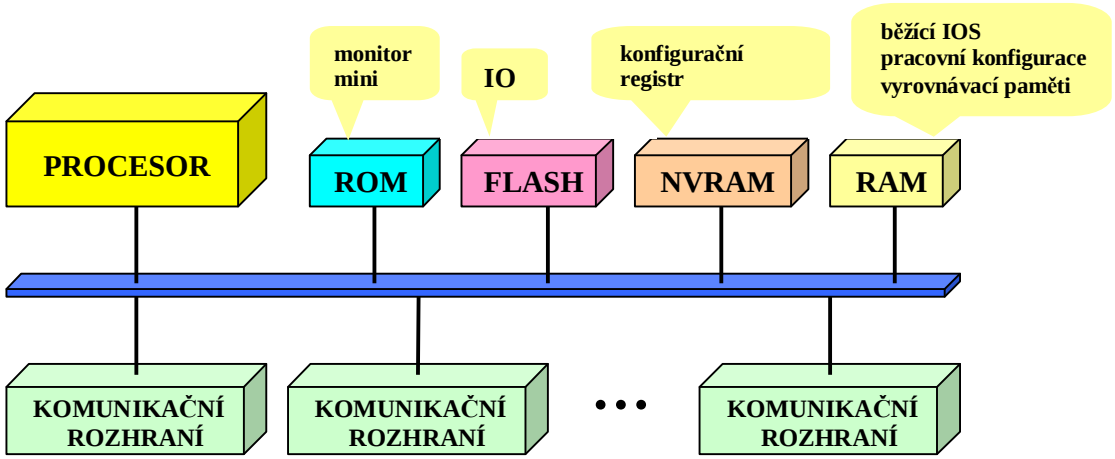
# Anatomie routerů CISCO

Vnitřní uspořádání routerů CISCO je velmi podobné uspořádání běžných univerzálních počítačů:




**Paměť ROM** obsahuje monitor a zjednodušenou verzi operačního systému IOS. **Monitor** (program, podobný ladícím programům běžných počítačů) je spuštěn automaticky po zapnutí počítače. V normální situaci monitor zkontroluje správnost funkce hardware, zavede operační systém IOS z paměti FLASH do paměti RAM (podobně jako zavaděč v PC zavede OS z disku) a aktivuje ho. V kritické situaci však monitor umožňuje přímé ovládání hardware počítače (čtení a modifikace paměti RAM, modifikace konfiguračního registru, zavedení mini-IOS z ROM a pod.). Tyto funce monitoru lze využít např. k instalaci IOS do paměti FLASH (aktualizace IOS nebo obnovení IOS po výměně paměti), smazání neznámého přístupového hesla nebo zavedení speciálního diagnostického software. Obsah paměti ROM nelze měnit.

**Paměť FLASH** uchovává svůj obsah i v době, kdy je vypnuto napájení a v routerech CISCO plní úlohu, kterou u běžných počítačů zastávají **diskové paměti** – je v ní totiž dlouhodobě uložen obraz operačního systému (image) IOS, který je po zapnutí routeru zaveden do operační paměti RAM a aktivován. IOS je do paměti FLASH zapsán již výrobcem, ale díky přepisovatelnosti paměti ho lze kdykoliv nahradit novou verzí (upgrade). Teoreticky lze do paměti FLASH zapsat také jakýkoliv jiný, pro daný hardware napsaný program (např. speciální diagnostické testy či alternativní operační systém).

**Paměť NVRAM** rovněž uchovává svůj obsah i v době, kdy je vypnuto napájení a používá se k dlouhodobému uložení **konfigurace routeru** (podobně jako např. v mobilních telefonech, modemech, TV přijímačích ...). Na rozdíl od paměti FLASH umožňuje paměť NVRAM mazání a zápis po slovech (u paměti FLASH se pracuje s bloky) a vyšší počet zápisových cyklů. V počítačích PC hraje podobnou roli paměť CMOS, napájená záložní baterií.

**Paměť RAM** slouží k uložení programu a dat během činnosti zařízení. Po zapnutí se do paměti RAM zavede operační systém IOS, který si po aktivaci vytvoří v paměti RAM další potřebné datové struktury (tabulky, seznamy, vyrovnávací paměti apod.). Obvykle se po spuštění routeru okopíruje do paměti RAM také konfigurace routeru z paměti NVRAM.

**Komunikační rozhraní** (Interfaces) umožňují routeru připojit se k jednotlivým segmentům LAN nebo propojit se pomocí různých technologií WAN s dalšími routery v síti. Komunikačních rozhraní je v routeru obvykle několik; výběrem vhodného modelu routeru či instalací výměnných modulů lze router přizpůsobit požadavkům (dostupná jsou např. rozhraní Ethernet, HDLC, FDDI, ISDN, ATM). To je samozřejmě žádaná vlastnost, ale na druhé straně tato variabilita značně komplikuje IOS (velký počet příkazů) a konfiguraci routeru (každé rozhraní má specifické parametry).

# CLI (Command Line Interface)

CLI je uživatelské rozhraní operačního systému IOS, umožňující konfiguraci, monitorování a údržbu zařízení CISCO. Podobně jako v jiných operačních systémech komunikuje uživatel se systémem pomocí řádkových příkazů, zadávaných z klávesnice řídícího terminálu (konsoly), přenášených po síti ze vzdáleného počítače (virtuální terminály) nebo zapsaných předem do souboru (konfigurace uložená v NVRAM nebo na vzdáleném počítači).

## Připojení a nastavení terminálu

Sériový port terminálu (resp. počítače s terminálovým emulátorem) se připojuje k zásuvce, označené jako CONSOLE (CON). U terminálů a osobních počítačů se obvykle používá rozhraní RS-232, zatím co u routerů CISCO je použit 8-vývodový konektor RJ-45. Pro připojení routeru je proto nutné použít speciální adaptér z RS-232 na 8-vývodový konektor RJ-45, který se dodává s routerem (pro 9- nebo 25-vývodový konektor). Navíc musí být propojovací kabel „přetočený“ (Roll-Ower), tj. vývody konektorů RJ-45 musí být propojeny zrcadlově (1-8, 2-7, 3-6, 4-5, 5-4, 6-3, 7-2, 8-1). Také tento kabel se dodává jako příslušenství routeru.Terminál (resp. terminálový emulátor) musí mít nastaveny následující parametry:

| *parametr* | *nastavení* | *poznámka* |
|---|---|---|
| typ terminálu: | VT100 | nejvhodnější, jinak nemusí fungovat všechny klávesy |
| přenosová rychlost: | 9600 Bd | pokud přenosová rychlost CON portu nebyla změněna |
| počet datových bitů:<br>parita:<br>počet stop-bitů: | 8<br>bez parity<br>1 | zkráceně se označuje obvykle jako 8N1 |
| řízení toku: | vypnuto | pokud nejde vypnout, tak hardwarové (RTS/CTS) |

## Zapnutí a zavedení IOS

Činnost monitoru routeru po zapnutí napájení závisí na na obsahu tzv. **konfiguračního registru**. Tímto názvem se označuje jedno 16-bitové slovo paměti NVRAM. Jeho obsah např. určuje, odkud se bude zavádět IOS, zda a odkud se bude načítat konfigurace, jakou rychlostí bude router komunikovat s terminálem (1200 až 9600 Bd) a další údaje. Při standardním nastavení konfiguračního registru na hodnotu **0x2102** se po zapnutí routeru se IOS zavede z paměti FLASH, konfigurace se načte z paměti NVRAM a přenosová rychlost portu COM je nastavena na 9600 Bd.

Během zavádění IOS se na obrazovce připojeného terminálu vypisují některé informace o systému. Pokud router dosud nebyl nakonfigurován (nebo uživatel příkazem *erase startup-config* vymazal obsah paměti NVRAM), objeví se po zavedení IOS dotaz, zda chcete spustit konfigurační menu. Pokud tuto nabídku odmítnete nebo pokud byla automaticky zavedena konfigurace z NVRAM, vypíše systém po stisku klávesy ENTER prompt-řetězec, skládající se ze jména routeru (hostname) a znaku > (implicitně **Router>** ). Od tohoto okamžiku je CLI aktivní a routeru lze zadávat příkazy.

## Nápověda

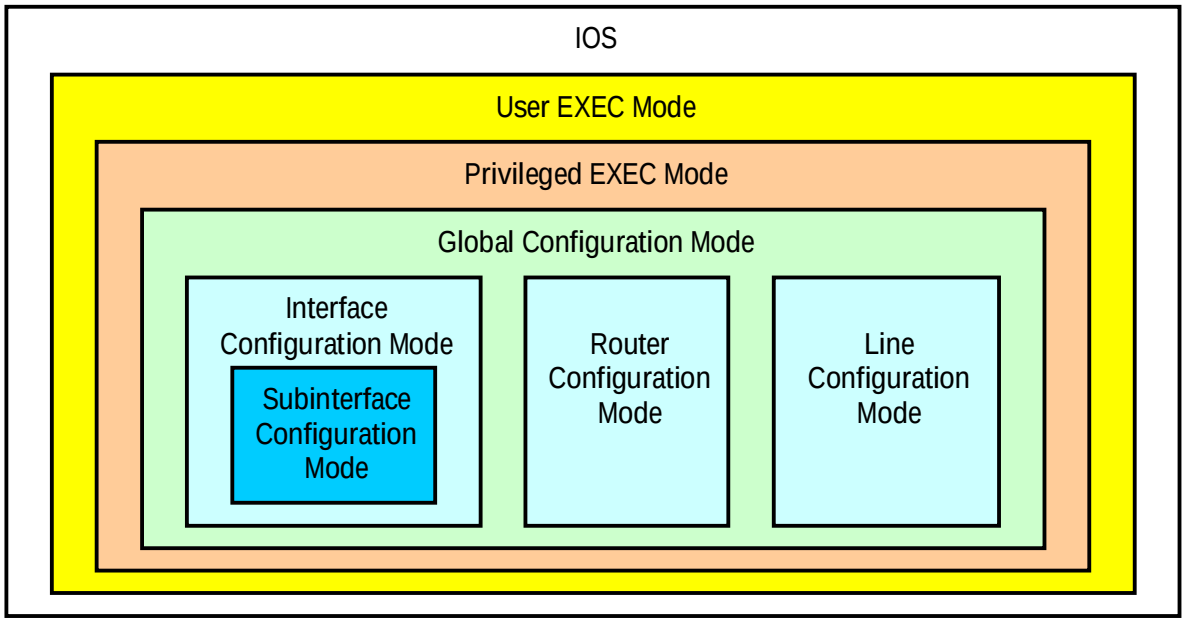
Uživatel může získat nápovědu několika způsoby:

- podle vzhledu **prompt** řetězce lze zjistit, který **příkazový mod** (viz dále) je právě nastaven
- příkaz **?** (otazník) vypíše seznam všech příkazů dostupných v aktuálním modu
- příkaz ve tvaru **abc?** vypíše seznam příkazů, začínajících řetězcem **abc**
- znak **?** v pozici argumentu příkazu vypíše seznam argumentů příkazu (např. **show ?**)

Kromě nápovědy systém usnadňuje práci také automatickým doplňováním nedopsaných klíčových slov (např. příkazů). Pokud je nedopsané klíčové slovo jednoznačně určeno, není nutné ho dopsat celé. Tak např. místo **copy running-config startup-config** lze napsat pouze **copy run start**, místo **configure terminal** pouze **conf t**, atd. Pokud má některý argument implicitní hodnotu, je uživatel informován výpisem této hodnoty v hranatých závorkách (např. **[yes]** )

## Příkazové mody

Přístup uživatelů je rozvrstven do několika úrovní, mezi kterými může uživatel přecházet speciálními příkazy:




Přestože lze přístup do User EXEC modu telnetem zabezpečit heslem, jsou příkazy kritické pro bezpečnost dostupné až v **Privileged EXEC modu**. Přístup do tohoto modu lze zabezpečit zvláštním heslem (obdoba uživatele root v UNIXu). Do konfiguračních modů lze vstoupit pouze z **Privileged EXEC modu**. Přechody mezi jednotlivými mody jsou popsány v následující tabulce:

| *mod* | *vyvolání* | *prompt* | *ukončení* |
|---|---|---|---|
| User EXEC | přihlášením uživatele (login) | host > | příkazem logout |
| Privileged EXEC | z User EXEC modu příkazem enable | Host# | příkazem disable |
| Global Configuration | z Privileged EXEC modu příkazem configure terminal | host (config)# | příkazem exit nebo end nebo CTRL+Z (do Privil. EXEC modu) |
| Interface Configuration | z Global Configuration modu specifikací rozhraní přikazem interface | host (config-if)# | příkazem exit (do Global Conf. modu), příkazem end nebo CTRL+Z (do Privil. EXEC modu) |
| Subinterface Configuration | z Interface Configuration modu specifikací sub-rozhraní příkazem interface | host (config-subif)# | příkazem exit (do Global Conf. modu), příkazem end nebo CTRL+Z (do Privil. EXEC modu) |
| Router Configuration | z Global Configuration modu specifikací rozhraní přikazem router | host (config-router)# | příkazem exit (do Global Conf. modu), příkazem end nebo CTRL+Z (do Privil. EXEC modu) |
| Router Configuration | z Global Configuration modu specifikací rozhraní přikazem line | host (config-line)# | příkazem exit (do Global Conf. modu), příkazem end nebo CTRL+Z (do Privil. EXEC modu) |

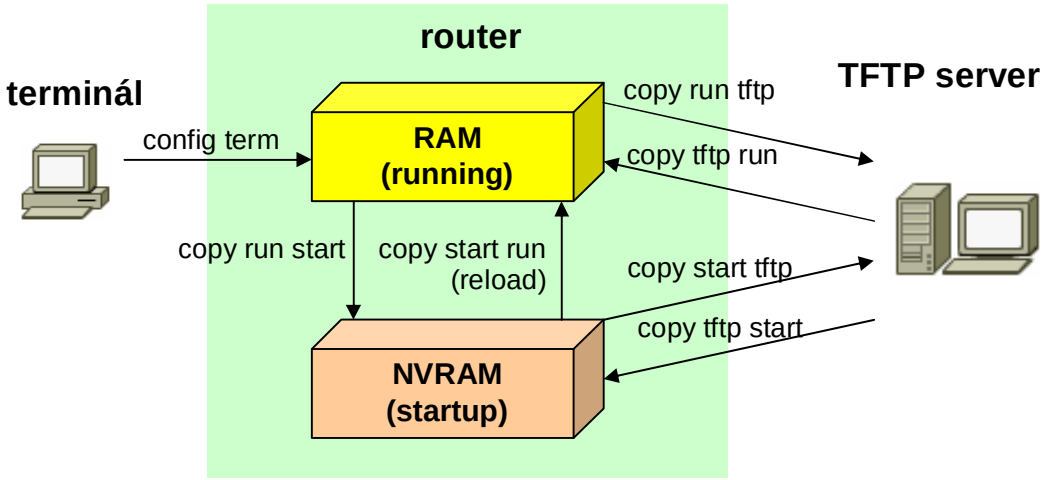
## ROM monitor

ROM monitor je software, který je trvale uložen v paměti ROM. Jeho základní funkcí je kontrola hardware a zavedení operačního systému po zapnutí routeru, ale má i další primitivní funkce (čtení a modifikace obsahu paměti, spuštění programu, načtení IOS do paměti FLASH a pod.). Postup pro vyvolání monitoru je následující:

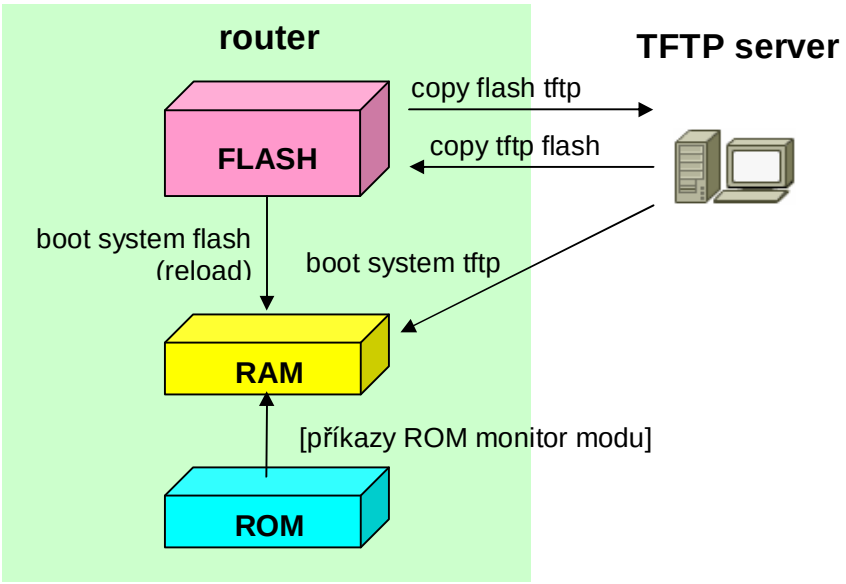
| *vyvolání* | *prompt* | *ukončení* |
|---|---|---|
| 1. restartovat systém (vypnutím a zapnutím napájení);<br>2. po cca 20 sec přerušit zavádění IOS (z terminálu připojeného na CON port odeslat signál BREAK) | ><br>nebo boot><br>nebo rommon> *) | příkazem continue nebo C lze pokračovat v normálním procesu zavádění IOS *) |

*) V routerech CISCO byly postupem času používány různé verze ROM monitorů, jejichž chování a ovládání se liší; podrobnosti hledejte v doprovodné dokumentaci dodané s routerem.

# Schéma možností manipulace s konfigurací:




# Schéma možností manipulace s IOS:



# Základní příkazy

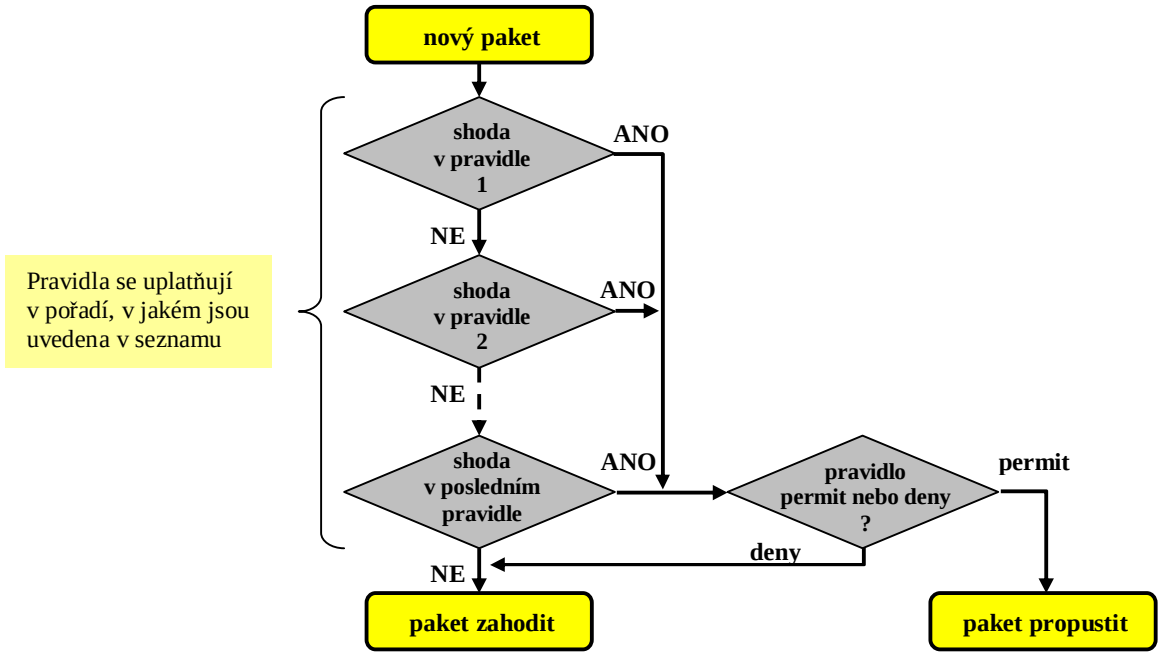
| řádková edice a historie příkazů | |
|---|---|
| kurzor zpět o znak | ← nebo CTRL+B |
| kurzor vpřed o znak | → nebo CTRL+F |
| kurzor na začátek řádku | CTRL+A |
| kurzor na konec řádku | CTRL+E |
| automatické dokončení příkazu | TAB |
| nový výpis příkazového řádku | CTRL+L |
| vyvolání předešlého příkazu z historie | ↑ nebo CTRL+P |
| vyvolání následujícího příkazu z historie | ↓ nebo CTRL+N |
| výpis paměti historie příkazů | show history |
| **základní operace** | |
| nové zavedení systému příkazem<br>nové zavedení systému krátkodobým vypnutím napájení | reload<br>power OFF, po cca 5 sec power ON |
| přechod do privilegovaného modu | enable |
| návrat do uživatelského modu | disable |
| přechod z konfiguračních modů do privilegovaného modu | end nebo CTRL+Z |
| návrat zpět do výchozího modu (odhlášení uživatele) | exit |
| **nastavení konfiguračního registru** | |
| diagnostický mod<br>zavést IOS z ROM, konfiguraci z NVRAM<br>zavést IOS z FLASH, konfiguraci z NVRAM<br>zavést IOS z ROM, konfiguraci v NVRAM ignorovat<br>zavést IOS z FLASH, konfiguraci v NVRAM ignorovat | config-reg 0x2000<br>config-reg 0x2101<br>config-reg 0x2102<br>config-reg 0x2141<br>config-reg 0x2142 |
| **zobrazení informací o routeru** | |
| verze IOS | show version |
| aktuální pracovní konfigurace (RAM) | show running-config |
| aktuální záložní konfigurace (NVRAM) | show startup-config |
| soubor obsahující IOS a velikost paměti FLASH | show flash |
| využití procesoru | show processes cpu |
| **Cisco Discovery Protocol** | |
| zjištění přímo připojených sousedů | show cdp neighbor |
| zjištění rozhraní s aktivním protokolem CDP | show cdp interface |
| zobrazení detailních informací o zvoleném sousedovi | show cdp entry P1R1 |
| deaktivace CDP pro celý router | no cdp run |
| deaktivace CDP ve zvoleném rozhraní | no cdp enable |
| nastavení periody zasílání CDP informací | cdp timer 120 |
| nastavení doby držení CDP informací o sousedech | cdp holdtime 240 |
| **manipulace s IOS** | |
| uložení IOS z paměti FLASH na TFTP server<br>přepis IOS z TFTP serveru do paměti FLASH<br>zavedení IOS z paměti FLASH<br>zavedení IOS z TFTP serveru | copy flash tftp<br>copy tftp flash<br>boot system flash [filename]<br>boot system tftp [filename] |
| **manipulace s konfigurací routeru** | |
| smazání záložní konfigurace (NVRAM) | erase startup-config |
| přepis záložní konfigurace (NVRAM) do pracovní (RAM)<br>přepis pracovní konfigurace (RAM) do záložní (NVRAM)<br>uložení pracovní konfigurace (RAM) na TFTP server<br>načtení pracovní konfigurace (RAM) z TFTP serveru | copy startup-config running-config<br>copy running-config startup-config<br>copy running-config tftp<br>copy tftp running-config |

| globální konfigurace | |
|---|---|
| změna pracovní konfigurace (RAM) z terminálu | configure terminal |
| nastavení jména routeru | hostname HOST |
| nastavení času (3. duben 2002, 10 hod, 21 min, 5 sec) | clock set 10:21:05 april 3 2002 |
| nastavení hesla pro CON port | line console 0<br>login<br>password CCCC |
| nastavení hesla pro virtuální terminály | line vty 0 4<br>login<br>password TTTT |
| nastavení hesla pro privilegovaný mod | enable secret SSSS (uloženo šifrovaně) nebo<br>enable password PPPP (uloženo nešifrovaně!) |
| aktivace HTTP serveru<br>umožňuje správu routeru přes web (jméno uživatele root) | ip http server |
| konfigurace seriového rozhraní | |
| zjištění typu seriového rozhraní (DTE nebo DCE?) | show controller serial 1 |
| přechod z Global Configuration mode<br>aktivace rozhraní<br><br>nastavení hodin (jen DCE)<br>nastavení šířky pásma (kb/s) | interface serial 1<br>ip address 157.89.1.3 255.255.0.0<br>no shutdown<br>clock rate 64000<br>bandwidth 64 |
| kontrola nastavení | show interface serial 1<br>show ip interface brief |
| konfigurace rozhraní ethernet | |
| přechod z Global Configuration mode<br>aktivace rozhraní | interface ethernet 0<br>ip address 208.1.1.4 255.255.255.0<br>no shutdown |
| kontrola nastavení (v privileg. modu) | show interface ethernet 0<br>show ip interface brief |
| TCP/IP | |
| získání IP adresy protokolem DHCP (pouze ethernet) | interface ethernet 0<br>ip address dhcp |
| zákaz IP směrování (implicitně povoleno) | no ip routing |
| konfigurace RIP protokolu | router rip<br>network 157.89.0.0<br>network 208.1.1.0 |
| konfigurace IGRP protokolu<br>(autonomní systém 200) | router igrp 200<br>network 157.89.0.0<br>network 208.1.1.0 |
| zobrazení směrovací tabulky | show ip route |
| ladění RIP | debug ip rip |
| ladění IGRP | debug ip igrp events<br>debug ip igrp transactions |
| deaktivace ladění | no debug |
| obnovení přístupu při neznámém hesle (password recovery) | |
| vyvolání ROM Monitor modu<br>změna nastavení konfiguračního registru<br>zavedení IOS | power OFF..... ON, do 60 sec BREAK<br>o/r 0x2142<br>i |
| přechod do privilegovaného modu<br>okopírování záložní konfigurace do RAM<br>přechod do modu globální konfigurace<br>změna hesla<br>obnovení obsahu konfiguračního registru<br>návrat do privilegovaného modu<br>uložení opravené konfigurace | > enable<br># copy start run<br># config term<br>(config)# enable secret HESLO<br>(config)# config-reg 0x2102<br>(config)# exit<br># copy run start |

# Přístupové seznamy

Přístupové seznamy (Access List, ACL) umožňují řídit průchod paketů rozhraním směrovače. Přístupový seznam obsahuje množinu pravidel, podle kterých lze přesně stanoveným postupem určit, zda má rozhraní nově doručený paket propustit dál nebo ne.

**Algoritmus filtrace podle ACL (vývojový diagram):**




V konfiguraci směrovače lze definovat řadu přístupových seznamů, označených pořadovými čísly nebo jmény. Seznamy jsou nezávislé na rozhraních, tj. mohou být definovány bez ohledu na to, zda jsou použity některým rozhraním k filtraci. Vazba mezi rozhraním a seznamem vzniká **přiřazením seznamu k rozhraní**.

Ke každému rozhraní lze přiřadit jeden **vstupní** a jeden **výstupní** seznam. Podle vstupního seznamu (**in**) se filtrují pakety, přicházející z externích uzlů (host) do směrovače, podle výstupního seznamu (**out**) se filtrují pakety, které mají být odeslány ze směrovače do externích uzlů.

Pokud k rozhraní **není** přiřazen žádný přístupový seznam, propustí rozhraní **všechny pakety**!

| číslování ACL | |
|---|---|
| <1-99> | standard IP ACL |
| <100-199> | extended IP ACL |
| <200-299> | Protocol type-code ACL |
| <300-399> | DECnet ACL |
| <400-499> | XNS standard ACL |
| <500-599> | XNS extended ACL |
| <600-699> | Appletalk ACL |
| <700-799> | 48-bit MAC address ACL |
| <800-899> | IPX standard ACL |
| <900-999> | IPX extended ACL |
| <1000-1099> | IPX SAP ACL |
| <1100-1199> | Extended 48-bit MAC address ACL |
| <1200-1299> | IPX summary address ACL |

| přístupové seznamy (ACL) | |
|---|---|
| Standard IP ACL = 1-99, filtrace podle Source | |
| zablokuj šíření paketů z podsítě 200.1.1.0<br>255.255.255.0 do rozhraní ethernet 0 | access-list 1 deny 200.1.1.0 0.0.0.255<br>access-list 1 permit any<br>interface e 0<br>ip access-group 1 out (výstupní filtr) |
| Extended IP ACL = 100-199, filtrace podle Source & Dest & port & protocol .... | |
| hostovi 10.1.1.1 z rozhraní serial 1<br>povol přístup k hostovi 2.2.2.2 telnetem<br>(využívá se implicitní deny) | access-list 101 permit tcp host 10.1.1.1 host 2.2.2.2 eq 23<br>interface s 1<br>ip access-group 101 in (vstupní filtr) |
| podsíti 3.3.0.0 255.255.0.0 z rozhraní ethernet 0<br>zablokuj přístup kamkoliv webem | access-list 102 deny tcp 3.3.0.0 0.0.255.255 any eq 80<br>access-list 102 permit ip any any<br>interface e 0<br>ip access-group 102 in (vstupní filtr) |
| Standard IPX ACL = 800-899, filtrace podle Source & Dest | |
| blokuj síti 7A přístup do sítě 6000<br>povol vše ostatní<br>navaž ACL na rozhraní eth 0 | access-list 800 deny 7A 6000<br>access-list 800 permit –1<br>interface e 0<br>ipx access-group 800 out (výstupní filtr) |
| Extended IPX ACL = 900-999, filtrace podle Source & Dest + Socket, ... | |
| blokuj SAP na socketu 3378<br>povol vše ostatní<br>navaž ACL na rozhraní e 0 | access-list 900 deny sap any 3378 –1<br>access-list 900 permit sap any all –1<br>interface e 0<br>ipx access-group 900 out (výstupní filtr) |
| IPX SAP filtry = 1000-1099, filtrace podle Source, Port, Service Name | |
| blokuj SAP ze serveru 1<br>povol vše ostatní<br>navaž ACL na rozhraní e 0<br>potlač vstup<br>nebo výstup | access-list 1000 deny 7A.0000.0000.0001 4<br>access-list 1000 permit –1<br>interface e 0<br>ipx input-sap-filter 1000 (vstupní filtr)<br>ipx output-sap-filter 1000 (výstupní filtr) |
| Appletalk ACL = 600-699, filtrace dle Cable range a Zone | |
| odmítni Cable Range 1000-1999<br>povol ostatní Cable Range<br>odmítni zónu Workgroup1<br>povol ostatní zóny<br>navaž ACL na rozhraní e 0 | access-list 600 deny cable-range 1000-1999<br>access-list 600 permit other-access<br>access-list 600 deny zone Workgroup1<br>access-list 600 permit additional-zones<br>interface e 0<br>appletalk access-group 600 (implicitně výstupní filtr) |
| pojmenované IP a IPX ACL | |
| podobné jako nepojmenované, ale při změnách<br>není nutné vymazat a znovu vytvořit celý seznam<br>(lze editovat jednotlivé řádky seznamu) | ip access-list standard cool_list<br>deny 1.1.1.1<br>permit any<br>interface e 0<br>ip access-group cool_list in (vstupní filtr) |
| informace o ACL | |
| přehled konfigurace ACL | show running-config |
| přehled použití ACL<br>zobrazí, ve kterých rozhraních jsou použity které ACL | show { ip \| ipx \| appletalk } interface e 0 |
| přehled přístupových seznamů<br>vypíše všechny ACL (specifikovanou třídu ACL);<br>u každého pravidla oznámí aktuální počet paketů,<br>u nichž došlo při porovnávání ke shodě (match) | show access-lists<br>show { ip \| ipx \| appletalk } access-lists |

# Další příkazy

| DHCP server | | |
|---|---|---|
| aktivace serveru DHCP<br>adresy se přidělují z intervalu 10.1.1.0 - 10.1.1.255<br>adresa se přiděluje na na 0 dní, 0 hodin, 5 minut | ip dhcp pool p1<br>network 10.1.1.0 255.255.255.0<br>lease 0 0 5 | |
| **PPP** | | |
| povolení provozu PPP na rozhrani<br>a volba typu zapouzdření<br>povolení a volba typu autentizace (CHAP, PAP)<br>specifikace jména pro CHAP (impl. hostname)<br>specifikace hesla pro CHAP (impl. enable password)<br>specifikace jména uživatele pro PAP<br>vytvoření záznamu pro přihlášení odjinud<br>sledování procesu autentizace | interface serial 0<br>encapsulation ppp<br>ppp authentication chap<br>ppp chap hostname HOST<br>ppp chap password HESLO<br>ppp pap sent-username JMENO<br>username XHOST password XHESLO<br>debug ppp authentication | |
| **X.25** | | |
| povolení provozu X.25 na rozhraní<br>volba typu rozhraní a zapouzdření<br>specifikace místní adresy x121<br>nastavení mapování IP adres na X121 adresy<br>a povolení broadcastu | interface serial 0<br>encapsulation x25 dce ietf<br>x25 address 301222333444<br>x25 map ip 200.1.1.1 301222333444 broadcast | |
| nastavení velikosti příchozích paketů<br>nastavení velikosti odchozích paketů<br>nastavení velikosti okna pro příchozí pakety<br>nastavení velikosti okna pro odchozí pakety | x25 ips 512<br>x25 ops 512<br>x25 win 7<br>x25 wout 7 | na obou stranách spoje<br>musí být nastavení stejné |
| **Frame Relay** | | |
| povolení provozu FR na rozhrani<br>a volba typu zapouzdření<br>specifikace typu LMI (od verze 11.2 autosenze)<br>nastavení lokálního DLCI (nefunguje v LMI)<br>mapování IP na lokální DLCI (když nefunguje RARP)<br>nastavení periody paketů pro udržení spojení | interface serial 0<br>encapsulation frame-relay ietf<br>frame-relay lmi-type ansi<br>frame-relay local-dlci 100<br>frame-relay map ip 3.3.3.3 100 broadcast<br>keepalive 10 | |
| výpis statistiky PVC<br>výpis směrovacích map FR<br>výpis informací o LMI | show frame-relay pvc<br>show frame-relay map<br>show frame-relay lmi | |
| **nastavení routeru jako Frame Relay ústředny** | | |
| aktivace režimu ústředny FR<br>nastavení rozhraní serial 0<br>povolení provozu FR a volba typu zapouzdření<br><br>specifikace logického typu rozhraní DCE<br>nastavení hodin<br>pakety z s0 (DLCI=21) do s1 (DLCI=20)<br>nastavení rozhraní serial 1<br>povolení provozu FR a volba typu zapouzdření<br><br>specifikace typu rozhraní DCE<br>nastavení hodin<br>pakety z s1 (DLCI=20) do s0 (DLCI=21) | frame-relay switching<br>interface serial 0<br>no ip address<br>encapsulation frame-relay ietf<br>frame-relay intf-type dce<br>clockrate 64000<br>frame-relay route 21 interface serial 1 20<br>interface serial 1<br>no ip address<br>encapsulation frame-relay ietf<br>frame-relay intf-type dce<br>clockrate 64000<br>frame-relay route 20 interface serial 0 21 | |

| IPX/SPX | |
|---|---|
| povolení provozu IPX (implicitně zakázán)<br>povolení dělení zátěže (Load Balancing) | ipx routing<br>ipx maximum-paths 6 |
| povolení IPX provozu (impl. zakázán) a směrování<br>... s implicitním zapouzdřením (e=802.3, s=HDLC)<br>... se zapouzdřením 802.3<br>... se zapouzdřením 802.2<br>... se zapouzdřením Ethernet II<br>... se zapouzdřením SNAP | interface serial 0<br>ipx network 4A<br>ipx network 4A encap novell-ether<br>ipx network 4A encap sap<br>ipx network 4A encap arpa<br>ipx network 4A encap snap |
| výpis směrovací tabulky IPX<br>kontrola IPX adresy rozhraní<br>výpis tabulky SAP<br>výpis provozní statistiky | show ipx route<br>show ipx interface<br>show ipx servers<br>show ipx traffic |
| ladění IPX-RIP<br>ladění SAP | debug ipx routing activity<br>debug ipx sap |
| Appletalk | |
| povolení provozu Appletalk (implicitně zakázán)<br>volba jiného směrovacího protokolu (impl. RTMP)<br>přiřazení Cable Range k rozhraní<br>přiřazení zóny k rozhraní<br>uvedení rozhraní do vyhledávacího režimu<br>(automatické zjištění Cable Range a zóny) | appletalk routing<br>appletalk protocol eigrp<br>appletalk cable-range 1000-1999<br>appletalk zone Workgroup1<br>appletalk cable-range 0-0<br>nebo appletalk discovery |
| kontrola adresy appletalk rozhraní<br>výpis směrovací tabulky Appletalk<br>výpis zón Appletalk<br>výpis nastavení Appletalk | show appletalk interface serial 0<br>show appletalk routing<br>show appletalk zones<br>show appletalk globals |
| sledování událostí appletalk v reálném čase<br>ladění RTMP | debug appletalk events<br>debug appletalk routing |

# Příloha A. Break Key sekvence

Break Key sekvenci terminálu potřebujete znát např. pro obnovení přístupu při ztrátě hesla (Password Recovery Procedure) a v dalších sice málo obvyklých, ale zato velmi nepříjemných situacích. Pokud totiž tuto sekvenci pro vámi používaný terminálový emulátor neznáte, nedokážete přejít do **ROM monitor** modu.

### Co vlastně je Break Key Sekvence?

U klasické dálnopisné linky bylo vedení v klidovém stavu pod proudem (stav linky v okamžiku přenosu STOP-bitů) a pouze během přenosu značky se proudový okruh krátkodobě přerušoval (minimálně po dobu přenosu START-bitu). Při přenosu značky se vždy nejprve vyslal START-bit, pak datové bity (max. 8 bitů) a paritní bit (jeden bit). Po každé značce vždy následuje alespoň krátce klidový stav, umožňující přijímači připravit se na příjem další značky (1 až 2 STOP-bity). Pak vedení zůstalo v klidovém stavu (pod porudem), dokud vysílač nezahájil vysílání další značky. Při správné funkci vysílače tedy nemohlo dojít k přerušení proudového okruhu na dobu delší než **10 bitových intervalů**. Souvislé přerušení proudového okruhu na delší dobu (**BREAK**) tedy byl příznakem poruchy – obvykle přerušení vedení.

Komunikační řadiče UART, které jsou elektronickou obdobou dálnopisného přijímače a vysílače, mají nejen vestavěnou detekci tohoto stavu, ale dokáží také signál **Break** generovat. Obvykle je tento signál definován jako uvedení výstupu do úrovně start-bitu na dobu potřebnou k přenesení dvou značek. U většiny terminálů a terminálových emulátorů existuje kombinace či posloupnost kláves, kterou lze odeslání signálu **Break** vyvolat. Této kombinaci (posloupnosti) kláves se říká **Break Key sekvence**.

V následující tabulce najdete Break Key sekvence pro nejčastěji používané terminálové emulátory a operační systémy:

| *software* | *platforma* | *operační systém* | *kombinace (posloupnost) kláves* |
|---|---|---|---|
| Telix | IBM Compatible | DOS | Ctrl-End |
| ProComm Plus | IBM Compatible | DOS, Windows | Alt-b |
| MicroPhone Pro | IBM Compatible | Windows | Ctrl-Break |
| Teraterm | IBM Compatible | Windows | Alt-b |
| Terminal | IBM Compatible | Windows | Break / Ctrl-Break |
| Windows NT | IBM Compatible | Windows | Break-F5 / Shift-F5 / Shift-6 Shift-4 Shift-b (^$B) |
| Hyperterminal v.595160 | IBM Compatible | Windows 95 | Ctrl-F6-Break |
| Hyperterminal | IBM Compatible | Windows NT/2000/XP | Ctrl-Break |
| Minicom | IBM Compatible | Linux | Ctrl-a f |
| Kermit | Sun Workstation | UNIX | Ctrl-\l / Ctrl-\b |
| Tip | Sun Workstation | UNIX | Ctrl-], pak Break nebo Ctrl-c / ~# |
| Z-TERMINAL | Mac | Apple | Command-b |
| Telnet to Cisco | – | – | Ctrl-] |
| VT 100 Emulation | Data General | – | F16 |

POZNÁMKY:

1. Pokud chcete vyvolat ROM monitor, musíte být připojeni na konsolový port routeru (CONSOLE, CON). Přídavný port routeru (AUXILIARY, AUX) není během zavádění systému aktivní a proto odeslání Break-sekvence na tento port nemá žádný efekt!
2. Některé verze Windows NT měly v programu Hyperterminal chybu, způsobující nefunkčnost Break Key sekvence (v tomto případě doporučujeme upgrade OS nebo alespoň aplikace Hyperterminal).

### Simulace signálu Break

Tento postup je sice dosti komplikovaný, ale může se vám hodit, pokud terminál či emulátor funkci **Break** nepodporuje, pokud nemáte k dispozici potřebnou dokumentaci a proto nevíte, jak se signál **Break** generuje, nebo pokud generace signálu **Break** z nějakých důvodů nefunguje.

Trik je založen na tom, že při 8-násobném zpomalení vysílače UART (z 9600 na 1200 Bd) se značka pro znak **mezera** jeví přijímači UART jako signál **Break**, odeslaný rychlostí 9600 Bd. Postup je následující:

1. Připojte se k routeru s následujícím nastavením parametrů spoje:

   Baud Rate 1200
   8 data bits, No parity, 1 stop bit (8N1)
   No Flow Control

   Od této chvíle neuvidíte na vaší obrazovce smysluplný text, ale to je ***normální!***

2. Restartujte router vypnutím a zapnutím napájení. Po uplynutí cca 15 sekund několikrát stiskněte klávesu ***mezera***.

3. Odpojte terminál (emulátor), upravte jeho parametry zpět na standardní nastavení (rychlost 9600Bd) a znovu ho připojte.

Pokud vše proběhlo správně, je router v ROM-monitor modu a můžete provádět příkazy monitoru.

Někdy lze potřebného efektu dosáhnout mnohem jednodušeji. Propojte CON port routeru se seriovým portem terminálu nebo PC při vypnutých zařízeních. Pak nejprve zapněte router a teprve po dalších cca 30 sekundách zapněte počítač. U některých počítačů router naběhne do monitoru i tímto postupem.

Uvědomte si, že popsaná situace může nastat i **nechtěně**. Proto jestliže se na terminálu po zapnutí routeru neobjeví obvyklé zprávy o zavádění IOS, prompt má neobvyklý tvar (např. pouze znak >) a router nereaguje na příkazy, komunikujete pravděpodobně místo s IOS s monitorem. Zkuste napsat příkaz **i** (zavedení IOS) nebo router restartujte vypnutím a zapnutím napájení.

# Příloha B. Terminálový emulátor v OS Linux

V OS Linux je standardně dostupný terminálový emulátor **minicom**. Obvykle je nainstalován při instalaci systému a proto není nutné ho instalovat samostatně.

Při prvním použití programu obvykle nezkušený uživatel narazí na problém s implicitní konfiguraci. Pokud program **minicom** spouštíte poprvé od instalace systému, musíte ho spustit s volbou **–s** (tj. příkazem **minicom -s**). V tomto případě vám automaticky naběhne menu pro konfiguraci.

Nejprve v submenu **Serial Port Setup** zkontrolujte a případně upravte nastavení portu. Zařízení **/dev/modem** je nutné změnit na zařízení sériového portu, kterým se budete připojovat k routeru (u PC odpovídá portu COM1 zařízení **/dev/ttyS0** a portu COM2 zařízení **/dev/ttyS1**), např.

```
Serial Device         : /dev/ttyS1
```

Dále musíte nastavit následující parametry:

```
Bps/Par/Bits          : 9600 8N1
Hardware Flow Control : no
Software Flow Control : no
```

Pak pomocí submenu **Save setup as dfl** uložte konfiguraci jako implicitní, aby při dalším spuštění programu již nebylo nutné volbu **-s** používat.

Pokud pracujete pouze se sériovou linkou (bez modemu), můžete při dalším použití emulátor spouštět s volbou **–o** (tj. příkazem **minicom -o**). V tomto případě se program nepokusí inicializovat modem a naběhne proto rychleji. Podobně pro ukončení práce s emulátorem je vhodné používat sekvenci **CTRL+A, Q**, která ukončí program bez resetování modemu.

Všechny speciální příkazy emulátoru začínají kombinací **CTRL+A**, po které se stiskne odpovídající písmeno příkazu – např. nápovědu získáte sekvencí **CTRL+A, Z**. Nejčastěji používané sekvence jsou uvedeny v následující tabulce:

| | |
|---|---|
| CTRL+A, Z | vyvolání nápovědy;<br>nápověda má podobu menu, ze kterého lze vyvolat ostatní funkce |
| CTRL+A, F | odeslání signálu BREAK (pro přerušení bootu) |
| CTRL+A, L | zapnutí nebo vypnutí opisu obrazovky do souboru (Log);<br>umožňuje např. uložit výpis konfigurace routeru do souboru |
| CTRL+A, W | zapnutí nebo vypnutí lámání řádků (Line Wrap) |
| CTRL+A, C | smazání obrazovky (Clear Screen) |
| CTRL+A, Q | ukončení práce (Quit) bez resetu modemu |

Pokud nebyl program **minicom** korektně ukončen, může v adresáři **/var/lock** zůstat zámek (lock), bránící vícenásobnému spuštění programu. V tomto případě program **minicom** nejde spustit a je nutné nejprve zámek smazat.

# Příloha C. Nastavení TCP/IP v OS Linux

Při práci v laboratoři CNA se obvykle nepoužívá DHCP protokol a konfigurace pracovních stanic se provádí ručně. U počítače s jednou síťovou kartou stačí nastavit IP adresu počítače, masku a IP adresu brány (default gateway). Nastavovat či měnit IP adresy DNS serverů není nutné, protože se pracuje pouze s numerickými IP adresami.

V distribuci Red-Hat Linux jsou potřebné konfigurační údaje uloženy v adresáři **/etc/sysconfig**. V souboru **/etc/sysconfig/network** jsou společné údaje, týkající se všech síťových rozhraní:

```
NETWORKING=yes
HOSTNAME=localhost.localdomain
GATEWAYDEV=eth0
GATEWAY=192.168.1.1
```

V souboru **/etc/sysconfig/network-scripts/ifcfg-eth0** jsou údaje, vztahující se zařízení **/dev/eth0** (implicitně první síťová karta):

```
DEVICE=eth0
IPADDR=192.168.1.103
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255
ONBOOT=yes
```

Obsah konfiguračních souborů lze měnit libovolným textovým editorem nebo pomocí odpovídajících specializovaných nástrojů - v řádkovém modu programem **setup** (vyberte **Network configuration**), v grafickém prostředí KDE nástrojem **Network** (je v submenu **System Settings**).

Aby se nové nastavení uplatnilo, je nutné po změně údajů restartovat počítač.

Síťové nastavení v Linuxu lze změnit také pomocí příkazů **ifconfig** a **route**. Ale pozor - pokud změníte síťové nastavení tímto způsobem, platí nové nastavení pouze do příštího restartu počítače. Při restartu se automaticky nastaví uložená konfigurace.

Jestliže nepoužíváte dělení na podsítě (tj. maska odpovídá třídě adresy), nemusíte v příkazu **ifconfig** uvádět argumenty **netmask** a **broadcast**, protože program si potřebné údaje odvodí sám. Stačí tedy zadat např.:

```
ifconfig eth0 192.168.100.2
route add default gw 192.168.100.1
```

Pokud potřebujete použít podsíť, musíte si nejprve vypočítat správné hodnoty argumentů **netmask** a **broadcast** a tyto argumenty v příkazu **ifconfig** zadat, např.:

```
ifconfig eth0 192.168.3.66 netmask 255.255.255.192 broadcast 192.168.3.127
route add default gw 192.168.3.65
```

Nastavení můžete zkontrolovat příkazy **ifconfig** a **netstat -r**. Nepodléhejte panice, jestliže se při provádění příkazu **netstat** delší dobu nebude nic dít – provedení tohoto příkazu chvíli trvá.

# Příloha D. TFTP server v OS Linux

Služba TFTP v Linuxu obvykle není standardně nainstalována a proto je nutné ji doinstalovat ručně. V distribucích RedHat Linuxu je TFTP server v rpm-balíku **tftp-server**. Po instalaci balíku je nutné vytvořit ručně adresář **/tftpboot** a nastavit jeho přístupová práva na **rwxrwxrwx**. Pro úplnost si můžete nainstalovat i TFTP klienta (rpm-balík **tftp**).

Při běžné konfiguraci síťových služeb se tftp démon spouští nepřímo, prostřednictvím "superdémona" xinetd. Před prvním použitím je proto nutné v konfiguračním souboru **/etc/xinetd.d/tftp** změnit položku **disable =yes** na **disable = no**, čímž se povolí automatická aktivace démona po příchodu požadavku (pro navázání spojení služba TFTP používá port serveru **69/tcp** nebo **69/udp**).

Vhodné je také upravit v tomto konfiguračním souboru položku **server_args = –s /tftpboot** na **server_args = -c –s /tftpboot**, aby tftp démon mohl v adresáři **/tftpboot** vytvářet nové soubory (při původním nastavení smí pouze přepisovat již existující soubory).

Přístup ke službě TFTP ovlivňuje také nastavení firewallu. Pokud je firewall zapnutý, je nutné patřičně upravit pravidla nebo firewall vypnout.