

# Základní příkazy Cisco IOS pro správu směrovačů a přepínačů

Josef Kaderka

Universita obrany, Brno

Verse 22

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}**).

## Správa směrovačů

Konfigurační módy – význam promptu	
Uživatelský EXEC mód	Router >
Privilegovaný EXEC mód	Router #
Globální konfigurační mód	Router (config) #
Specifický konfigurační mód – konfigurace rozhraní	Router(config-if)#
– konfigurace logického rozhraní	Router (config-subif) #
– konfigurace směrování	Router(config-router) #
– konfigurace linky (CON, AUX)	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>
Přerušování operace (Break)	<Shift><Ctrl><6><x>
Prosté obnovení 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	
Verze IOSu, velikosti paměti 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

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)	copy startup-config running-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
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	boot system tftp {filename}
Vytvoření lokálního uživatele a přiřazení hesla	username {user} password {password}

<b>Hesla, vzdálený přístup</b>	
Nastavení hesla „class“ pro přístup přes konsolu	<b>line console 0 password class login</b>
Nastavení hesla „class“ pro vzdálený přístup (telnet, ssh), současně až 5 uživatelů (virtuální terminály 0 až 4)	<b>line vty 0 4 password class login</b>
Počet minut do automatického odhlášení (0 – nikdy)	<b>exec-timeout {n}</b>
Nastavení hesla „cisco“ pro přechod do privilegovaného módu	<b>enable password cisco</b>
Hashování (MD5) hesla „cisco“ pro přechod do privilegovaného módu	<b>enable secret cisco</b>
Šifrování všech hesel (slabým algoritmem)	<b>service password-encryption</b>

<b>Vzdálený přístup pomocí ssh</b>	
Nastavení jména vlastní domény	<b>ip domain-name skoleni.org</b>
Vygenerování asymetrických klíčů	<b>crypto key generate rsa</b>
Bude se používat ssh protokol verze 2	<b>ip ssh version 2</b>
Přístup pouze pomocí ssh	<b>line vty 0 4 transport input ssh</b>

<b>Konfigurace sériového rozhraní</b>	
Je to DCE nebo DTE?	<b>show controller serial 0/1/0</b>
Konfigurovat rozhraní (čísla udávají "pozici" modulu)	<b>interface serial 0/1/0</b>
U DCE nutno nastavit kmitočet hodinového signálu	<b>clock rate 64000</b>
Zápis šířky pásma [kb/s] (nemá přímý funkční význam!)	<b>bandwidth 64</b>
Aktivace rozhraní	<b>no shutdown</b>
Ověření stavu rozhraní	<b>show interface serial 0/1/0</b>
Sumární přehled stavu všech rozhraní	<b>show ip interface brief</b>

<b>Konfigurace virtuálního rozhraní (loopback)</b>	
Vytvoření rozhraní typu loopback se zvoleným číslem 0	<b>interface loopback 0</b>
Přiřazení IP adresy rozhraní loopback 0	<b>ip address 10.0.0.1 255.255.255.255</b>

<b>TCP/IP</b>	
Zákaz směrování (standardně je povoleno)	<b>no ip routing</b>
Přiřazení IP adres rozhraním a jejich aktivace	<b>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</b>

<b>Směrování – RIP, RIPv2, EIGRP, OSPF</b>	
Statický směrovací záznam – cílová síť, maska, následující směrovač (157.89.10.1)	<b>ip route 160.216.0.0 255.255.0.0 157.89.10.1</b>
Statický směrovací záznam pro výchozí cestu (default router/gateway - 157.89.10.1)	<b>ip route 0.0.0.0 0.0.0.0 157.89.10.1</b>
Zahrnutí statického směrovacího záznamu o výchozí cestě do informací předávaných směrovacím protokolem	<b>default-information originate</b>
Konfigurace směrovacího protokolu RIP Budou propagovány adresy sítí 157.89.0.0 a 208.1.1.0	<b>router rip network 157.89.0.0 network 208.1.1.0</b>

Konfigurace směrovacího protokolu RIP verze 2 Budou propagovány adresy sítí 157.89.0.0 a 208.1.1.0	<b>router rip version 2 network 157.89.0.0 network 208.1.1.0</b>
Autentizace (jen RIP v2) – místní pojmenování hesla (klíče) Místní číslo klíče Vlastní heslo – sdíleno sousedícími směrovači Zapnutí autentizace (zadat na sousedících rozhraních) Totéž s využitím MD5	<b>key chain KLIC1 key 1 key-string heslo1234 ip rip authentication key-chain KLIC1 ip rip authentication mode md5</b>
Konfigurace směrovacího protokolu EIGRP, autonomní systém 1, zákaz agregace adres podsítí Budou propagovány adresy sítí 157.89.0.0 a 208.1.1.0	<b>router eigrp 1 network 157.89.0.0 network 208.1.1.0 no autosummary</b>
Autentizace EIGRP – místní pojmenování hesla (klíče) Místní číslo klíče Vlastní heslo Zapnutí autentizace (zadat na sousedících rozhraních) Specifikace hesla	<b>key chain MYCHAIN key 1 key-string hojeheslo1234 ip authentication mode eigrp 10 md5 ip authentication key-chain eigrp 10 MYCHAIN</b>
Konfigurace směrovacího protokolu OSPF, tato instance procesu OSPF má číslo 1, area 0 Budou propagovány adresy sítí 157.89.0.0 a 208.1.1.0	<b>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</b>
Autentizace – heslo se zadává se na sousedících rozhraních Autentizace – všechna rozhraní v rámci oblasti 0, heslo se předává otevřeně	<b>ip ospf authentication-key heslo1234 router ospf 1 area 0 authentication</b>
Výpis IP směrovací tabulky	<b>show ip route</b>
Vypisování údajů vyměřovaných protokolem RIP	<b>debug ip rip</b>
Vypisování údajů vyměřovaných protokolem EIGRP	<b>debug ip eigrp events debug ip eigrp transactions</b>
Vypisování údajů vyměřovaných protokolem OSPF	<b>debug ip ospf events</b>

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

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

<b>Rozšířené přístupové seznamy, čísla 100-199, filtruje se dle IP adres odesílatele a příjemce, portů aj.</b>	
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	<b>access-list 100 deny tcp host 1.1.1.1 host 2.2.2.2 eq 23</b>

B. Zákaz surfování uživatelům sítě 3.3.3.0	<b>access-list 100 deny tcp host 3.3.3.0 0.0.0.255 any eq 80</b>
C. Implicitně platí „deny all“, proto je nutno ostatní explicitně povolit	<b>access-list 100 permit ip any any</b>
D. Přiřadit ACL k rozhraní, teprve pak se ACL aktivuje	<b>interface fastethernet 0/0 ip access-group 100 out</b>

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

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

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

<b>Frame-Relay</b>	
<b>Rozhraní</b>	
Povolení Frame-Relay na daném rozhraní a specifikace typu zapouzdření	<b>encapsulation frame-relay ietf</b>
Specifikace typu LMI Type (IOS od verze 11.2 zjišťuje automaticky)	<b>frame-relay lmi-type ansi</b>
Jestliže nebude pracovat inverzní ARP, namapovat vzdálenou IP adresu na naše číslo DLCI (místní)	<b>frame-relay map ip 3.3.3.100 broadcast</b>
<b>Lze rovněž povolit rozhlašování a specifikovat typ zapouzdření</b>	
Definovat místní DLCI (nepracuje-li LMI)	<b>frame-relay local-dlci 100</b>
Nastavit periodu pro kontrolu udržení spojení	<b>keepalive 10</b>
<b>Kontrola nastavení</b>	
Výpis informací o DLCI a LMI	<b>show interface serial 0</b>
Výpis statistik o provozu PVC	<b>show frame-relay pvc</b>
Výpis směrovací mapy (statické nebo dynamické)	<b>show frame-relay map</b>
Výpis LMI informací	<b>show frame-relay lmi</b>
<b>Degradace směrovače do role Frame Relay přepínače (pro laboratorní účely)</b>	
<b>Poznámka –příkazy je nutno symetricky zadat vždy na obou DCE rozhraních, která mají propojena pomocí Frame Relay</b>	

Povolit Frame-Relay přepínání (na té straně směrovače, kde je DCE)	<b>frame-relay switching</b>
Řekni DCE straně, aby podporovala frame-relay funkce DCE na daném rozhraní	<b>frame-relay intf-type dce</b>
Řekni DCE straně, na které jiné místní rozhraní {int_o} a DLCI {dlci_o} přepínat DLCI {dlci_i} z právě konfigurovaného rozhraní	<b>frame-relay route {dlci_i} interface {int_o} {dlci_o}</b>
Nastavit na DCE rozhraní hodinový kmitočet [b/s]	<b>clock rate 64000</b>

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

<b>DHCP</b>	
Explicitní aktivace DHCP serveru (jen u některých IOSů)	<b>service dhcp</b>
Tyto adresy IP z přidělování (viz uvedený rozsah) vynechat	<b>ip dhcp exclude-address 157.89.1.1 157.89.1.2</b>
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).	<b>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</b>
Přeposílání DHCP žádostí z místního segmentu vzdálenému DHCP serveru (příkaz je umístěn na místním rozhraní).	<b>ip helper-address 169.223.2.2</b>
Rozhraní směrovače získá IP adresu od DHCP serveru	<b>interface fa0/0 ip address dhcp</b>
Diagnostika	<b>show ip dhcp bindings</b>

<b>NAT (PAT)</b>	
Nastavení rozhraní do vnitřní sítě	<b>interface FastEthernet0 ip nat inside</b>
Nastavení rozhraní do vnější sítě	<b>interface FastEthernet1 ip nat outside</b>
Překládat se bude veškerý provoz (obecně ACL může mít jakoukoliv jinou podobu)	<b>access-list 10 permit any</b>
Celá vnitřní síť se ukryje za jedinou adresu. Překlad se uplatní na provoz vyhovující ACL 10	<b>ip nat inside source list 10 interface Ethernet1 overload</b>

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

<b>Password Recovery - obnova hesla (postup pro směrovače)</b>	
1. Přerušit start pomocí konsoly (vyžaduje se fyzické přístupu)	<b>&lt;Ctrl&gt;&lt;Break&gt;</b>
2. Zavést IOS z flash, nenačítat konfigurační soubor z NVRAM	<b>confreg 0x2142</b>

2a. Jiná syntaxe platná u starších zařízení	<b>o/r 0x2142</b>
3. Restart operačního systému	<b>reset</b>
4. Přejít do privilegovaného módu; nenačtením konfiguračního souboru lze provést bez hesla	<b>enable</b>
5. Nyní v privilegovaném módu překopírovat konfigurační soubor z NVRAM do RAM	<b>copy startup-config running-config</b>
6. Změnit enable hesla na "NoveHeslo" (případně provést další operace)	<b>enable password NoveHeslo</b>
7. Uložit aktuální konfiguraci do NVRAM (tj. s novým heslem)	<b>copy running-config startup-config</b>
8. Příští start směrovače necht' proběhne normálně (IOS z flash, konfigurační soubor z NVRAM)	<b>config-reg 0x2102</b>

<b>Obnova chybějícího operačního systému IOS (pouze u směrovačů, s rozhraním Ethernet)</b>	
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, nýbrž postupovat standardně – <b>copy tftp flash</b> (tedy spustit tftp server, připravit záložní IOS). U nových směrovačů s výměnnou pamětí flash na ni lze IOS zapsat v externí zařízení (PC), rovněž lze použít 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).	<b>rommon 1 &gt; set</b> <b>IP_ADDRESS=172.18.16.76</b> <b>IP_SUBNET_MASK=255.255.255.192</b> <b>DEFAULT_GATEWAY=172.18.16.65</b> <b>TFTP_SERVER=172.18.16.2</b> <b>TFTP_FILE=c2600-ik9o3s3-mz.123-13.bin</b>
Příklad nastavení/změny hodnoty proměnné	<b>TFTP_SERVER=172.18.16.88</b>
Spustit stahování a instalaci IOSu	<b>tftpdnld</b>
Restartovat směrovač	<b>reset</b>

<b>Obnova chybějícího operačního systému IOS (pouze u směrovačů bez rozhraní Ethernet)</b>	
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 v emulačním programu Restartovat směrovač.	<b>rommon 1 &gt; confreg 0x3822</b>  <b>rommon 2 &gt; reset</b>
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)	<b>rommon 1 &gt; xmodem c2600-ik9o3s3-mz.123-13.bin</b>
Nastavit výchozí hodnotu konfiguračního registru	<b>config-register to 0x2102</b>
Restartovat směrovač	<b>reset</b>

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

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

<b>Správa sítě - SNMP</b>	
Nastavení hesla „admins“ pro čtení a zápis SNMP dat	<b>snmp-server community admins rw</b>
Nastavení hesla „topsecret“ pro čtení a zápis SNMP dat jen z 10.1.1.1	<b>snmp-server community topsecret rw 60</b> <b>access-list 60 permit 10.1.1.1</b>

Nastavení hesla „others“ pro čtení SNMP dat (běžná hodnota je „public“)	<b>snmp-server community others ro</b>
Toto je pán směrovače	<b>snmp-server contact Josef Kaderka</b>
Tady se směrovač nalézá	<b>snmp-server location Brno, Sumavska 4, 3/11a</b>
SNMP manager, tam posílat zprávy (traps) s community public	<b>snmp-server host 10.1.1.1 public</b>
Povolení odesílat zprávy při vzniku jakékoliv události	<b>snmp-server enable traps</b>
Odesílat zprávy jen při vzniku události daného typu	<b>snmp-server enable traps config snmp-server enable traps envmon temperature</b>



## Správa přepínačů

(základní úkony jsou stejné jako u směrovačů)

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

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

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.	<b>interface VLAN1 shutdown interface VLAN99 ip address 192.168.1.2 255.255.255.0 ip default-gateway 192.168.1.1 no shutdown</b>
Výpis tabulky přepínači známých MAC adres	<b>show mac-address-table</b>
Počet MAC adres v tabulce (vhodné při podezření na přeplnění)	<b>show mac-address-table count</b>
Vymazání tabulky MAC adres	<b>clear mac-address-table</b>

Konfigurace rozhraní pro připojení stanice	
Volba rozhraní	<b>interface gigabit 0/1</b>
Tatáž operace nad více rozhraními (jen u novějších přepínačů); syntax vyžaduje uvedení mezer kolem pomlčky!	<b>interface range fastethernet 0/1 – 12</b>
Volba plného duplexu	<b>duplex full</b>
Volba rychlosti 100 Mb/s	<b>speed 100</b>
K rozhraní bude připojena výhradně stanice	<b>switchport mode access</b>
Rozhraní se po připojení stanice ihned aktivuje, nečeká se na STP	<b>spanning-tree portfast</b>

Zabezpečení rozhraní přepínače	
Přes rozhraní může komunikovat jen stanice s danou MAC adresou	<b>switchport port-security mac-address {adr}</b>
Přes rozhraní může komunikovat nejvýše {n} stanic	<b>switchport port-security maximum {n}</b>
Rozhraní se učí zaslechnuté MAC adresy	<b>switchport port-security mac-address sticky</b>
Po {n} minutách bude naučená adresa zahozena	<b>switchport port-security aging time {n}</b>
Nepovolená komunikace bude zahazována, povolená nikoliv	<b>switchport port-security violation protect</b>
Pošle se SNMP trap	<b>switchport port-security violation restrict</b>
Rozhraní bude zablokováno, standardně nutný ruční zásah	<b>switchport port-security violation shutdown</b>
Automatické znovuobdobování rozhraní po určité době:	<b>errdisable recovery cause psecure-violation errdisable recovery interval 60</b>

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

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

<b>Obnova hesla u přepínačů 2900/2950/3500/3550</b>	
1. Vypnout napájení přepínače	
2. Stisknout a držet tlačítko "Mode" na předním panelu přepínače	<b>&lt;mode&gt;</b>
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	<b>flash_init</b> <b>load_helper</b>
7. Přejmenovat konfigurační soubor (je uložen ve flash, ne v NVRAM)	<b>rename flash:config.text flash:config.old</b>
8. Zavést operační systém přepínače	<b>boot</b>
9. Přeskočit konfigurační dialog, přejít do privilegovaného módu	<b>enable</b>
10. Obnovit konfigurační soubor	<b>rename flash:config.old flash:config.text</b>
11. Načíst uloženou konfiguraci, tj. se starým heslem	<b>copy startup-config running-config</b>
12. Nastavit nové heslo pro přechod do privilegovaného módu	<b>enable secret class</b>
13. Uložit aktuální konfiguraci, tj. s novým heslem	<b>copy running-config startup-config</b>

<b>Virtuální LAN (VLAN) a trunking</b>	
Globální konfigurační mód, vytvoření VLAN s číslem 20 a její pojmenování "VLAN20"	<b>vlan 20</b> <b>name VLAN20</b>
Zařazení rozhraní do VLAN číslo 20 . Pokud dosud neexistovala, bude vytvořena.	<b>interface fastethernet 0/1</b> <b>switchport mode access</b> <b>switchport access vlan 20</b>
Seznam virtuálních LAN a do nich zařazených rozhraní	<b>show vlan</b>
Volba zapouzdření (ISL nebo 802.1q; jen pokud IOS podporuje obě dvě) a vytvoření trunku	<b>interface fastethernet0/2</b> <b>switchport trunk encapsulation dot1q</b> <b>switchport mode trunk</b>
Netagované rámce dávat do VLAN 5 (implicitně jdou do VLAN 1)	<b>switchport trunk native vlan 5</b>
Trunkem mohou procházet pouze rámce z/do VLAN 5, 10, 20	<b>switchport trunk allowed vlan 5,10,20</b>

<b>Virtuální LAN (VLAN) a trunking u starších přepínačů</b>	
Privilegovaný EXEC mód, vytvoření VLAN s číslem 20 a její pojmenování "VLAN20"	<b>vlan database</b> <b>vlan 20 name VLAN20</b>
Zařazení rozhraní do VLAN20	<b>interface ethernet 0/1</b> <b>vlan static 20</b>
Seznam virtuálních LAN a do nich zařazených rozhraní	<b>show vlan-membership</b>
Volba zapouzdření (ISL nebo 802.1q; jen pokud IOS podporuje obě dvě) a vytvoření trunku	<b>interface fastethernet0/2</b> <b>switchport trunk encapsulation isl</b> <b>switchport mode trunk</b>

<b>Komunikace mezi virtuálními LAN (metoda „router on a stick“)</b>	
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	<b>interface fastethernet 0/0</b> <b>no shutdown</b>
Vytvoření logického rozhraní (číslo libovolné, např. totéž jako u VLAN)	<b>interface fastethernet 0/0.20</b>
Volba zapouzdření a specifikace čísla VLAN	<b>encapsulation dot1q 20</b>
Přiřazení IP adresy logickému rozhraní	<b>ip address 192.168.5.20 255.255.255.0</b>

<b>Sdružení několika rozhraní do jediného o kumulované rychlosti (Etherchannel)</b>	
---	--

Volba rozhraní (všechna musí být nastavena stejně; v režimu trunk nebo access) a skupiny	<b>interface range FastEthernet0/1 - 4 channel-group 1 mode auto</b>
--	--

<b>Monitorování provozu jednoho či více rozhraní či VLAN jiným rozhraním (SPAN - Switched Port Analyzer)</b>	
--	--

Volba zdroje provozu (všechna rozhraní musí být nastavena stejně)	<b>monitor session 1 source interface FastEthernet0/1 monitor session 1 source interface FastEthernet0/2</b>
---	--

Zde se bude provoz monitorovat	<b>monitor session 1 destination interface gigabitEthernet0/1</b>
--------------------------------	---

Ověření stavu	<b>show monitor session 1</b>
---------------	-------------------------------