vzdialený router **clear interface bri** – reštartne rozhranie s ISDN prepínačom. Router si musí opäť dohodnúť jeho SPIDs s ISDN prepínačom.

Frame Relay

### 5.1.1. Úvod do Frame Relay

Frame relay je štandard pre *Telecommunication Union Telecommunications Standardization Sector* (**ITU-T**) a *American National Standards Institute* (**ANSI**). Je paketovo prepínaná , spojito orientovaná WAN služba. Pracuje na 2. vrstve OSI modelu, využíva HDLC. Dáta sú nesené medzi užívateľským zariadením DTE a DCE na okraji WAN.
Pôvodne bol určený pre sprístupnenie ISDN zariadeniam prístup na paketové prepínanie služby na B kanáloch, ale nebol štandardizovaný.
Je často používané na prepojenie LAN.




### 5.1.2. Terminológia vo Frame Relay

(**VC**) *virtual circuit* – spojenie medzi dvoma DTE.
(**SVCs**) *switched virtual circuits* – VC vytvorený dynamicky, poslaním signálnej správy na sieť, menej používaný, viac sú používané PVCs.
Technológia Frame Relay bola navrhnutá pre digitálne linky, nemá zabudovaný opravný mechanizmus, ak je nájdená chyba v rámci, je zahodený bez oznámenia.
Frame Relay access device (FRAD) alebo router pripojený na Frame Relay môže mať viaceré virtuálne okruhy pripojené na rôzne koncové body, je to náhrada za mesh.
Viacej virtuálnych okruhov na samostatnej prístupovej linke sa od seba rozoznáva podľa vlastného

identifikátora *Data Link Channel Identifier* (**DLCI**), má len lokálny význam a môžu byť rôzne na každom konci VC.


### 5.1.3. Frame Relay stack layered support

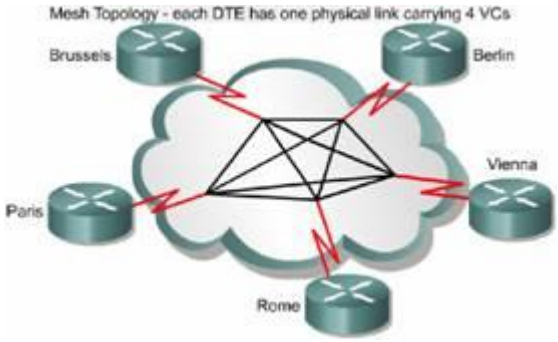
Funkcie Frame Relay:
berú dátové pakety zo sieťovej vrstvy, IP alebo IPX
zapuzdrujú ich ako časti Frame Relay rámcov
prechádzajú na fyzickú vrstvy na doručenie po drôte
Fyzická vrstva je typicky EIA/TIA-232, 449, 530, V.35 alebo X.21.
Frame Relay je podmnožina HRLC rámcového typu. Je využívaný 1-bajt pre vlajku 01111110. *Frame Check Sequence* (FCS) je používaná na určenie chýb na 2. vrstve adresného poľa počas prenosu, pri nastaní chyby nie je realizovaná notifikácia zdroju, kontrola chýb je realizovaná vyššou vrstvou OSI modelu.

1

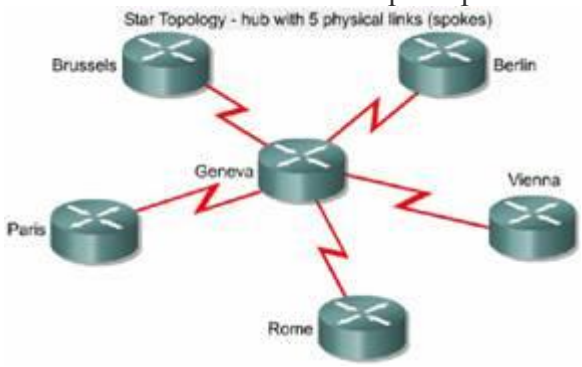
### 5.1.4. Kontrola prúdu a šírky pásma vo Frame Relay

Sériová linka alebo prístupová linka do Frame Relay siete je normálne prenajatá linka. Rýchlosť linky je prístupová rýchlosť alebo portová rýchlosť. Rýchlosť sa typicky pohybuje od 64kbps do 4Mbps, niektorí poskytovatelia až do 45Mbps.
(**CIR**) *committed information rate* – dohodnutá rýchlosť medzi jednotlivými VC na jednej linke. Jednotlivé CIR sú normálne menšie, než portová rýchlosť. Ale súčet CIR býva normálne vyšší než portová rýchlosť. Pri posielaní rámcov býva medzera medzi VC.
(**EIR**) *Excess Information Rate* – rozdiel medzi maximálnou rýchlosťou linky a CIR.
Zariadenie môže posielať pakety na prepínač aj vyššou ako dohodnutou rýchlosťou, ak prepínač má dostatok voľných prostriedkov. Dáta posielané nad dohodnutú rýchlosť budú označené v *Discard Eligible* (**DE**) bite na 1.
Keď pakety stoja vo fronte, je to príznak neúmerného množstva posielaných dát na prepínač, tento stav spôsobuje oneskorenie a pád sieťového výstupu. Na zamedzenie tohto stavu, prepínače s Frame Relay budú z fronty zahadzovať pakety z označenými DE bitmi.
DTE zariadenie bude informované o probléme nastavením *Explicit Congestion Notification* (**ECN**) v rámci adresného poľa.
*Forward ECN* (**FECN**) bit je nastavený na každom rámci, ktorý prepínač príjme na preťaženej linke
*Backward ECN* (**BECN**) bit je nastavený na každom rámci, ktorý prepínač umiestni na preťaženú linku.
DTE zariadenie príma rámce s nastaveným ECN bitom a pokúša sa zredukovať prúd rámcov, kým ECN nie je nulové.

### 5.1.5. Mapovanie adries a topológia vo Frame Relay




Frame Relay je cenovo výhodnejšie pri prepojení viacerých strán, ako pri point-to-point spojení. WAN sú často prepojené do hviezdicovej topológie, kde centrála je v strede a ostatní hosti pristupujú na jej služby cez samostatné VC. HUB má prístupovú linku s viacerými VC.




Z hviezdicovej topológie je možné vyrobiť plnú mesh topológiu pomocou ďalších VC na existujúcej linke. Viacnásobné VC vedú k lepšiemu využitiu Frame Relay cez statické smerovanie.
Vo Frame Relay, kde jedno rozhranie je použité na prepojenie viacerých sietí sa používa nonbroadcast multiaccess (NBMA). Na prevenciu smerovacích slučiek je zavedený split horizon, neposielajú sa smerovacie aktualizácie na rozhranie, z ktorého prišli, čo môže však viesť k problému pri viacerých PVC. Riešením je mapovanie medzi adresou linkovej vrstvy Frame Relay každého FRAD alebo routra a sieťovou adresou ako IP. Router potrebuje vedieť, že routre sú dosiahnuteľné za jednotlivými rozhraniami.
DLCI pre každý VC musia byť asociované so sieťovou adresou z jeho vzdialeného routra, môže byť zadávaná manuálne prostredníctvom príkazu **map** alebo automaticky použitím *Inverse ARP*.

### 5.1.6. Frame Relay LMI

FR bolo navrhnuté na poskytovanie paketovo prepínaných dátových prenosov z minimálnym oneskorením.
*Local Management Interface* (**LMI**) – dynamické získavanie informácií o stave siete pre DTE.

2

Identifikáciu VC umožňuje 10 bitov v DLCI poli, rozsah je od 0 -1023, tieto identifikátory sú zahrnuté v LMI službách.

| **VC Identifiers** | **VC Non-data DLCIsI Ty pes** |
|---|---|
| 0 | LMI(ANSI, ITU) |
| 1..15 | Reserved lor future use |
| 992.1007 | CLLM |
| **1008.. 1022** | Reserved for future use (ANSI, ITU) |
| 1019.1022 | Multicasting (Cisco) |
| 1023 | **LMI** (Cisco) |

LMI rozšírenie obsahuje nasledujúce:

mechanizmus *keepalive*, overuje, či VC je otvorený
*multicast* mechanizmus
kontrolu prúdu
poskytovať DLCI hodnoty
- mechanizmus stavu VC

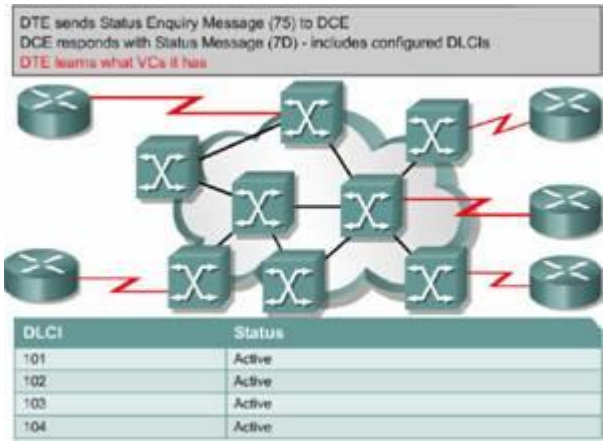
Typy LMI podporované pre CISCO:
***Cisco***, originálne Cisco rozšírenie
***Ansi***, zodpovedajúci ANSI štandardu T1.617 Annex D
- ***q933a***, zodpovedajúci štandardu Q933 Annex A

Po LMI hlavičke nasleduje 1 alebo viac informačných prvkov.
Každý informačný prvok *information elements* (**IE**) pozostáva :
1 bajt pre identifikátor
IE dĺžka poľa
- 1 alebo viac bajtov obsahujúcich stav DLCI

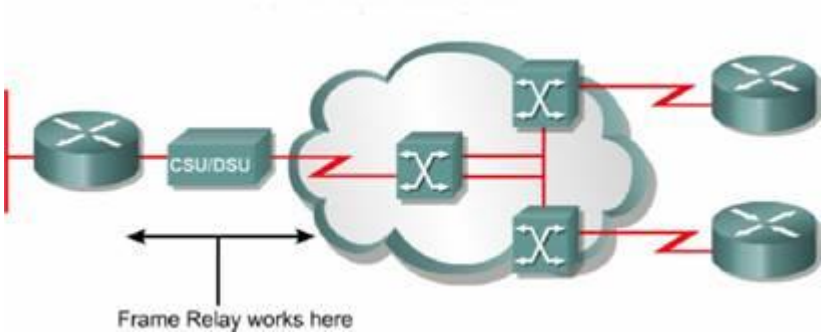
Stavové správy pomáhajú overovať integritu logickej a fyzickej linky.

### 5.1.7. Postup inverzného ARP a LMI operácií

LMI stavové správy kombinované s inverznými ARP správami umožňujú routrom priraďovať adresy sieťovej vrstvy k adresám linkovej vrstvy.




Keď pripojený router štartuje vo Frame Relay sieti, pošle LMI stavovú prieskumnú správu na sieť. Sieť odpovie s LMI stavovou správou, ktorá obsahuje detaily o všetkých VC konfigurovaných na prístupovej linke.
Router periodicky opakuje stavové otázky, ale odpovede obsahujú len zmeny. Po nastavenom počte skrátených správ sa vyšle plná správa.
Ak router potrebuje mapovať VC na adresy sieťovej vrstvy, pošle inverznú ARP správu na každý VC.
Inverzná ARP odpoveď umožňuje routru vytvárať nevyhnutné mapovacie záznamy jeho adries do DLCI mapovacej tabuľky.



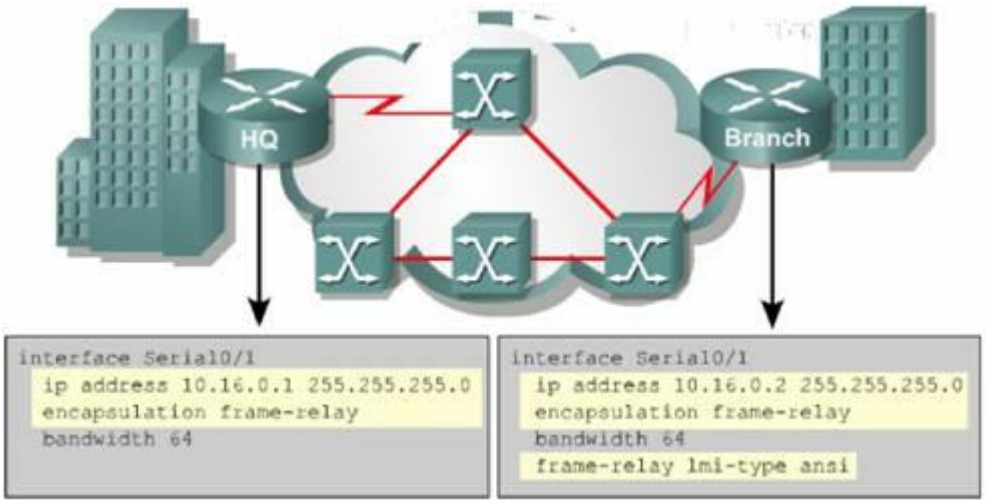

### 5.2.1. Základné konfigurovanie Frame Relay DCE or Frame Relay Switch

Frame Relay pracuje na sériovom rozhraní, prednastavené zapuzdrenie je HDLC.

3

**encapsulation frame-relay[cisco | ietf]** – príkaz na zmenu zapuzdrenia vo Frame Relay
**cisco**, využíva vlastné Cisco Frame Relay zapuzdrenie, využíva sa pri pripojení na iný Cisco router.
**ietf**, zapuzdrovacia metóda prispôsobená Engineering Task Force (IETF) standard RFC 1490, využitie pri pripojení na nie Cisco smerovač.
**ip address** – príkaz na nastavenie IP adresy rozhrania.
**bandwidth** – príkaz na nastavenie šírky pásma na rozhraní, udáva sa v kbps, musí byť nastavená pre správne určenie metriky pri *Gateway Routing Protocol* (IGRP), *Enhanced Interior Gateway Routing Protocol* (EIGRP) a *Open Shortest Path First* (OSPF).
**frame-relay lmi-type [ansi | cisco | q933a]** – nastavenie a konfigurovanie LMI spojenia, je potrebný

vo výstupe je aj informácia o type LMI. **IOS**
**11.2 Router ,^^ ^^ IOS 10.3 Router**
**show interfaces**

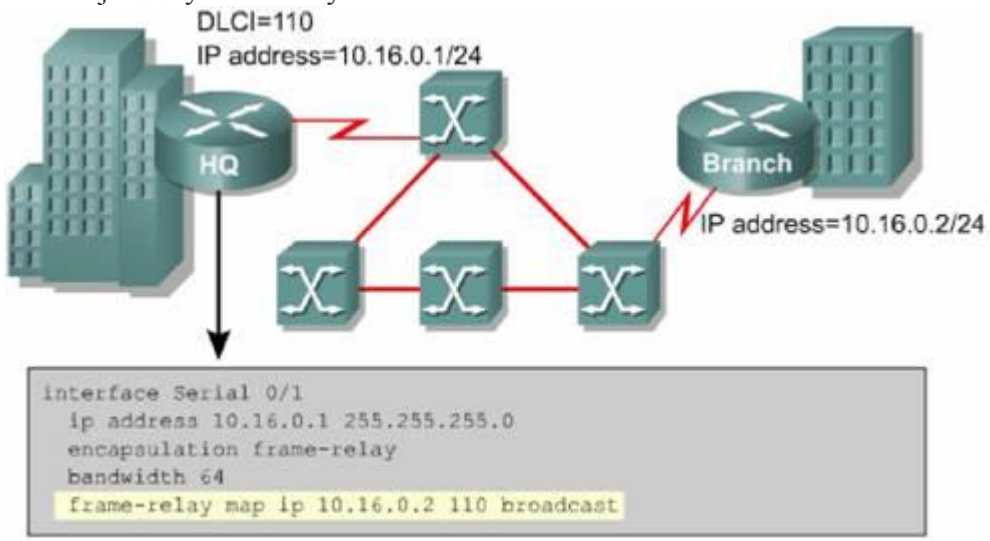



len pri IOS 11.2. alebo skorších. Pri novších nie je potrebné zadávať, prednastavené je Cisco.

### 5.2.2. Konfigurovanie statického mapovania Frame Relay

DLCI musí byť staticky mapované na sieťovú adresu vzdialeného hosta, keď vzdialený host nepodporuje inverzný ARP.
**frame-relay map** *protocol protocol-address dlci* [**broadcast**] – príkaz na statické mapovanie vzdialenej

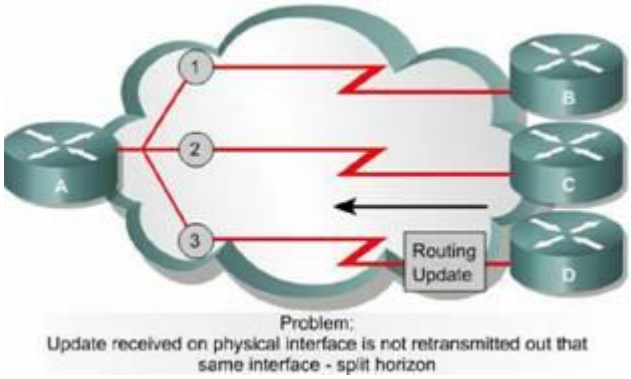
sieťovej adresy na lokálny DLCI.




4

### 5.2.3. Otázky spojené so smerovacími aktualizáciami na NBMA

Štandardne Frame Relay siete poskytujú *non-broadcast multi-access* (NBMA) spojenie medzi vzdialenými stranami. Fyzická topológia pozostáva z viacerých PVC.



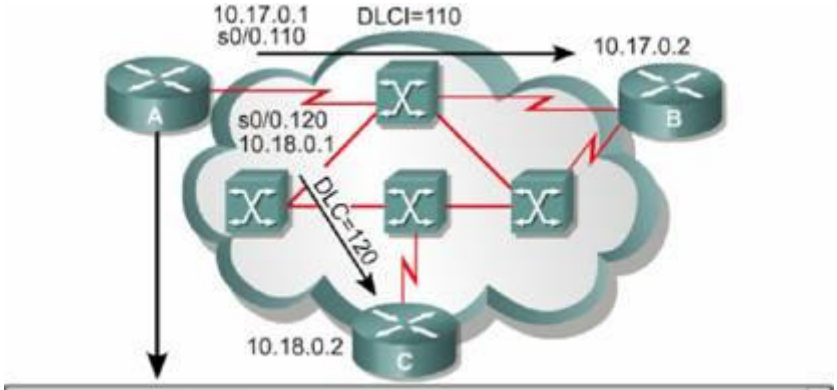

2 problémy vo Frame Relay topológii:
dosiahnuteľnosť vzhľadom na smerovacie aktualizácie
potreba replikovať broadcast na každý PVC, ak fyzické rozhranie obsahuje viac než 1 PVC, je to kvôli Split horizont.
Riešenie je využiť subrozhranie.

### 5.2.4. Subrozhrania vo Frame Relay

Na umožnenie broadcastových smerovacích aktualizácií vo hub-and-spoke Frame Relay topológii je potrebné nakonfigurovať logicky pridelené rozhrania. Týmto sa hovorí **subrozhrania**. **Subrozhranie** – logická časť fyzického rozhrania Frame Relay subrozhrania môžu byť konfigurované:
**Point-to-point,** samostatné bod - bod subrozhranie je použité na zabezpečenie jedného PVC spojenia na iné rozhranie alebo subrozhranie na vzdialenom routri. Subrozhranie má vlastné HLCI.
**Multipoint**, samostatné viacnásobné subrozhranie je použité na zabezpečenie viacnásobného PVC spojenia na viacnásobné fyzické rozhranie alebo subrozhranie na vzdialenom routri.
**encapsulation frame-relay** – príkaz je použitý na fyzické rozhranie, ostatné parametre sa zadávajú samostatne pre jednotlivé subrozhrania.

### 5.2.5. Konfigurovania subrozhrania pre Frame Relay

HLCI prideľuje poskytovateľ služby pre Frame Relay v rozsahu 16 – 992, vždy má len lokálny význam.



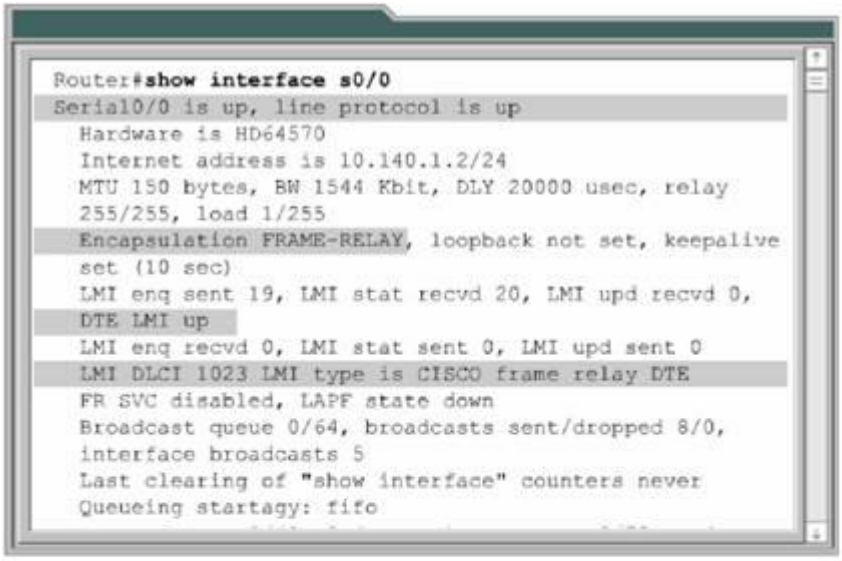

```
interface Serial0/0
  no ip address
  encapsulation frame-relay
  !
  interface Serial0/0.110 point-to-point
   ip address 10.17.0.1 255.255.255.0
   bandwidth 64
   frame-relay interface-dlci 110
  !
  interface Serial0/0.120 point-to-point
   ip address 10.18.0.1 255.255.255.0
   bandwidth 64
   frame-relay interface-dci 120
  !
```

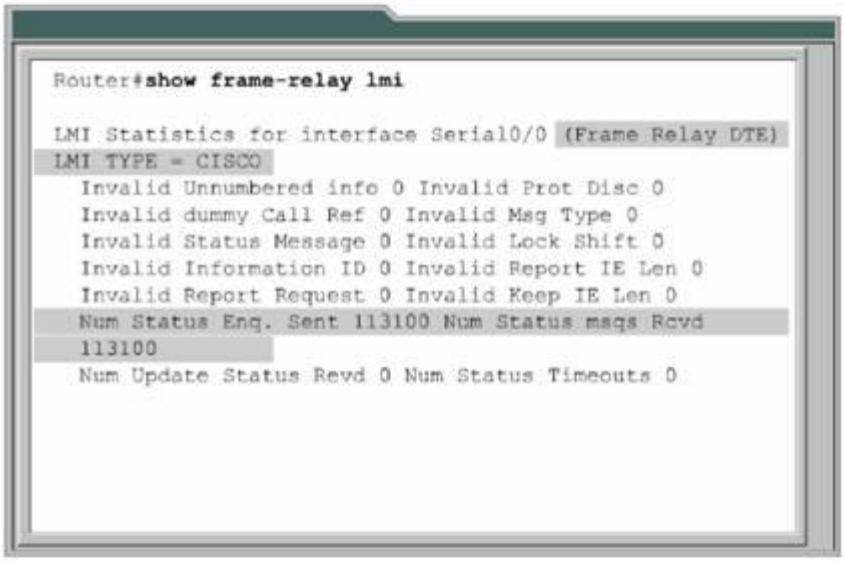
Router A má 2 bod – bod subrozhrania. s0/0.110 na router B s0/0.120 na router C Požiadavky na konfiguráciu subrozhrania na fyzickom rozhraní:
**encapsulation frame-relay**, nakonfigurovať zapuzdrenie
pre každý PVC vytvoriť subrozhranie

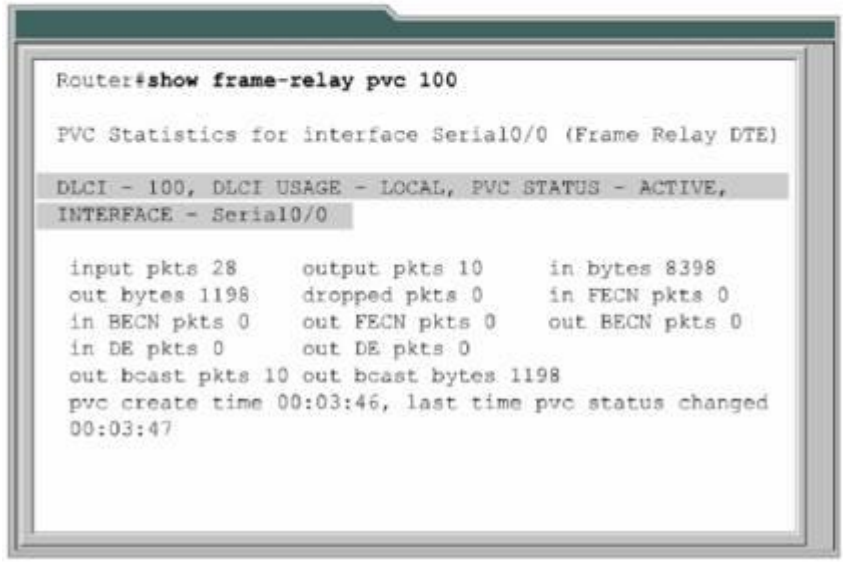


**interface serial** - na vytvorenie subrozhrania, treba určiť číslo portu a za (**.**) číslo subrozhrania. Pri konfigurácii sú vyžadované **multipoint** alebo **point-to-point** kľúčové slová. **frame-relay interface-dlci** – príkaz na konfigurovanie lokálneho DLCI na subrozhraní.

### 5.2.6. Overovanie konfigurácie Frame Relay



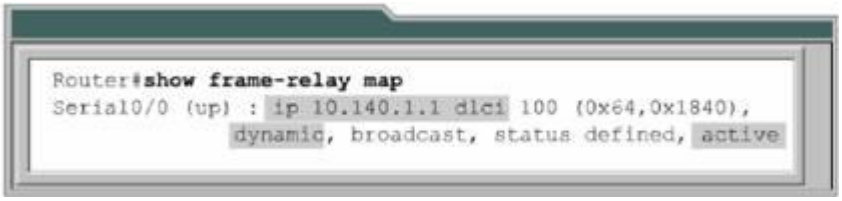

**show interfaces** – zobrazí informácie o zapuzdrení a stave 1. a 2. vrstvy, je zobrazený typ LMI, LMI DLCI, typ *Frame Relay data terminal equipment /data circuit-terminating equipment* (DTE/DCE).

**show frame-relay lmi**

zobrazí štatistiku LMI dopravy

**show frame-relay pvc [interface** *interface***] [dlci]** – zobrazí stav každého nakonfigurovaného PVC a štatistiku dopravy. Využívaný na overenie množstva BECN a FECN paketov. Stav PVC môže byť *aktívny, neaktívny* alebo *zmazaný*.

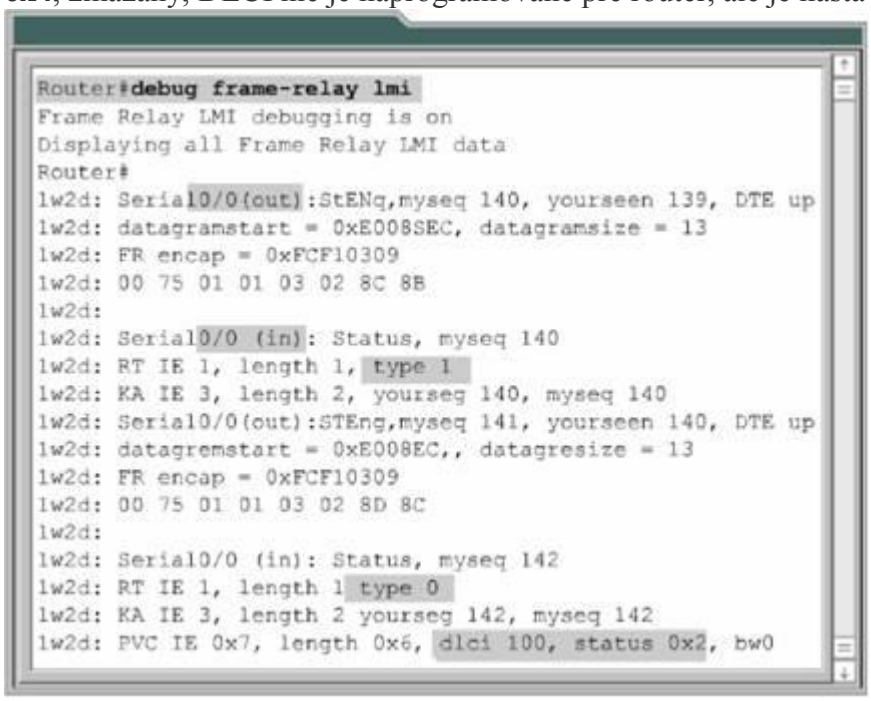
**show frame-relay map** – zobrazí aktuálne mapované záznamy a informácie o spojení.




10.140.1.1 – je IP adresa vzdialeného routra, naučená cez inverzné ARP 100 desiatkové DLCI číslo 0x64 – je hexa konverzia DLCI 0x64 = 100 decimal
0x1840 – hodnota, aká by bola na drôte
Broadcast/multicast – je povolený na PVC
aktívny stav PVC
**frame-relay-inarp** – príkaz na zmazanie Frame Relay mapy vytvorenej cez inverzný ARP

### 5.2.7. Riešenie problémov v konfigurácii Frame Relay

**debug frame-relay lmi** – príkaz na overenie, či router správne posiela a príma LMI pakety.
Plná LMI správa je *typu 0*. LMI výmena je *typy 1*.
dlci 100, status 0x2 – znamená, že stav DLCI 100 je aktívny.
Možné hodnoty pre status:
**0x0**, neaktívny, problém môže byť na druhom routri, PVC je dole
**0x2**, aktívny, všetko pracuje
**0x4**, zmazaný, DLCI nie je naprogramované pre router, ale je nastavené na niektorom konci.




Úvod do správy siete

### 6.1.1. Pracovná stanica

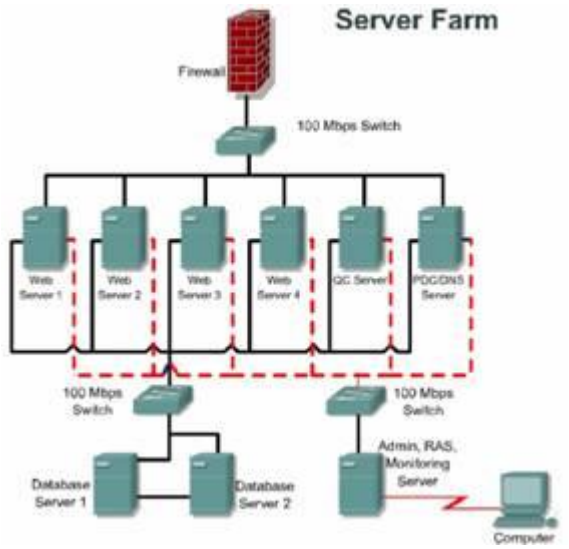
**Workstation** (pracovná stanica) je klientsky počítač, na ktorom bežia aplikácie a je pripojený na server, z ktorého získava dáta zdieľané inými PC. **Server** je počítač na ktorom beží NOS. Využitie pracovnej stanice:
zachytáva užívateľke dáta a aplikačné príkazy
rozhoduje či príkaz je pre lokálny OS a NOS

smeruje príkazy pre miestny OS alebo na NIC pre vykonanie procesu na sieti
- doručuje komunikáciu zo siete aplikáciám, bežiacich na stanici

OS Windows môže byť inštalované na pracovnej stanici aj na serveri.
UNIX alebo Linux môže byť taktiež na pracovných staniciach aj na serveroch. **Využitie UNIX workstation**:
počítačový riadený návrh ( CAD )
návrh tlačených spojov
analýza počasia
počítačové grafické animácie
telekomunikačných zariadeniach
**Bezdiskové pracovné stanice** – neobsahujú HDD, bootovacie inštrukcie sú v ROM a NIC. Na zabezpečenie sieťovej konektivity sa používa software nahratý v ROM NIC. Keďže neobsahuje HDD, nie je možné odcudziť dáta z daného PC, prispieva to k zvýšeniu bezpečnosti. **Laptopy** môžu tiež slúžiť ako pracovná stanica, do siete sa pripájajú buď cez NIC na MB, PCMCIA alebo cez externú sieťovú kartu v docking station.

### 6.1.2. Servery

Servery poskytujú zdroje veľa súčasne pripojeným klientom. NOS má prídavné nástroje na správu a podporujú veľké množstvo simultánnych prístupov užívateľov. Servery majú obyčajne vysoký výkon, veľké, výkonné disky, veľkú RAM, vysokorýchlostný NIC, obyčajne aj viac CPU. Využívajú obyčajne CTP/IP protokol a veľa jeho služieb.
Servery slúžia na autentifikáciu užívateľa do siete a k zdieľaným zdrojom. Identifikácia a autentifikácia je realizovaná prístupovým menom a heslom. Vďaka centralizovaným užívateľským prístupom, bezpečnosťou a kontrolou prístupov je dosiahnutá **jednoduchšia** správa siete.
Na dosiahnutie vyššieho výpočtového výkonu sú servery osadené viacerými procesormi, sú označované za **multiprocesorové** systémy.




Servery musia byť schopné pracovať pod veľkým zaťažením. Poskytujú:
webové služby využitím HTTP, FTP, DNS
emailové služby využitím SMTP, POP3, IMAP
zdieľanie súborov cez *Sun Microsystems Network File System* (NFS) a *Microsoft Server Message Block* (SMB)
tlačové služby
DHCP *Dynamic Host Configuration Protocol*
firewall, NAT
Pri veľkých sieťach je každá služba spustená na samostatnom serveri.

### 6.1.3. Vzťah klient – server

Model klient server distribuuje spracovanie na viaceré počítače. Umožňuje vzdialeným systémom prístup k zdieľaným informáciám a zdrojom. Definície termínov:
**miestna stanica**, stroj, na ktorom užívateľ aktuálne pracuje
**vzdialený host**, systém, ktorý bude sprístupnený pre užívateľa pre iný systém
**server**, poskytuje zdroje pre jedného alebo viacerých používateľov na sieti
- **klient**, zariadenie, ktoré využíva služby jedného alebo viacerých serverov

Príkladom je napríklad FTP spojenie, na serveri musí bežať služba, aby klient mohol požiadať o prenos súborov. Ďalším príkladom klient – server aplikácie je databázový server.
Servery sú typicky viac výkonné než klientske počítače a lepšie spracovávajú veľké množstvá dát. Servery pre svoju spoľahlivosť vyžadujú ďalší hardware a špecializovaný software, ktorý v podstate pridáva na cene.

### 6.1.4. Úvod do NOS

OS je **základ**, na ktorom bežia aplikácie a služby na pracovnej stanici. Umožňuje komunikovať medzi viacerými zariadeniami a zdieľať zdroje cez sieť.
Medzi všeobecné funkcie OS na pracovnej stanici patrí *kontrola hardvéru, spúšťanie programov a poskytovanie užívateľského prostredia*. Tieto funkcie sú poskytované pre jedného užívateľa, stanicu môžu zdieľať viacerí používatelia, ale len jeden naraz.
OS poskytuje sieťové prostriedky, akoby boli súčasťou miestneho systému.
OS pre servery musia poskytovať podporu pre viacerých používateľov súčasne, sú to **viac užívateľské** systémy. Administrátor vytvorí účet pre každého užívateľa, na jeho základe je autentifikovaný.
V multitaskingovom OS bežia viaceré procesy naraz. Pre jednotlivých užívateľov sa spúšťajú samostatné procesy.
Hlavné črty pri výbere NOS:
výkon, musí poskytnúť prístup pre rýchle čítanie a zápis súborov cez sieť aj pri veľkom zaťažení
manažovatelnosť a monitorovacie nástroje, poskytuje nástroje pre monitorovanie serveru, správu klientov, súborov, tlač a právu diskového priestoru. Rozhranie manažmentu poskytuje nástroje pre inštalovanie nových služieb.
bezpečnosť, musí chrániť zdieľané zdroje. Zabezpečuje autentifikáciu užívateľov k zdieľaním prostriedkom. Zabezpečuje kryptovanie a ochranu informácií pri prenose medzi serverom a užívateľom.
škálovatelnosť, je schopnosť zoskupovať sa bez degradácie výkonu. NOS musí byť schopný udržiavať výkon aj pri nových užívateľoch a
stabilita, je schopnosť udržať službu aj pri vysokej záťaži alebo pri zlyhaní komponentu

### 6.1.5. Microsoft NT, 2000, and .NET

| OS | Versions | Uses |
|---|---|---|
| **Windows NT** | • Workstation<br>• Server | • Corporate users<br>• Departmental server |
| **Windows 2000** | • Professional<br>• Server<br>• Advanced server<br>• .NET | • Corporate users or small businesses<br>• Internet or remote access server<br>• Departmental server<br>• Enterprise server<br>• Enterprise internet server |

2

**NT4** bol navrhnutý pre poskytovanie prostredia pre úlohy kritických služieb, ktoré by boli viac stabilné, než OS Microsoftu pre spotrebiteľov. Bol pre pracovné stanice aj pre servery. Na tomto OS bolo možné spúšťať staršie programy na *virtual machines* (**VMs**). Pri zlyhaní programu nebolo nutný reštart.
Windows NT poskytuje doménovú štruktúru na kontrolovanie užívateľov a klientsky prístup na

zdieľané zdroje siete. Sú manažované cez *User Manager for Domains application* na doménovom kontroléry.
Na doménovom kontroléry sú uložené *Security Accounts Management Database* (**SAM).** Na sieti môže byť jeden alebo viac záložných doménových kontrolérov, na ktorých je kópia SAM.
**Windows 2000** je postavený na jadre NT, podporuje plug-and-play, podporuje inštaláciu nových zariadení bez reštartu, obsahuje tiež nový kódovací systém.
**organizational units** (OUs) – kontajner, do ktorého je možné umiestniť užívateľov alebo zdroje.
**Windows 2000 Professional** – klientsky OS, možné ďalšie využitie je ako súborový server, FTP server, web server ale len pre 10 simulovaných pripojení.
**Windows 2000 Server** – môže pracovať ako súborový, tlačový, webový a aplikačný server.
- *Active Directory Services* je centralizovaný bod správy užívateľov, skupín a zabezpečených služieb a sieťových zdrojov.
- má zabudovanú konektivitu na Novell NetWare, UNIX a AppleTalk systémy.

**Windows 2000 Advanced Server** – určený pre extrémne veľké siete.
**Windows .NET Server** – je bezpečný a spoľahlivý systém pre podnikové weby a FTP. Poskytuje XML web služby

### 6.1.6. UNIX, Sun, HP a LINUX

Počiatky *UNIXu.*
Od roku 1969 boli vyvíjané v Bell laboratóriách. Od počiatku boli určené ako viacužívateľský, multitaskingový OS. Zo začiatku bol písaný v asembléry, neskúr v C.
Sú rôzne verzie UNIXu. Je to bezpečný OS, určený pre beh kritických aplikácií, je doňho zabudovaná podpora pre TCP/IP. Najpoužívanejší je Sun Microsystems Solaris Operating Environment
Počiatky *Linuxu.*
Od roku 1991, určený pre desktopy, je voľne šíriteľný. Tiež je veľa rôznych verzií. Je veľmi výkonný a spoľahlivý OS.
Výhody:
32 bitový OS
podporuje multitasking a virtuálnu pamäť
kód je open source

### 6.1.7. Apple

Sú navrhnuté pre jednoduché siete peer-to-peer alebo pracovné skupiny. Sieťové rozhrania sú súčasťou hardvéru a sieťové komponenty sú zabudované v MAC OS. Využívajú sa ethernet a tokeng ring adaptéry.
MAC sa prevažne využíva v grafickej oblasti. Pracovné stanice môžu byť pripojené na iné stanice alebo na AppleShare file servery. Podporujú tiež pripojenie na Microsoft, NetWare alebo UNIX.
*Mac OS X (10)* – sa niekedy tiež označuje ako Apple System 10. Je plne kompatibilný so staršími verziami. Prostredie je medzi Microsoft Windows XP a Linux X-windows GUI, je nazývané **AQUA.**.
Je určený pre domácnosti na internet, video, editovanie fotografií a hry.
Jadro OS je nazývané Darwin, je založené na UNIXe.
3

### 6.1.8. Pojem služba na serveroch

| **Service** | **TCP/IP Proto-col** ^ |
|---|---|
| World WldeWeb | HTTP |
| Filé Transfer | **FTRTFTP** |
| FileSharing | NFS |
| Intemet Mail | SMTP, POP3, IMAP |
| Remote Administration | Telnet |
| Directory Serviges (Intemet) | DNS, LDAP |
| Automatic Network Address | DHCP |

Configuration
Network Administraliori SNMP
NOS sú určené na poskytovanie sieťových procesov klientom.
Sieťové služby obsahujú:
WWW
zdieľanie súborov
mailový výmenu
directory services
vzdialenú správu
tlačové služby
Tieto procesy sú vo Windows 2000 označované ako **služby** a UNIXoch a LINUXoch ako **démoni.** V závislosti na NOS sú niektoré sieťové procesy povolené počas inštalácie, avšak pri nových NOS je potrebné služby spúšťať ručne. *Zdieľanie súborov:*
je dôležitá sieťová služba, na zdieľanie existuje veľa protokolov a aplikácií. V podnikoch alebo domácich sieťach sa používa **Windows File Sharing** alebo **NFS** protokol. *FTP:*
FTP služby sú vytvárané spoločne s webovými službami. FTP servery je možné nakonfigurovať pre autorizáciu alebo pre anonymné prihlásenie. Pri nečinnosti na servery je klient odpojený, tento čas sa nazýva **idle timeout.** *WEB služby:*
- World Wide Web je grafická sieťová služba. Webové stránky sú nazývané websites, sú umiestnené na serveroch alebo skupinách serverov. Webový klientsky software obsahuje GUI **web prehliadač** ako Netscape Navigator alebo Internet Explorer. Webové stránky bežia na službách **webového softwaru** ako je *Microsoft Internet Information Services (IIS)* a *Apache Web Server*.

*DNS*
- slúži na preklad internetových mien, ako www.cisco.com, na IP adresy.

*DHCP*
- ich účelom je umožniť individuálnym počítačom naučiť sa ich TCP/IP konfiguráciu z DHCP servera.

### 6.2.1. Úvod do sieťovej správy

Povinnosti pri sieťovom manažmente:
monitorovanie sieťovej dostupnosti
zlepšovanie automatizácie
monitorovanie času odozvy
poskytovať bezpečnostné výhody
smerovanie dopravy
obnovu kapacity
- registrovanie užívateľov

Hnacie sily sieťového manažmentu:
kontrolovanie podnikových aktivít.
kontrolovanie komplexnosti
zlepšovanie služieb
vyrovnávanie premenných potrieb
redukovanie prestojov
kontrolovanie ceny

Network Manaqement Reauirements Basic Terms

| **Term** | **Definition** |
|---|---|

| | |
|---|---|
| SNMP | Simple Network Management Pratocol is the štandard for managing network resources, defined by the IETF. |
| MIB | Managemenl Information Base is the dala definilions/slructuna of a managed object. |
| RMOM | Remote Monitoring is a MIBiagent specificaťon wtiich defines functions for monitoring remote devices. |
| RFC | Request for Comment are documents posted by the IETF, Some are adopted as Intemet sta n dards. |
| NMS | Network Management Staiion i s an SNMP-based management slation for managing network devices. Typically this is a UNIX or NT box running, H P Openveiw, SunNET Mgr or NetView for AIX. |

4

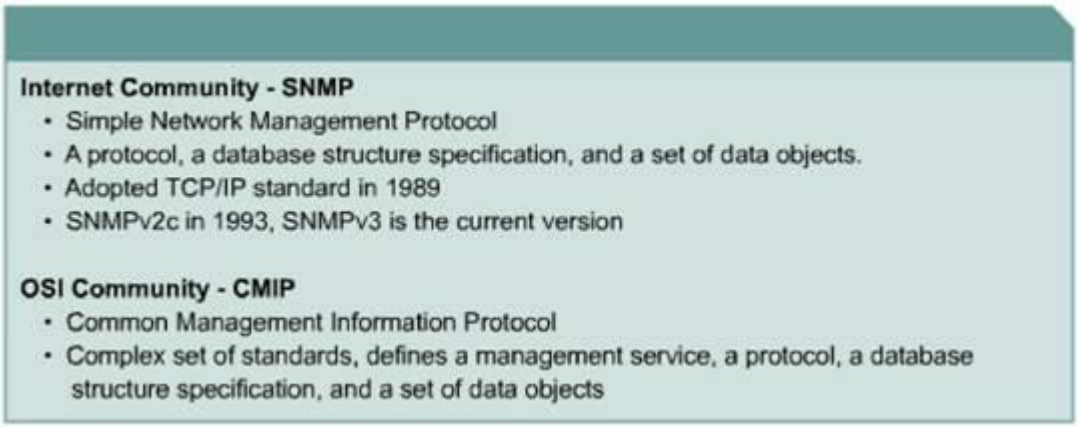
### 6.2.2. OSI a sieťový model správy

International Standards Organization (ISO) vytvorila model pre správu siete, pozostáva zo 4 častí:
**organizačný** model, popisuje komponenty sieťovej správy ako manažér, agent.
**informačný** model, týka sa štruktúry a ukladania sieťových, manažovaných informácií. Sú uložené v databázach nazývaných in *management information base* (MIB).
**komunikačný** model, zaoberá sa spôsobom komunikácie medzi agentom a manažovaným procesom, je prepojený s prekladovým protokolom a aplikačným protokolom a príkazmi medzi mini.
- **funkčný** model, adresuje sieťové manažovateľské aplikácie, majú 5 oblastí funkcií:

o zlyhanie
o konfiguráciu
o prístupy
o výkon
o bezpečnosť

### 6.2.3. SNMP a CMIP štandardy

Na umožnenie veľa rôznych platforiem boli vytvorená 2 základné štandardy:
*Simple Network Management Protocol* – IETF spoločnosti, štandardy sieťovú správu, zahŕňajú protokoly, špecifikáciu databázovej štruktúry
*Common Management Information Protocol* – telekomunikačné spoločnosti, na monitorovanie a kontrolovanie heterogénnych sietí

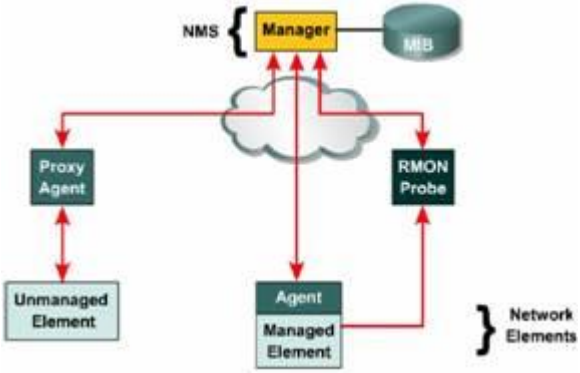



### 6.2.4. SNMP operácie

SNMP je protokol aplikačnej vrstvy, určený na výmeny manažmentských informácií medzi sieťovými zariadeniami.
Prvky organizačného modelu SNMP:
manažované stanice
management agent
manažovaný informačný základ (MIB)

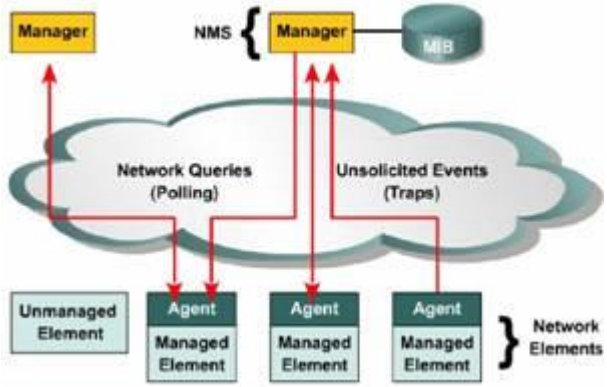
sieťový manažovaný protokol
*Network management application* (NMA) – obsahuje rozhranie, ktoré sieťovému manažerovy umožňuje manažovať sieť. Agent môže sledovať:
počet a stav jeho virtuálnych okruhov
počet prenesených chybových správ
počet bytov a paketov prenesených obojsmerne rozhraním
maximálnu dĺžku výstupnej fronty pre routre a iné sieťové zariadenia
poslané a prijaté broadcastové správy
zapnutie a vypnutie sieťového rozhrania
5

Network management station (NMS) vykonáva monitorovacie funkcie vyberaním hodnôt z MIB. Komunikácia medzi manažérom a agentom je na UDP, komunikuje cez porty 161 a 162. Všeobecné typy správ pre dvoj **vrstvový model**, komunikácia len cez SNMP:
**get**, umožňuje manažmentskej stanici aktualizovať hodnoty MIB objektov z agenta
**set**, umožňuje manažmentskej stanici nastaviť hodnoty MIB objektov na agentovi




- **trap**, umožňuje agentovi oznámiť manažmentskej stanici významnú udalosť.

**Trojvrstvový model** sa využíva pri komunikácii medzi zariadeniami, ktoré majú proprietárne manažované rozhranie. Sieťový manager, ktorý chce získať alebo kontrolovať tieto informácie komunikuje s proxy agentom.

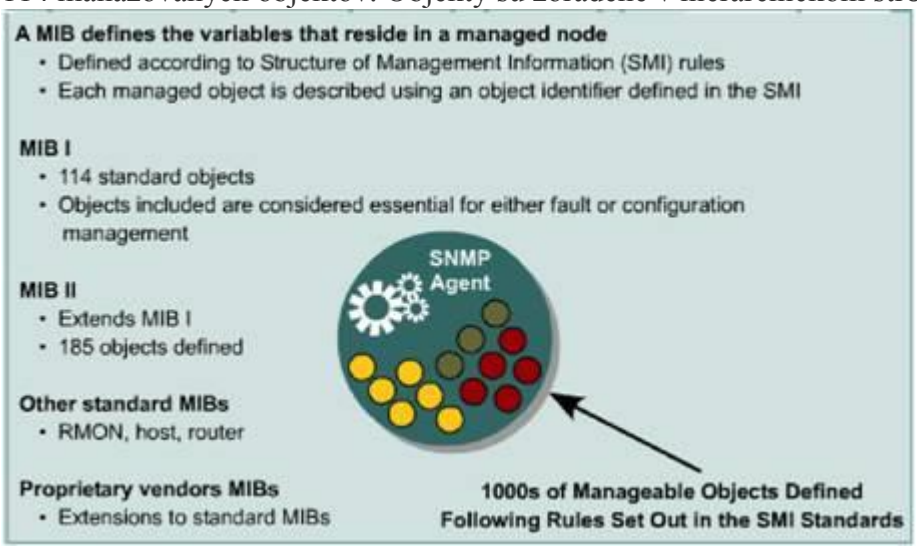



NMS je obyčajne pracovná stanica, na ktorej beží typický operačný systém. Sieťová manažérska aplikácia sa spolieha na OS. Príkladom aplikácií sú *Ciscoworks2000, HP Openview a SNMPv2c.*

### 6.2.5. Štruktúra management information a MIBs

**MIB** je použitý na ukladanie štruktúrovaných informácií predstavujúcich sieťové prvky a ich atribúty, štruktúra je definovaná v štandarde **SIM**. Originálne SMI MIB boli rozdelené do 8 skupín, dohromady

114 manažovaných objektov. Objekty sú zoradené v hierarchickom strome.




### 6.2.6. SNMP protokol

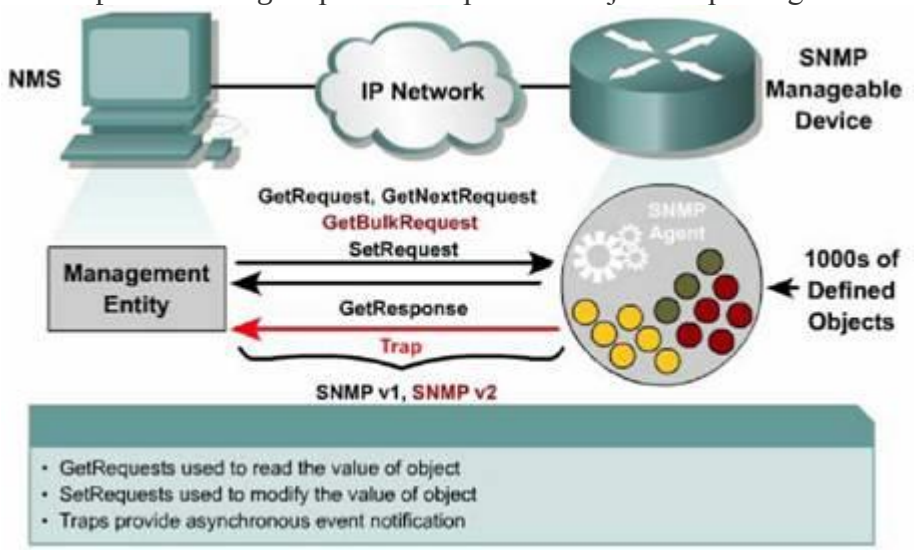
Agent je softwarová funkcia vložená vo veľa sieťových zariadeniach, ako routre, prepínače, manažované huby, tlačiarne a servery. Vzťah medzi manažérom a klientom je umožnený cez SNMP. 3 typy SNMP správ pre NMS:

GetRequest

GetNextRequest

- SetRequest.

GetResponse message – potvrdenie predchádzajúcich správ agentom




Management entity alebo NMS ponúka informácie z agenta. Komunikácia medzi manažérom a zariadením predstavuje komunikáciu na sieti, pri agresívnom monitorovaní môže dôjsť k negatívnym vplyvom na výkon siete. Každá SNMP správa obsahuje čistý textový reťazec nazývaný *community string*. Je využívaný ako heslo na prístup k zariadeniu.

### 6.2.7. Konfigurovanie SNMP

Na komunikáciu NMS so sieťovým zariadením, musí byť na sieťovom zariadení povolený SNMP a nakonfigurovaný komunity string. Prednastavený KS je public. Nastavenie read-only komunity stringu:

Router(config)#**snmp-server community** string **ro**

String, predstavuje heslo na prístup k SNMP protokolu

**ro** – (Optional) predstavuje read-only prístup, manažovateľské stanice môžu len čítať MIB objekty.

Router(config)#**snmp-server community** string **rw**

- **rw,** (Optional) predstavuje read-write prístup**,** manažovateľské stanice môžu čítať a modifikovať MIB objekty

Router(config)#**snmp-server location** text Router(config)#**snmp-server contact** text

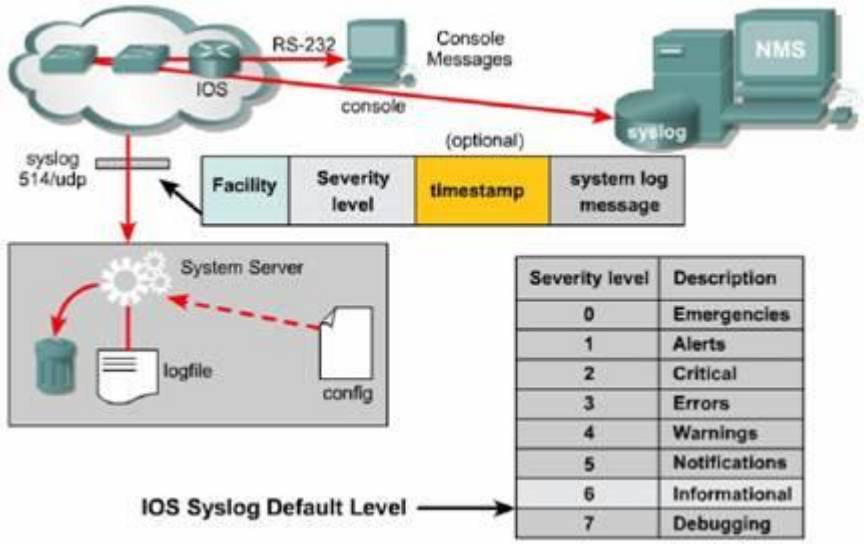
- text, popisuje informácie o umiestnení a hlavný kontakt na manažované zariadenie

### 6.2.8. RMON

Je hlavným prístupom v medzisieťovom manažmente, manažér môže získavať informácie, ktoré sú umiestnené na samostatných zariadeniach. Bol navrhnutý pre monitorovanie a diagnostiku pre distribuované LAN siete. Monitorovacie zariadenie je nazývané agent, umožňuje definovať užívateľské alarmy, vytvárať množstvo štatistík. RMON monitorovacie funkcie:
**štatistická skupina**, využitie a chybová štatistika
**skupina histórie**, štatistické záznamy pre štatistické skupiny, príklad: využitie, počet chýb, počet paketov
**alarm skupina**, umožňuje admin. nastaviť prahové intervaly pre agentov.
**host skupina**, definuje mieru rôznych typov dopravy
**Host TopN skupina**, poskytuje reporty o TopN hostoch, založených na štatistike hostov
**Traffic matrix skupina**, ukladá chyby a využitie štatistík pre páry komunikujúcich bodov na sieti
**skupina filtrov**, vytvárajú sa podľa užívateľsky definovaných kritérií
**skupina zachytených paketov**, definuje, ako pakety ktoré sa zhodujú s filtrom sú bufrované
**skupina udalostí**, umožňuje logovať udalosti, napr. alarm.
7

### 6.2.9. Syslog

*Cisco syslog logging utility* sú založené na UNIXových syslog utilitách. Systémové udalosti sú zobrazené na konzole.
Stupeň závislosti indikuje kritický druh chybových správ od 0 – 7.
0 Emergencies
1 Alerts
2 Critical
3 Errors
4 Warnings
5 Notifications
6 Informational
7 Debugging
Router(config)#**logging on**, povolenie logovania na všetky povolené ciele Router(config)#**logging** *host-name | ip address*, posielanie systémových logovacích správ na syslog server, napr. CiscoWorks2000
Router(config)#**service timestamps log datetime**, správa obsahuje časovú značku




| Severity level | Description |
|---|---|
| 0 | Emergencies |
| 1 | Alerts |
| 2 | Critical |
| 3 | Errors |
| 4 | Warnings |
| 5 | Notifications |
| 6 | Informational |
| 7 | Debugging |