Základní příkazy Cisco IOS pro správu směrovačů a přepínačů

Josef Kaderka

Verse 38

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 – konfigurace logického rozhraní – konfigurace směrování – konfigurace linky (CON, AUX)	**Router(config-if)#** **Router (config-subif) #** **Router(config-router) #** **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:**
Souhrnný přehled o stavu všech rozhraní (jejich systémová označení, IP adresy, stav fyzické a linkové vrstvy)	**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** **password class** **login**
Nastavení hesla „class“ pro vzdálený přístup (telnet), současně až 5 uživatelů (virtuální terminály 0 až 4)	**line vty 0 4** **password class** **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 (Nastavit heslo pro přechod do privilegovaného režimu!)	**line vty 0 4** **transport input ssh**
Mají-li se přenášet soubory, aktivovat scp server (secure copy)	**ip scp server enable**

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**

Konfigurace virtuálního rozhraní (loopback)	
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**
Ukončení 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 Zákaz příjmu LLDP ze specifikovaného rozhraní	**interface gigabitethernet 0/0** **no lldp transmit** **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 (standardně je povoleno),	**no ip routing**
Přiřazení IP adres rozhraním a jejich aktivace	**interface serial 0/1/0** **ip address 157.89.1.3 255.255.0.0** **no shutdown** **interface fastethernet 0/0** **ip address 208.1.1.4 255.255.255.0** **no shutdown**

Směrování – RIP, RIPv2, EIGRP, OSPFv2	
Statický směrovací záznam – cílová síť, maska, následující 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**
Šíření místního statického směrovacího záznamu prostřednictvím směrovacího protokolu	**redistribute static**
Zahrnutí statického směrovacího záznamu o výchozí cestě do informací předávaných směrovacím protokolem (jen OSPF)	**default-information originate**
Konfigurace směrovacího protokolu RIP verse 2 (implicitně v1) Budou propagovány adresy sítí 157.89.0.0 a 208.1.1.0	**router rip** **version 2** **network 157.89.0.0** **network 208.1.1.0**
Autentizace (jen RIP v2) – místní pojmenování hesla (klíče) Místní číslo klíče Vlastní heslo – sdíleno mezi sousedícími směrovači Zapnutí autentizace (zadat na sousedících rozhraních) Totéž s využitím MD5	**key chain KLIC1** **key 1** **key-string heslo1234** **ip rip authentication key-chain KLIC1** **ip rip authentication mode md5**
Konfigurace směrovacího protokolu EIGRP, autonomní systém 1, zákaz agregace adres podsítí (nutné, existuje-li několik jinými sítěmi oddělených podsítí téže sítě) Budou propagovány adresy sítí 157.89.0.0 a 208.1.1.0	**router eigrp 1** **network 157.89.0.0** **network 208.1.1.0** **no auto-summary**
Autentizace EIGRP – místní pojmenování hesla (klíče) Místní číslo klíče Vlastní heslo Zapnutí autentizace (zadat na sousedících rozhraních) Specifikace hesla	**key chain MYCHAIN** **key 1** **key-string heslo1234** **ip authentication mode eigrp 10 md5** **ip authentication key-chain eigrp 10 MYCHAIN**
Konfigurace směrovacího protokolu OSPFv2 (IPv4), tato instance procesu OSPFv2 má lokálně platné číslo 1, area 0 Budou propagovány adresy sítí 157.89.0.0 a 208.1.1.0 Do sítě za rozhraním fastethernet 0/0 nebudou vysílány OSP informace, adresa této sítě však do OSPF propagována bude	**router ospf 1** **network 157.89.0.0 0.0.255.255 area 0** **network 208.1.1.0 0.255.255.255 area 0** **passive-interface fastethernet 0/0**
Autentizace – heslo se zadává se na sousedících rozhraních Autentizace – všechna rozhraní v rámci oblasti 0, heslo se předává otevřeně	**ip ospf authentication-key heslo1234** **router ospf 1** **area 0 authentication**
Autentizace OSPF sousedů pomocí MD5, nastavuje se na rozhraní	**ip ospf message-digest-key 1 md5 cisco12345** **ip ospf authentication message-digest**

Autentizace OSPF sousedů pomocí SHA – volba „jména“ hesla Identifikátor hesla (např. číslo) Vlastní heslo Volba algoritmu, kterým bude před uložením zpracováno Heslo bude použito na rozhraní fastethernet 0/1 Heslo bylo zadáno	**key chain JMENO** **key KEY-ID** **key-string HESLO** **cryptographic-algorithm hmac-sha-256** **interface fastethernet 0/1** **ip ospf authentication key-chain JMENO**
Výpis IP směrovací tabulky	**show ip route**
Vypisování údajů vyměňovaných protokolem RIP	**debug ip rip**
Vypisování údajů vyměňovaných protokolem EIGRP	**debug ip eigrp events** **debug ip eigrp** **transactions**
Vypisování údajů vyměňovaných protokolem OSPF	**debug ip ospf events**

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

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

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** **show ip access-list**

Standardní přístupové seznamy, čísla l-99, filtruje se pouze dle zdrojové IP adresy (tj. podle odesílatele)	
Účel – nepovolit uživatelům 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** **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** **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** **deny 1.1.1.1** **permit any**
Přiřadit ACL k rozhraní, teprve pak se ACL aktivuje	**interface fastethernet 0/0** **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** **ip address 1.1.1.2 255.255.255.0** **ppp multilink** **ppp multilink group 1**
Všechna fyzická rozhraní sdružená do multilinku nakonfigurovat stejně	**interface serial 0/1/0** **no ip address** **encapsulation ppp** **ppp multilink** **ppp multilink group 1**

Frame-Relay (pro informaci)	
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) 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** **network 157.89.1.0 255.255.255.128** **domain-name unob.cz** **default-router 192.168.12.1** **dns-server 192.168.12.100 192.168.12.101** **netbios-name-server 192.168.12.99** **lease 2**
Přeposílání DCHCP žádostí z místního segmentu vzdálenému DHCP serveru (příkaz je umístěn na místním rozhraní).	**ip helper-address 169.223.2.2**
Rozhraní směrovače získá IP adresu od DHCP serveru	**interface fa0/0** **ip address dhcp**
Diagnostika	**show ip dhcp bindings**

NAT (PAT)	
Nastavení rozhraní do vnitřní sítě	**interface FastEthernet0** **ip nat inside**
Nastavení rozhraní do vnější sítě	**interface FastEthernet1** **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, bez něj NAT). Překlad se uplatní na provoz vyhovující ACL 10	**ip nat inside source list 10 interface Ethernet1 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) Ověřit nastavení uvedených proměnných (viz příklad) Nejsou-li v pořádku, pak proměnné nastavit (změnit) tak, jak ukazuje tento výpis	**rommon 1 > set** **IP_ADDRESS=172.18.16.76** **IP_SUBNET_MASK=255.255.255.192** **DEFAULT_GATEWAY=172.18.16.65** **TFTP_SERVER=172.18.16.2** **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. Restartovat směrovač	**rommon 1 > confreg 0x3822** **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) 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 Nastavení hesla „topsecret“ pro čtení a zápis SNMP dat jen z 10.1.1.1	**snmp-server community admins rw** **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** **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** **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** **shutdown** **interface VLAN99** **ip address 192.168.1.2 255.255.255.0** **ip default-gateway 192.168.1.1** **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	
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}**
Rozhraní se učí zaslechnuté MAC adresy Po {n} minutách bude naučená adresa zahozena	**switchport port-security mac-address sticky** **switchport port-security aging time {n}**
Nepovolená komunikace bude zahazována, povolená nikoliv	**switchport port-security violation protect**
Navíc se pošle SNMP trap	**switchport port-security violation restrict**
Rozhraní bude zablokováno, standardně nutný ruční zásah	**switchport port-security violation shutdown**
Automatické odblokování rozhraní po určité době:	**errdisable recovery cause psecure-violation** **errdisable recovery interval 60**

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*}**
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*}** **ip http authentication local**

Password recovery - obnova hesla (postup pro přepínače 29xx/35xx)	
1. Vypnout napájení přepínače	
2. Stisknout a držet tlačítko "Mode" na předním panelu přepínače	**<mode>**
3. Zapnout napájení přepínače	
4. Po zhasnutí STAT LED uvolnit tlačítko "Mode"	
5. Vyčkat ukončení výpisu a na přechod do ROMMONu	
6. Zadat sekvenci příkazů	**flash_init** **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** **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** **switchport mode access** **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 Explicitní vytvoření trunku	**interface fastethernet0/2** **switchport trunk encapsulation dot1q** **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 pojmenování "KUCHYNE"	**vlan database** **vlan 20 name KUCHYNE**
Zařazení rozhraní do VLAN20	**interface ethernet 0/1** **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** **switchport trunk encapsulation isl** **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** **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** **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** **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** **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** **name RSPAN-VLAN** **remote-span**
Monitorovaný přepínač - volba zdroje dat (fyzického rozhraní) a jejich kopírování do určené VLAN	**monitor session 1 source interface Gi0/1 rx** **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** **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> Šifrovat se bude algorimem AES Bude použito sdílené heslo Diffie-Hellman skupina 14 (2048 bitů) Zadání sdíleného hesla a IP adresy druhé strany tunelu	**crypto isakmp policy 10** **encryption aes** **authentication pre-share** **group 14** **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** **set peer 192.168.23.3** **set transform-set MOJE** **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** **ip address 192.168.12.1 255.255.255.0** **crypto map MOJEMAPA**
Ověření stavu tunelu – fáze 1 Ověření stavu tunelu – fáze 2	**show crypto isakmp sa** **show crypto ipsec sa**