# Základní příkazy Cisco IOS pro správu směrovačů a přepínačů

Josef Kaderka

Verse 43

Inspirace Boson

Příkazy jsou uváděny v základním tvaru, bez kontextu (tj. aktuálního módu), předpokládá se jeho znalost nebo vypěstování Cisco IOS intuice. Například je uveden příkaz pro přiřazení IP adresy rozhraní **ip address {adr} {sm} .** Pro jeho zadání je ale nutno napřed přejít do privilegovaného módu (příkaz **enable**), pak do globálního konfiguračního módu (příkaz **configure terminal**) a pak do specifického konfiguračního módu (příkaz **interface *{int}***).

Operační systém Cisco IOS se pro jedno zařízení dodává v několika versích. Ne všechny verse (zejména starší) podporují všechny zde uváděné příkazy.

# Správa směrovačů

| Konfigurační módy – význam promptu | |
|---|---|
| Uživatelský EXEC mód | **Router >** |
| Privilegovaný EXEC mód | **Router #** |
| Globální konfigurační mód | **Router (config) #** |
| Specifický konfigurační mód – konfigurace rozhraní<br>– konfigurace logického rozhraní<br>– konfigurace směrování<br>– konfigurace linky (CON, AUX) | **Router(config-if)#**<br>**Router (config-subif) #**<br>**Router(config-router) #**<br>**Router (config-line) #** |

| Základní operace se směrovačem | |
|---|---|
| Přechod do privilegovaného EXEC módu | **enable** |
| Návrat do uživatelského EXEC módu | **disable** |
| Odhlášení se od směrovače | **exit**, **logoff** |
| Restart operačního systému směrovače | **reload** |
| Předchozí příkaz | **<šipka nahoru>** nebo **<Ctrl><p>** |
| Následující příkaz | **<šipka dolů>** nebo **<Ctrl><n>** |
| Přesun o jeden znak vpravo | **<šipka vpravo>** nebo **<Ctrl><f>** |
| Přesun o jeden znak vlevo | **<šipka vlevo>** nebo **<Ctrl><b>** |
| Přerušení operace (Break) | **<Shift><Ctrl><6><x>** |
| Prosté obnova obsahu displeje (bez vložení příkazu) | **<Ctrl>+<L>** |
| Automatické doplňování příkazu a parametrů | **<Tab>** |
| Nápověda (vždy kontextově orientovaná) | **<?>** nebo **help** |
| Stačí uvést tolik znaků, aby byl příkaz jednoznačný | **sh run** místo **show running-config** |
| Počet řádků konsoly na stránku | **terminal length {n}** |

| Zjišťování údajů o směrovači | |
|---|---|
| Verse IOSu, velikosti pamětí a hodnota konfiguračního registru | **show version** |
| Výpis aktuální konfigurace (z operační paměti - RAM) | **show running-config** |
| Výpis uložené konfigurace (z pevné paměti - NVRAM) | **show startup-config** |
| Využití procesoru | **show processes cpu** |
| Obsah paměti flash, volné, obsazené a celkové místo | **show flash:** |
| Obsah paměti flash | **dir flash:** |
| Souhrn stavů všech rozhraní (jejich systémová označení, IP adresy, stav fyzické a linkové vrstvy), lze **sh ip int br** | **show ip interface brief** |

| Konfigurace směrovače | |
|---|---|
| Smazání uloženého konfiguračního souboru | **erase startup-config** |
| Restart (v případě výzvy nic neukládat!) | **reload** |
| Přechod do globálního konfiguračního módu | **configure terminal** |
| Směrovač se bude jmenovat Brno | **hostname Brno** |
| Návrat o jednu úroveň konfigurace zpět | **exit** |
| Návrat z libovolné úrovně do základního EXEC módu | **end, Ctrl-z** |
| Kopírování z tftp serveru do operační paměti (RAM) | **copy tftp running-config** |
| Z pevné paměti (NVRAM) do operační paměti (RAM); použít jen nebyla-li již provedena konfigurace – vznikla by směs | **copy startup-config running-config** |
| Z pevné paměti (NVRAM) do operační paměti (RAM); aktuální konfigurace v RAM bude přepsána | **configure replace nvram:startup-config** |
| Z tftp serveru do paměti flash | **copy tftp flash** |
| Z paměti flash do tftp serveru | **copy flash tftp** |
| Uložení aktuální konfigurace u operační paměti (RAM) do pevné paměti (NVRAM) | **copy running-config startup-config** |
| Uložení aktuální konfigurace u operační paměti (RAM) do pevné paměti (NVRAM) – stará, leč funkční alternativa | **write** |
| Exaktní specifikace IOS (souboru jej obsahující), který má být zaveden z paměti flash (použití, je-li ve flash více IOSů) | **boot system flash {*filename*}** |
| Exaktní specifikace IOS (souboru jej obsahující), který má být zaveden z tftp serveru (bude vyžádána IP adresa) | **boot system tftp {*filename*}** |
| Vytvoření lokálního uživatele a přiřazení hesla | **username {user} password {password}** |

| | |
|---|---|
| Vytvoření lokálního uživatelského účtu s implicitními právy administrátora | **username {*user*} privilege 15 password {password}** |
| Vytvoření lokálního uživatele a přiřazení hesla; toto budiž uloženo po zpracování zvoleným algoritmem | **username {user} algorithm-type {md5\|scrypt\|sha256} secret {password}** |
| **Hesla, vzdálený přístup** | |
| Minimální délka hesla bude 8 znaků | **security passwords min-length 8** |
| Nastavení hesla „class“ pro přístup přes konsolu | **line console 0**<br>**password class**<br>**login** |
| Nastavení hesla „class“ pro vzdálený přístup (telnet), současně až 5 uživatelů (virtuální terminály 0 až 4) | **line vty 0 4**<br>**password class**<br>**login** |
| Počet minut do automatického odhlášení (0 – nikdy) | **exec-timeout {n}** |
| Nastavení hesla „cisco“ pro přechod do privilegovaného módu | **enable password cisco** |
| Hashování hesla „cisco” pro přechod do privilegovaného módu zvoleným algoritmem | **enable algorithm-type** {**md5**\|**scrypt**\|**sha256**} **cisco** |
| Šifrování všech hesel (slabým algoritmem) | **service password-encryption** |

| **Vzdálený přístup pomocí ssh (scp)** | |
|---|---|
| Nutno změnit výchozí jméno zařízení (Router, Switch) | **hostname Brno** |
| Nastavení jména domény (jakékoliv) | **ip domain-name skoleni.org** |
| Vygenerování asymetrických klíčů | **crypto key generate rsa** |
| Bude se používat ssh protokol verse 2 | **ip ssh version 2** |
| Vytvořit lokálního uživatele | **username {*user*} password {*password*}** |
| Přístup na virtuální terminál pouze pomocí ssh<br>(Nastavit heslo pro přechod do privilegovaného režimu!) | **line vty 0 4**<br>**transport input ssh** |
| Mají-li se přenášet soubory, aktivovat scp server (secure copy) | **ip scp server enable** |

| **Základní konfigurace sériového rozhraní** | |
|---|---|
| Je to DCE nebo DTE? | **show controller serial 0/1/0** |
| Konfigurovat rozhraní (čísla udávají "pozici" modulu) | **interface serial 0/1/0** |
| U DCE nutno nastavit kmitočet hodinového signálu | **clock rate 64000** |
| Zápis šířky pásma [kb/s] (nemá přímý funkční význam!) | **bandwidth 64** |
| Aktivace rozhraní | **no shutdown** |
| Ověření stavu rozhraní | **show interface serial 0/1/0** |

| **Vytvoření virtuálního rozhraní (loopback) a konfigurace jeho IP adresy** | |
|---|---|
| Vytvoření rozhraní typu loopback se zvoleným číslem 0 | **interface loopback 0** |
| Přiřazení IP adresy rozhraní loopback 0 | **ip address 10.0.0.1 255.255.255.255** |

| **Cisco Discovery Protocol (CDP) – proprietární** | |
|---|---|
| Spuštění CDP (implicitně běží, rámce každých 60 s) | **cdp run** |
| Přehled přímo připojených Cisco zařízení (jméno, identifikátor místního rozhraní, vlastnosti, typ, identifikátor vzdáleného rozhraní) | **show cdp neighbors** |
| Navíc podrobnosti o operačním systému, IP adrese a hardware | **show cdp neighbors detail** |
| Vypnutí CDP | **no cdp run** |

| **Link Layer Discovery Protocol – standard IEEE (používá EtherType 0x88CC)** | |
|---|---|
| Spuštění LLDP (rámce každých 30 s) | **lldp run** |
| Zákaz vysílání LLDP do specifikovaného rozhraní<br>Zákaz příjmu LLDP ze specifikovaného rozhraní | **interface gigabitethernet 0/0**<br>**no lldp transmit**<br>**no lldp receive** |
| Zjištění stavu LLDP | **show lldp** |
| Přehled přímo připojených zařízení (jméno, identifikátor místního rozhraní, vlastnosti, identifikátor vzdáleného rozhraní) | **show lldp neighbors** |
| Navíc podrobnosti o operačním systému, IP adrese, hardware aj. | **show lldp neighbors detail** |
| Ukončení LLDP | **no lldp run** |

| TCP/IP | |
|---|---|
| Zákaz směrování IPv4 (standardně je povoleno), | **no ip routing** |
| Povolení směrování IPv6 (standardně je zakázáno!) | **ipv6 unicast routing** |
| Nastavení IP adres rozhraním a jejich aktivace | **interface serial 0/1/0**<br>**ip address 157.89.1.3 255.255.0.0**<br>**no shutdown**<br>**interface fastethernet 0/0**<br>**ip address 208.1.1.4 255.255.255.0**<br>**no shutdown** |

| Statické směrování | |
|---|---|
| Statický směrovací záznam – cílová síť, maska, vlastní odchozí rozhraní | **ip route 160.216.0.0 255.255.0.0 Fastethernet 0/0** |
| Statický směrovací záznam – cílová síť, maska, sousední směrovač (157.89.10.1) | **ip route 160.216.0.0 255.255.0.0 157.89.10.1** |
| Statický směrovací záznam pro výchozí cestu (default router/gateway - 157.89.10.1) | **ip route 0.0.0.0 0.0.0.0 157.89.10.1** |

| Dynamické směrování – RIP, RIPv2 | |
|---|---|
| Konfigurace směrovacího protokolu RIP verse 2 (implicitně v1)<br><br>Budou propagovány adresy sítí 157.89.0.0 a 208.1.1.0 | **router rip**<br>**version 2**<br>**network 157.89.0.0**<br>**network 208.1.1.0** |
| Šíření místního statického směrovacího záznamu prostřednictvím směrovacího protokolu | **redistribute static** |
| Autentizace (jen RIP v2) – místní pojmenování hesla (klíče)<br>Místní číslo klíče<br>Vlastní heslo – sdíleno mezi sousedícími směrovači<br>Zapnutí autentizace (zadat na sousedících rozhraních)<br>Totéž s využitím MD5 | **key chain KLIC1**<br>**key 1**<br>**key-string heslo1234**<br>**ip rip authentication key-chain KLIC1**<br>**ip rip authentication mode md5** |

| Dynamické směrování – EIGRP | |
|---|---|
| Konfigurace směrovacího protokolu EIGRP, autonomní systém 1, zákaz agregace adres podsítí (nutné, existuje-li několik jinými sítěmi oddělených podsítí téže sítě)<br>Budou propagovány adresy sítí 157.89.0.0 a 208.1.1.0 | **router eigrp 1**<br>**network 157.89.0.0**<br>**network 208.1.1.0**<br>**no auto-summary** |
| Autentizace EIGRP – místní pojmenování hesla (klíče)<br>Místní číslo klíče<br>Vlastní heslo<br>Zapnutí autentizace (zadat na sousedících rozhraních)<br>Specifikace hesla | **key chain MYCHAIN**<br>**key 1**<br>**key-string heslo1234**<br>**ip authentication mode eigrp 10 md5**<br>**ip authentication key-chain eigrp 10 MYCHAIN** |

| Dynamické směrování - OSPFv2 - IPv4 | |
|---|---|
| Konfigurace směrovacího protokolu OSPFv2 (IPv4), tato instance procesu OSPFv2 má lokálně platné číslo 1, area 0<br>Budou propagovány adresy sítí 157.89.0.0 a 208.1.1.0 | **router ospf 1**<br>**network 157.89.0.0 0.0.255.255 area 0**<br>**network 208.1.1.0 0.255.255.255 area 0** |
| Do sítě za rozhraním fastethernet 0/0 nebudou vysílány OSPF informace, adresa této sítě však do OSPF propagována bude | **passive-interface fastethernet 0/0** |
| Předání statického směrovacího záznamu o výchozí cestě do informací předávaných OSPF | **default-information originate** |
| Autentizace – heslo se zadává se na sousedících rozhraních<br>Autentizace – všechna rozhraní v rámci oblasti 0, heslo se předává otevřeně | **ip ospf authentication-key heslo1234**<br>**router ospf 1**<br>**area 0 authentication** |
| Autentizace OSPF sousedů pomocí MD5, nastavuje se na rozhraní | **ip ospf message-digest-key 1 md5 cisco12345**<br>**ip ospf authentication message-digest** |
| Autentizace OSPF sousedů pomocí SHA – volba „jména“ hesla<br>Identifikátor hesla (např. číslo)<br>Vlastní heslo<br>Volba algoritmu, kterým bude před uložením zpracováno<br>Heslo bude použito na rozhraní fastethernet 0/1<br>Heslo bylo zadáno | **key chain JMENO**<br>**key KEY-ID**<br>**key-string HESLO**<br>**cryptographic-algorithm hmac-sha-256**<br>**interface fastethernet 0/1**<br>**ip ospf authentication key-chain JMENO** |

| Dynamické směrování - OSPFv3 - IPv6 (tradiční konfigurace) | |
|---|---|
| Směrování IPv6 paketů je nutno explicitně povolit | **ipv6 unicast routing** |
| Tradiční konfigurace směrovacího protokolu OSPFv3<br>Identifikátor OSPFv3 směrovač musí být vždy zadán explicitně<br>Kromě uvedené IPv6 adresy bude mít rozhraní automaticky ještě další adresu typu link-local<br>Redistribuce statických cest a výchozí cesty jako u OSPFv2 | **ipv6 router ospf 1**<br>**router-id 6.6.6.6.**<br>**interface gigabitethernet 0/0**<br>**ipv6 address 2001:DB8:CAFE:1::1/64**<br>**ipv6 ospf 1 area 0** |

| Dynamické směrování - IPv4 a IPv6 - OSPFv3 (nový styl konfigurace) | |
|---|---|
| Společná konfigurace směrovače IPv4 a IPv6<br><br>Kromě zadané IPv6 adresy bude mít rozhraní ještě další vygenerovanou adresu typu link-local (lze zadat i ručně)<br><br><br>Redistribuce statických cest a výchozí cesty jako u OSPFv2<br>Pasivní rozhraní totéž | **router ospfv3 1**<br>**..address-family ipv4 unicast**<br>**router-id 1.1.1.1**<br>**address-family ipv6 unicast**<br>**router-id 6.6.6.6**<br>**interface gigabitethernet 0/0**<br>**ip address 192.168.1.1 255.255.255.0**<br>**ipv6 address 2001:DB8:CAFE:1::1/64**<br>**ospfv3 1 ipv4 area 0**<br>**ospfv3 1 ipv6 area 0** |

| Výpisy směrovacích údajů, ladění | |
|---|---|
| Výpis IP směrovací tabulky | **show ip route** |
| Vypisování údajů vyměňovaných protokolem RIP | **debug ip rip** |
| Vypisování údajů vyměňovaných protokolem EIGRP | **debug ip eigrp events**<br>**debug ip eigrp transactions** |
| Vypisování údajů vyměňovaných protokolem OSPF | **debug ip ospf events** |

| Přístupové seznamy (Access Control Lists - ACL) – výběr | |
|---|---|
| Význam číselných rozsahů přístupových seznamů (Access Control Lists -ACL) | |
| <l-99> | **IP standard access list** |
| <100-199> | **IP extended access list** |
| <600-699> | **Appletalk access list** |
| <700-799> | **48-bit MAC address access list** |
| <800-899> | **IPX standard access list** |
| <1100-1199> | **Extended 48-bit MAC address access list** |
| <1200-1299> | **IPX summary address access list** |
| <1300-1999> | **IP standard access list (expanded range)** |
| Které ACL jsou přiřazeny na dané rozhraní? | **show ip interface serial 0/1/0** |
| Výpis všech ACL; výpis jen IP ACL | **show access-lists**<br>**show ip access-list** |

| Standardní přístupové seznamy, čísla l-99, filtruje se pouze dle zdrojové IP adresy (tj. podle odesílatele) | |
|---|---|
| Účel – nepovolit uzlům z podsítě 200.1.1.0 255.255.255.0 odesílat pakety přes rozhraní Fastethernet 0/0 | |
| A. Zakázat danou podsíť | **access-list 1 deny 200.1.1.0 0.0.0.255** |
| B. Implicitně platí „deny all“, takže nutno explicitně povolit ostatní | **access-list 1 permit any** |
| C. Přiřadit ACL k příslušnému rozhraní, teprve pak se ACL aktivuje | **interface fastethernet 0/0**<br>**ip access-group 1 in** |

| Rozšířené přístupové seznamy, čísla l00-199, filtruje se dle IP adres odesilatele a příjemce, portů aj. | |
|---|---|
| Účel – nepovolit stroji 1.1.1.1 používat telnet přes rozhraní fa0/0 do stroje 2.2.2.2 a nepovolit uživatelům podsítě 3.3.3.0 žádné surfování | |
| A. Syntax: access-list {číslo} povolit\|zakázat protokol zdroj cíl port volby | **access-list 100 deny tcp host 1.1.1.1 host 2.2.2.2 eq 23** |
| B. Zákaz surfování (http) uživatelům sítě 3.3.3.0 | **access-list 100 deny tcp 3.3.3.0 0.0.0.255 any eq 80** |
| C. Implicitně platí „deny all“, proto je nutno ostatní explicitně povolit | **access-list 100 permit ip any any** |
| D. Přiřadit ACL k rozhraní, teprve pak se ACL aktivuje | **interface fastethernet 0/0**<br>**ip access-group 100 out** |

| Pojmenovaný přístupový seznam (Named ACL) | |
|---|---|
| Výhoda: lze editovat i jediný řádek víceřádkového ACL místo jinak nutného zrušení celého ACL a jeho znovuvytvoření | **ip access-list standard COOLLIST**<br>**deny 1.1.1.1**<br>**permit any** |
| Přiřadit ACL k rozhraní, teprve pak se ACL aktivuje | **interface fastethernet 0/0**<br>**ip access-group COOLLIST in** |

| PPP | |
|---|---|
| Komunikace mezi směrovači **router-a** a **router-b**, na obou analogická konfigurace | |
| **Příkazy zadávané na rozhraní směrovače router-a** | |
| Povolení PPP | **encapsulation ppp** |
| Autentizace bude pomocí protokolu chap | **ppp authentication chap** |
| **Globální mód** | |
| Vzdálený směrovač je "router-b", sdílené heslo je "cisco" | **username router-b password cisco** |
| **Výpisy** | |
| Zjištění typu zapouzdření, aktivovaných protokolů linkové vrstvy (LCP) aj. | **show interface serial 0/1/0** |
| **Ladění** | |
| Vypisování procesu autentizace | **debug ppp authentication** |

| PPP multilink (sdružení několika fyzických sériových rozhraní do jediného logického) | |
|---|---|
| Vytvoření a konfigurace logického rozhraní | **interface multilink 0**<br>**ip address 1.1.1.2 255.255.255.0**<br>**ppp multilink**<br>**ppp multilink group 1** |
| Všechna fyzická rozhraní sdružená do multilinku nakonfigurovat stejně | **interface serial 0/1/0**<br>**no ip address**<br>**encapsulation ppp**<br>**ppp multilink**<br>**ppp multilink group 1** |

| Frame-Relay (pro informaci – zastaralý protokol) | |
|---|---|
| **Rozhraní** | |
| Povolení Frame-Relay na daném rozhraní a specifikace typu zapouzdření | **encapsulation frame-relay ietf** |
| Specifikace typu LMI Type (IOS od verse 11.2 zjišťuje automaticky) | **frame-relay lmi-type ansi** |
| Jestliže nebude pracovat inversní ARP, namapovat vzdálenou IP adresu na naše číslo DLCI (místní) | **frame-relay map ip 3.3.3.100 broadcast** |
| **Lze rovněž povolit rozhlašování a specifikovat typ zapouzdření** | |
| Definovat místní DLCI (nepracuje-li LMI) | **frame-relay local-dlci 100** |

| | |
|---|---|
| Nastavit periodu pro kontrolu udržení spojení | **keepalive 10** |
| **Kontrola nastavení** | |
| Výpis informací o DLCI a LMI | **show interface serial 0** |
| Výpis statistik o provozu PVC | **show frame-relay pvc** |
| Výpis směrovací mapy (statické nebo dynamické) | **show frame-relay map** |
| Výpis LMI informací | **show frame-relay lmi** |
| **Přeměna směrovače do role Frame Relay přepínače (pro laboratorní účely)**<br>Poznámka –příkazy je nutno symetricky zadat na obou DCE rozhraních, která mají propojena pomocí Frame Relay | |
| Povolit Frame-Relay přepínání (na té straně směrovače, kde je DCE) | **frame-relay switching** |
| Řekni DCE straně, aby podporovala frame-relay funkce DCE na daném rozhraní | **frame-relay intf-type dce** |
| Řekni DCE straně, na které jiné místní rozhraní {int_o} a DLCI {dlci_o} přepínat DLCI {dlci_i} z právě konfigurovaného rozhraní | **frame-relay route {dlci_i} interface {int_o} {dlci_o}** |
| Nastavit na DCE rozhraní hodinový kmitočet [b/s] | **clock rate 64000** |

| **DNS** | |
|---|---|
| IP adresa reálného jmenného serveru | **ip name-server 169.223.2.2** |
| Jméno vlastní domény | **ip domain-name skoleni.org** |
| Nepřevádět doménová jména na IP adresy | **no ip domain-name lookup** |
| Router bude sloužit jako jmenný server (typu cache) | **ip dns server** |

| **DHCP** | |
|---|---|
| Explicitni aktivace DHCP serveru (jen u některých IOSů) | **service dhcp** |
| Tyto adresy IP z přidělování (viz uvedený rozsah) vynechat | **ip dhcp excluded-address 157.89.1.1 157.89.1.2** |
| Pojmenování poolu a definice parametrů posílaných klientům (max. 124 adres, jméno domény, IP adresy výchozího routeru, DNS a netbios servery, doba platnosti přidělení 2 dny). | **ip dhcp pool MOJE_ZASOBARNA**<br>**network 157.89.1.0 255.255.255.128**<br>**domain-name unob.cz**<br>**default-router 192.168.12.1**<br>**dns-server 192.168.12.100 192.168.12.101**<br>**netbios-name-server 192.168.12.99**<br>**lease 2** |
| Nalézá-li se DHCP server v jiné síti, je třeba sdělit jeho IP adresu (zadá se na rozhraní směrovače připojeném do segmentu s DHCP klienty). | **ip helper-address 169.223.2.2** |
| Rozhraní směrovače získá IP adresu od DHCP serveru | **interface fa0/0**<br>**ip address dhcp** |
| Komu byla přidělena IP adresa | **show ip dhcp bindings** |

| **NAT (PAT)** | |
|---|---|
| Nastavení rozhraní do vnitřní sítě | **interface FastEthernet0**<br>**ip nat inside** |
| Nastavení rozhraní do vnější sítě | **interface FastEthernet1**<br>**ip nat outside** |
| Překládat se bude veškerý provoz (obecně ACL může mít jakoukoliv jinou podobu) | **access-list 10 permit any** |
| Celá vnitřní síť se ukryje za jedinou adresu (zajistí **overload**=PAT, jinak NAT), nastavenou na Fasthenernet1. Překlad se uplatní na provoz vyhovující ACL 10 | **ip nat inside source list 10 interface FastEthernet1 overload** |

| **Konfigurační registr** | |
|---|---|
| RXBOOT (speciální diagnostický mód, pokračování pomocí "b") | **confreg 0x2000** |
| Systém zavádět z ROM, načíst konfigurační soubor (upgrade flash - u směrovačů, které zavádí IOS z flash) | **confreg 0x2101** |
| Systém zavádět z ROM, nenačíst konfigurační soubor (obnova po havárii) | **confreg 0x2141** |
| Systém zavádět z flash, načíst konfigurační soubor (normální stav) | **confreg 0x2102** |
| Systém zavádět z flash, nenačíst konfigurační soubor (obnova hesla) | **confreg 0x2142** |

| **Password Recovery - obnova hesla (postup pro směrovače)** | |
|---|---|
| 1. Přerušit start pomocí konsoly (vyžaduje se fyzické přístup) | **<Ctrl><Break>** |
| 2. Zavést IOS z flash, nenačítat konfigurační soubor z NVRAM | **confreg 0x2142** |

| | |
|---|---|
| *2a. Jiná syntaxe platná jen u starých zařízení* | **o/r 0x2142** |
| 3. Restart operačního systému | **reset** |
| 4. Přejít do privilegovaného módu; nenačtením konfigurační souboru lze provést bez hesla | **enable** |
| 5. Nyní v privilegovaném módu překopírovat konfigurační soubor z NVRAM do RAM – směrovač ožije, ale zůstane privilegovaný mód | **copy startup-config running-config** |
| 6. Změnit neznámé enable heslo na "NoveHeslo" | **enable password NoveHeslo** |
| 7. Uložit aktuální konfiguraci do NVRAM (tj. s novým heslem) | **copy running-config startup-config** |
| 8. Příští start směrovače nechť proběhne normálně (IOS z flash, konfigurační soubor z NVRAM) | **config-reg 0x2102** |

| **Obnova chybějícího operačního systému IOS (pouze u směrovačů, s rozhraním Ethernet)** | |
|---|---|
| IOS je třeba mít předem zálohován (tftp server) – nelze jej volně stáhnout. V nouzi lze použít stejný IOS z jiného směrovače téže řady. Dojde-li ke smazání IOSu z flash, ale směrovač dosud běží, nevypínat jej (!), nýbrž postupovat standardně – **copy tftp flash** (tedy spustit tftp server, připravit záložní IOS). U směrovačů s výměnnou pamětí (Compact Flash) na ni lze IOS zapsat v externí zařízení (PC), obdobně má-li směrovač USB port. | |
| Připojit ethernetové rozhraní s nejnižším ID (např. fa0/0)<br>Ověřit nastavení uvedených proměnných (viz příklad)<br>Nejsou-li v pořádku, pak proměnné nastavit (změnit) tak, jak ukazuje tento výpis | **rommon 1 > set**<br>**IP_ADDRESS=172.18.16.76**<br>**IP_SUBNET_MASK=255.255.255.192**<br>**DEFAULT_GATEWAY=172.18.16.65**<br>**TFTP_SERVER=172.18.16.2**<br>**TFTP_FILE=c2600-ik9o3s3-mz.123-13.bin** |
| Příklad nastavení/změny hodnoty proměnné | **TFTP_SERVER=172.18.16.88** |
| Spustit stahování a instalaci IOSu | **tftpdnld** |
| Restartovat směrovač | **reset** |

| **Obnova chybějícího operačního systému IOS (pouze u směrovačů bez rozhraní Ethernet)** | |
|---|---|
| Není-li k dispozici rozhraní Ethernet, lze k instalaci IOSu použít konsolový port o nízké rychlosti. | |
| Připojit sériový port PC ke konsolovému portu směrovače. V PC použít terminálový program podporující protokol Xmodem (Hyperterminal, modifikovaný putty). | |
| Nastavit maximální přípustnou přenosovou rychlost dle typu směrovače (0x3822 = 115,2 kb/s, 0x2102 = 9,6 kb/s), tutéž nastavit u terminálu.<br>Restartovat směrovač | **rommon 1 > confreg 0x3822**<br><br>**rommon 2 > reset** |
| Spustit instalaci IOSu, vyčkat konce přenosu (při IOS 15 MB a 115,2 kb/s asi 30 minut, při 9,6 kb/s asi 4,5 hodiny)<br>K oživení je vhodné použít co nejmenší (např. starý) IOS, z něj pak (již po síti) nainstalovat cílovou versi | **rommon 1 > xmodem c2600-ik9o3s3-mz.123-13.bin** |
| Nastavit výchozí hodnotu konfiguračního registru | **config-register to 0x2102** |
| Restartovat směrovač, vrátit rychlost terminálu na 9600 b/s! | **reset** |

| **Přesný čas – NTP** | |
|---|---|
| Toto je zdroj přesného času: **tik.cesnet.cz** | **ntp server tik.cesnet.cz** |
| Časová zóna budiž pojmenována CET, posun od UTC je +1 hodina | **clock timezone CET 1** |

| **Záznam událostí - syslog** | |
|---|---|
| Toto je syslog server, tam půjdou zprávy (lze užít i doménové jméno) | **logging 172.16.1.1** |
| Zpráva bude mít příznak (facility) local5 | **logging facility local5** |
| Odesílat zprávy typu (s prioritou) debugging | **logging trap debugging** |

| **Správa sítě - SNMP** | |
|---|---|
| Nastavení hesla „admins“ pro čtení a zápis SNMP dat<br>Nastavení hesla „topsecret“ pro čtení a zápis SNMP dat jen z 10.1.1.1 | **snmp-server community admins rw**<br>**snmp-server community topsecret rw 60 access-list 60 permit 10.1.1.1** |
| Nastavení hesla „others“ pro čtení SNMP dat (běžná hodnota je „public“) | **snmp-server community others ro** |
| Toto je pán směrovače | **snmp-server contact Josef Kaderka** |
| Tady se směrovač nalézá | **snmp-server location Brno, Sumavska 4, 3/11a** |
| SNMP manager, tam posílat zprávy (traps) s community public | **snmp-server host 10.1.1.1 public** |

| | |
|---|---|
| Povolení odesílat zprávy při vzniku jakékoliv události | **snmp-server enable traps** |
| Odesílat zprávy jen při vzniku události daného typu | **snmp-server enable traps config**<br>**snmp-server enable traps envmon temperature** |

# Správa přepínačů

(základní úkony jsou stejné jako u směrovačů)

| Zjištění stavu přepínače | |
|---|---|
| Verse IOSu, hardware aj. (konfigurační registr se liší od směrovačů) | **show version** |
| Výpis uložené konfigurace (z pevné paměti - NVRAM) | **show startup-config** |
| Výpis aktuální konfigurace (z operační paměti - RAM) | **show running-config** |
| Výpis obsahu paměti flash | **show flash:** nebo **dir flash:** |
| Výpis bezpečnostních nastavení rozhraní (řada variant) | **show port-security** |
| Stav všech rozhraní (řada variant) | **show interfaces** |
| Výpis schopností rozhraní a jejich aktuálního nastavení | **show interfaces fa0/1 capabilities** |

| Uvedení přepínače do výchozího stavu | |
|---|---|
| Zamezení komunikace přepínače se sousedními přepínači zablokováním rozhraní (odpojením kabelů, nastavením VTP režimu Transparent) | **interface fastethernet 0/1**<br>**shutdown** |
| Smazání uložené databáze virtuálních LAN | **delete flash:vlan.dat** |
| Smazání uloženého konfiguračního souboru | **erase startup-config** |
| Restart (v případě výzvy nic neukládat) | **reload** |

| Základní operace s přepínačem | |
|---|---|
| Konfigurace IP údajů umožňujících vzdálený přístup k přepínači (přepínač má jedinou IP adresu). Vždy je nutno nejprve zablokovat všechna dosud použitá rozhraní VLAN, pak povolit žádané. | **interface VLAN1**<br>**shutdown**<br>**interface VLAN99**<br>**ip address 192.168.1.2 255.255.255.0**<br>**ip default-gateway 192.168.1.1**<br>**no shutdown** |
| Výpis tabulky přepínači známých MAC adres | **show mac-address-table** |
| Počet MAC adres v tabulce (vhodné při podezření na přeplnění) | **show mac-address-table count** |
| Vymazání tabulky MAC adres | **clear mac-address-table** |

| Zapnutí podpory protokolu IPv6 | |
|---|---|
| Jen u některých přepínačů, nutný následný restart | **sdm prefer dual -ipv4-and-ipv6 default** |

| Konfigurace rozhraní pro připojení koncové stanice | |
|---|---|
| Volba rozhraní | **interface gigabit 0/1** |
| Tatáž operace nad více rozhraními (může být i seznam) | **interface range fastethernet 0/1–12** |
| Volba plného duplexu (není-li uveden, bude režim duplexu vyjednán) | **duplex full** |
| Volba rychlosti 100 Mb/s (není-li uvedena, bude rychlost vyjednána) | **speed 100** |
| K rozhraní bude připojena výhradně stanice | **switchport mode access** |
| Rozhraní se po připojení stanice ihned aktivuje, nečeká se na STP | **spanning-tree portfast** |

| Zabezpečení rozhraní přepínače | |
|---|---|
| Nastavení režimu rozhraní access (nikoliv trunk) | **switchport mode access** |
| Zapnutí bezpečnosti na rozhraní (jinak nebudou další příkazy funkční) | **switchport port-security** |
| Přes rozhraní může komunikovat jen stanice s danou MAC adresou | **switchport port-security mac-address {adr}** |
| Přes rozhraní může komunikovat nejvýše {n} stanic | **switchport port-security maximum {n}** |
| Po {n} minutách neaktivity bude zaslechnutá adresa zahozena | **switchport port-security aging time {n}** |
| Rozhraní se učí zaslechnuté MAC adresy a zapisuje je do běžící konfigurace, takže je lze uložit do startovací konfigurace | **switchport port-security mac-address sticky** |
| Nepovolená komunikace bude zahazována, povolená nikoliv | **switchport port-security violation protect** |
| Totéž, navíc se činí záznam do logu, ev. posílá SNMP trap | **switchport port-security violation restrict** |
| Rozhraní bude zablokováno, nutný ruční zásah (výchozí nastavení) | **switchport port-security violation shutdown** |
| Automatické odblokování rozhraní po určité době: | **errdisable recovery cause psecure-violation**<br>**errdisable recovery interval 60** |

| DHCP Snooping | |
|---|---|
| Globální zapnutí DHCP Snoopingu | **ip dhcp snooping** |

| | |
|---|---|
| Zapnutí DHCP Snoopingu jen ve VLAN 10 | **ip dhcp snooping vlan 10** |
| Přes toto rozhraní mohou chodit DHCP pakety bez omezení | **interface f0/1**<br>**ip dhcp snooping trust** |
| Přes tato rozhraní mohou chodit DHCP pakety, nejvýše však 5 za sekundu | **interface f0/18**<br>**ip dhcp snooping limit rate 5** |
| Zachytil DHCP Snoopingu něco? | **show ip dhcp snooping binding** |

| **Protokol Spanning Tree (STP)** | |
|---|---|
| Zjištění MAC adresy přepínače | **show interface vlan 1** |
| Výpis tabulky spanning tree a zjištění, kdo je kořenovým přepínačem | **show spanning-tree** |
| Explicitní volba kořenového přepínače nastavením priority {n} | **spanning-tree priority {*n*}** |

| **Zabezpečení protokolu Spanning Tree (STP)** | |
|---|---|
| Pokud dané rozhraní přijme paket BPDU, bude blokováno | **spanning-tree bpduguard enable** |
| Odblokování takto zablokovaného rozhraní (varianta 1) | **errdisable recovery cause psecure_violation** |
| Odblokování takto zablokovaného rozhraní (varianta 2) | **disable**<br>**enable** |
| Varianta - rychlá aktivace rozhraní, za kterým není přepínač (tudíž není nutno čekat na konvergenci STP) | **switchport mode access**<br>**spanning-tree portfast** |

| **Vzdálený správa pomocí webového rozhraní** | |
|---|---|
| Zákaz protokolu http (implicitně povolen přístup i bez hesla; je-li nastaveno, použije se heslo pro přechod do privilegovaného režimu) | **no ip http server** |
| Povolení protokolu https | **ip http secure-server** |
| Vytvoření lokálního uživatelského účtu s právy administrátora a povolení lokální autentizace | **username {***user***} privilege 15 password {***password***}**<br>**ip http authentication local** |

| **Password recovery - obnova hesla (postup pro přepínače 29xx/35xx)** | |
|---|---|
| 1. Vypnout napájení přepínače | |
| 2. Na předním panelu přepínače stisknout a držet tlačítko "Mode" | **<mode>** |
| 3. Zapnout napájení přepínače a dosti dlouho čekat | |
| 4. Po zhasnutí STAT LED uvolnit tlačítko "Mode" | |
| 5. Vyčkat ukončení výpisu a na přechod do ROMMONu | |
| 6. Zadat sekvenci příkazů (dle přepínače ne vždy oba) | **flash_init**<br>**load_helper** |
| 7. Přejmenovat konfigurační soubor (je uložen ve flash, ne v NVRAM) | **rename flash:config.text flash:config.old** |
| 8. Zavést operační systém přepínače | **boot** |
| 9. Přeskočit konfigurační dialog, přejít do privilegovaného módu | **enable** |
| 10. Obnovit konfigurační soubor | **rename flash:config.old flash:config.text** |
| 11. Načíst uloženou konfiguraci, tj. se starým heslem | **copy startup-config running-config** |
| 12. Nastavit nové heslo pro přechod do privilegovaného módu | **enable secret class** |
| 13. Uložit aktuální konfiguraci, tj. s novým heslem | **copy running-config startup-config** |

| **Virtuální LAN (VLAN) a trunking** | |
|---|---|
| Globální konfigurační mód, vytvoření VLAN s číslem 20 a její pojmenování "KUCHYNE". | **vlan 20**<br>**name KUCHYNE** |
| Zařazení rozhraní do VLAN číslo 20. Pokud dosud neexistovala, bude vytvořena, explicitně nepojmenované budou mít jméno VLANxxxx, kde xxxx je její číslo (s vedoucími nulami) | **interface fastethernet 0/1**<br>**switchport mode access**<br>**switchport access vlan 20** |
| Seznam virtuálních LAN a do nich zařazených rozhraní | **show vlan** |
| Pokud IOS podporuje dva druhy zapouzdření (standardní 802.1q nebo historické Cisco proprietární ISL), zvolit požadované<br>Explicitní vytvoření trunku | **interface fastethernet0/2**<br>**switchport trunk encapsulation dot1q**<br>**switchport mode trunk** |
| Netagované rámce dávat do VLAN 5 (implicitně jdou do VLAN 1) | **switchport trunk native vlan 5** |
| Trunkem mohou procházet pouze rámce z/do VLAN 5, 10, 20 | **switchport trunk allowed vlan 5,10,20** |

| **Virtuální LAN (VLAN) a trunking u starších přepínačů** | |
|---|---|
| Privilegovaný EXEC mód, vytvoření VLAN s číslem 20 a její | **vlan database** |

| | |
|---|---|
| pojmenování "KUCHYNE" | **vlan 20 name KUCHYNE** |
| Zařazení rozhraní do VLAN20 | **interface ethernet 0/1**<br>**vlan static 20** |
| Seznam virtuálních LAN a do nich zařazených rozhraní | **show vlan-membership** |
| Volba zapouzdření (ISL nebo 802.1q; jen pokud IOS podporuje obě dvě) a vytvoření trunku | **interface fastethernet0/2**<br>**switchport trunk encapsulation isl**<br>**switchport mode trunk** |

| **Komunikace mezi virtuálními LAN (metoda „router on a stick“)** | |
|---|---|
| Mezi přepínačem a směrovačem jediný fyzický spoj, nakonfigurovaný na straně přepínače jako trunk, na straně směrovače je pak pro každou VLAN vytvořeno logické rozhraní (subinterface). | |
| Konfigurace fyzického rozhraní směrovače | **interface fastethernet 0/0**<br>**no shutdown** |
| Vytvoření logického rozhraní (číslo libovolné, nejlépe shodné s VLAN) | **interface fastethernet 0/0.20** |
| Volba zapouzdření a specifikace čísla VLAN | **encapsulation dot1q 20** |
| Přiřazení IP adresy logickému rozhraní | **ip address 192.168.5.20 255.255.255.0** |

| **Sdružení několika rozhraní do jediného o kumulované rychlosti (Etherchannel)** | |
|---|---|
| Výběr rozhraní (všechna musí být nastavena stejně; tj. v režimu trunk nebo access) a volba čísla skupiny, proprietární protokol PAgP | **interface range FastEthernet0/1 - 4**<br>**channel-group 1 mode on** |
| Výběr rozhraní (všechna musí být nastavena stejně; tj. v režimu trunk nebo access) a volba čísla skupiny, IEEE protokol LACP | **interface range FastEthernet0/1 - 4**<br>**channel-group 1 mode auto** |
| Zjištění stavu | **show etherchannel 1 summary** |

| **Monitorování provozu jednoho či více rozhraní či VLAN jiným rozhraním (SPAN - Switched Port Analyzer)** | |
|---|---|
| Volba zdroje provozu (všechna rozhraní musí být nastavena stejně) | **monitor session 1 source interface FastEthernet0/1**<br>**monitor session 1 source interface FastEthernet0/2** |
| Zde se bude provoz monitorovat | **monitor session 1 destination interface gigabitEthernet0/1** |
| Ověření stavu | **show monitor session 1** |

| **Vzdálené monitorování provozu jednoho či více rozhraní či VLAN rozhraním jiného přepínače (RSPAN – Remote Switched Port Analyzer)** | |
|---|---|
| Vytvoření VLAN pro přenos monitorovaných dat v monitorovaném i monitorujícím přepínači (nutno zajistit přenos dat této VLAN trunkem) | **vlan 30**<br>**name RSPAN-VLAN**<br>**remote-span** |
| Monitorovaný přepínač - volba zdroje dat (fyzického rozhraní) a jejich kopírování do určené VLAN | **monitor session 1 source interface Gi0/1 rx**<br>**monitor session 1 destination remote vlan 30** |
| Monitorující přepínač - volba zdroje dat (VLAN) a jejich kopírování do určeného fyzického rozhraní | **monitor session 1 source remote vlan 30**<br>**monitor session 1 destination interface Gi0/2** |
| Ověření stavu | **show monitor session 1** |

| **Virtuální privátní síť mezi dvěma směrovači – varianta - IPSec tunel** | |
|---|---|
| Vytvoření politiky protokolu ISAKMP č. 10 - <u>fáze 1</u><br>Šifrovat se bude algorimem AES<br>Bude použito sdílené heslo<br>Diffie-Hellman skupina 14 (2048 bitů)<br>Zadání sdíleného hesla a IP adresy druhé strany tunelu | **crypto isakmp policy 10**<br>**encryption aes**<br>**authentication pre-share**<br>**group 14**<br>**crypto isakmp key heslo1234 address 192.168.23.3** |
| Zadání přijatelných kombinací kryptografických protokolů (jiné označení „IPSec proposals“) – fáze 2 | **crypto ipsec transform-set MOJE esp-des esp-sha-hmac** |
| Vytvoření politiky protokolu IPSec (kryptomapy) | **crypto map MOJEMAPA 10 ipsec-isakmp**<br>**set peer 192.168.23.3**<br>**set transform-set MOJE**<br>**match address 101** |
| Tento provoz půjde tunelem | **access-list 101 permit ip 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255** |
| Aplikace kryptomapy na rozhraní | **interface FastEthernet0/0**<br>**ip address 192.168.12.1 255.255.255.0**<br>**crypto map MOJEMAPA** |
| Ověření stavu tunelu – fáze 1<br>Ověření stavu tunelu – fáze 2 | **show crypto isakmp sa**<br>**show crypto ipsec sa** |