Konfigurace směrovačů a přepínačů s Cisco IOS

Petr Grygárek

Konfiguraci směrovače nebo přepínače s operačním systémem IOS firmy Cisco si můžeme představit jako textový soubor. Jednotlivé řádky tohoto souboru jsou příkazy, ovlivňující chování směrovače nebo přepínače (dale o nich budeme hovořit společně jako o "zařízení").. Příkazy můžeme zadávat buďto z konzoly připojené k zařízení přímo přes rozhraní RS232 nebo pomocí služby Telnet. Příkazy lze zadávat i přes WWW rozhraní, ale to je zejména pro konfiguraci směrovačů dosti nepohodlné.

Konfigurační soubor může vypadat například takto:

```
hostname RouterISP
enable password cisco

interface FastEthernet 0/1
 ip address 192.168.1.1 255.255.255.0
 ip access-group ONLYWWW in
 no shutdown

interface Serial 0/1
 ip address 200.120.12.1 255.255.255.0
 clock rate 64000
 no shutdwon

access-list extended ONLYWWW
 permit tcp any host  192.168.1.100 eq 80
 permit tcp any any established
 deny tcp any any
 permit ip any any
```

Všimněte si, že se konfigurační soubor dělí do sekcí, každá sekce pak obsahuje své vlastní příkazy. Konfigurace se tím stává hierarchická – na nejvyšší úrovni jsou příkazy ovlivňující chování zařízení jako celku, v sekcích pak příkazy týkajících se jednotlivých rozhraní (interface) zařízení nebo parametrizující chování zvlášť spouštěných procesů (např. směrovacích protokolů). Samostatnou sekci mohou tvořit také příkazy společně definující nějakou pojmenovanou entitu, například ACL (Access-Control List)

Při práci se zařízením můžeme přecházet mezi několika režimy:

- Uživatelský režim neprivilegovaný
- Uživatelský režim privilegovaný
- Konfigurační režim

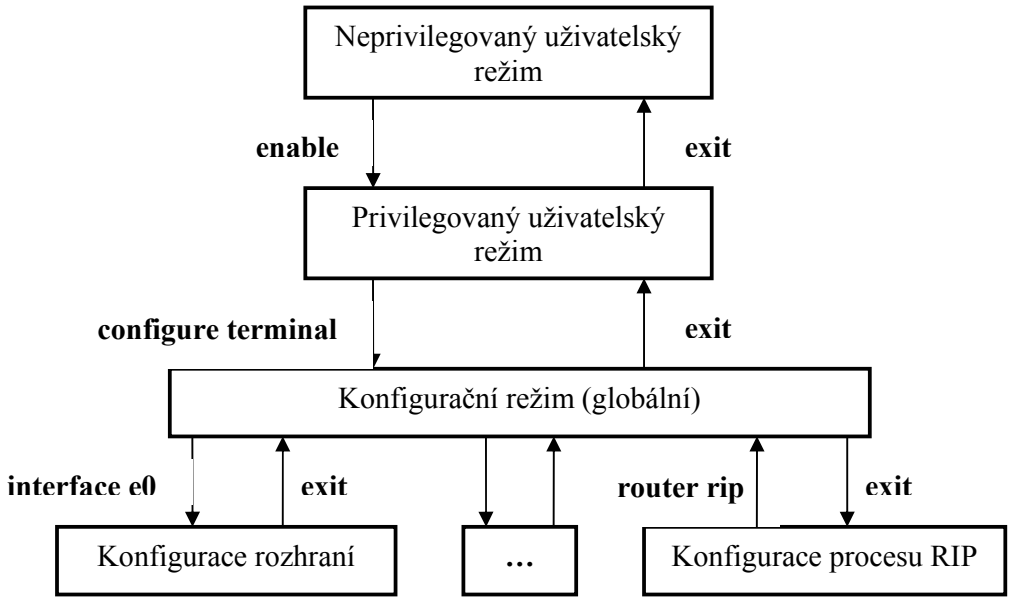
Při přihlášení na zařízení se dostáváme do uživatelského neprovilegovaného režimu. V něm je možná velmi omezená práce – pouze výpis některých informací o hardware a instalovaném operačním systému IOS. Proto správu zařízení téměř vždy začínáme přechodem do

privilegovaného uživatelského režimu, při němž se musíme autentizovat heslem (je-li heslo nakonfigurováno).

V uživatelském privilegovaném režimu můžeme vypisovat veškeré informace o činnosti zařízení a spouštět příkazy, které ovlivňují okamžitý stav zařízení, nikoli však jeho konfiguraci. Příkazy zadávané v uživatelském privilegovaném režimu se tedy pouze provedou, avšak neuchovávají se v konfiguraci směrovače.

Pokud chceme zadávat příkazy trvale konfigurující zařízení, musíme přejít do konfiguračního režimu. Všimněte si, že zde máme k dispozici jinou sadu příkazů, než v režimech uživatelských (privilegovaném nebo neprivilegovaném). Každý příkaz zadaný v konfiguračním režimu se stane trvalou součástí konfigurace zařízení a zařízení začne podle tohoto příkazu ihned pracovat.

Obrázek 1 ukazuje, jak lze mezi jednotlivými režimy přecházet. Do privilegovaného uživatelského režimu se dostaneme z režimu neprivilegovaného zadáním příkazu **enable** (a správného hesla), zpět pak příkazem **disable** nebo **exit**. Z privilegovaného uživatelského režimu se můžeme dostat do režimu konfiguračního příkazem **configure terminal**, zpět opět příkazem **exit**.



Obrázek 1

Konfigurační režim

Při vstupu do konfiguračního režimu můžeme zadávat globální konfigurační příkazy. Pokud chceme zadávat konfigurační příkazy jednotlivých sekcí (např. směrovacího procesu nebo

rozhraní), přepneme se nejprve příslušným příkazem do režimu konfigurace příslušné sekce – např. **interface FastEthernet 0/0** nebo **router rip**. Pak můžeme vkládat příkazy dané sekce. Do globálního konfiguračního režimu se vrátíme zadáním příkazu **exit**. Je užitečné vědět, že namísto opakovaného zadávání příkazu **exit** pro postupný přesun z konfigurace sekce do globálního konfiguračního režimu a dále do režimu privilegovaného je možné stisknout klávesy Ctrl+Z.

Příkazy vložené v globálním konfiguračním režimu nebo jako příkaz některé sekce můžeme z konfigurace odstranit tak, že příkaz znovu napíšeme stejně, avšak s uvedením klíčového slova **no** na jeho začátku. Například jméno zařízení (globální) a příkaz **access-group** definující ACL na rozhraní vložené pomocí příkazů

```
hostname XXX

interface FastEthernet 0/0
 access-group 1 in
```

můžeme odstranit vložením příkazů

```
no hostname XXX

interface FastEthernet 0/0
 no access-group 1 in
```

Příkazem **no** můžeme odstranit i celou sekci, pokud jsme ji předtím vytvořili, například sekci

```
router rip
 network 10.0.0.0
 network 192.168.0.0
```

Odstraníme příkazem

```
no router rip
```

Samozřejmě nemá smysl odstraňovat jako celek sekce popisující např. jednotlivá rozhraní zařízení, tyto sekce jsou v konfiguraci přítomny trvale. Můžeme pouze odstranit příkazy vložené do této sekce.

Zadávání příkazů

Při zadávání příkazů si lze kdykoli stiskem otazníku nechat vypsat seznam příkazů, které jsou v daném režimu k dispozici. Pokud stiskeme otazník po zadání příkazu, který má nějaké volby, vypíše se jejich seznam. Příkazy nemusíme vypisovat celé, stačí napsat jen několik počátečních písmen, které příkaz jednoznačně identifikují. Po napsání dostatečného počtu písmen lze příkaz doplnit stiskem tabulátoru. Tím se zároveň ověří, zda je začátek příkazu jednoznačný – pokud zapsanými písmeny začíná více příkazů, jsou tyto příkazy vypsány a je

třeba zadání příkazu upřesnit. Pokud si jednoznačné začátky příkazů pamatujeme, můžeme používat pouze tyto a stisku tabulátoru se úplně vyhnout.
Namísto

```
enable
configure terminal
hostname MyRouter
interface gigabitethernet 0/0
 ip address 172.16.10.1 255.255.255.0
 no shutdown
 exit
interface fastethernet 1/0
shutdown
exit
```

pak můžeme psát

```
en
conf t
hostn MyRouter
int giga 0/0
 ip addr 172.16.10.1 255.255.255.0
 no shut
 exit
int fa 0/0
 sh
 exit
```

Při vkládání příkazů v konfiguračním režimu systém vždy příkaz automaticky rozvine do plné formy a v plné formě je také uvidíme při výpisu konfigurace (viz dále).

Při psaní příkazů lze využít běžných editačních kláves – backspace pro smazání znaku před kurzorem a šipky vpravo a vlevo pro posun kurzoru. Systém si pamatuje několik naposledy zadaných příkazů, v historii příkazů se lze pohybovat stiskem šipek nahoru a dolů.

Kontrola a uložení konfigurace

Konfiguraci vloženou v konfiguračním režimu si můžeme prohlédnout v režimu privilegovaném zadáním příkazu **show running-config**. Konfigurace bude vypsána na terminál po stránkách způsobem obdobným využití příkazu more známého s Unixu. Po vypsání stránky se výpis zastaví, k další stránce lze přejít stiskem mezerníku, posun o jeden řádek zajistí stisk klávesy Enter. Stiskem písmene q se výpis ukončí.

Konfiguraci je možné uložit do flash paměti (NVRAM-Non Volatile RAM) pomocí příkazu **copy running-config startup-config** zadaného v privilegovaném uživatelském režimu. Po tomto uložení konfigurace přetrvá vypnutí zařízení nebo znovuzavedení operačního systému.

Poznámky:

- Může se stát, že některé (spíše speciální) příkazy manuálně vložené do konfigurace se ve výpisu konfigurace neobjeví. Je to způsobeno tím, že zařízení považuje takovýto příkaz za implicitní. Pokud bychom však vložili opak tohoto příkazu, nastavení by již implicitní nebylo a v konfiguraci by se objevilo.

- Konfiguraci je možné ze zařízení uložit na TFTP server nebo nahrát do zařízení z TFTP serveru. Protože je na TFTP serveru uložena jako textový soubor, je také někdy výhodné konfiguraci upravovat na TFTP serveru s použitím vhodného textového editoru.

Základní konfigurace směrovače

V následujících odstavcích se dozvíte, jak zkonfigurovat základní funkci směrovače pro směrování IP paketů.

Konfigurace rozhraní

Každému rozhraní musí být přiřazena IP adresa a příslušná maska podsítě. To lze provést z globálního konfiguračního režimu po přepnutí do sekce příslušného rozhraní:

```
interface Serial 0/1
  ip address 192.168.1.1 255.255.255.0
```

Pokud konfigurujeme sériové synchronní rozhraní, které má sloužit jako DCE, musí být uvedená taktovací rychlost generovaného hodinového signálu, určujícího bitovou rychlost.daného rozhraní:

```
interface Serial 0/1
 ip address 192.168.1.1 255.255.255.0
 clock rate 64000
```

Každé rozhraní je implicitně administrativně deaktivováno (shutdown). Aby mohlo začít fungovat, je třeba jej manuálně aktivovat:

```
interface Serial 0/1
 ip address 192.168.1.1 255.255.255.0
 clock rate 64000
 no shutdown
```

Stav rozhraní si můžeme ověřit v uživatelském privilegovaném režimu příkazem

```
 show interface Serial 0/1
```

Ve výpisu je indikováno, zda je aktivní (Up) samotné rozhraní a zda byl detekován (Up) linkový protokol. Pro správnou funkci rozhraní je nutné obojí.

Konfigurace hesla a vzdáleného přístupu

Heslo pro přechod do privilegovaného režimu se konfiguruje příkazem

```
 enable password MYPASSWD
```

Aby bylo možné zařízení konfigurovat pomocí služby Telnet, je třeba konfigurovat virtuální terminály a přístupové heslo pro připojení:

```
line vty 0 4
 password TELNETPASSWD
 login
```

Poté se je možné pomocí Telnetu připojit na směrovač s použitím adresy jeho libovolného (aktivního) rozhraní.

Poznámka:
Bez znalosti nakonfigurovaného hesla je třeba pro přístup na zařízení provést časově náročnou proceduru obnovení hesla. Proto **pokud konfigurujete na zařízeních v laboratoři jakékoli heslo, vkládejte vždy výhradně jen dohodnuté heslo 'cisco'.**

Konfigurace směrování

Směrovací tabulku si můžeme vypsat z privilegovaného režimu příkazem

```
show ip route
```

Směrovací tabulka by měla obsahovat záznamy o přímo připojených sítích a o cestách do vzdálených sítích, které byly vloženy staticky nebo naučeny ze směrovacího protokolu. Záznamy jsou označeny písmeny podle toho, jakým způsobem se do směrovací tabulky dostaly. Setkáte se zejména s těmito písmeny:

- C (Connected) – přímo připojené sítě
- S (Static) – staticky konfigurované cesty
- R (RIP) – sítě naučené ze směrovacího protokolu RIP
- O (OSPF) – sítě naučené ze směrovacího protokolu OSPF

Konfigurace statického směrování

Statický záznam do směrovací tabulky můžeme vložit z globálního konfiguračního režimu příkazem

ip route <adresa cílové sítě> <maska cílové sítě> <adresa dalšího skoku>

Například

ip route 192.168.12.0 255.255.255.0 192.168.1.2

Při zadávání default cesty zadáme cílovou síť i masku podsítě jako samé nuly:

ip route 0.0.0.0 0.0.0.0 192.168.20.1

Konfigurace směrovacího protokolu RIP

Při konfiguraci směrovacího protokolu RIP nejprve router instruujeme ke spuštění příslušného směrovacího procesu příkazem

router rip

Tím vznikne nová sekce konfiguračního souboru, týkajícího se tohoto směrovacího procesu. V ní musíme určit, které přímo připojené sítě se směrování pomocí RIP mají účastnit (často to budou všechny). Každou síť, na které se mají generovat i poslouchat zprávy protokolu RIP a která má být ve zprávách protokolu RIP propagována, musíme explicitně uvést pomocí příkazu **network**:

```
router rip
 network 192.168.1.0
 network 192.168.2.0
 network 172.16.0.0
```

Výměnu paketů se směrovacími tabulkami mezi sousedními směrovači můžeme sledovat po zadání příkazu

debug ip rip packet

z privilegovaného uživatelského režimu. Výpis zrušíme odstraněním předchozího příkazu:

no debug ip rip packet

Konfigurace přepínače

Na většině moderních přepínačů se vyskytují rozhraní rozhraní 10/100BaseT. Označují se podle schematu FastEthernet <modul>/<číslo portu> např.:

interface FastEthernet 0/0

Rozhraní gigabit Ethernetu (jsou-li přítomny) se označují jako

interface GigabitEthernet<modul>/<čísloportu>.

Konfigurace portů

Na jednotlivých rozhraních (portech) lze konfigurovat tyto základní příkazy

interface FastEthernet 0/0
duplex half | full | auto
stanovení režimu duplexu (pevně nebo dohodou zařízení)
speed 10 | 100 | auto
stanovení rychlosti (pevně nebo dohodou zařízení)

Konfigurace virtuálních sítí

Vytvořit VLAN je možné z privilegovaného (pozor, nikoli konfiguračního !) režimu takto:

```
vlan database
 vlan 2 name MUJVLAN
 exit
```

Virtuální sítě nakonfigurované na přepínači a porty přiřazené do jednotlivých VLAN lze zkontrolovat z privilegovaného režimu příkazem

```
show vlan
```

Na každém portu lze stanovit, zda bude staticky přiřazen do jedné z VLAN (tzv. „access“ port), nebo se bude jednat o trunk:

```
configure terminal
 interface FastEthernet 0/0
  switchport mode access | trunk
```

Mód portu (trunk/access) lze zjistit z privilegovaného uživatelského režimu příkazem

```
show interface fastethernet 0/1 switchport
```

Jedná-li se o access port, je třeba stanovit, do které VLAN bude přiřazen:

interface FastEthernet 0/0
switchport mode access
switchport access VLAN <číslo VLAN>

Není-li port explicitně přiřazen do žádné VLAN, bude implicitně ve VLAN 1, která je na přepínači vždy.

Pokud konfigurujeme trunk, je třeba na rozhraní také udat způsob značkování rámců číslem VLAN, ze které rámec pochází. Standardní řešení je značkování podle standardu IEEE 802.1q, které zajistíme příkazem

.

switchport trunk encapsulation dot1q

Upozornění:
U přepínačů, které podporují pouze enkapsulaci 802.1q, nemusí být příkaz **switchport trunk encapsulation dot1q** vůbec implementován a je implicitní.

Konfigurace vzdáleného přístupu

Přestože je přepínač zařízení pracující ve své podstatě na 2. vrstvě OSI RM, je pro zabezpečení jeho vzdálené správy třeba přidělit přepínači vlastní IP adresu. Tato adresa nijak nesouvisí s vlastní přepínací funkcí přepínače, slouží pouze k tomu, abychom přepínač mohli konfigurovat nejen z přímo připojené konzoly, ale i pomocí klienta služby Telnet. V přepínači je vlastně realizován server služby Telnet.

IP adresu pro management přepínače vkládáme na virtuální rozhraní, které odpovídá virtuální síti, přes kterou chceme přepínač spravovat. Lze spravovat vždy jen z jedné virtuální sítě, kterou je vhodné z bezpečnostních důvodů vyčlenit pouze pro tyto účely. Pokud virtuální sítě nepoužíváme, patří všechny porty implicitně do VLAN1 a na toto virtuální rozhraní také přiřadíme IP adresu pro správu:

interface VLAN1
ip address 192.168.1.100 255.255.255.0
no shutdown

Všimněte si, že virtuální rozhraní musí být také administrativně povoleno příkazem **no shutdown**.

Po nakonfigurování IP adresy pro správu přepínače je třeba také přiřadit heslo pro privilegovaný režim (**enable password**) a heslo na virtuální rozhraní serveru služby Telnet v sekci **line vty** stejně jako u směrovačů.

Konfigurace modemového připojení

Konfigurace směrovače pro směrování na asynchronním portu

Některé směrovače Cisco umožňují svá sériová rozhraní přepnout do režimu kompatibility s RS-232 a připojit k těmto portům asynchronní sériovou linkou modem. Tím se ke směrovači může připojit prostřednictvím telefonní sítě i vzdálený uživatel, taktéž vybavený modemem. Po spojení telefonního okruhu se při správném nakonfigurování asynchronní linka chová stejně, jako každé jiné rozhraní směrovače. Pakety tvořené daty přicházejícími z modemu pak mohou být normálně směrovány na ostatní rozhraní. U směrovačů, jejichž sériová rozhraní schopnost práce v asynchronním režimu nemají, lze modem napojit alespoň na AUX (auxiliary) port, který běžně slouží pro vzdálenou správu směrovače pomocí modemu. Jelikož AUX-portem jsou vybaveny všechny směrovače Cisco a možnost přepnutí sériového portu do asynchronního režimu RS-232 je jen u některých typů sériových portů, zaměříme se na připojení modemu pomocí AUX portu.

AUX port je vybaven (stejně jako port konzolový) konektorem RJ-45. Pro připojení k modemu je proto třeba použit konzolového kabelu ukončeného z jedné strany RJ-45 a z druhé strany konektorem DB9/DB25 (samec), který lze zasunout do konektoru RS-232 na běžných (asynchronních) modemech.

Konfiguraci směrovače pro modemové připojení zahájíme konfigurací hardwarových parametrů AUX portu:

line aux 0
modem InOut
AUX port bude použit pro příchozí (a příp. i odchozí) volání z modemu
transport input all
dovolíme, aby portem procházely všechny protokoly (např. i IP)
speed 19200
rychlost v bps pro komunikaci s modemem
flowcontrol hardware
způsob řízení toku dat mezi modemem a routerem – zde pomocí signálů RTS-CTS

Poté zkonfigurujeme logické rozhraní **async 1**, které odpovídá fyzickému portu AUX 0:

interface async 1
ip address 192.168.1.1 255.255.255.0
konfigurace IP adresy rozhraní
encapsulation ppp
mezi vzdáleným účastníkem a routerem bude jako linkový protokol (protokol spojové vrstvy) použit PPP
async mode dedicated
port bude vyhrazen výhradně pro provoz protokolu PPP
peer default ip address 192.168.1.2
protokol PPP bude automaticky vzdálenému účastníkovi přidělovat tuto adresu (musí být ve stejném IP subnetu jako adresa rozhraní **async 1**)

ppp authentication pap

protokol PPP bude před zahájením vlastní komunikace vyžadovat, aby se vzdálený účastník autentizoval protokolem PAP

Na závěr musíme v globálním konfiguračním režimu zadat uživatelské jméno a heslo, jímž se bude autentizovat vzdálený účastník:

username cnap password cisco

Poznámka:
připojení funguje i bez konfigurace autentizace (příkazů **ppp authentication pap** a **username-password**). Nicméně v reálných aplikacích je nezbytné autentizaci používat. Pro účely ladění je někdy výhodné nejprve ověřit funkčnost připojení bez autentizace a až po jejím ověření autentizaci doplnit.

Poznámka:
Na routeru, který má vestavěny asynchronní sériová rozhraní, může být číslo logického rozhraní **async** odpovídajícího portu AUX 0 posunuto. Např. u platformy Cisco 2509, vybavené osmi vestavěnými asynchronními sériovými rozhraními, je logické rozhraní odpovídající portu AUX 0 označeno jako **interface async 9**.

Konfigurace modemu připojeného ke směrovači

Modem, který bude připojen ke směrovači, je třeba předem nakonfigurovat, aby přijímal spojení. To lze provést následujícími AT příkazy:

AT&F
Obnovení původnách továrních nastavení (factory defaults)
ATS0=1
Po prvním zazvonění vyzvednout linku
AT&W
Konfiguraci zapsat do EEPROM

Toto nakonfigurování lze provést dvěma způsoby:

- Pomocí emulátoru terminálu za dočasného připojení modemu k PC
- Přímo z routeru použitím funkce "reverse telnet". Reverse telnet umožňuje zasílat uživatelem zapisované znaky přímo na některé z asynchronních sériových rozhraní směrovače a naopak vypisovat znaky, které přicházejí ze zařízení napojeného na toto rozhraní. Takovéto přímé propojení se realizuje ze směrovače pomocí příkazu **telnet** (uživatelský privilegovaný režim) na některé aktivní rozhraní směrovače a na číslo portu odpovídající číslu požadovaného asynchronního rozhraní. Poznamenejme, že rozhraní **async** do navázání spojení od vzdáleného účastníka aktivní není, telnet je třeba nasměrovat na některé z funkčních LAN nebo WAN rozhraní směrovače. Číslo portu se odvozuje z čísla požadovaného asynchronního rozhraní přičtením konstanty 2000. Tak například pro napojení na zařízení připojené na rozhraní **async 1** použijeme na routeru, jehož Ethernet rozhraní má adresu 192.168.0.1 a je aktivní příkaz
  telnet 192.168.0.1 2001

Po spojení již můžeme zadávat AT příkazy modemu. Nakonec spojení ukončíme stiskem

Ctrl+Shift+6
x

čímž bude relace Telnet přerušena. Definitivní ukončení relace poté provedeme příkazem **disconnect**.

Konfigurace klienta modemového připojení

Konfiguraci klienta popíšeme pro Microsoft Windows 2000. Na ostatních OS bude třeba realizovat obdobné kroky, pouze odlišným způsobem.

Nejprve je třeba instalovat ovladač modemu a svázat jej s příslušným (fyzickým nebo simulovaným) sériovým portem PC:

Start/Nastavení/Ovládací panely/Možnosti telefonu a modemu

V záložce *Modemy* je třeba stiskem tlačítka *Přidat* přidat nový ovladač pro použitý modem. Často je vhodné předejít autodetekci modemu zaškrtnutím volby *"Nerozpoznávat modem"* a pro experimentální účely volit ovladač standardního modemu, např. *„Standardní modem 14400 bps"*.
Nakonec je třeba vybrat port, na kterém je modem připojen a dokončit instalaci.

Poté, co máme nainstalován ovladač modemu, můžeme přikročit k vytvoření vlastního síťového přípojení:

Start/Nastavení/Síťová a telefonická připojení/Vytvořit nové připojení

Tím se spustí Průvodce, kde je postupně třeba zvolit
- volbu Telefonické připojení k privátní síti
- modem použitý pro přístup (vybrat pouze modem nakonfgurovaný při instalaci ovladače modemu v předchozím kroku)
- telefonní číslo modemu routeru
- zda bude připojení použitelné všemi uživateli stanice nebo pouze aktuálním uživatelem

Poté je třeba zadat jméno telefonického připojení, pod nímž bude připojení vidět uživatel buďto na ploše nebo alespoň ve složce *Start/Nastavení/Síťová a telefonická připojení*

V posledním kroku je již možné připojení vyzkoušet zadáním správného jména a hesla a stiskem tlačítka *Připojit*. Pokročilejší vlastnosti připojení můžeme případně konfigurovat stiskem tlačítka *Vlastnost*i. Připojovací dialog můžeme kdykoli přivolat z menu volbou

Start/Nastavení/Síťová a telefonická připojení

Poznámka:
Pokud toto nastavení není v operačním systému implicitní, je v podmínkách naší telefonní sítě nutné instruovat modem, aby nečekal před vytáčením na oznamovací tón obvyklý v USA. To lze provést vložením příkazu **ATX3** do inicializačního řetězce modemu nakonfigurovaném v příslušném operačním systému. S ohledem na typ ústředny je také třeba správně zvolit, zda bude použito tónové nebo pulsní volby.

Ladění

V případě potíží s připojováním je užitečné na směrovači sledovat proces navazování logického spojení PPP protokolu a proces autentizace. Výpis příslušných ladících zpráv se zapne z privilegovaného uživatelského režimu příkazy

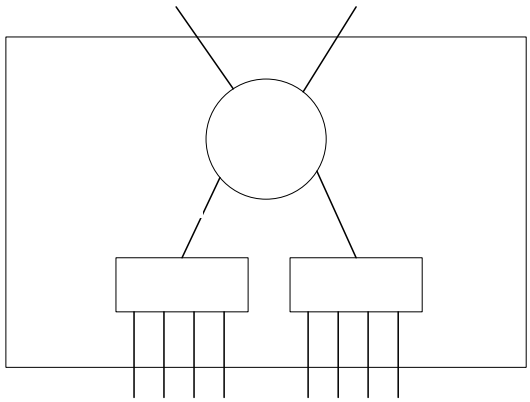
debug ppp negotiation
debug ppp autentization

Konfigurace L3 switche

Layer 3 (L3) switch je přepínač pracující na 2. i 3. vrstvě referenčního modelu OSI-RM. Jde v podstatě o kombinaci směrovače a přepínače, který v hardware zpracovává nejen přepínání na základě MAC adres, ale i směrování podle IP adres. Na L3 switch tak můžeme pohlížet z hledista funkce stejně jako na směrovač, který je však vzhledem k hardwarové podpoře směrování oproti klasickému směrovači výrazně rychlejší. Další popis se zaměří na L3 switch Cisco C3550.

Porty C3550 jsou implicitně nastaveny jako porty L2, takže mezi nimi probíhá přepínání rámců na základě MAC adresy. Pokud nejsou porty nakonfigurovýny jinak, patří všechny implicitně do VLAN 1. Kterýkoli z portů však lze přepnout příkazem **no switchport** do režimu směrovaného (L3) portu. Pak s nim můžeme pracovat stejně jako s rozhraním normálního směrovače. Konfigurujema tedy na něm IP adresu a L3 switch provádí směrování paketů mezi ním a všemi ostatními směrovanými porty a virtuálními rozhraními (viz dále)..

Přepínané (L2) porty mohou být seskupeny do nezávislých virtuálních sítí. L3 switch C3550 pak umí mezi těmito virtuálními sítěmi (a mezi případnými dalšími směrovanými porty) směrovat. Každý skupina L2 portů příslušející do téže virtuální sítě je z hlediska směrování reprezentována jedním logickým L3 rozhraním, označované podle čísla VLAN jako **interface VLAN n**. Pokud je to třeba, konfigurují se směrovací protokoly (a také statické cesty) stejně jako na běžném směrovači. Je pouze nutné explicitně povolit směrování protokolu IP v konfiguračním režimu příkazem **ip routing**. Schema směrování mezi virtuálními sítěmi a směrovanými porty pomocí L3 switche je názorně zobrazeno na obr. 2.



Obrázek 2

Směrování mezi VLAN 1 a 2 a mezi dvěma nezávislými směrovanými porty Fa0/20 a Fa0/21 lze nakonfigurovat pomocí následujících příkazů:

ip routing

interface FastEthernet 0/20

```
 no switchport
 ip address 192.168.1.1 255.255.255.0

interface FastEthernet 0/21
 no switchport
 ip address 192.168.2.1 255.255.255.0

interface range FastEthernet 0/1 - 4
 switchport mode access
 switchport access vlan 1

interface range FastEthernet 0/5 - 8
 switchport mode access
 switchport access vlan 2

interface VLAN 1
 ip address 192.168.3.1 255.255.255.0
 no shutdown

interface VLAN 2
 ip address 192.168.4.1 255.255.255.0
 no shutdown
```

Poznámka

Častou chybou konfigurace je, že virtuální rozhraní **interface VLAN n** není administrativně povoleno příkazem **no shutdown**.