EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Vysoká škola báňská – Technická univerzita Ostrava

Fakulta strojní

KONFIGURACE SÍŤOVÝCH PRVKŮ A PROTOKOLŮ

Studijní opora předmětu „Počítačové systémy“

Marek Babiuch

Ostrava 2011

Tyto studijní materiály vznikly za finanční podpory Evropského sociálního fondu (ESF) a rozpočtu České republiky v rámci řešení projektu OP VK CZ.1.07/2.3.00/09.0147 „Vzdělávání lidských zdrojů pro rozvoj týmů ve vývoji a výzkumu“.

Recenze: <Jméno recenzenta> [Poznámka: případně se tento řádek odstraní]

Název: Konfigurace síťových prvků a protokolů
Autor: Marek Babiuch
Vydání: první, 2011
Počet stran: 65
Náklad:
Studijní materiály pro studijní obor 3902T004-00 Automatické řízení a inženýrská informatika Fakulty strojní
Jazyková korektura: nebyla provedena.

Tyto studijní materiály vznikly za finanční podpory Evropského sociálního fondu a rozpočtu České republiky v rámci řešení projektu Operačního programu Vzdělávání pro konkurenceschopnost.

Název: Vzdělávání lidských zdrojů pro rozvoj týmů ve vývoji a výzkumu
Číslo: CZ.1.07/2.3.00/09.0147
Realizace: Vysoká škola báňská – Technická univerzita Ostrava

ISBN <(bude zajištěno hromadně)>

POKYNY KE STUDIU

KONFIGURACE SÍŤOVÝCH PRVKŮ A PROTOKOLŮ

Pro předmět 2. semestru oboru Automatické řízení a inženýrská informatika jste obdrželi studijní balík obsahující:

Pro studium problematiky konfigurace síťového hardwarového zařízení jste obdrželi studijní balík obsahující:

- Učební oporu s výkladem a praktickými příklady,
- přístup do e-learningového portálu obsahující doplňkové animacemi vybraných částí kapitol,
- CD-ROM s doplňkovými animacemi vybraných částí kapitol,

Prerekvizity

Pro studium tohoto předmětu se nepředpokládá absolvování nějakého speciálního předmětu, počítačová gramotnost a základy administrace nějakého operačního systému je však nutností.

Pro studium této opory se předpokládá znalost na úrovni absolventa předmětu Internet a sítě popř. Programování aplikací pro Internet bakalářského oboru Aplikovaná informatika a řízení.

Cílem učební opory

Cílem je seznámení se základními pojmy konfigurace síťových zařízení, především tedy routeru. Po prostudování modulu by měl student být schopen administrovat na konzoli routeru složitější topologie počítačových síti.

Pro koho je předmět určen

Modul je zařazen do magisterského studia oboru 3902T004-00 Automatické řízení a inženýrská informatika, ale může jej studovat i zájemce z kteréhokoliv jiného oboru, pokud splňuje požadované prerekvizity.

Při studiu každé kapitoly doporučujeme následující postup:

Čas ke studiu: xx hodin

Na úvod kapitoly je uveden čas potřebný k prostudování látky. Čas je orientační a může vám sloužit jako hrubé vodítko pro rozvržení studia celého předmětu či kapitoly. Někomu se čas může zdát příliš dlouhý, někomu naopak. Jsou studenti, kteří se s touto problematikou ještě nikdy nesetkali a naopak takoví, kteří již v tomto oboru mají bohaté zkušenosti.

Cíl: Po prostudování tohoto odstavce budete umět

- Popsat …
- Definovat …
- Vyřešit …

Ihned potom jsou uvedeny cíle, kterých máte dosáhnout po prostudování této kapitoly – konkrétní dovednosti, znalosti.

Výklad

Následuje vlastní výklad studované látky, zavedení nových pojmů, jejich vysvětlení, vše doprovázeno obrázky, tabulkami, řešenými příklady, odkazy na animace.

Otázky

Pro ověření, že jste dobře a úplně látku kapitoly zvládli, máte k dispozici několik teoretických otázek.

Úlohy k řešení

Protože většina teoretických pojmů tohoto předmětu má bezprostřední význam a využití v praxi, jsou Vám nakonec předkládány i praktické úlohy k řešení. V nich je hlavním významem předmětu schopnost aplikovat čerstvě nabyté znalosti pro řešení reálných situací.

Řešený příklad

Zadání a řešení praktického příkladu jako součást výukového textu. Tento příklad je velmi důležitý pro pochopení výkladu.

Pojmy k zapamatování

Pojem k zapamatování je velice důležitý fakt, který je důležité znát, neboť s ním budeme neustále pracovat.

Korespondenční úkol

Zadání samostatné úlohy, které pomůže pochopit probíranou problematiku.

Další zdroje

Seznam další literatury, www odkazů apod., pro zájemce o dobrovolné rozšíření znalostí popisované problematiky.

Odkaz na animaci

Popis animace, která je součástí výukového modulu a je přiřazena k dané kapitole.

Odpovědi na otázky

Na závěr učebního textu jsou připraveny odpovědi na otázky ze všech kapitol učebního textu. Tato kapitola je umístěna záměrně až na závěr a doporučuji si nejprve na otázky zkusit odpovědět bez použití nápovědy.

Úspěšné a příjemné studium s tímto učebním textem Vám přeje Marek Babiuch.

OBSAH

1 PROSTŘEDÍ APLIKACE CISCO PACKET TRACER

V učební opoře si budeme moci probrané učivo praktického charakteru vyzkoušet přímo v aplikačním prostředí firmy Cisco, která je největším světovým výrobcem síťových prvků a technologií. V tomto programu můžeme nejen vyzkoušet propojování síťových prvků a navrhování topologie sítě, ale můžeme zde přímo simulovat reálný běh aplikací s konfigurací síťových prvků a sledováním paketů mnoha síťových protokolů.

Čas ke studiu: 3 hodiny

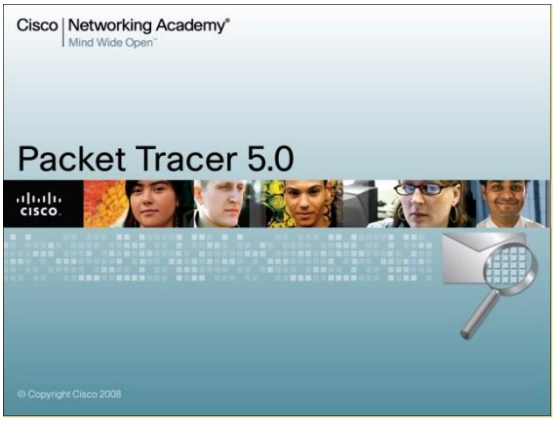
Cíl: Po prostudování tohoto odstavce budete umět

- Pracovat v prostředí Cisco Packet Tracer.
- Navrhovat zapojení síťových prvků.
- Tvořit topologii sítě ze síťových a koncových prvků.
- Používat návrhový a simulační mód aplikace.
- Simulovat komunikaci dvou zařízení.

Výklad

1.1 Základní popis prostředí

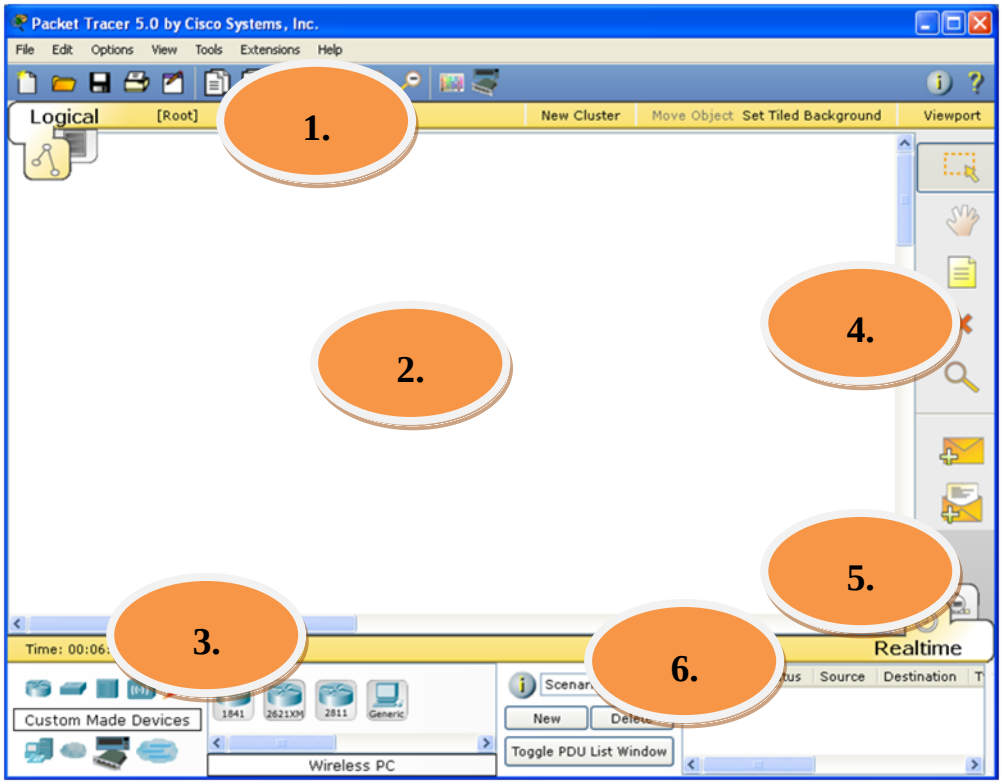
Program Packet Tracer nevyžaduje žádné speciální HW nároky a jeho instalace je jednoduchá. Po spuštění programu uvidíme *splashscreen* aplikace viz obr. 1.1 a poté se již spustí aplikace a zobrazí se pracovní plocha.



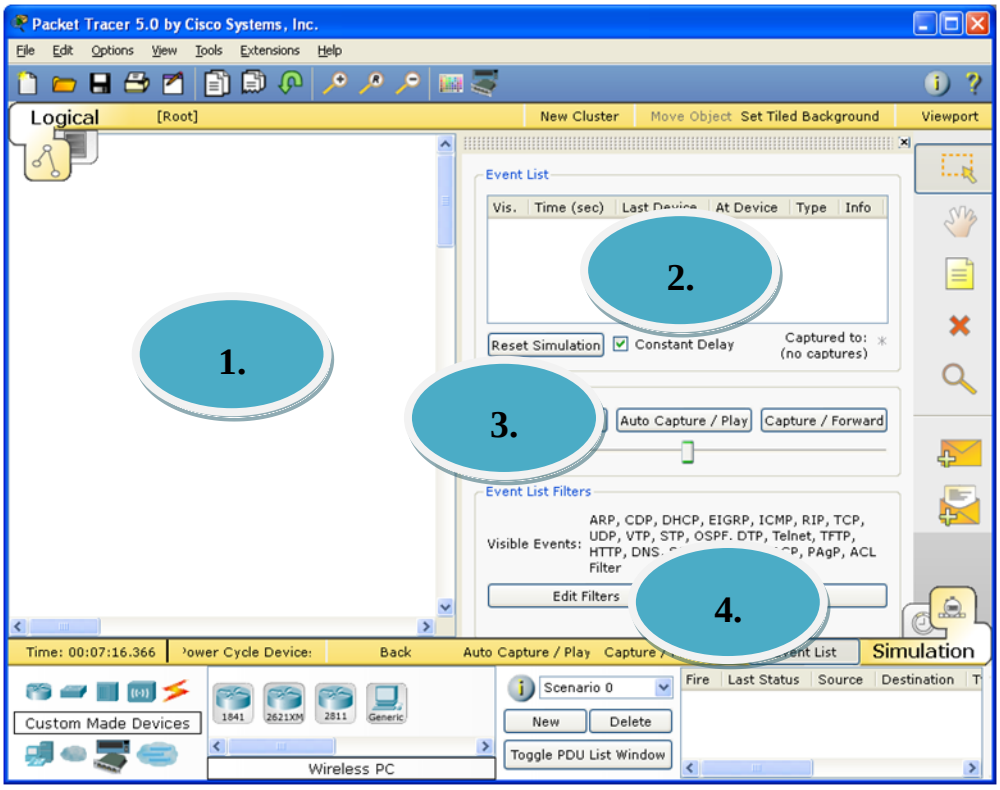
Obrázek 1.1 – Cisco Packet Tracer 5.0

Okno aplikace je zobrazeno na obrázku 1.2. Při spuštění aplikace vidíme její tyto součásti: 1. Menu programu a panel rychlého spuštění, 2. Pracovní plocha aplikace, na kterou budeme vkládat všechny prvky a vytvářet topologie sítě, 3. Výběr všech dostupných síťových

a koncových zařízení, 4. Panel nástrojů, 5. Přepínač reálného a simulačního módu a 6. Výběr simulačních scénářů a jejich status.



Obrázek 1.2 – Pracovní plocha programu Packet Tracer 5.0

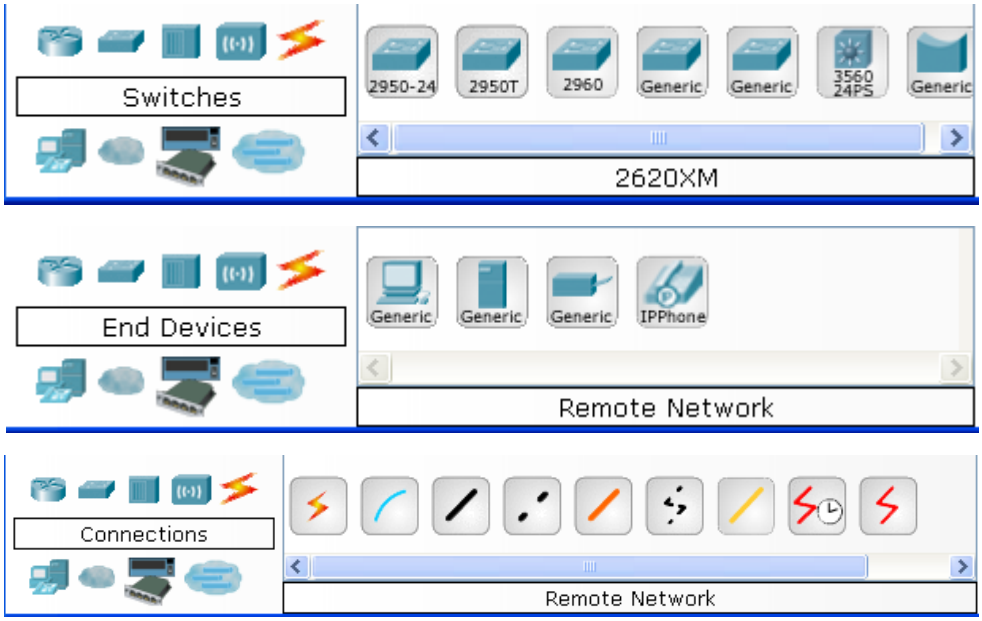


Obrázek 1.3 – Okno simulačního režimu programu Packet Tracer 5.0

Při přepnutí do simulačního módu zůstane z minulého zobrazení pracovní plocha - 1, dále se objeví okno zobrazení simulace paketů – 2, Tlačítka pro souvislé či částečné snímkování paketů – 3 a také seznam dostupných protokolů s filtrem zobrazující výběr paketů - 4.

1.2 Vkládání prvků na pracovní plochu a jejich propojení

Ve spodní části aplikace vidíme možné síťové a koncové prvky, které můžeme vkládat na pracovní plochu. Patří mezi ně převážně routery, switche a koncová zařízení typu PC, server a tiskárna. Důležitým prvkem je typ propojení, viz obrázek 1.4 dole, kterým propojíme všechny prvky v síťové topologii.



Obrázek 1.4 – Možnosti vložení zařízení typu switch, koncové zařízení a jejich propojení

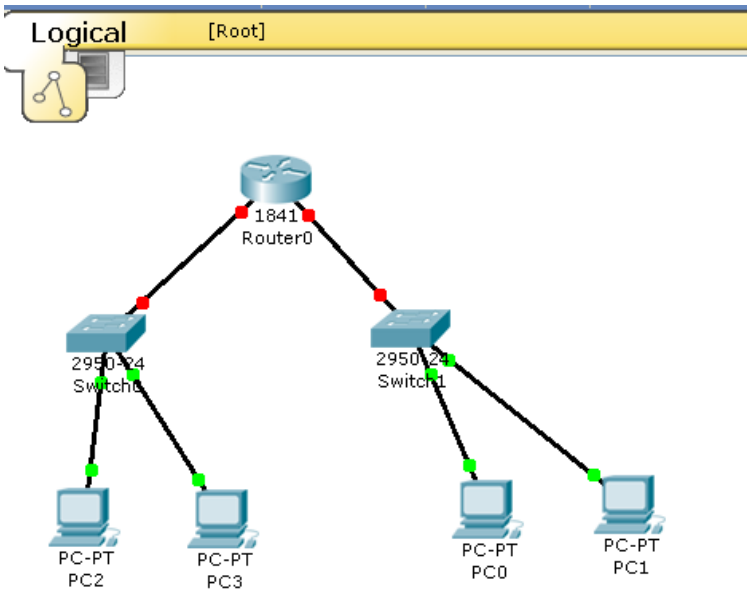
Řešený příklad 1.1 – Vytvoření jednoduché topologie

V prvním příkladu vytvoříme jednoduchou topologii, která bude obsahovat router, do něj připojené dva switche, z nichž každý bude obsahovat dvojici PC. V tomto příkladu budeme prvky pouze umisťovat na pracovní plochu a následně propojovat, ještě je nebudeme konfigurovat. Konfiguraci jednotlivých prvků probereme v následující kapitole. Základní postup je následující:

1. Ve spodním panelu viz obr. 1.2 – označení panelu 3 vybereme záložku *Routers* a libovolný router přetáhneme myší na pracovní plochu.
2. Ve stejném panelu překlikneme a záložku *switches* a přetáhneme na pracovní plochu dva switche.
3. Obdobným způsobem přesuneme na pracovní plochu čtyři PC ze záložky *End devices*.
4. V záložce *connections* vybereme přímý kabel (*Copper Straight-Through*) a klikneme na router. Ten nabídne dostupné ethernetové zařízení, které zvolíme a

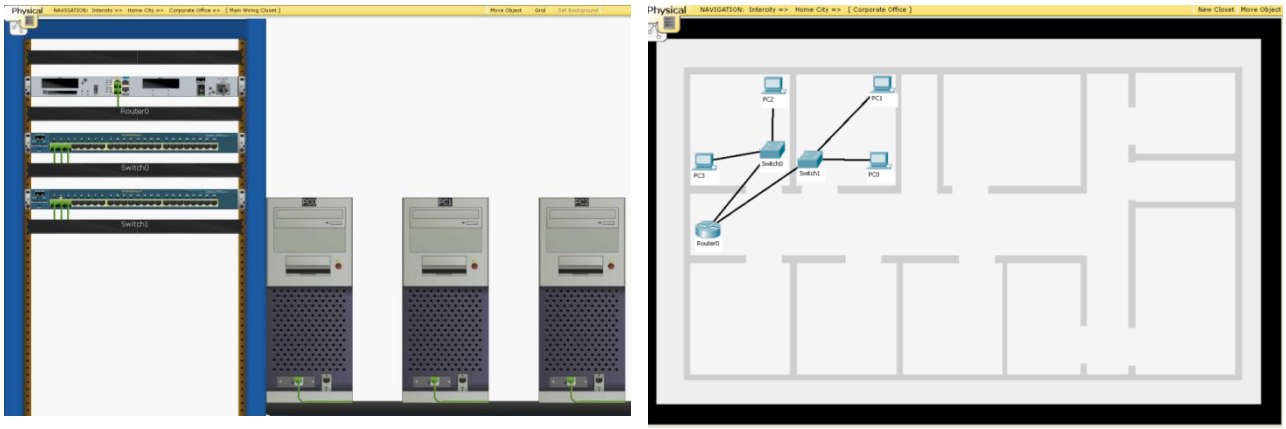
propojíme router se switchem. Switch obsahuje dle své funkčnosti větší množství eternetových portů. Jeden z nich zvolíme a tím dokončíme propojení routeru se switchem. Propojení na druhý switch má stejný postup.

5. Zbývá propojit switch s PC. Zvolíme opět přímý kabel a libovolný port switche, při propojení s PC máme obvykle na výběr pouze jeden ethernetový port. Dokončíme tak propojení a stejným postupem propojíme zbylá PC na switche. Výsledná logická topologie je na obrázku 1.5.



Obrázek 1.5 – Návrh logické topologie

V horním rohu pracovní plochy se nachází přepínač mezi logickou a fyzickou topologií. Logická topologie je pracovní návrh, který vidíme na obrázku 1.5. Oproti tomu fyzické rozmístění v *rackové* skříni a dokonce umístění v jednotlivých místnostech můžeme navrhnout po přepnutí na fyzickou topologii. Na obrázku 1.6 vidíme fyzická zařízení a jejich návrh rozmístění. Fyzickým rozmístěním se však nebudeme vůbec zabývat, v tomto učebním materiálu nám půjde především o funkčnost a konfigurace jednotlivých prvků.



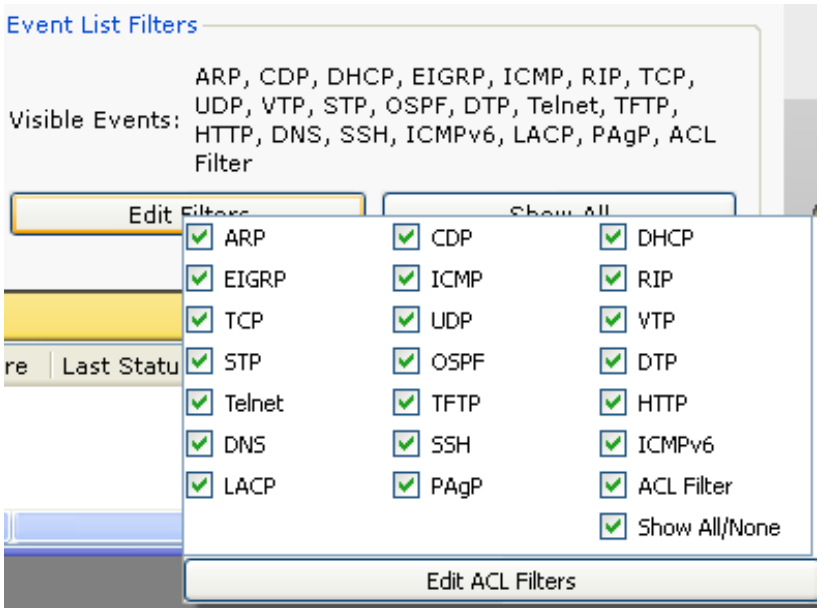
Obrázek 1.6 – Šasi síťových prvků, koncových zařízení a fyzická topologie

1.3 Monitorování paketů v simulačním režimu

Program *Cisco Packet Tracer* je mocným nástrojem, který umí simulovat běh paketů v síti. Tuto funkcionalitu zajistíme přechodem mezi *real-time* a simulačním módem přepínačem v pravém dolním rohu aplikace.

Obrázek 1.7 – Přepínací záložky mezi reálným a simulačním režimem

Před samotným přepnutím do simulačního módu však musíme označit dvě koncová zařízení komunikace. Tu nejčastěji ověřujeme příkazem *ping*, v panelu nástrojů k tomu máme přizpůsobenou ikonu s obálkou s názvem *add komplex PDU*. Po označení komunikujících zařízení můžeme přejít do simulačního módu.

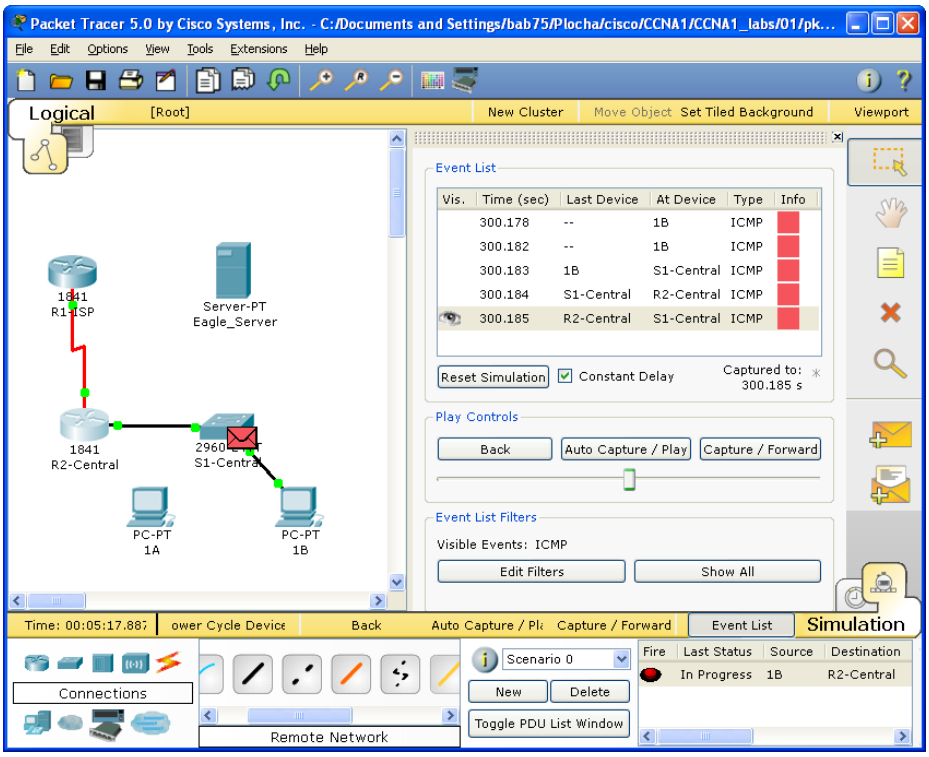


Obrázek 1.8 – Možnost volby sledování konkrétních paketů protokolů

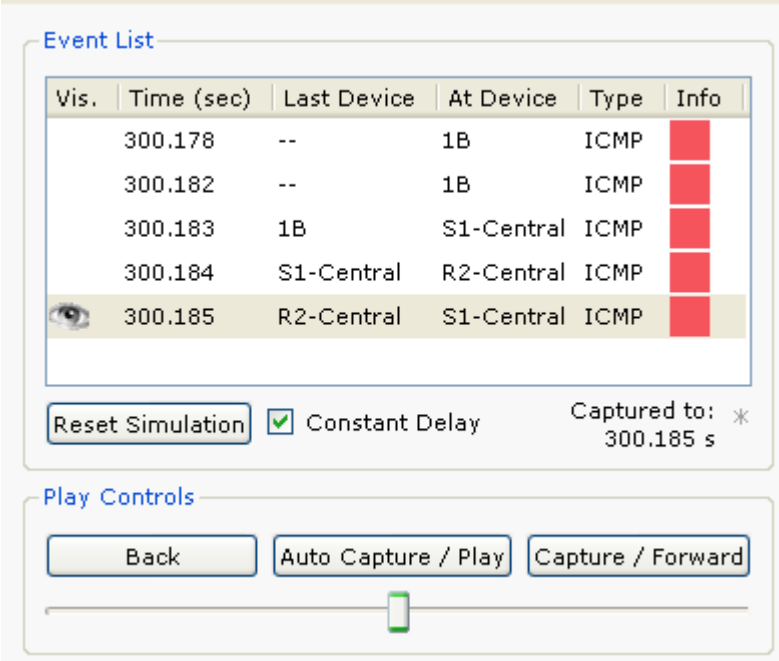
V simulačním módu můžeme ihned spustit simulaci toku paketů po síti tlačítkem *Play* popřípadě krokovat komunikaci tlačítkem *Capture*. Můžeme však také využít filtru na konkrétní typ protokolu, pokud nás zajímají pouze určité typy paketů. Na obr. 1.8 vidíme všechny protokoly, které můžeme v naší simulaci sledovat.

Po spuštění simulace ať už tlačítkem *Play* či *Capture* můžeme v okně událostí *Event List* prohlídnout posloupnost probíhajících paketů podle filtru. Aktuální paket je označen vlevo obrázkem oka viz obr. 1.9.

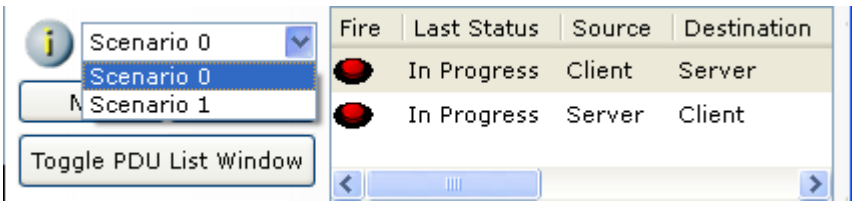
Pokud na aktuální paket klikneme, zobrazíme množství detailů paketu včetně náhledů celého paketu resp. PDU na vrstvách ISO/OSI modelu. Na obr. 1.10 můžeme vidět právě probíhající posloupnost paketů (*Event List*). Každá simulace, která vznikne při propojení dvou prvků pomocí *add komplex PDU* se zobrazí v seznamu scénářů, viz obr. 1.11. Můžeme vytvářet libovolné množství scénářů, jejich simulace přitom probíhá najednou, tak jako v běžném provozu sítě.



Obrázek 1.9 – Simulace toku ICMP paketů v definované topologii



Obrázek 1.10 – Posloupnost paketů s možností detailního náhledu

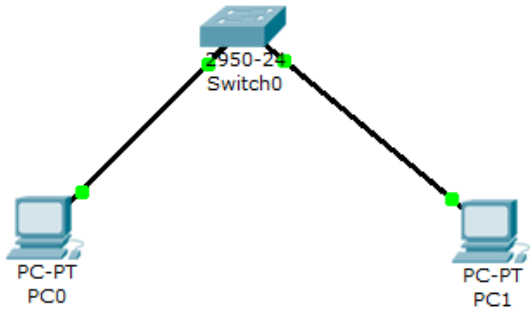


Obrázek 1.11 – List scénářů simulace

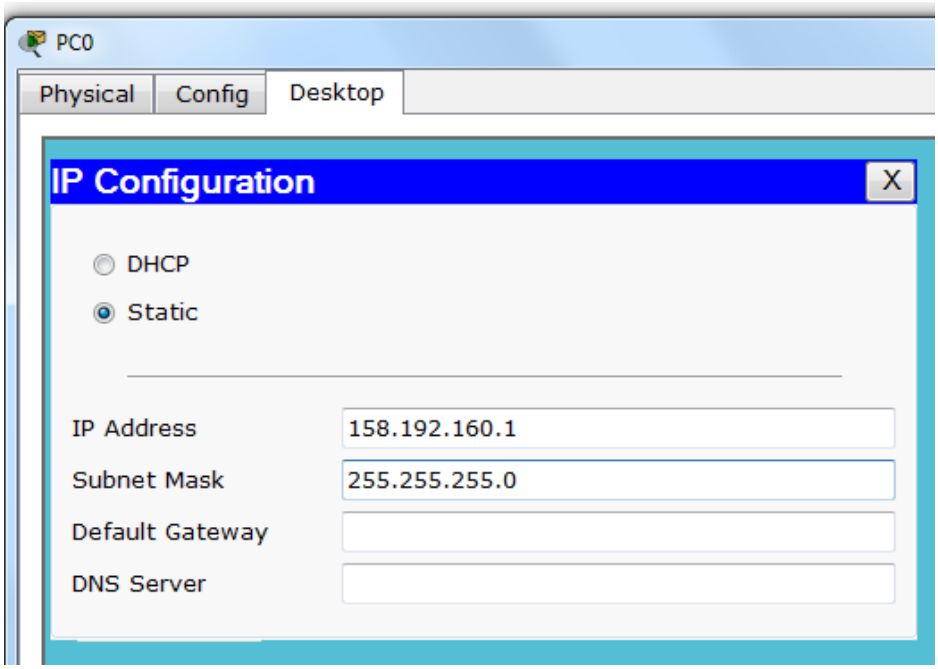
Řešený příklad 1.2 – Sledování paketů v simulačním režimu

Protože v této kapitole ještě nebudeme konfigurovat síťové prvky a přesto chceme vyzkoušet simulační režim toku paketů, vytvoříme úplně jednoduchou topologii, kdy propojíme přes switch dvě PC:

1. Vložíme na pracovní plochu switch a dvě PC.
2. Přejdeme na záložku *connections* a vybereme přímý kabel, propojíme oba počítače se switchem.
3. Je nutné nakonfigurovat IP adresy počítačů, přejdeme kliknutím do konfiguračního režimu PC a zadáme IP adresu počítačů, tak aby byli ze stejného adresového rozsahu, např. 158.192.160.1 a 158.192.160.2 s maskou 255.255.255.0
4. Z panelu nástrojů vybereme ikonku s obálkou (*add komplex PDU*) a klikneme postupně na obě PC.
5. Přepneme se přepínačem do simulačního režimu. Tlačítkem *Capture* sledujeme pohyb paketů v jednoduché síti. Detaily paketu si můžeme prohlédnout.



Obr. 1.12 – Vytvoříme toto propojení pro simulaci pingu dvou PC



Obr. 1.13 – Nastavení IP adresy prvního PC

Pojem k zapamatování - Paket

Pojem paket se v běžné řeči používá obecně pro datovou jednotku putující v počítačové síti. Tento pojem je však zavádějící, neboť datová jednotka má na každé vrstvě síťového modelu své přesné pojmenování. Obecný termín je protokolová datová jednotka (*Protocol Data Unit*).

- Data – Na aplikační vrstvě je pro PDU používán termín data.
- Segment – Transportní vrstva přidá na začátek hlavičku svého konkrétního protokolu.
- Paket – na síťové vrstvě je k segmentu z předchozí vrstvy přidána na začátek hlavička síťového protokolu.
- Rámec – Na úrovni vrstvy síťového rozhraní protokol přibaluje nejen hlavičku ale také zakončení rámce.

Ke kapitole 1 je připravena animace č. 1

V této animaci si ukážeme, jaké prvky budeme používat při tvorbě síťových topologií. Na pracovní plochu si umístíme zařízení typu router, switch a PC a budeme je propojovat různým typem kabelu. Ukážeme si jednoduchou konfiguraci IP adres s ping ověřením v reálném i simulačním módu s prohlížením detailů paketů.

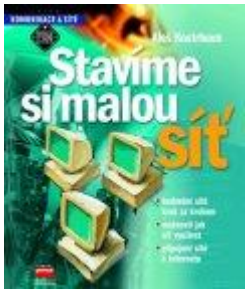
Otázky ke kapitole 1

1. K čemu slouží příkaz *ping*?
2. Je nějaký rozdíl mezi paketem a rámcem nebo je to jen podobný termín?

Úlohy k řešení ke kapitole 1

1. Vytvořte svou vlastní topologii na pracovní plochu včetně propojení zařízení.
2. Propojte dvě PC přes switch, nastavte IP adresy a odsimulujte *ping* z jednoho PC na druhý.

Další zdroje



Aleš Kostrhoun, Stavíme si malou síť, 216 stran, nakladatelství: Computer press, 2001,

Úvod je věnován přednostem počítačových sítí, dále nejdůležitějším pojmům, bez jejichž znalosti by nebylo možné pochopit pokročilejší kapitoly, je zde rovněž detailně prodiskutována finanční a technická náročnost vybudování sítě. V dalších kapitolách najdete veškeré nutné úkony a operace, které je třeba provést ve fázi instalace síťových komponent a následného propojení počítačů do sítě.

eArchiv.cz
archiv článků a přednášek Jiřího Peterky

Jiří Peterka, Počítačové sítě, online dostupné z: http://www.earchiv.cz/.

2 ROUTER A JEHO KONFIGURAČNÍ KONZOLE

V této kapitole se již budeme věnovat konfiguraci routeru, nejprve obecně konfiguračním módům, poté již konkrétním příkazům. Na začátku konfiguračních nastavení je nezbytné umět konfigurační konzoli zabezpečit hesly. Poté se budeme věnovat samotnému nastavení rozhraní routeru, tak abychom dokázali definovat síťové topologie. Všechny konfigurace budou ověřeny přímo v aplikačním prostředí firmy Cisco, v programu Packet Tracer, který nám umožní přesné chování skutečného routeru.

Čas ke studiu: 3 hodiny

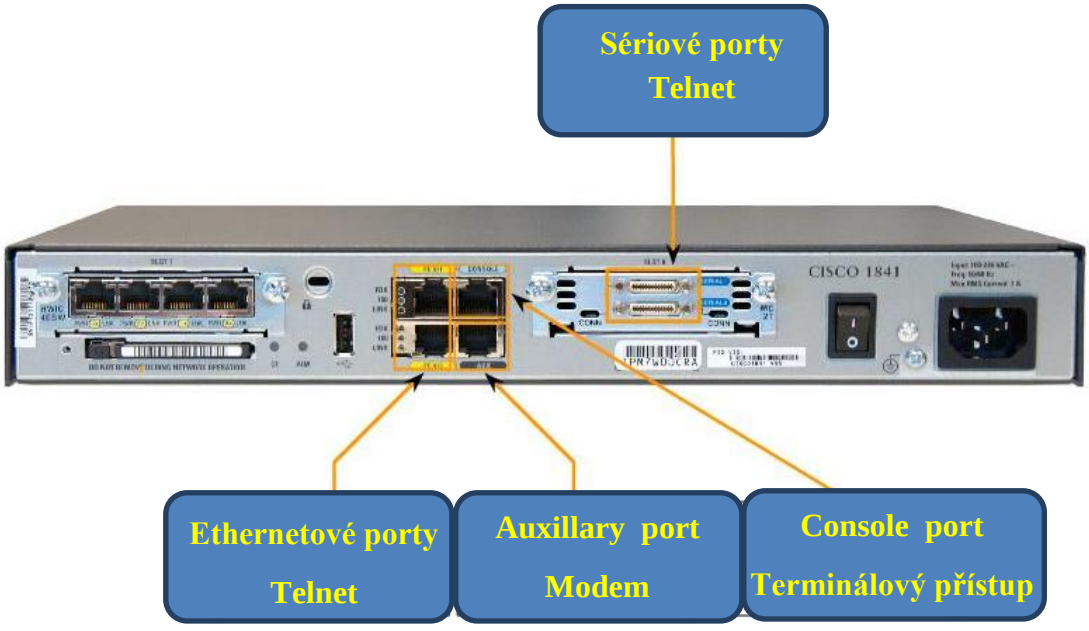
Cíl: Po prostudování tohoto odstavce budete umět

- Přechody mezi konfiguračními režimy routeru.
- Základní konfigurační příkazy routeru.
- Zabezpečit konzoli routeru, vzdálený přístup i privilegovaný konfigurační mód.
- Konfigurovat sériový i ethernetový interface routeru.
- Připojit se vzdáleně ke konzoli routeru pomocí telnet utility.

Výklad

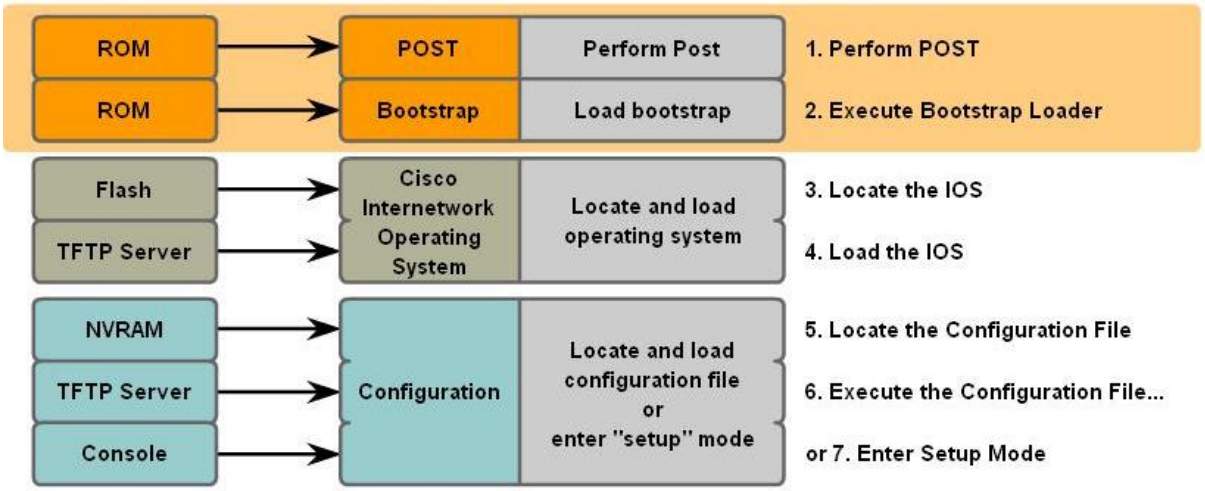
2.1 Router jako počítač

Na prvním obrázku vidíme router Cisco 1841, respektive jeho zadní část. Ačkoliv



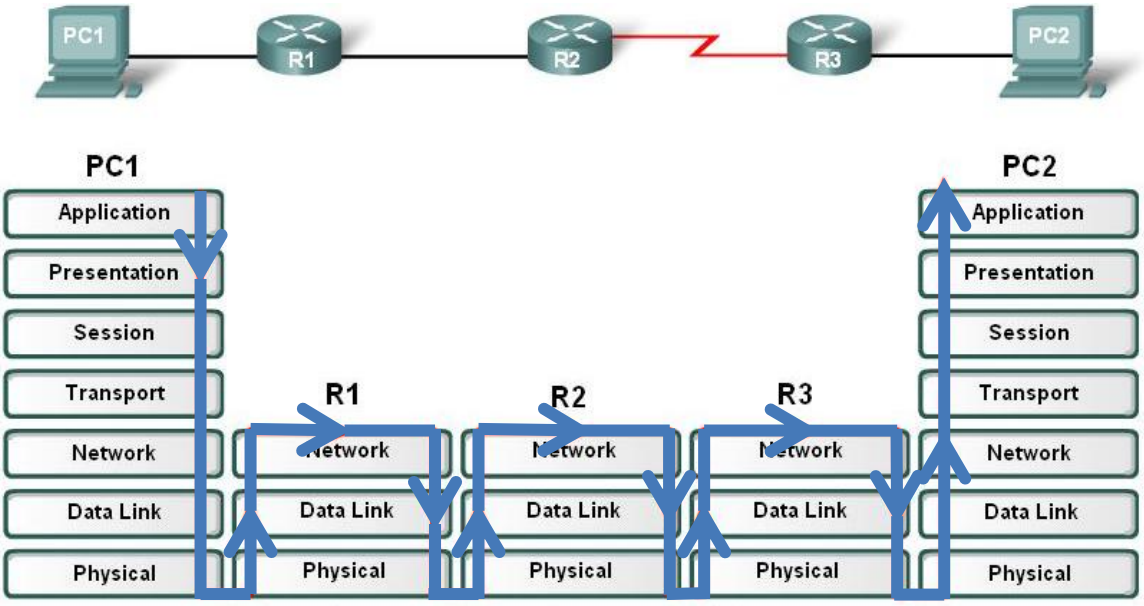
Obrázek 2.1 – Porty routeru

tento obrázek spíše vypadá na pohled nějaké hifi, video či audio komponenty, router je především počítač, který disponuje podobnými komponenty jako procesor, paměti a co je nejdůležitější zásuvnými moduly jednotlivých rozhraní. Router se samozřejmě *bootuje* a nahrává do paměti svůj operační systém, který umožňuje provádět pomocí tisíce konfiguračních příkazů síťová nastavení a umožňuje tak provoz na lokálních, ale také rozsáhlých počítačových sítích.



Obrázek 2.2 – Bootovací proces routeru

Nyní si popíšeme základní úlohu routeru, který je síťovým zařízením pracujícím na třetí vrstvě ISO/OSI modelu. To znamená, že pracuje s IP adresami, na rozdíl od switche, který pracuje na druhé vrstvě síťového modelu s MAC adresami.



Obrázek 2.3 – Router operuje na třech vrstvách ISO/OSI modelu

Hlavním úkolem třetí vrstvy síťového modelu je zajistit výměnu dat mezi jednotlivými uživateli sítě. Zajištění správného chodu této komunikace se skládá ze čtyř základních procesů: adresování, enkapsulace, směrování a dekapsulace.

Adresování

Mechanismus adresování koncových zařízení je zajištěn IP adresou, každé zařízení v síti je identifikováno jednoznačnou IP adresou, jejíž IPv4 (IP protokol verze 4) jsme si definovali v minulé kapitole.

Enkapsulace

Síťová vrstva zajišťuje proces zabalení segmentu z nadřazené transportní vrstvy. K tomuto segmentu je přidána IP hlavička, proces enkapsulace tak vytvoří paket síťové vrstvy. IP hlavička obsahuje zdrojovou a cílovou IP adresu komunikačního procesu. Po ukončení enkapsulačního procesu je paket předán nižší vrstvě síťového modelu.

Směrování

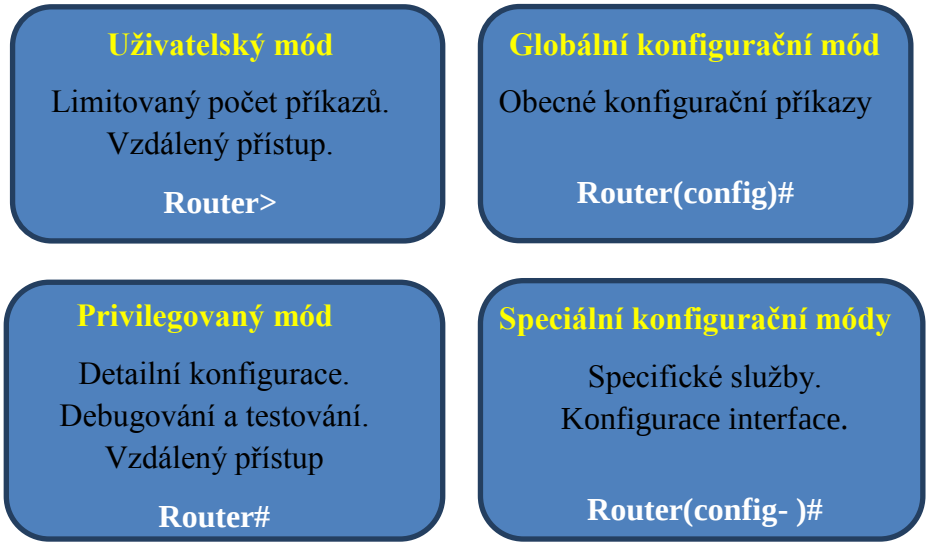
Zdrojové a cílové zařízení nejsou obvykle ve stejné síti, proto síťová vrstva musí zajistit směrování paketů do správného segmentu sítě. To se provádí pomocí zprostředkujících zařízení, kterým říkáme routery. Proto se pro termín směrování často používá jeho anglický ekvivalent *routing*. Router je zařízení na třetí vrstvě síťového modelu a proto je vždy na síťové cestě prováděn proces enkapsulace a dekapsulace. Pouze segment neboli informační jednotka transportní jednotky zůstane nedotčena, zatímco paket je měněn podle toho, jak je směrován síťovou vrstvou.

Dekapsulace

Routery a v samotném závěru také cílové zařízení provádějí na síťové vrstvě proces dekapsulace, neboli samotné rozbalení paketu. Zatímco router musí rámec znovu zabalit a vyslat dále do sítě, cílové zařízení rozbalený rámec zpracuje a jeho segment vyšle nadřazené transportní vrstvě.

2.2 Konfigurační režimy konzole routeru

Při konfiguraci routeru, potřebujeme konkrétní funkce konfigurovat v režimu, který je

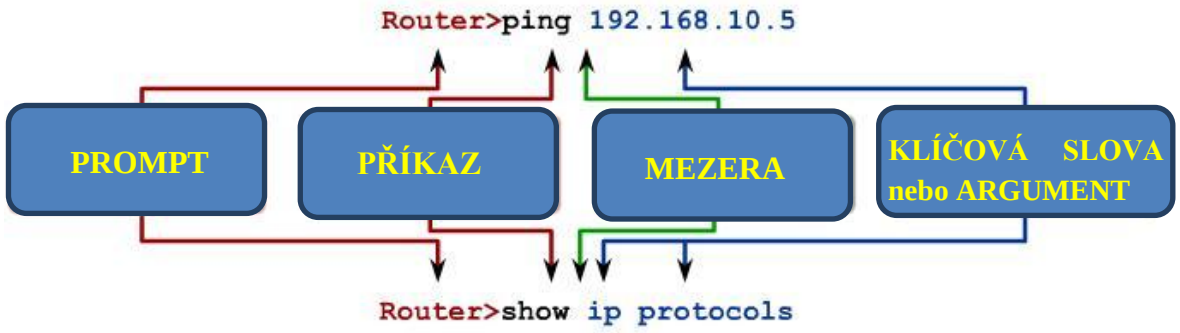


Obrázek 2.4 – Na routeru pracujeme ve čtyřech konfiguračních režimech

k tomu určen, to znamená, že pokud budeme chtít konfigurovat třeba interface, musí přejít do speciálního módu konfigurace interfacu. Pokud budeme chtít pouze konfigurace prohlížet, bude nám k tomu stačit uživatelský mód.

Pojem k zapamatování – konfigurační mód a prompt

Konfigurační mód je režim konfigurace, ve kterém se na konzoli routeru právě nacházíme. Každý mód má svou množinu příkazů, které se dají v dané chvíli použít. V jakém módu se právě nacházíme, poznáme podle zobrazeného promptu, který se skládá s názvu zařízení a dalších znaků či slov.



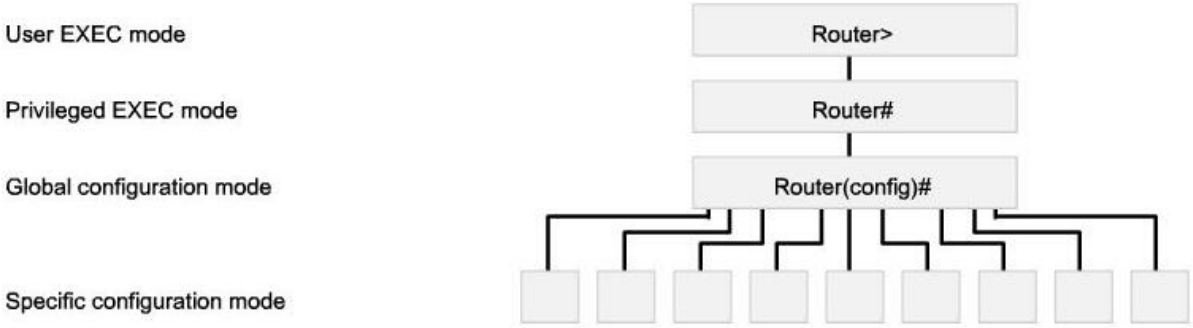
Obrázek 2.5 – Syntaxe promptu a příkazu

Konfigurační příkazy píšeme na konzoli routeru ihned za promptem. Jednotlivé argumenty jsou odděleny mezerou, tak jak je tomu v běžné administrační či programátorské praxi.

```
Router con0 is now available.

Press RETURN to get started.

User Access Verification
Password:
Router>                    <-- User-Mode Prompt
Router>enable
Password:
Router#                    <-- Privileged-Mode
Router#disable
Router>                    <-- User-Mode Prompt
Router>exit
```

Obrázek 2.6 – Přechod mezi uživatelským a privilegovaným módem

Posloupnost jednotlivých režimů včetně zobrazení jejich promptů vidíme na obrázcích 2.6 a 2.7. Do globálního konfiguračního módu přecházíme příkazem **configure terminal.**



Obrázek 2.7 – Hierarchie konfiguračních módů

Konfigurační mód	Prompt
Interface	**Router(config-if)#**
Line	**Router(config-line)#**
Router	**Router(config-router)#**

Obrázek 2.8 – Příklady specifických konfiguračních promptů

Řešený příklad 2.1 – Konfigurační módy

Po spuštění konfigurační konzole routeru se můžeme pohybovat v uživatelském, privilegovaném, globálním a speciálním módu. Každý konfigurační mód poznáme podle promptu. Z hierarchicky vyšších módů přecházíme do nižších pomocí příkazu exit. Tento příklad ukazuje přechod všemi konfiguračními módy směrem nahoru a zpět. Jako specifický konfigurační mód byl zde zvolen mód konfigurace ethernetového interface. Jeho nastavení ukážeme v dalších příkladech.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface f0/0
Router(config-if)#exit
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router#exit
```

Obrázek 2.9 – Přechod mezi konfiguračními módy a zobrazení jejich promptů

2.3 Nastavení zabezpečení konfiguračního módu routeru

Pro zabezpečení konfiguračních nastavení na routeru musíme použít sadu příkazu, pomocí kterých budou v jednotlivých režimech vyžadována hesla. Tyto hesla musíme zadat ihned po přechodu do příslušného módu. Heslo můžeme nastavit i šifrovaně, takže nebude čitelné ani v konfiguračním souboru routeru.

Základní konfigurační příkazy pro zabezpečení promptu routeru
Router(config)#hostname *name*
Router(config)#enable secret *password*
Router(config)#line console 0 **Router(config-line)#password** *password*

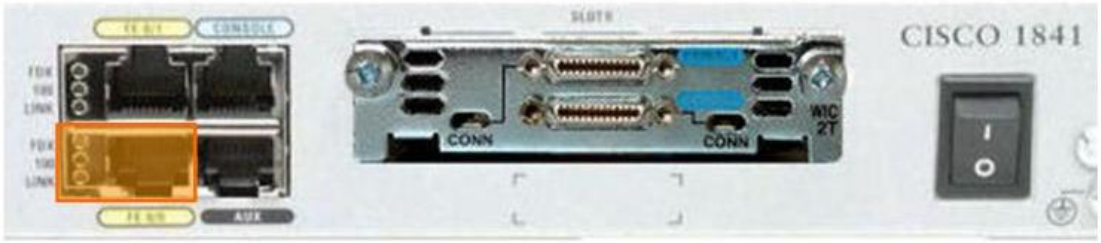
Router(config-line)#login
Router(config)#line vty 0 4 **Router(config-line)#password** *password* **Router(config-line)#login**
Router(config)#banner motd # message #

Obrázek 2.10 – Příkazy pro zabezpečení konfiguračních promptů

Ve výčtu příkazů vidíme i pojmenování zařízení příkazem *hostname* a také nastavení hlášení při přístupu na konzoli routeru. *Motd* znamená hlášení *message of the day* a bude zobrazováno před zadáním hesla. V seznamu příkazů vidíme také zabezpečení vzdáleného připojení přes *telnet*, které je možné na router až čtyřmi linkami, proto jsou tyto čísla v seznamu argumentů příkazu. Pro prověření těchto funkcionalit je připraven jeden z následujících řešených příkladů.

2.4 Konfigurace interface routeru

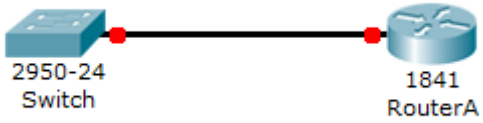
Na obrázku 2.14 a 2.11 vidíme zobrazeny moduly sériových a ethernetových portů. Následující příklady obsahují sadu příkazových konstrukcí pro jejich konfiguraci.



Obrázek 2.11 – Ethernetový interface routeru

Řešený příklad 2.2 – Nastavení ethernetového portu

Pro nastavení ethernetového portu routeru potřebujeme tento port připojit k nějakému zařízení (obvykle switch nebo PC). Příklad zobrazuje posloupnost příkazů, která zajišťuje konfiguraci IP adresy a masky a následnou aktivaci portu.



Obrázek 2.12 – Propojení ethernetového interface routeru se switchem

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa0/0
Router(config-if)#ip address 158.192.160.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
Router(config-if)#
```

Obrázek 2.13 – Posloupnost příkazů nastavení ethernetového interface

Obrázek 2.14 – Sériový interface routeru

Řešený příklad 2.3 – Nastavení sériového portu

Rozsáhlejší topologie a situace kdy potřebujeme více routerů, řešíme sériovým připojením mezi routery. Následuje konfigurace sériového portu routeru, která je obdobná jako u ethernetového, s tím rozdílem, že sériové propojení musíme na jedné straně (DCE zařízení) nastavit časovou synchronizaci.

Obrázek 2.15 – Propojení sériového interface routeru s dalším routerem

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface s0/0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

Obrázek 2.16 – Posloupnost příkazů nastavení sériového interface

Základní konfigurační příkazy pro nastavení interface	
Konfigurace interface	**Router(config)#interface** *type number* **Router(config-if)#ip address** *address mask* **Router(config-if)#description** *description* **Router(config-if)#no shutdown**
Uložení aktuální konfigurace	**Router#copy running-config startup-config**
Výstupy příkazu *show*	**Router#show running-config**
	Router#show ip route
	Router#show interfaces
	Router#show ip interface brief

Obrázek 2.17 – Základní konfigurační příkazy pro nastavení interface

Obrázek 2.17. shrnuje základní konfigurační příkazy, nejprve nastavení rozhraní, poté zobrazení konfiguračních nastavení. Tyto nastavení si ověříme v následujících příkladech.

2.5 Příklady konfiguračních nastavení

V předchozím výkladu jsme si popsali základy konfiguračních nastavení a přehled základních příkazů, kterým tuto konfiguraci ověříme. V této kapitole si ukážeme na demonstračních příkladech využití probraných příkazů a především zabezpečení konzole routeru.

Řešený příklad 2.4 – prohlížení konfigurace routeru

V privilegovaném módu můžeme pomocí příkazu show sledovat celou řadu nastavení. Zobrazení aktuální konfigurace zobrazíme příkazem show running-config. V případě, že však zařízení vypneme či restartujeme, uvedenou konfiguraci ztratíme. Proto bychom měli vytvořenou konfiguraci uložit příkazem copy running-config startup-config.

```
Router#show running-config
Building configuration...

Current configuration : 502 bytes
!
version 12.4
no service password-encryption
!
hostname Router
!
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 158.192.160.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
```

Obrázek 2.18 – Zobrazení aktuální konfigurace routeru

Řešený příklad 2.5 – Zobrazení směrovací tabulky

V privilegovaném módu můžeme sledovat i směrovací tabulku s cestami do sítí, které má router k dispozici. Směrovací tabulce i nastavením cest do různých podsítí se ještě budeme věnovat podrobně v následujících kapitolách.

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Serial0/0/0
     158.192.0.0/24 is subnetted, 1 subnets
C       158.192.160.0 is directly connected, FastEthernet0/0
Router#
```

Obrázek 2.19 – Zobrazení dostupných cest na routeru

Řešený příklad 2.6 – Zobrazení rozhraní routeru

Příkazem show interfaces v privilegovaném módu zjistíme všechny detailní informace o jednotlivých rozhraních na routeru. Tyto informace jsou tak podrobné, že pro informace o tom zda je interface aktivní a jakou má IP adresu častěji používáme příkaz show ip interface brief.

```
Router#show interfaces
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0001.64a6.1e01 (bia 0001.64a6.1e01)
  Internet address is 158.192.160.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
FastEthernet0/1 is administratively down, line protocol is down (disabled)
```

Obrázek 2.20 – Zobrazení detailních informací o rozhraní routeru

Řešený příklad 2.7 – zobrazení IP adres a statusu rozhraní

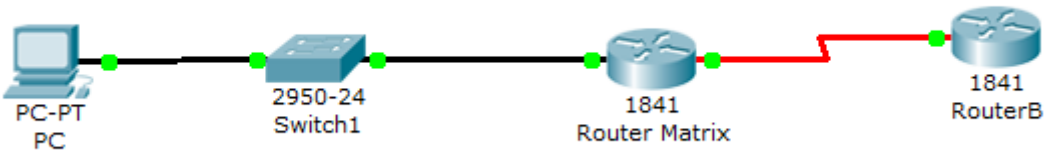
Příkaz show ip interface brief zobrazuje všechny nainstalované rozhraní, jejich IP adresy a stav, jestli je interface up nebo down.

```
Router#show ip int brie
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        158.192.160.1   YES manual up                    up

FastEthernet0/1        unassigned      YES manual administratively down down

Serial0/0/0            10.10.10.1      YES manual up                    up

Serial0/0/1            unassigned      YES manual administratively down down

Vlan1                  unassigned      YES manual administratively down down
```

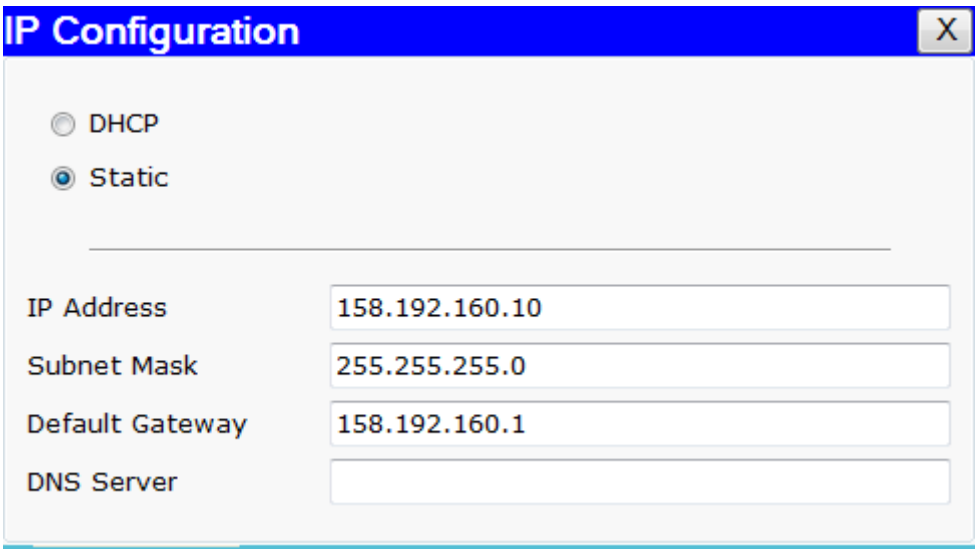
Obrázek 2.21 – Zobrazení rozhraní routeru se statusem aktivity a IP adresou

Řešený příklad 2.8 – Připojení PC do segmentu sítě

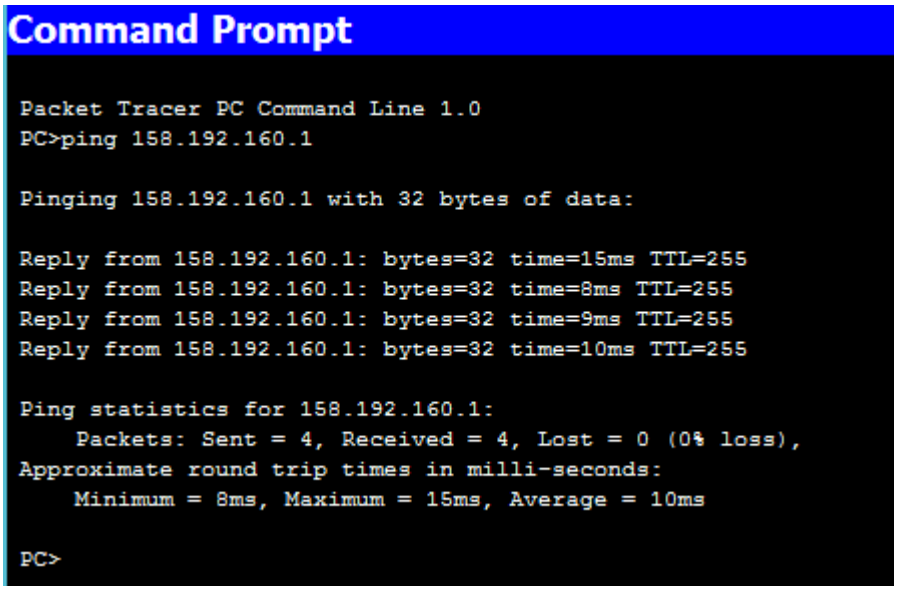
Pro následující sadu ukázek nastavení bezpečnosti přihlášení do jednotlivých konfiguračních módů nejprve vytvoříme jednoduchou topologii, kdy využijeme nastavení sériového a ethernetového routeru z minulých příkladů. Poté do segmentu sítě 158.192.160.0 připojíme počítač a nastavíme IP adresu a defaultní bránu. Připojený počítač poté využijeme pro vzdálený telnet přístup na router.



Obrázek 2.22 – topologie s PC, switchem a routery



Obrázek 2.23 – konfigurace IP adresy a brány na počítači, který připojíme do segmentu sítě 158.192.160.0



Obrázek 2.24 – ověření konektivity pingem na defaultní bránu

Řešený příklad 2.9 – Ukázka zabezpečení privilegovaného režimu

Nejprve pojmenujeme router příkazem hostname. Poté pomocí příkazu enable secret heslo nastavíme zabezpečení privilegovaného režimu. Atribut secret znamená zahešování hesla, takže i v textovém výpisu konfigurace bude zašifrované.

```
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Matrix
Matrix(config)#enable secret heslo
Matrix(config)#
```

Obrázek 2.25 – nastavení hostname routeru a zabezpečení privilegovaného módu

```
Matrix#show run
Building configuration...

Current configuration : 551 bytes
!
version 12.4
no service password-encryption
!
hostname Matrix
!
!
enable secret 5 $1$mERr$ffOlpJaHqi7NpitvaXsfE0
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 ip address 158.192.160.1 255.255.255.0
 duplex auto
 speed auto
```

Obrázek 2.26 – zašifrované heslo neuvidíme ani v textovém výpisu konfigurace

Řešený příklad 2.10 – Ukázka zabezpečení konzole routeru

Další příkazy zabezpečení se vztahují na konzoli routeru. Nejprve sadou příkazů nastavíme heslo na samotnou konzoli, další sadou příkazů nastavíme heslo pro vzdálený přístup. Příkazem telnet můžeme na router přistoupit čtyřmi linkami, proto je atributem příkazu telnet vty 0 4. Příkazem banner motd nastavíme hlášení pro přístup na konzoli. Atribut motd znamená hlášení Message of the day.

Výsledek těchto příkazů vidíme na dalším obrázku, kdy pro přístup na konzoli routeru je vyžadováno heslo a zobrazeno hlášení.

```
Matrix# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Matrix(config)#line console 0
Matrix(config-line)#password heslo
Matrix(config-line)#login
Matrix(config-line)#line vty 0 4
Matrix(config-line)#password heslo
Matrix(config-line)#login
Matrix(config-line)#banner motd #Pouze autorizovany pristup k routeru Matrix!#
Matrix(config)#
```

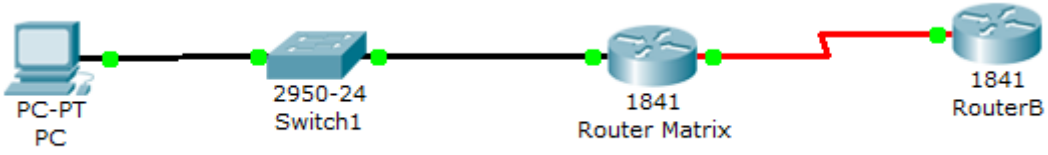
Obrázek 2.27 – Nastavení zabezpečení konzole routeru, vzdáleného přístupu přes telnet a hlášení při přístupu na konzoli

```
Press RETURN to get started.




Pouze autorizovany pristup k routeru Matrix!

User Access Verification

Password:

Matrix>enable
Password:
Matrix#
```

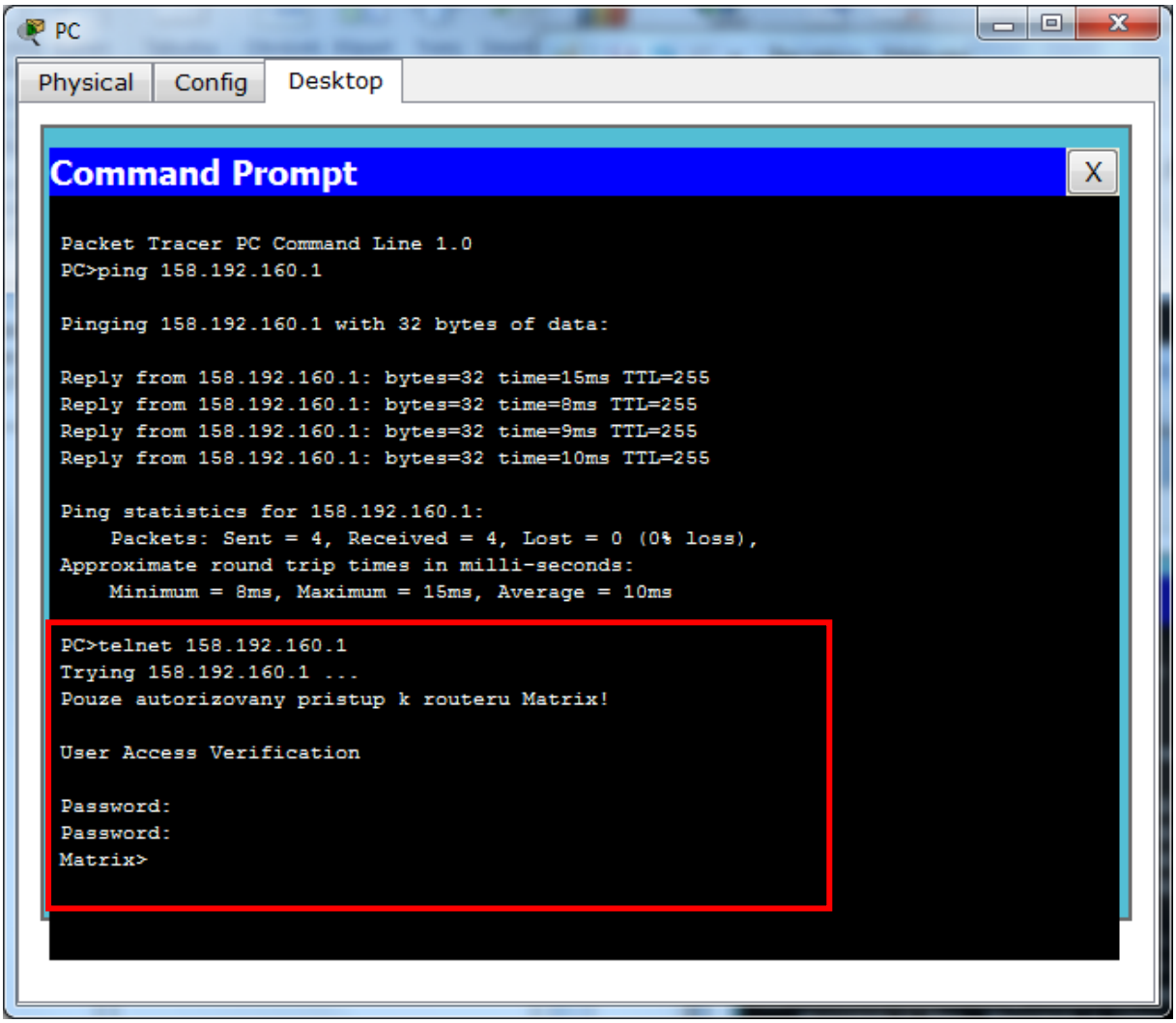
Obrázek 2.28 – Přístup na konzoli routeru nyní vyžaduje heslo

Řešený příklad 2.11 – Ukázka vzdáleného přístupu na konzoli routeru

V minulém příkladu jsme si zabezpečili konzoli routeru také pro vzdálený přístup pomocí příkazu telnet. V naší topologii se nyní pokusíme přistoupit z připojeného PC na router. Příklad potvrzuje vyžádání hesla vzdáleného přístupu a současného zobrazení hlášení motd.



Obrázek 2.29 – použitá topologie pro řešený příklad



Obrázek 2.30 – Vzdálený přístup na router pomocí telnet již vyžaduje heslo

.

Ke kapitole 2 je připravena animace č. 2

Animace č. 2 se věnuje tématům: Konzole routeru, konfigurační režimy a příkazy, nastavení hesel konzole a přístup přes telnet.

V této animaci si propojíme router s PC, nakonfigurujeme jejich rozhraní a přistoupíme pomocí telnet utility z počítače na router. Před tím si ale ukážeme konfigurační režimy, příkazy na routeru a zaheslování konfiguračních režimů.

Korespondenční úkol

Vyzkoušejte příkaz ipconfig /all na vašem PC. V případě, že pracujete v topologii sítě s více počítači vyzkoušejte ping na sousední počítač. V případě že vaše PC je jediným zařízením v segmentu vyzkoušejte nějaký síťový ping (např. *ping www.seznam.cz*).

Otázky ke kapitole 2

1. Jakým způsobem bude probíhat síťový provoz na PC, když nenastavíme defaultní bránu?
2. Kterým příkazem přejdu z hierarchicky vyššího konfiguračního režimu do nižšího?
3. Mohu v konfiguračním režimu používat příkazy *show*? Např. *show ip route.*

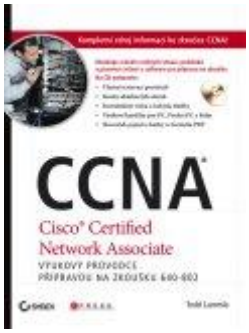
Úlohy k řešení ke kapitole 2

4. Navrhněte topologii sítě, kde router obsahuje dvě podsítě.
5. Nastavte IP adresy ethernetových interface routeru.
6. Do obou podsítí připojte PC a nastavte příslušnou IP adresu, masku a defaultní bránu.
7. Vyzkoušejte ping z obou PC na defaultní bránu.
8. Nastavte na routeru heslo pro vzdálený přístup telnet.
9. Vyzkoušejte vzdálený přístup na telnet z PC z libovolné podsítě.

Další zdroje

Scott Empson, *CCNA Kompletní přehled příkazů - Autorizovaný výukový průvodce,* 2009, 336 stran, nakladatelství COMPUTER PRESS.

Tato publikace patří do produktové řady Cisco Press Certification Self-Study, která čtenářům přináší možnost přípravy k certifikačním zkouškám Cisco v individuálním tempu. Tituly v této řadě jsou součástí doporučeného vzdělávacího programu od společnosti Cisco, který zahrnuje simulované i praktické školení od autorizovaných školicích partnerů Cisco Learning Partners a titulů k samostatnému studiu od vydavatelství Cisco Press



Todd Lammle, *CCNA - Výukový průvodce přípravou na zkoušku*, 2010, 928 stran, nakladatelství COMPUTER PRESS.

Tento metodicky vydařený průvodce vás provede všemi klíčovými tématy, a to včetně nejnovějších poznatků o přepínání, technologii NAT, IPv6 a OSPF. Autor z vás během pár hodin udělá odborníka, který bez mrknutí oka umí řešit potíže a konfigurovat malé, střední i rozlehlejší sítě tak, aby poskytovaly maximální výkon.

3 SMĚROVACÍ TABULKA A NASTAVENÍ STATICKÉ CESTY

V této kapitole budeme pokračovat v konfiguračních nastaveních routeru s důrazem na funkčnost provozu sítě. Nakonfigurujeme si celou topologii složenou z více sítí, budeme konfigurovat rozhraní PC, ethernetové a sériové rozhraní routeru a nově také statické cesty do vzdálenějších sítí.

Čas ke studiu: 3 hodiny

Cíl: Po prostudování tohoto odstavce budete umět

- Nakonfigurovat provoz sítě ve složitější topologii.
- Nakonfigurovat rozhraní routeru a PC v reálném provozu.
- Zobrazit směrovací tabulky na routerech a porozumět obsaženým údajům.
- Konfigurovat statické cesty na routeru do vzdálenějších sítí.
- Prohlížet detaily paketů na jednotlivých vrstvách v programu Packet Tracer.

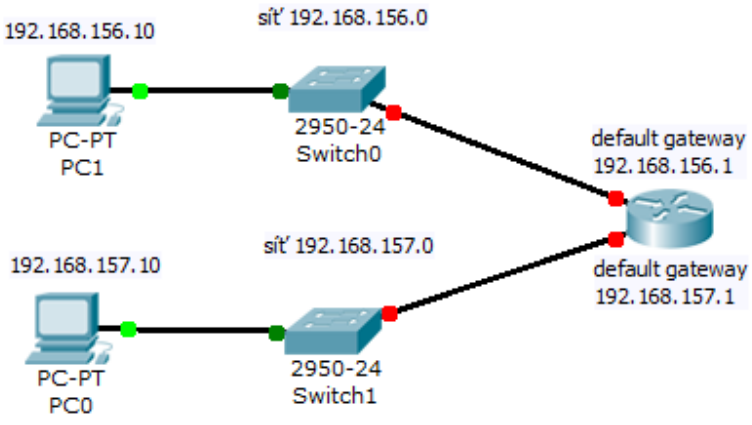
Výklad

3.1 Základní konfigurace rozhraní

Celou kapitolu rozdělíme do tří témat, nejprve zkonfigurujeme všechna konfigurační nastavení rozhraní, poté vyzkoušíme simulaci provozu v síti a nakonec nastavíme statické cesty do vzdálených sítí.

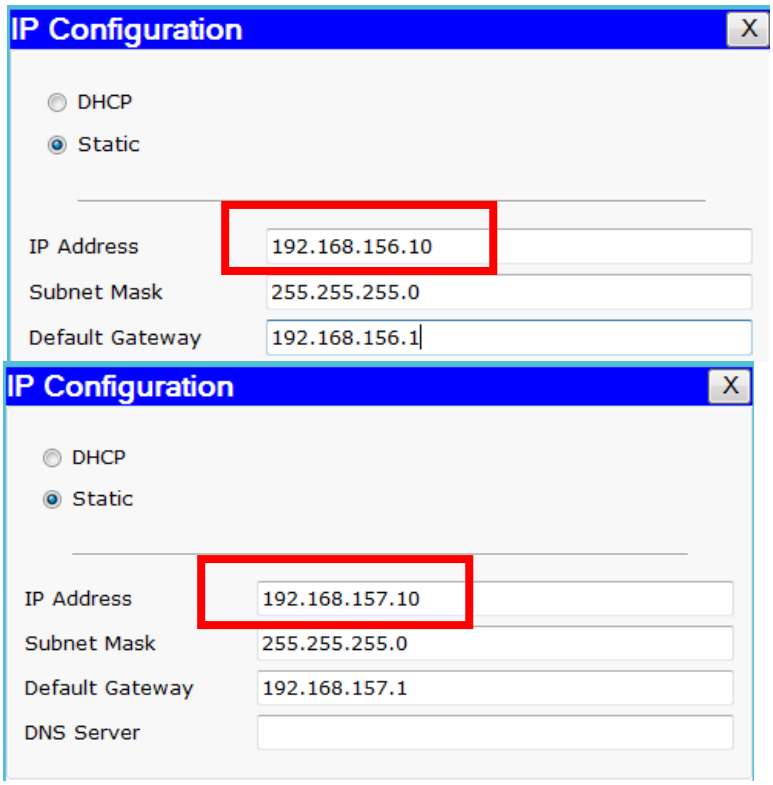
Řešený příklad 3.1 – Výchozí topologie

V našem příkladu, který bude pokračovat celou kapitolu, nejprve vytvoříme topologii, která bude obsahovat dvě lokální sítě připojené na ethernetové rozhraní routeru.



Obrázek 3.1 – Výchozí topologie s dvěma LAN sítěmi

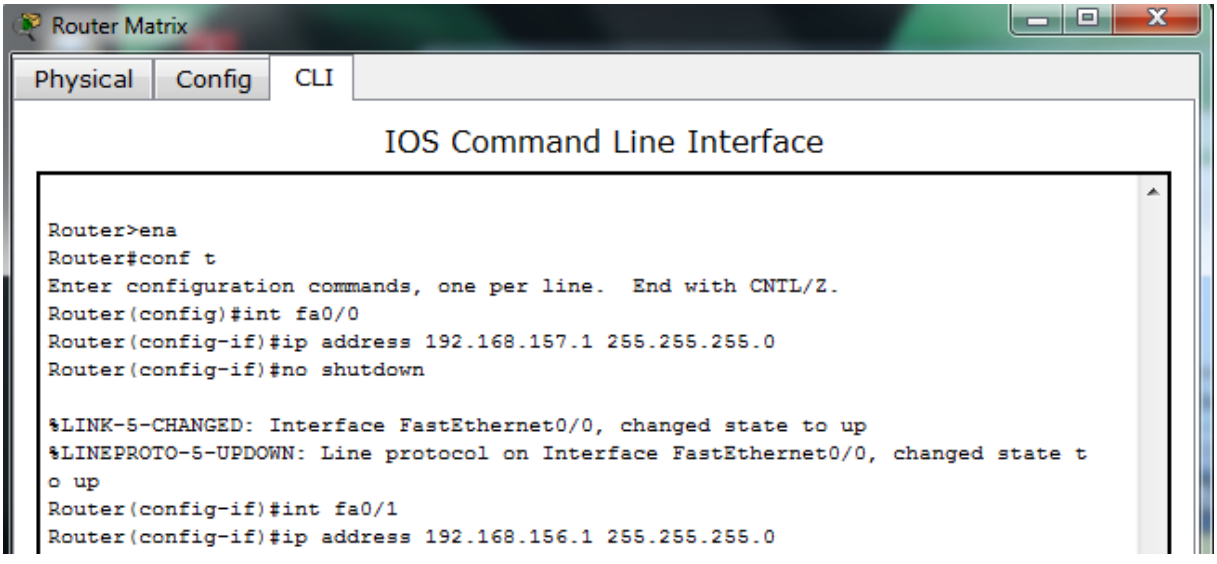
Nejprve dle topologie na obr. 3.1 nastavíme IP adresu, masku sítě a výchozí bránu pro oba počítače. V našem výukovém modulu budeme obvykle počítačům přidělovat v posledním oktetu adresy číslo **10.**



Obrázek 3.2 – Nastavení IP adres, masky a defaultní brány u PC0 a PC1

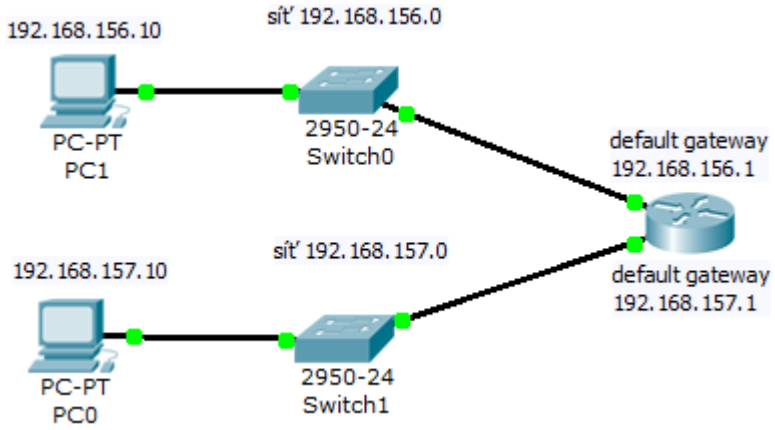
Řešený příklad 3.2 – Nastavení ethernetových rozhraní routeru

Nyní následuje pro obě lokální sítě nastavení ethernetového rozhraní routeru. Zde budeme dodržovat zvyk, že defaultní brána bude mít v posledním oktetu adresy vždy číslo 1.



Obrázek 3.3 – Nastavení ethernetových rozhraní routeru

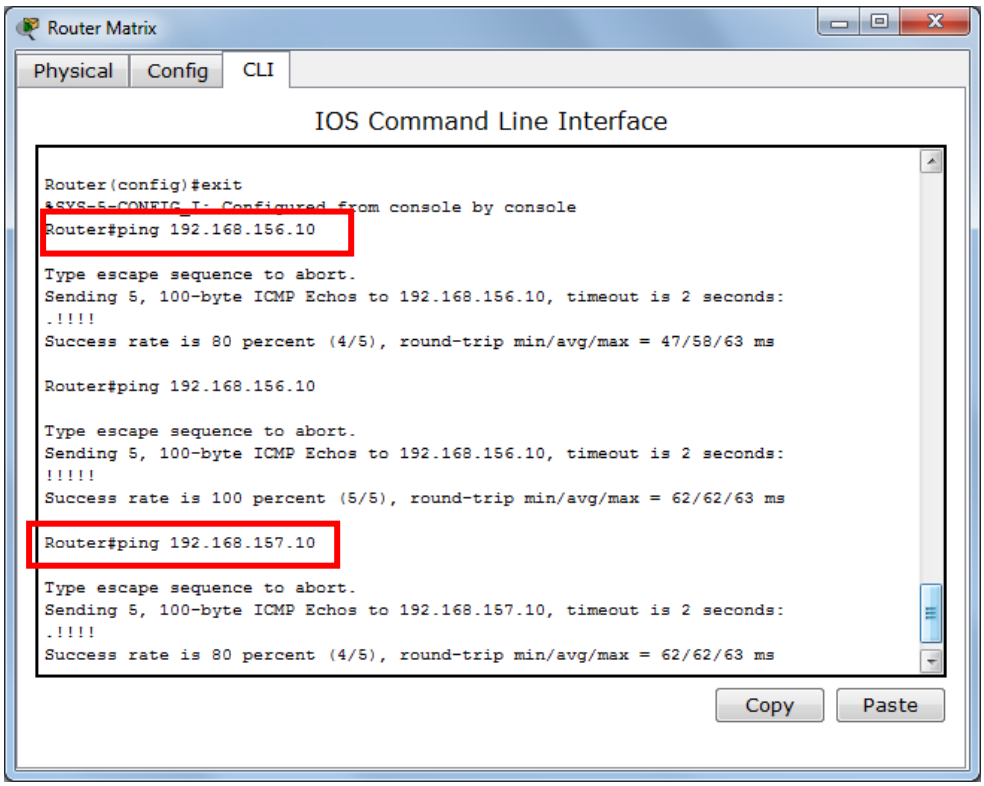
Program Packet Tracer na pracovní ploše zobrazuje topologie s barevným rozlišením jednotlivým propojení. Zatímco na obrázku 3.1 je propojení označeno červeně, po dokončení konfigurace vidíme všechny označení zelenou barvou. To je v podstatě potvrzení, že síť je nakonfigurována správně a prvky mezi sebou komunikují.



Obrázek 3.4 – Výchozí topologie po nastavení ethernetových rozhraní

Korespondenční úkol

Vyzkoušejte v uvedené topologii tzv. rozpojit síť. To znamená, že např. rozhraní routeru fa0/0 nebo fa0/1 ve specifickém módu (*config-if*) příkazem *shutdown* deaktivujeme. Druhou možností je např. změnit IP adresu PC nebo vytvořit obdobnou chybu na routeru. V uvedené topologii se zelená barva v konkrétním spojovacím bodě změní na červenou.

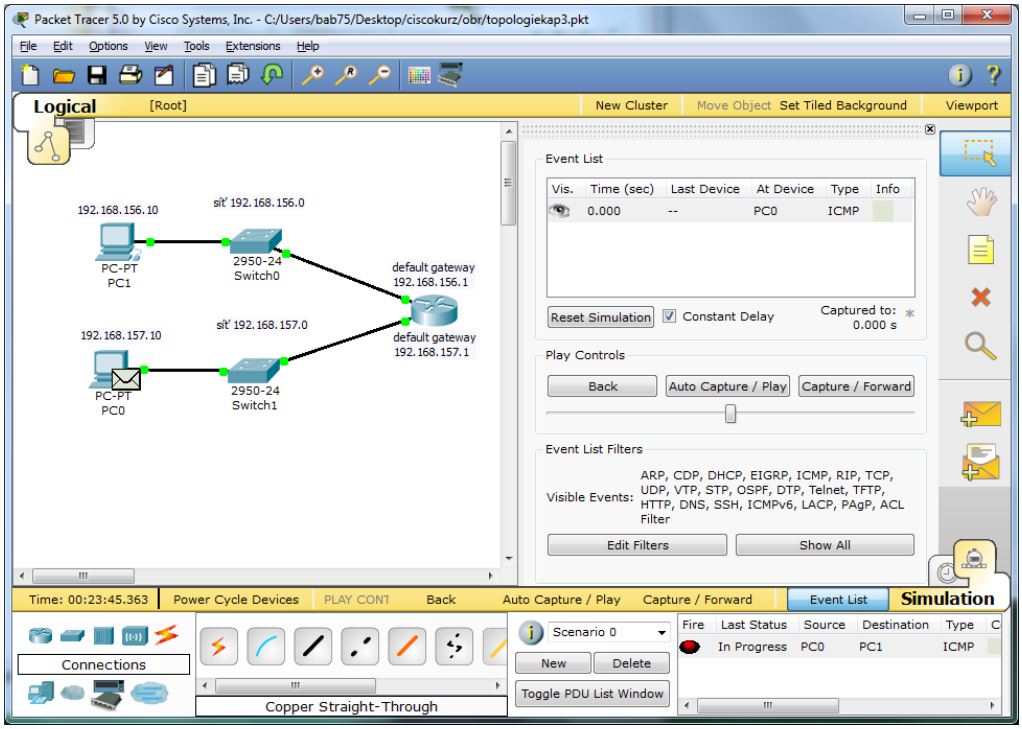


Obrázek 3.5 – Prověření dostupnosti připojených sítí příkazem ping z konzole routeru

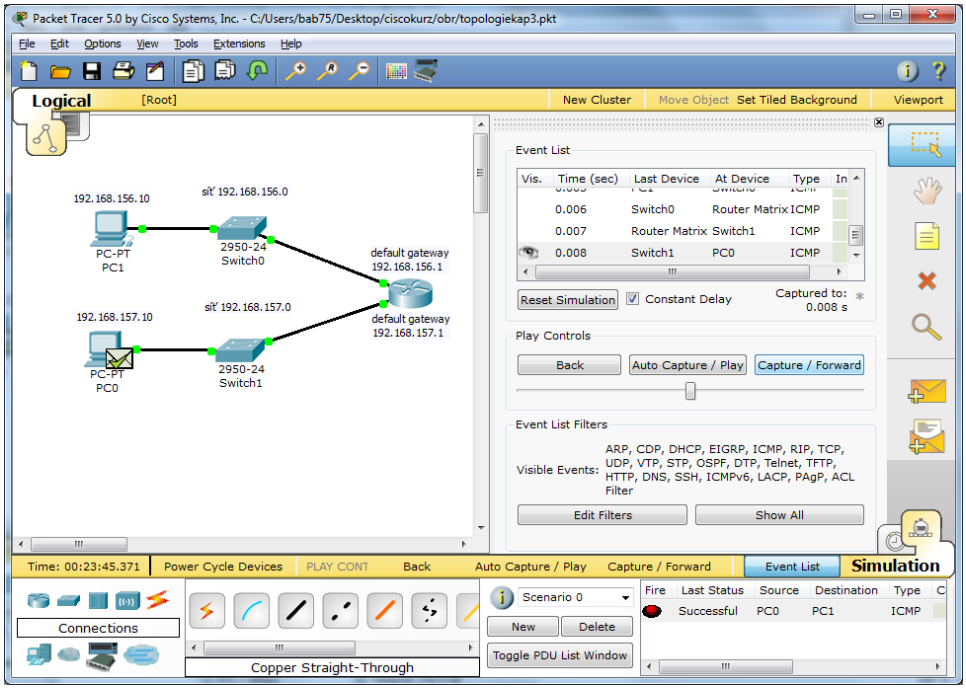
3.2 Simulace reálného provozu v programu Packet Tracer

Řešený příklad 3.3 – Simulační mód a prohlížení paketů

Pro simulaci provozu v síti klikneme na ikonku ping paketu v pravém panelu nástrojů. Poté zvolíme zařízení, jejichž komunikaci chceme ověřit, v našem případě se tedy jedná o komunikaci mezi PC0 a PC1.

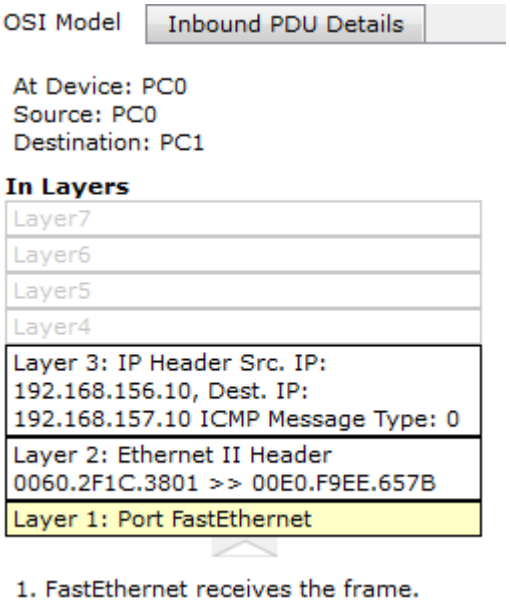


Obrázek 3.6 – Počáteční stav simulace pingu z PC0 na PC1



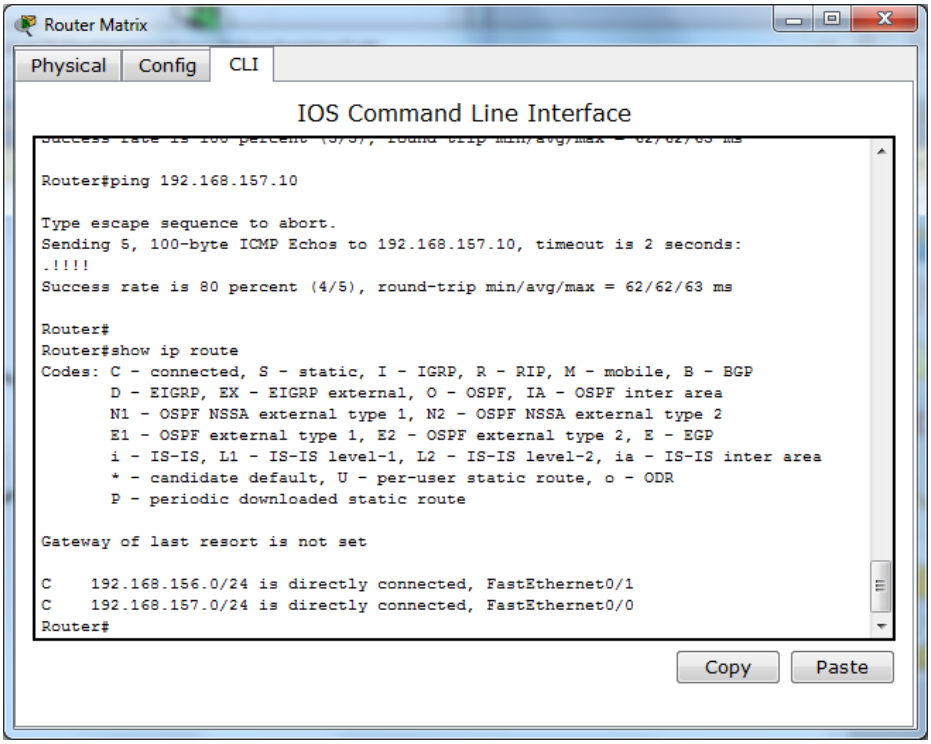
Obrázek 3.7 – ping z PC0 na PC1 byl úspěšný

*Poté tlačítkem **Capture** krokujeme komunikaci po jednotlivých paketech. V okně Event List vidíme seznam paketů, tak jak jdou za sebou. Poté co ping dorazí na PC1, tento počítač paket zpracuje a odpoví. Když dorazí odpověď pingu na PC0, simulační režim ukončí komunikaci zobrazením zeleného potvrzovacího zaškrtnutí paketu.*



Obrázek 3.8 – Detaily paketu v simulačním režimu

*Při kliknutí na ikonu obálky paketu můžeme zobrazit jeho detaily. Například na obrázku 3.8 vidíme v třetí vrstvě paketu zdrojovou a cílovou IP adresu. Znamená to tedy, že se jedná o paket z PC1 na PC0. Tlačítkem **Back** můžeme zobrazit všechny předchozí pakety komunikace a podívat se na detaily paketů.*



Obrázek 3.9 – Směrovací tabulka routeru

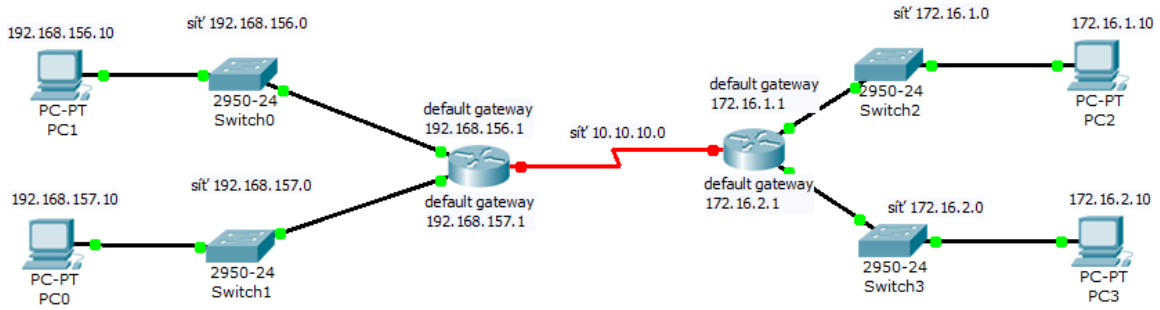
Korespondenční úkol

Krokujte tlačítkem **Back** komunikaci a sledujte detaily paketů. Všimněte si, že switche nepracují na třetí vrstvě síťového modelu. Zdrojové a cílové IP adresy můžeme sledovat na počítačích a routeru.

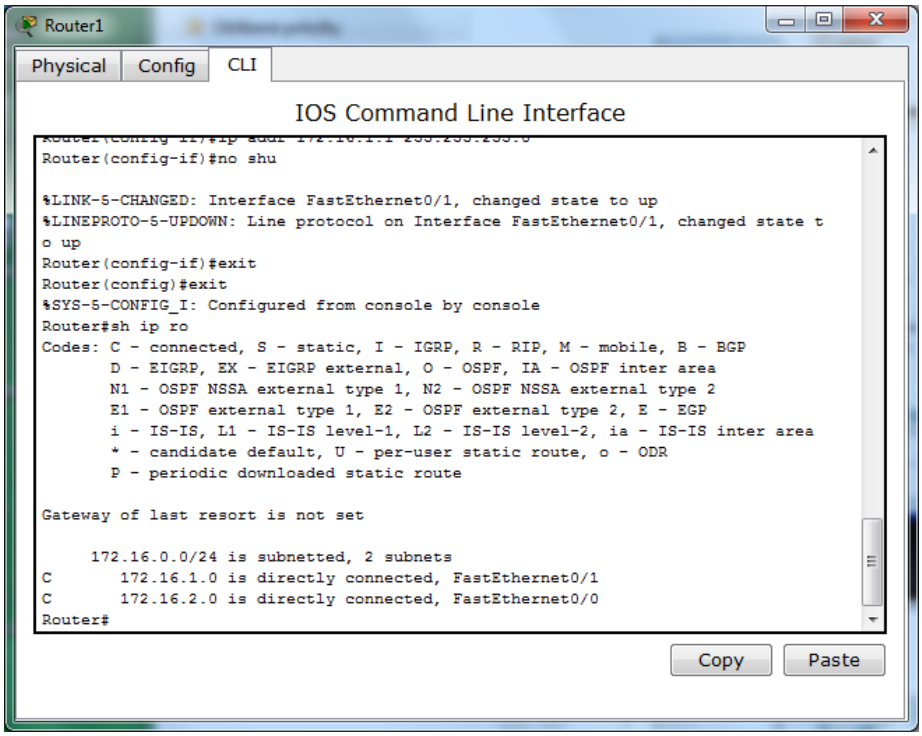
3.3 Rozšíření topologie pro příklad nastavení statických cest

Řešený příklad 3.4 – Kompletní topologie

Rozšíříme si topologii o další lokální sítě na jiném routeru, který s původním routerem spojíme sériovým wan kabelem. V podstatě do současné chvíle jsme pracovali na polovině kompletní topologie. Výsledkem bude topologie o 4 lokálních sítích a jedné spojovací síti mezi routery.



Obrázek 3.10 – Kompletní topologie pro příklad nastavení statických cest



Obrázek 3.11 – směrovací tabulka pravého routeru před spojením obou routerů.

Další postup je tedy následující: Stejně jako v původní topologii nastavíme nejprve IP adresy PC, nastavíme masku sítě a výchozí bránu. Opět u PC s adresou 10 v posledním oktetu a bránu s adresou 1. Poté stejným postupem jako v příkladu 3.2 nastavíme ethernetová rozhraní routeru. Pokud budeme mít konfiguraci hotovou, bude jako na obr. 3.10 topologie se zelenými body mimo propojení dvou routerů. Směrovací tabulka pravého routeru bude obsahovat dvě lokální sítě 172.16.1.0 a 172.16.2.0.

Zbývá tedy na obou routerech nakonfigurovat sériové rozhraní a na příslušné DCE straně také časování. Na obrázku 3.12 vidíme nastavení levého routeru i s časovou synchronizací, nastavení pravého routeru bude obdobné s IP adresou 10.10.10.2 a bez časové synchronizace viz obr 3.13.

```
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int s0/0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#
```

Obrázek 3.12 – Nastavení sériového rozhraní na levém routeru.

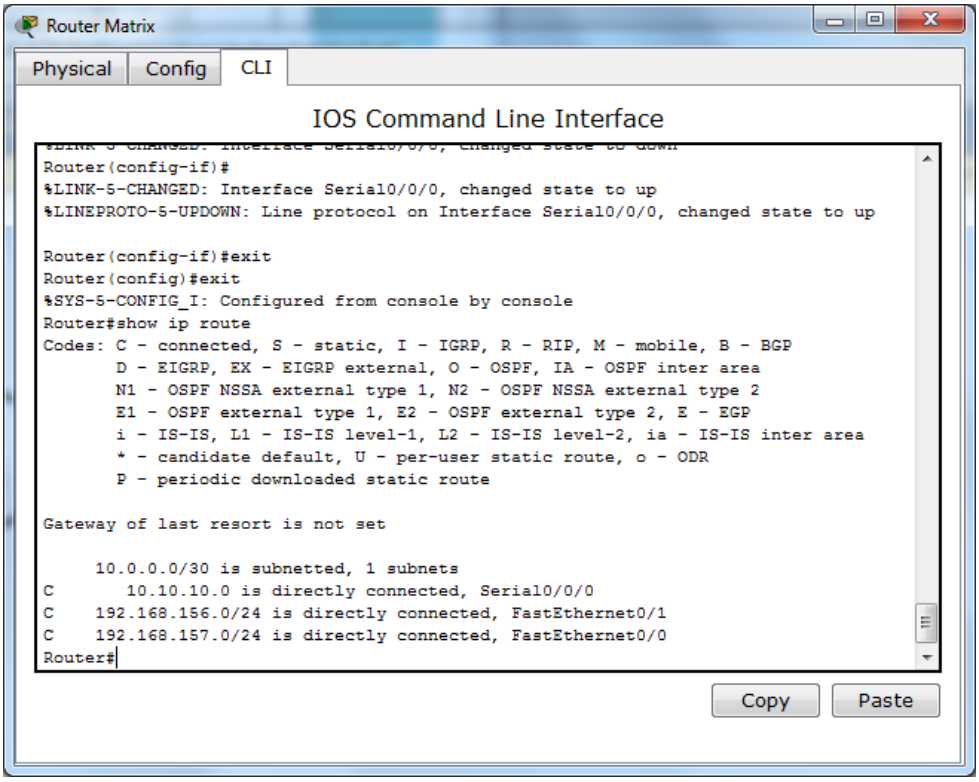
Až po nakonfigurování pravého routeru budou oba mít obě sériová rozhraní status ***up****, o čemž jsme informováni. Poté již bude celá topologie propojena zeleně. Můžeme vyzkoušet kontrolní ping z jednoho routeru na druhý.*

```
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int s0/0/0
Router(config-if)#ip address 10.10.10.2 255.255.255.252
Router(config-if)#no shu

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Router(config-if)#exit
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router#ping 10.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/28/31 ms

Router#
```

Obrázek 3.13 – Prověření dostupnosti připojených sítí příkazem ping z konzole routeru

Přesto, že celá topologie svítí zeleně, neznamená to, že všechna zařízení jsou mezi sebou dostupná. Lokální sítě levého routeru mezi sebou komunikovat mohou, stejně tak tomu je i na pravém routeru. Pokud však budeme chtít komunikovat mezi PC0 s IP adresou

192.168.157.10 a PC3 s IP adresou 172.16.2.10, ping bude neúspěšný. Na otázku proč tomu tak je nám odpoví obsah směrovacích tabulek routerů.



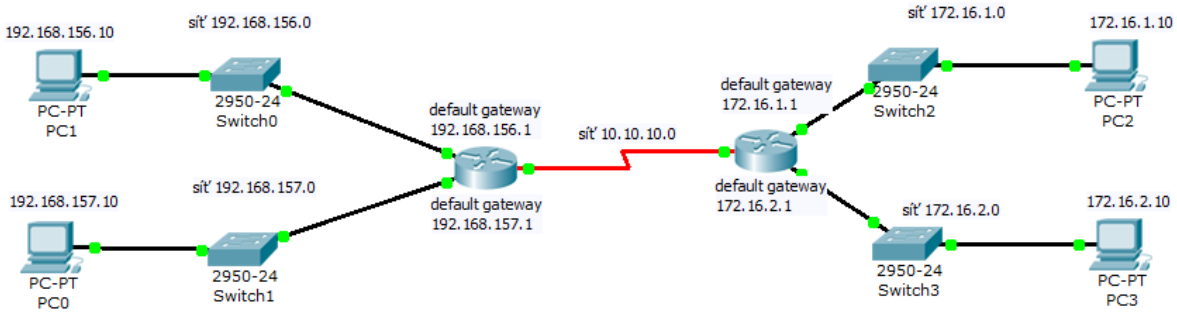
Obrázek 3.14 – Směrovací tabulka levého routeru

Ve směrovací tabulce totiž router má pouze přímo připojené tři sítě, to znamená, že levý router nemá vůbec žádné informace o sítích 172.16.1.0 a 172.16.2.0. Stejně tak pravý router nezná sítě 192.168.156.0 a 192.168.157.0. Aby tyto sítě mohly mezi sebou komunikovat, musí router tyto sítě mít ve směrovací tabulce. To lze zajistit dvěma způsoby, buď směrovacím protokolem, nebo nastavením statické cesty.

3.4 Nastavení statické cesty

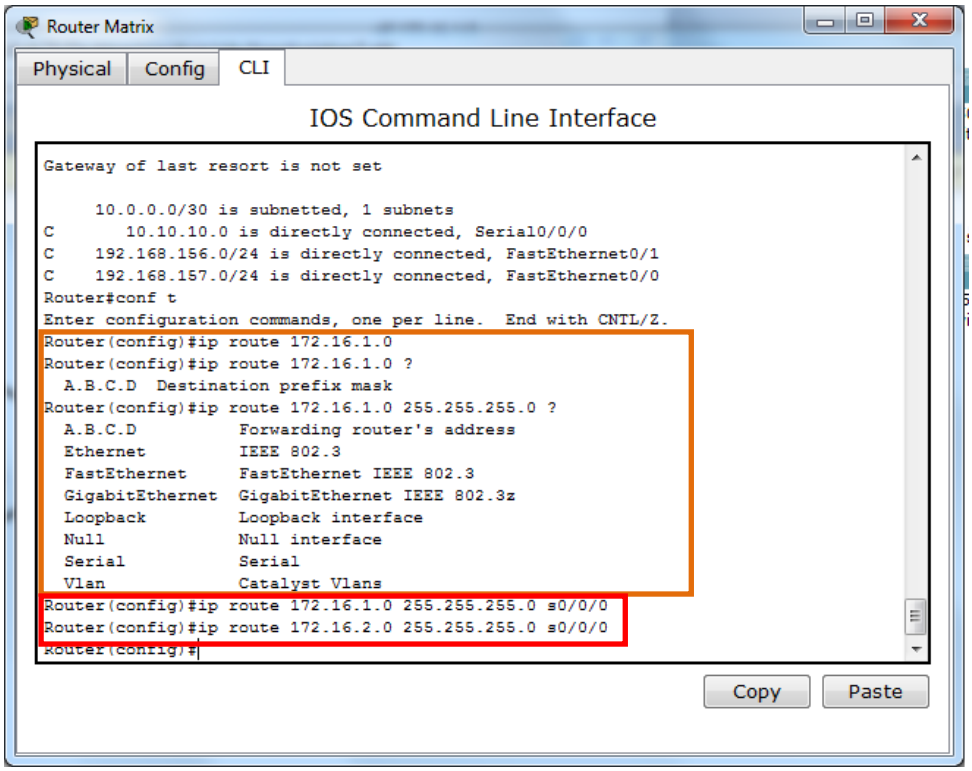
Řešený příklad 3.5 – Konfigurace statické cesty

Celou topologii tedy vidíme na obr. 3.15 a naším úkolem bude na obou routerech nastavit dvě statické cesty do sítě, která má připojen sousední router.

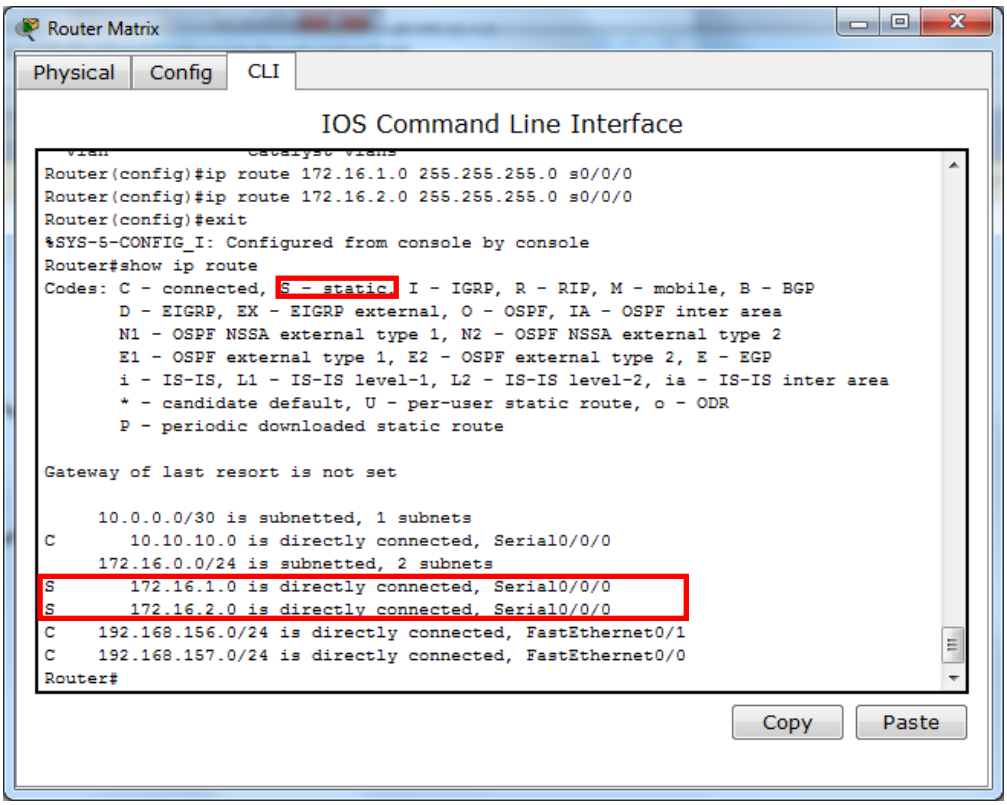


Obrázek 3.15 – Kompletní topologie

*Statickou cestu nastavíme příkazem **ip route** s argumenty síťové adresy, masky a rozhraní přes které je síť přístupná. Pokud si nejsme jisti syntaxí příkazu či tvarem argumentu, můžeme zadat v příkazu otazník a operační systém zařídí výpis nabídky použitelných nastavení.*

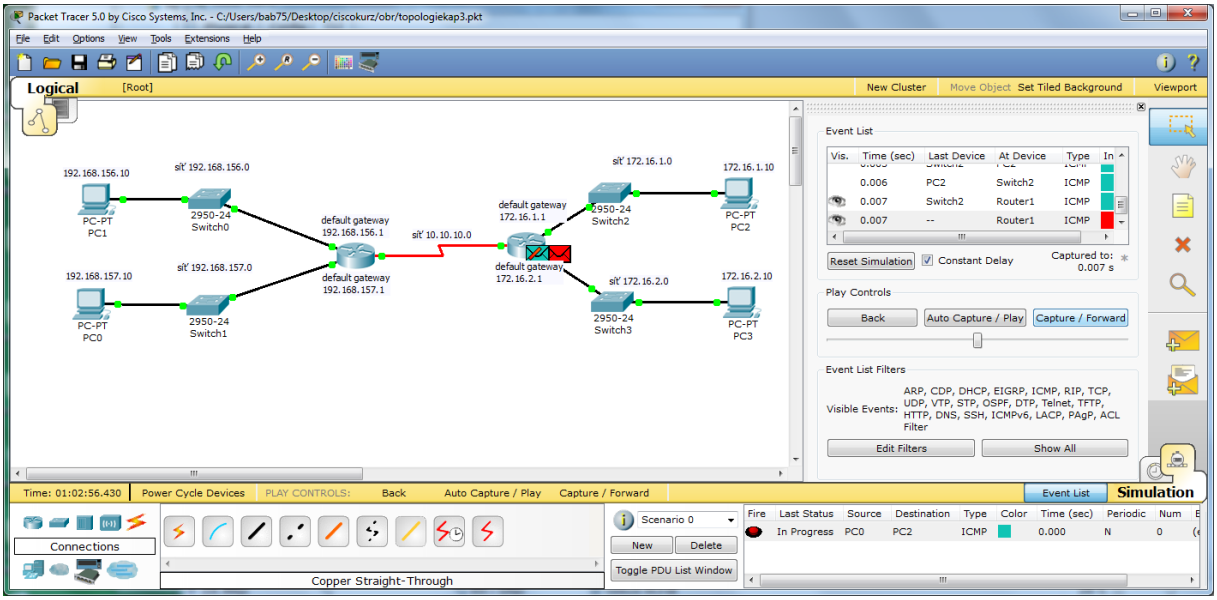


Obrázek 3.16 – Nastavení statických cest



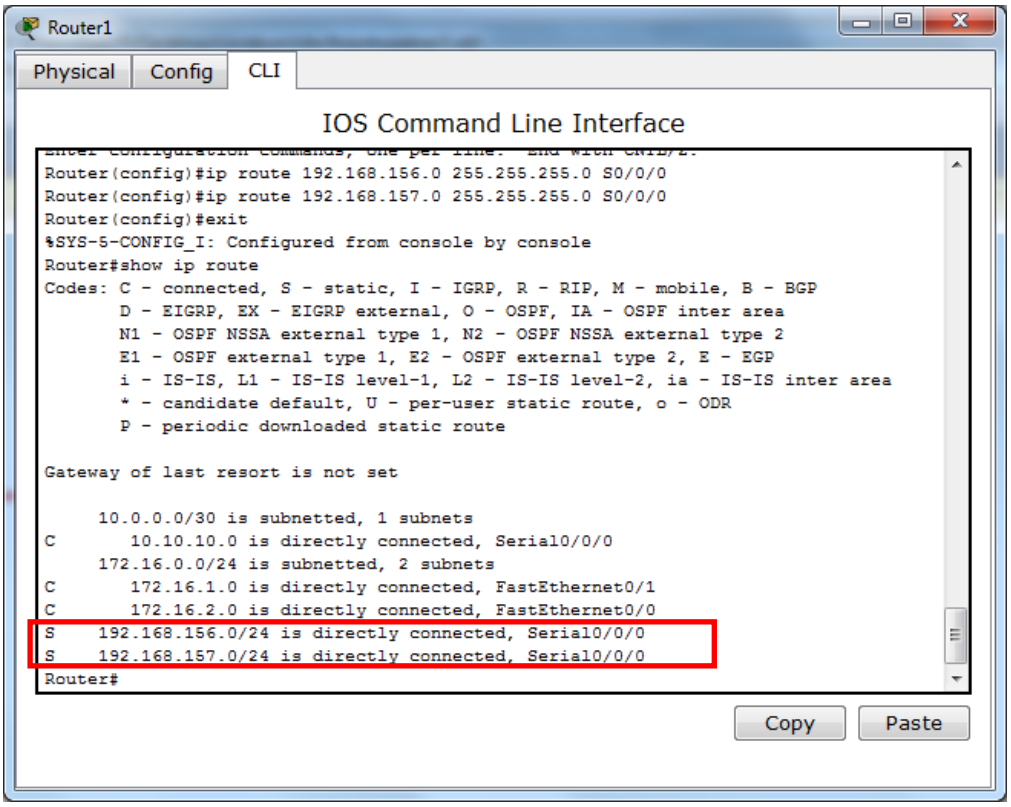
Obrázek 3.17 – Zobrazení statických cest ve směrovací tabulce levého routeru

Nastavili jsme tedy obě statické cesty do sítí 172.16.1.0 a 172.16.2.0 (obr. 3.16). Nyní při zobrazení směrovací tabulky levého routeru již vidíme 5 cest, z toho dvě statické. Takže router může směrovat paket do těchto sítí. Zopakujme si tedy otázku, bude ping z PC0 na PC3 úspěšný?



Obrázek 3.18 – Simulace pingu mezi vzdálenými sítěmi

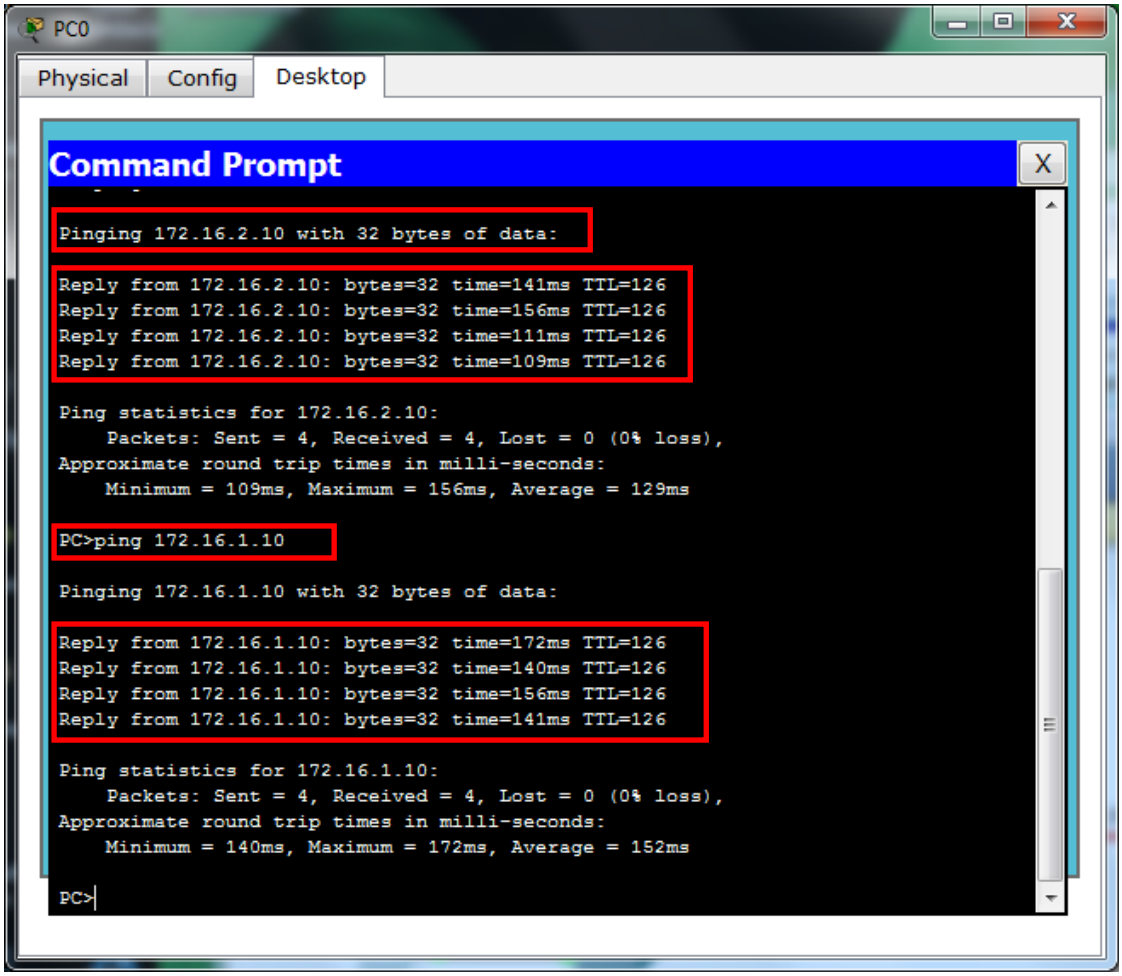
Odpověď je stále záporná. Pokud si uvedenou situaci spustíme v simulačním módu, vidíme, že paket z PC0 úspěšně dorazí na PC3, avšak na zpáteční cestě je paket zahozen, protože pravý router nezná cestu do sítě 192.168.157.0.



Obrázek 3.19 – Zobrazení statických cest ve směrovací tabulce pravého routeru

To znamená, že nám ještě chybí definovat statické cesty na pravém routeru. Obdobným způsobem jako na obr. 3.16 nastavíme příkazem ***ip route*** *cesty do sítí 192.168.156.0 a 192.168.157.0. Výslednou směrovací tabulku pravého routeru vidíme na obr. 3.19.*

Nyní již bude ping z PC0 do vzdálených sítí úspěšný. Obr. 3.20 demonstruje ping z PC0 na PC obou vzdálených sítí s IP adresami 172.16.1.10 a 172.16.2.10.



Obrázek 3.20 – ping z PC0 do vzdálených sítí 172.16.1.0 a 172.16.2.0

Ke kapitole 3 je připravena animace č. 3

V této animaci si vytvoříme topologii se dvěma routery, z nichž každý bude obsahovat své lokální sítě. Komunikace mezi lokálními sítěmi nevyžaduje žádnou úpravu směrovacích tabulek, neboť sítě jsou přímo připojené k routeru. Jinak je tomu v případě, kdy budeme chtít komunikovat z lokální sítě jednoho routeru do sítě druhého routeru. Tyto sítě routery neznají, a proto musíme zajistit směrování do těchto sítí. To lze v jednodušších topologiích provést nastavením statické cesty. Animace obsahuje nastavení statických cest a následné ověření komunikace mezi vzdálenými sítěmi.

Korespondenční úkol

Zjistěte, co na PC zobrazí v **command promptu** příkaz ***tracert***. Vyzkoušejte v dané topologii použít příkaz *tracert* 172.16.1.10 na počítači PC0.

Otázky ke kapitole 3

1. Jaký tvar argumentů má příkaz pro nastavení statické cesty?
2. Co znamená, že zařízení je typu DCE?
3. Jaké výhody a nevýhody má použití statické cesty?

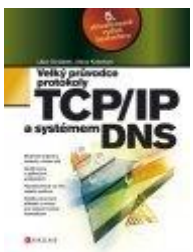
Úlohy k řešení ke kapitole 3

1. Vytvořte topologii o třech navzájem propojených routerech, každý z nich bude obsahovat jednu lokální síť.
2. V této topologii nastavte IP adresy ethernetových a sériových rozhraní routeru a IP adresy a výchozí brány na počítačích.
3. Na všech routerech nastavte statické cesty do lokálních sítí sousedních routerů.
4. Ověřte pingem komunikaci mezi všemi PC.
5. Přidejte na druhé ethernetové rozhraní každého routeru druhou lokální síť s dalším PC.
6. Kolik dalších statických cest je třeba v topologii vytvořit, aby byli všechny PC mezi sebou dostupné?

Další zdroje

Milan Keršláger, Jaroslav Horák, *Počítačové sítě pro začínající správce - 5. aktualizované vydání*, 2011, 304 stran, nakladatelství COMPUTER PRESS.

Sestavit, konfigurovat a provozovat vlastní síť nemusí být zapovězeno ani začátečníkům. Naučíte se vše, co má administrátor sítí pro začátek znát a umět. V 5. aktualizovaném vydání bestselleru, se dozvíte aktuální informace o moderní administraci sítí ve Windows i v Linuxu. Výklad doplňuje nejnutnější množství technických informací a principů stavby a fungování sítí i jejich protokolů. To vše bez nutnosti předchozích odborných znalostí.



Libor Dostálek, Alena Kabelová, *Velký průvodce protokoly TCP/IP a systémem DNS - 5. aktualizované vydání bestselleru*, 2008, 488 stran, nakladatelství COMPUTER PRESS.

Takřka kompletně přepracované vydání proslulé publikace zohledňuje nejen nové trendy v oblasti protokolů, ale i hojné dotazy a komentáře čtenářů předchozích dílů, a to včetně skladby jednotlivých kapitol. Výukovou i referenční příručku od odborníků ocení nejen ostřílení síťoví administrátoři, ale také začátečníci, kteří by rádi pochopili základní filozofii protokolů TCP/IP a systému DNS.

4 DHCP A STATICKÝ PŘEKLAD ADRES – STATIC NAT

V běžném síťovém provozu jsme zvyklí, že je nám IP adresa přidělována. Samozřejmě, jsou i situace, kdy IP adresu, masku a *default gateway* nastavujeme sami. V našem učebním textu jsme tyto nastavení prováděli v připravených příkladech a animacích. Tato kapitola naopak ukáže automatické nastavení IP adres pomocí DHCP protokolu. Druhá část kapitoly hovoří o překladu adres, kdy je počítač vně sítě reprezentován jinou IP adresou než uvnitř své lokální sítě.

Čas ke studiu: 3 hodiny

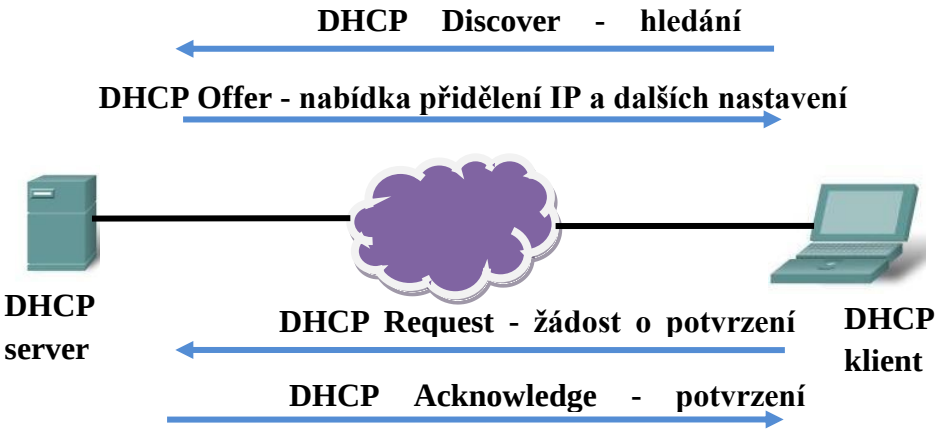
Cíl: Po prostudování tohoto odstavce budete umět

- Princip přidělení IP adresy pomocí DHCP protokolu.
- Prakticky nastavit router jako DHCP server.
- Vysvětlit princip překladu adres, tzv. NAT.
- Konfigurovat rozhraní routeru pro statický překlad adres.

Výklad

4.1 Protokol DHCP – Dynamic Host Configuration Protocol

Každý počítač v síti potřebuje být identifikován IP adresou. Pokud administrujete malou síť, můžete IP adresy nastavovat manuálně. Ale i v tomto případě se můžete dostat do různých problémů, jejichž řešení vám bude ubírat čas.



Obr. 4.1 DHCP komunikace

Ve velkých sítích manuální konfigurace IP adres již nepřichází v úvahu vůbec. IP adresy jsou přidělovány tzv. DHCP serverem, který má k dispozici určité množství IP adres a

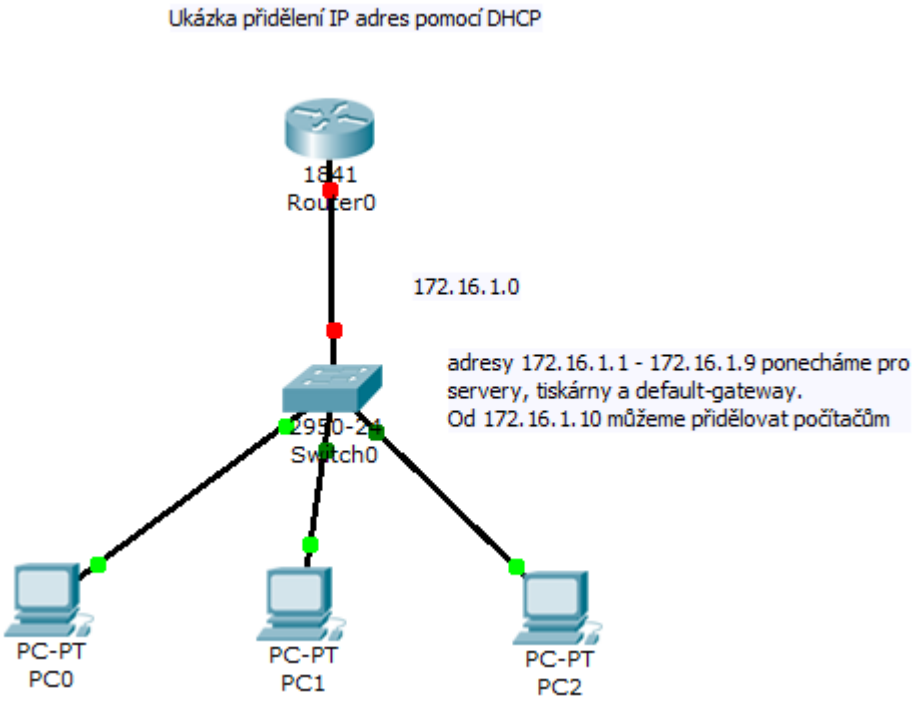
je připraven je přidělit počítačům, které se připojí do sítě, v níž má DHCP server oblast své působnosti. IP adresu počítač nedostane navždy. DHCP server zapůjčuje IP adresy počítačům na určitou dobu a pokud je počítač odpojen ze sítě, IP adresa se vrátí zpět do množiny volných IP adres.

Pojem k zapamatování – Proces přidělení IP adres pomocí DHCP

Proces přidělení IP adresy řídí komunikaci mezi PC v roli klienta a DHCP serveru. Jsou celkem zapotřebí čtyři komunikační fáze, než počítač obdrží IP adresu. Po připojení počítače do sítě počítač vyšle *broadcastový* paket tzv. DHP Discover, který hledá přítomnost DHCP serveru. *Broadcastový* znamená fakt, že je vyslán všem účastníkům sítě. Počítač totiž neví komu má žádost poslat, tak nejjednodušší je poslat paket všem. Tento způsob rozeslání žádosti není v počítačové síti neobvyklý, používá jej mnoho protokolů na různých vrstvách. *Broadcast* paket dojde jednotlivým zařízením a zařízení kterému je určen ho zpracuje, ostatní zařízení paket zahodí. *Discover* Paket tedy dojde na DHCP Server a ten odpoví paketem *DHCP Offer*, který obsahuje nabídku IP adresy, masky sítě, nastavení DNS serveru a výchozí brány. Klient dalším požadavkem oznamuje, že s přidělenými údaji souhlasí a na závěr přijde ze serveru potvrzení. Tohle je samozřejmě ideální situace. Pokud se klient a server na přidělených údajích nedomluví, nebo přijde ze serveru zamítnutí (místo **ACK** přijde paket **NACK**), celý proces se musí opakovat.

Řešený příklad 4.1 – Topologie pro nastavení DHCP protokolu

Pro ukázku přidělení IP adres třem počítačům pomocí DCP serveru vytvoříme topologii uvedenou na obrázku. Na počítačích zatím nebudeme nic nastavovat, na routeru nastavíme IP adresu ethernetového rozhraní a aktivujeme interface.



Obrázek 4.2 – Topologie tří PC připojených přes switch k routeru ve funkci DHCP

Řešený příklad 4.2 – Nastavení DCP protokolu na routeru

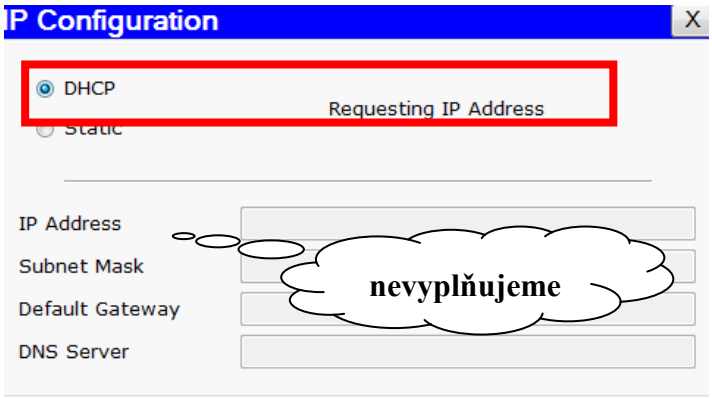
V konfiguračním režimu routeru pomocí sady příkazů ip dhcp s argumenty nastavíme celou funkcionalitu dhcp protokolu. Nejprve nastavíme rozsah adres, které nebudeme přidělovat, tyto adresy obvykle použijeme jako defaultní bránu, dns server, či třeba síťovou tiskárnu. Poté nastavujeme defaultní síť pro přidělení adres, defaultní bránu a dns server.

```
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.9
Router(config)#ip dhcp pool PRIDELENI_IP_ADRES
Router(dhcp-config)#network 172.16.1.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.1.1
Router(dhcp-config)#dns-server 172.16.1.2
Router(dhcp-config)#
```

Obrázek 4.3 – nastavení DHCP serveru na konzoli routeru

Řešený příklad 4.3 – Nastavení IP adresy na PC

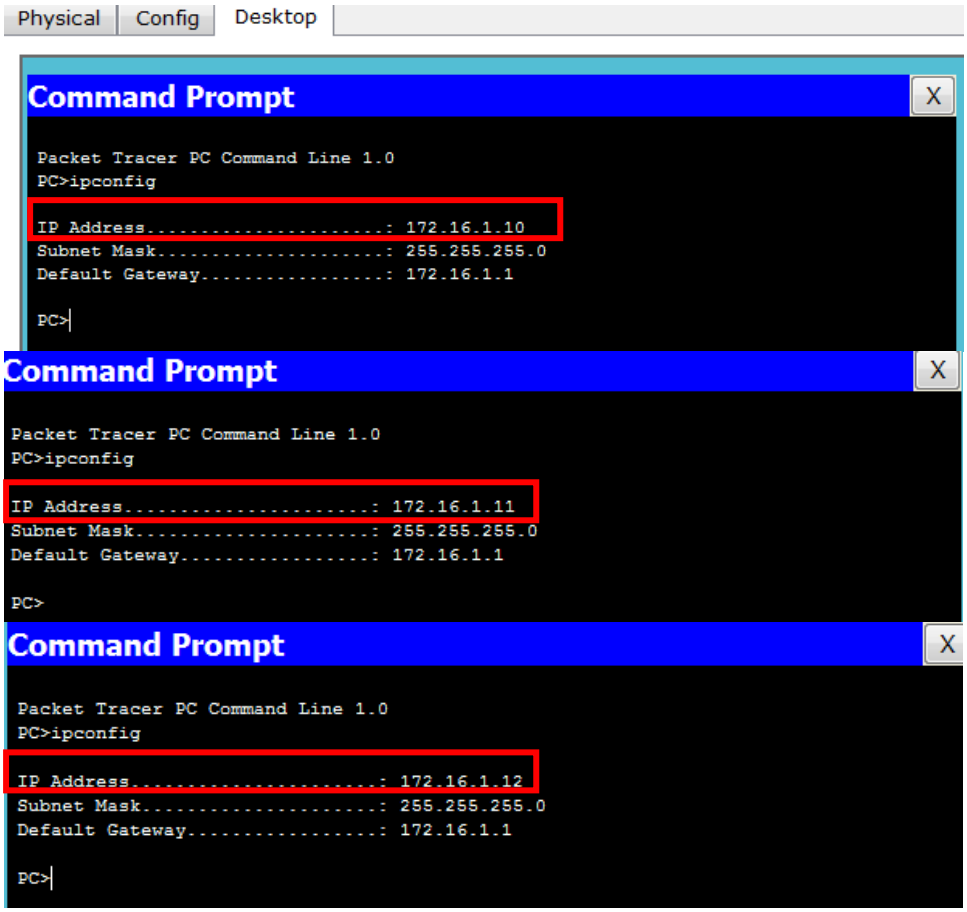
V naší topologii máme na switch připojeny tři počítače. U všech tří nastavíme IP konfiguraci na DHCP. Při zaškrtnutí této položky vidíme, že DHCP server vyřizuje požadavek: ***Requesting IP Address.***



Obrázek 4.4 – nastavení přidělení IP adresy na počítači pomocí DHCP serveru

Řešený příklad 4.4 – Ověření Přidělení IP adresy na PC

Na všech třech počítačích z naší topologie by měly být pomocí DHCP přiděleny IP adresy. V případě adresního prostoru jsme vyloučili adresy ***172.16.1.1 – 172.16.1.9****. Z toho vyplývá, že první počítač bude mít přidělenu adresu* ***172.16.1.10****, druhý bude mít v posledním oktetu* ***.11*** *a třetí* ***.12****. Nastavení jednoduše ověříme v příkazovém řádku příkazem* ***ipconfig****.*



Obrázek 4.5 – Ověření přidělení IP adresy na počítači pomocí DHCP serveru

Korespondenční úkol

V uvedené topologii přidejte další dva počítače a nastavte v jejich konfiguraci přidělení IP adresy pomocí DHCP. Poté se přesvědčte, jaké adresy PC obdržely v příkazovém řádku.

4.2 Statický překlad adres

Network Address Translation (NAT, česky *překlad síťových adres*, ***Native Address Translation*** (*nativní překlad adres*) je způsob úpravy síťového provozu přes router přepisem výchozí a/nebo cílové IP adresy, často i změnu čísla TCP/UDP portu u průchozích IP paketů.

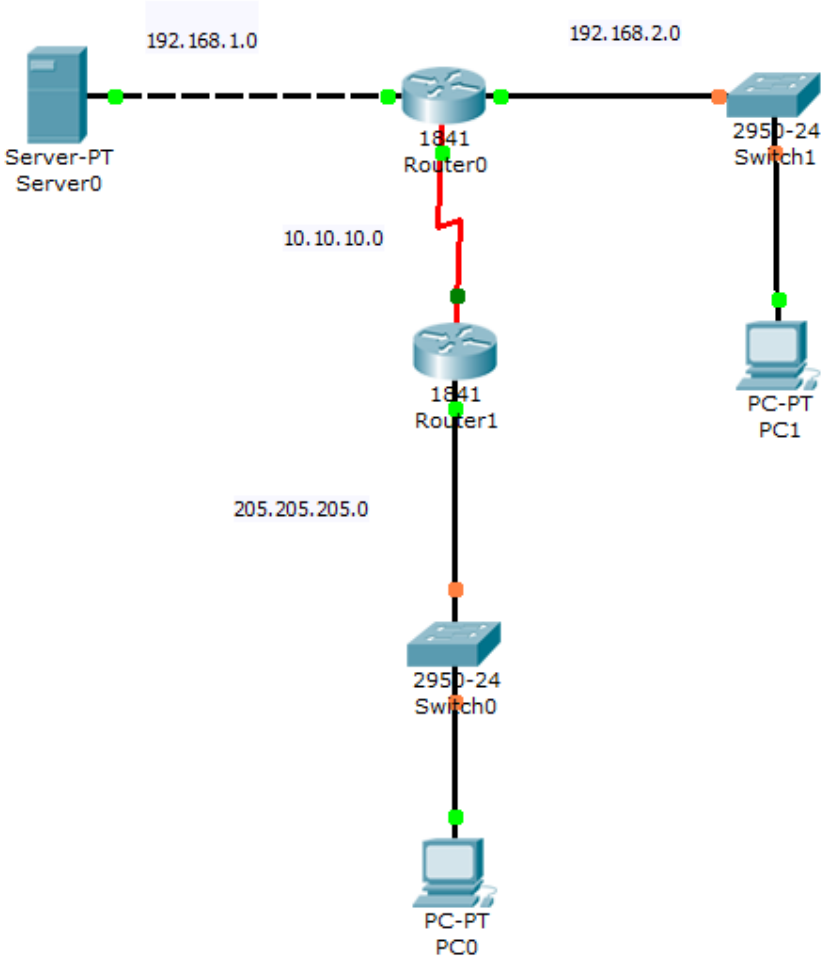
Překlad síťových adres je funkce, která umožňuje překládání adres. Což znamená, že adresy z lokální sítě přeloží na jedinečnou adresu, která slouží pro vstup do jiné sítě (např. Internetu).

Kromě statického překladu adres je definován také dynamický překlad, kdy je počítačům z lokální sítě definován rozsah adres pro překlad, tento rozsah je jim dynamicky přidělován při komunikaci mimo lokální síť. Lze také definovat překlad adres tak, že všechny počítače budou mít stejnou venkovní IP adresu a rozlišovány budou pouze jiným číslem

portu. V našem příkladu si ukážeme statický překlad adresy, kdy komunikující server bude v rámci venkovní sítě pod jinou adresou, než při komunikaci uvnitř sítě.

Řešený příklad 4.5 – Topologie pro statický překlad adres

Definujme příkladovou topologii. Server 192.168.1.10 v síti 192.168.1.0 bude komunikovat vně této sítě pod adresou 209.165.1.10. Před samotnou definicí překladu adres tedy nakonfigurujme rozhraní routeru 0 a routeru 1 dle obrázku.

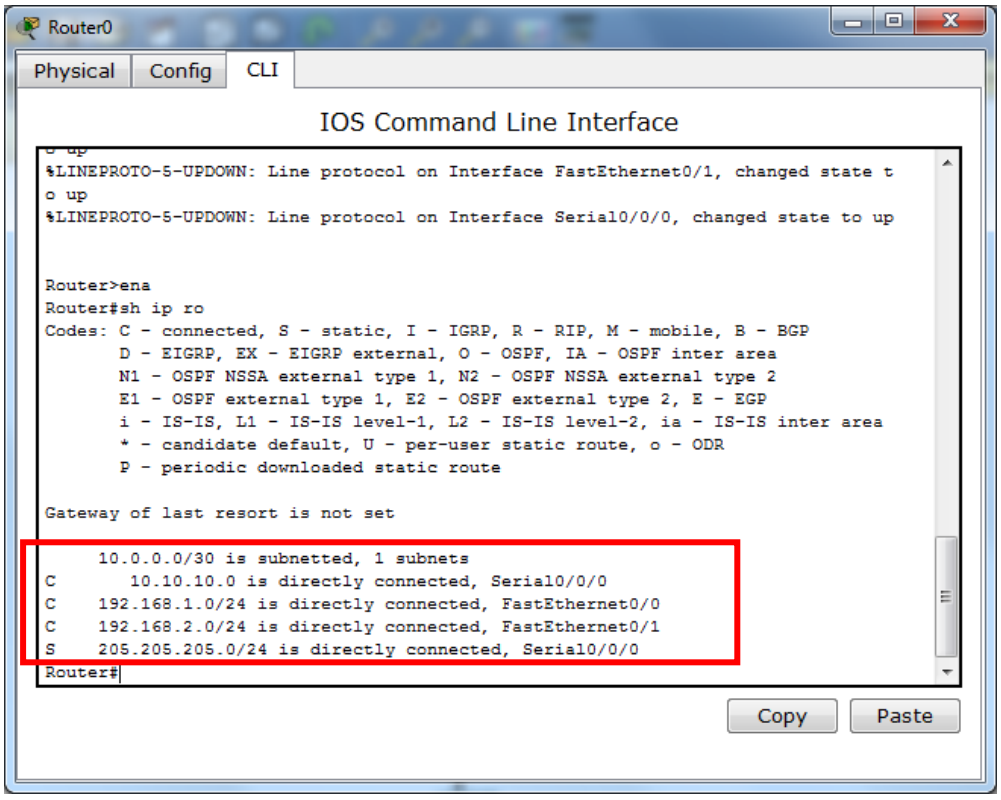


Obrázek 4.6 – Topologie pro překlad adres serveru v síti 192.168.1.0

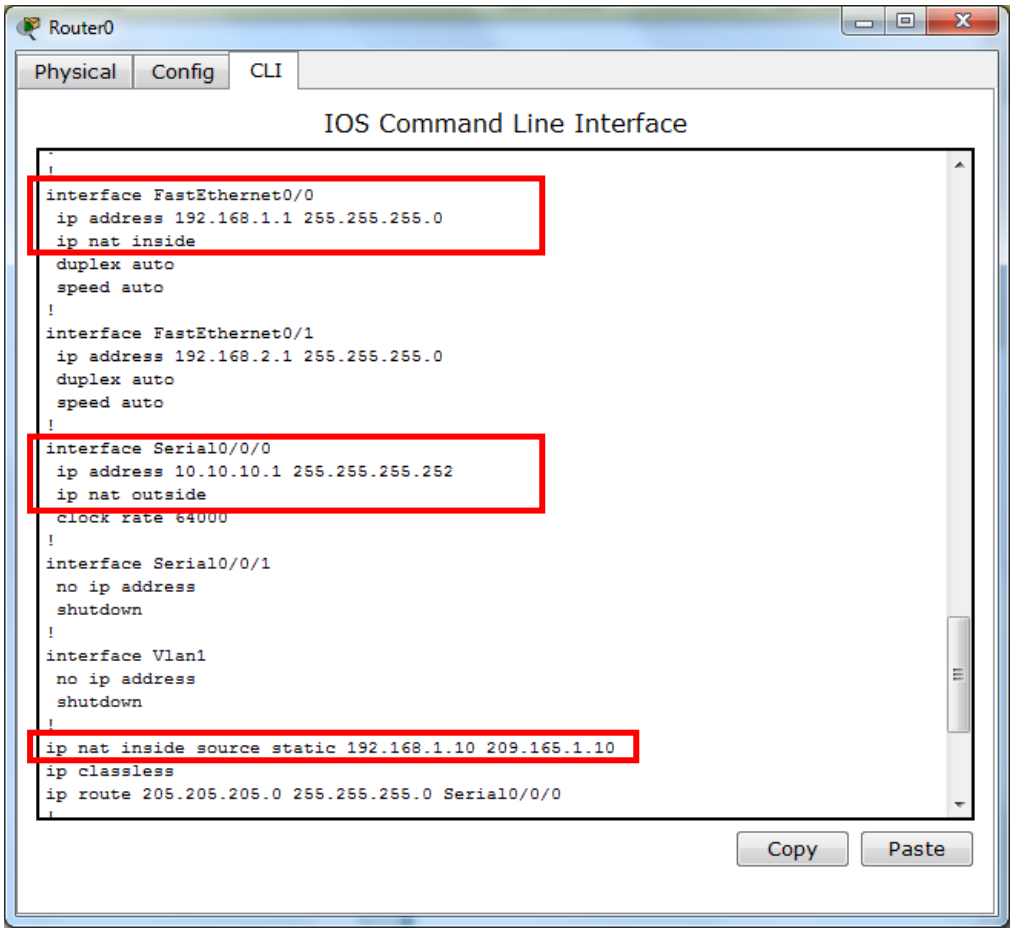
Řešený příklad 4.6 – Nastavení překladu adres

Pro samotnou přípravu řešení překladu adres si nejprve prohlédneme směrovací tabulku routeru 0. Vidíme tři přímo připojené sítě 192.168.1.0., 192.168.2.0 a 10.10.10.0 a nadefinovanou statickou cestu do sítě 205.205.205.0.

Samotný překlad adres se konfiguruje ve třech fázích, nejprve nastavíme vstupní interface do lokální sítě příkazem ***ip nat inside,*** *stejně tak výstupní interface* ***příkazem ip nat outside****. V našem případě je výstupním interfacem sériový port do okolní veřejné sítě. Třetím krokem je nastavení samotného překladu adres, překládáme adresu 192.168.1.10 na 209.165.1.10.*



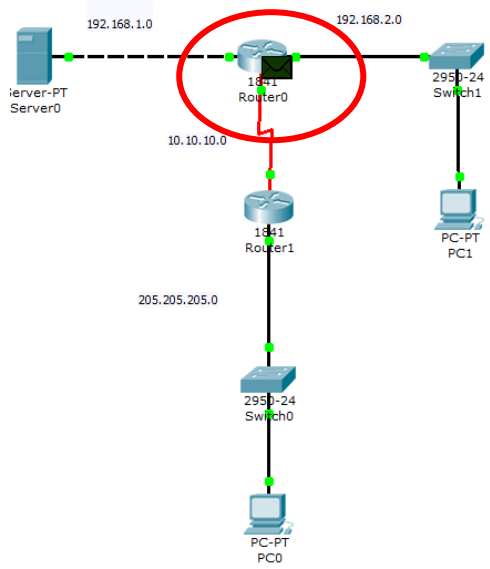
Obrázek 4.7 – Směrovací tabulka routeru, ze kterého bude uskutečněn překlad adres



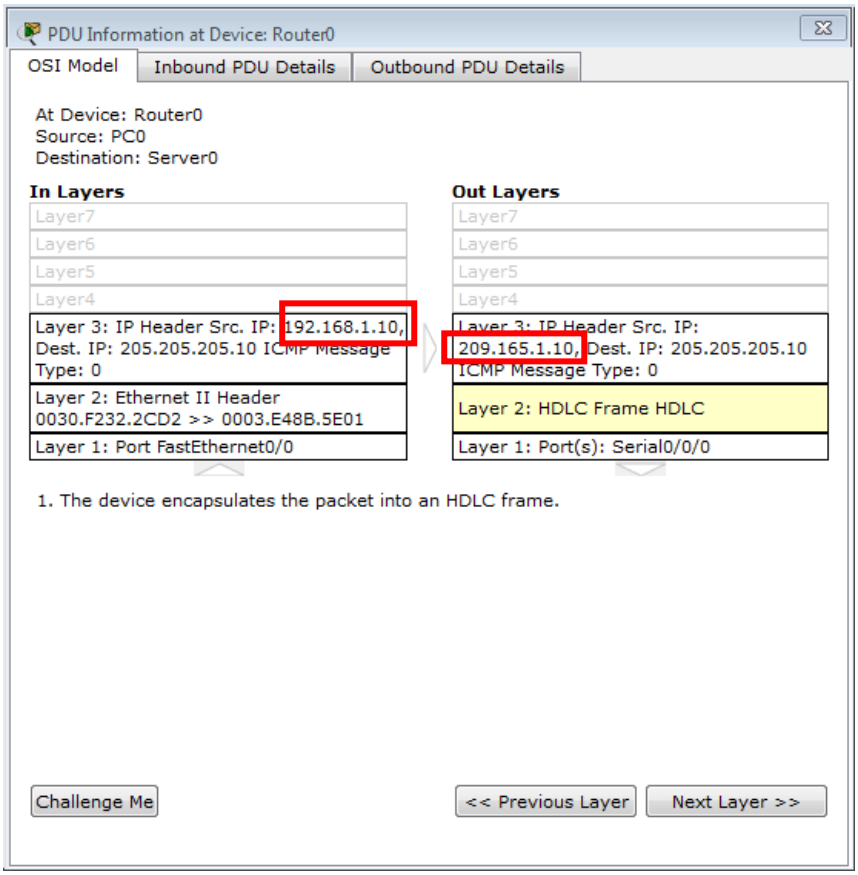
Obrázek 4.8 – Nastavení statického překladu adres

Řešený příklad 4.7 – Ověření překladu adres

Překlad adres ověříme simulací pingu ze serveru do vzdálené sítě na PC0 s IP adresou 205.205.205.10. Při vytvoření ping paketu v programu paket tracer můžeme zobrazený paket prohlížet. Vidíme zdrojovou adresu serveru (In Layers) 192.168.1.10 přeloženou v odchozí vrstvě (Out Layers) na 209.165.1.10.



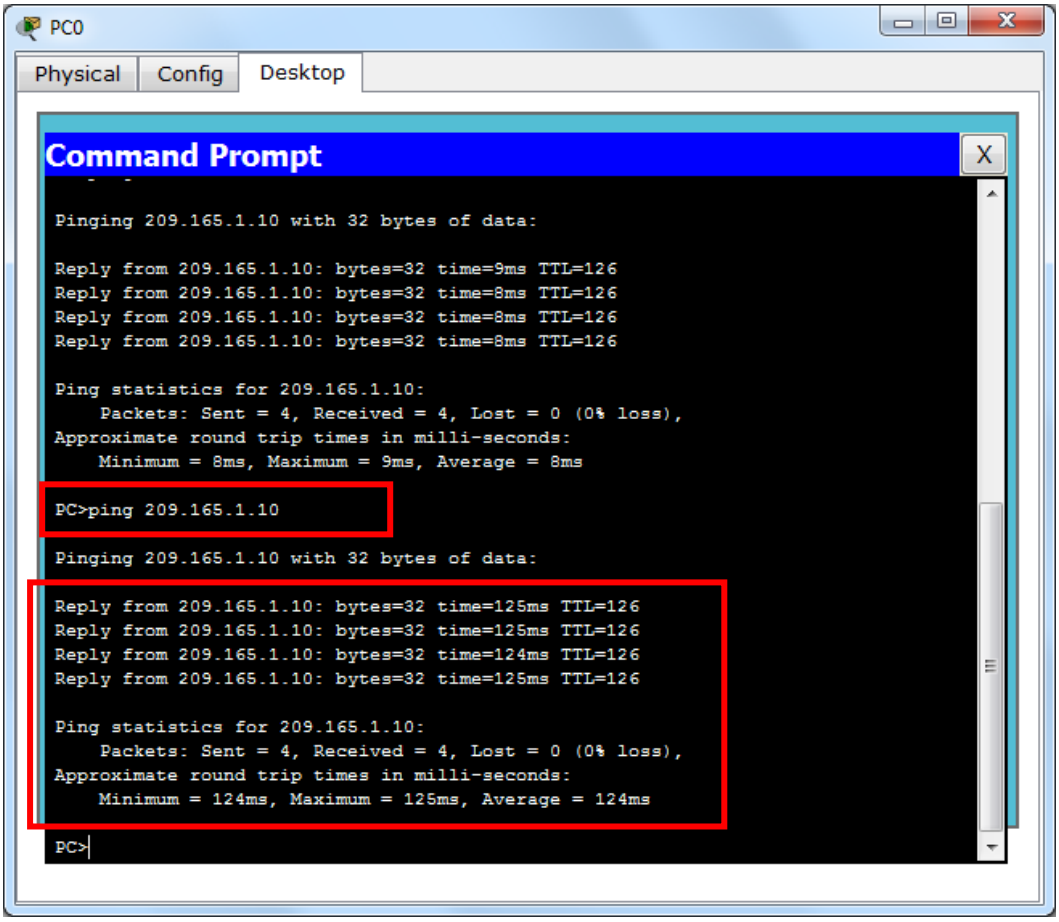
Obrázek 4.9 – Sledování paketu vyslaného ze serveru do okolní sítě



Obrázek 4.10 – Detaily sledovaného paketu vyslaného ze serveru do okolní sítě

Řešený příklad 4.8 – Ověření překladu adres II

Překlad adres ověříme také komunikací z opačné strany. Zkusíme ping ze vzdáleného počítače na 209.165.1.10. vidíme, že ping je úspěšný. Počítač komunikuje se serverem prostřednictvím této adresy, o jeho skutečné IP adrese 192.168.1.10 netuší nic.



Obrázek 4.11 – Vzdálené PC komunikuje se serverem prostřednictvím přeložené adresy

Ke kapitole 4 je připravena animace č. 4 a č. 5

V animaci č. 4 si ukážeme konfiguraci routeru jako dhcp serveru. Nejprve vytvoříme topologii se třemi počítači, které budou mít IP adresy přiděleny pomocí DHCP. Poté nakonfigurujeme router jako DHCP server a ověříme přidělené IP adresy na počítačích. Nakonec do topologie vložíme další PC a ověříme opět přidělení IP adresy pomocí DHCP. V animaci č. 5 si ukážeme, jak se nastavuje na rozhraní routeru překlad IP adresy. Server reprezentován v lokální síti určitou IP adresou bude mít mimo síť IP adresu zcela odlišnou. Pod touto adresou s ním bude komunikovat zařízení z jiné sítě, které jeho IP adresu v lokální síti nemůže znát. Animace ukáže simulaci komunikace s překladem adres včetně detailů paketů.

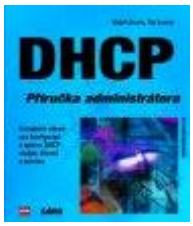
Otázky ke kapitole 4

1. Jak komunikuje DHCP protokol mezi DHCP serverem a koncovým zařízením?
2. Jaké druhy překladu adres se používají v administrátorské praxi?
3. K čemu slouží DNS server?

Úlohy k řešení ke kapitole 4

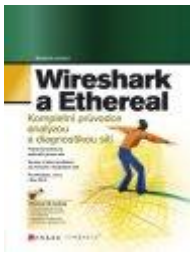
1. Navrhněte topologii sítě, kde router obsahuje dvě podsítě.
2. Do každé podsítě umístěte tři PC.
3. Pro obě podsítě nastavte DHCP přidělení adres, pro první síť v rozsahu .10 - .126. pro druhou .129 - .254.
4. Vyzkoušejte statický překlad adres pro obdobnou topologii jako v řešeném příkladu této kapitoly, s tím, že budou v lokální síti překládány IP adresy ze dvou serverů.
5. Ověřte komunikaci z vnější sítě.

Další zdroje



Ralph Droms, Ted Lemon, *DHCP –Příručka programátora*, 2004, 528 stran, nakladatelství COMPUTER PRESS.

Kniha je určena především administrátorům sítí, ale také architektům a realizátorům počítačových sítí – zkrátka každému, kdo je postaven před úkol navrhnout, implementovat, spravovat nebo odlaďovat počítačovou síť, která využívá DHCP.



Josh Burke, Joshua Wright, Greg Morris, Angela Orebaugh, Gilbert Ramirez, *Wireshark a Ethereal - Kompletní průvodce analýzou a diagnostikou sítí*, 2008, 448 stran, nakladatelství COMPUTER PRESS.

S tímto kompletním průvodcem hravě vyřešíte problémy se sítí, konfigurací systému i aplikacemi. A navíc vám umožní nahlédnout pod pokličku zdaleka nejpoužívanějšího síťového analyzátoru, jeho uživatelského prostředí i příkazů.

5 SMĚROVACÍ PROTOKOLY RIP, EIGRP A OSPF

Z minulých kapitol již víme, jaké údaje obsahuje směrovací tabulka, jakým způsobem ji na konzoli routeru zobrazíme, jak zobrazuje router cesty do přímo připojených sítí a také jakým způsobem nastavíme statickou cestu do sítě, kterou router nemá připojenou ke svému rozhraní. Zbývá nám tedy pro pochopení základů síťové komunikace získat informace o konfiguraci směrovacích protokolů. Těch existuje celá řada, my se budeme věnovat konfiguraci těch nejznámějších.

Čas ke studiu: 3 hodiny

Cíl: Po prostudování tohoto odstavce budete umět

- Popsat princip směrovacích protokolů.
- Nakonfigurovat na routeru směrovací protokol.
- Zobrazit a pochopit informace směrovacích protokolů ze směrovací tabulky.
- Konfigurovat směrování ve složitějších topologiích sítí.

Výklad

5.1 Podstata směrovacích protokolů

Pro větší topologie sítě je nutno využít služeb směrovacích protokolů, protože není v silách administrátor zadávat všechny cesty manuálně. Mezi nejznámější směrovací protokoly patří:

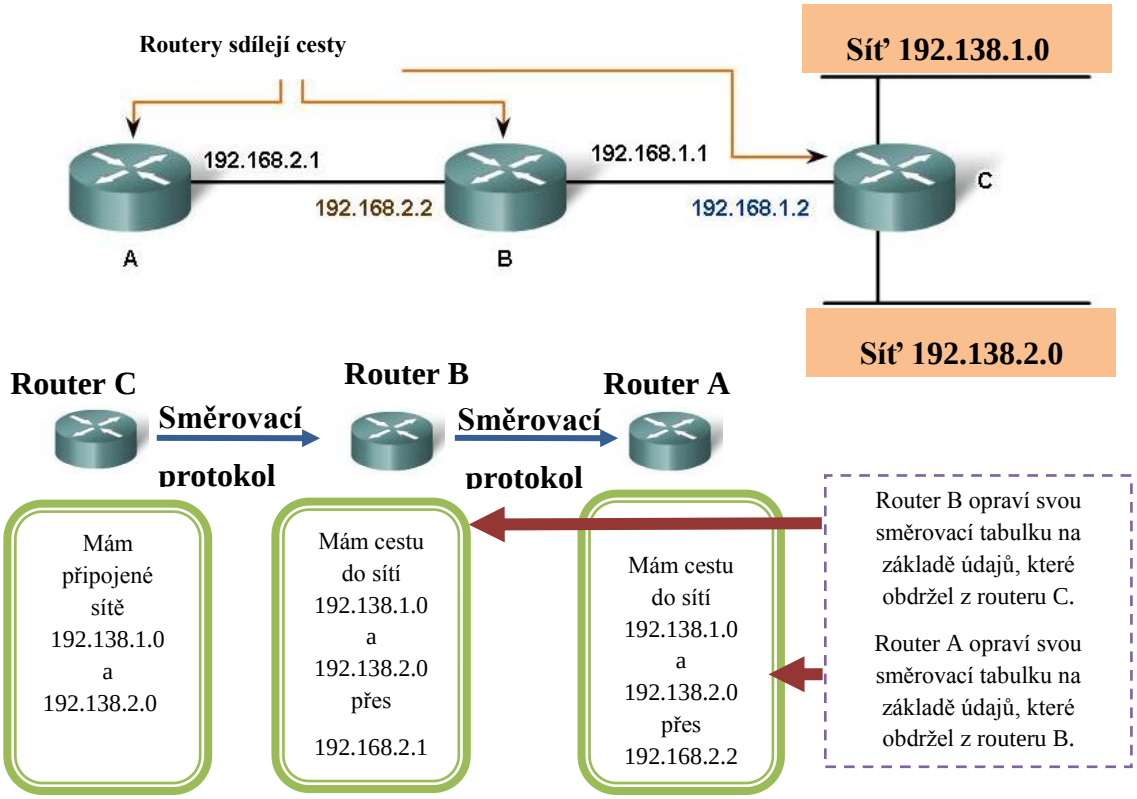
- RIP (*Routing Information Protocol*)
- EIGRP (*Enhanced Interior Gateway Protocol*)

OSPF (*Open Shortest Path First*)

Podstatou práce směrovacího protokolu je udržování aktuálních směrovacích tabulek na routerech, které jsou pod stejnou správou směrovacího protokolu. Tyto routery si prostřednictvím protokolu vyměňují své aktuální údaje ze směrovacích tabulek. Pokud se na nějakém routeru změní topologie sítě, router upraví svou směrovací tabulku a informuje o tom ostatní routery. Zjednodušeným příkladem by se tento proces předávání informací dal vyjádřit obrázkem 5.1.

Pojem k zapamatování – zobrazení směrovacích protokolů ve směrovací tabulce routeru

Dosud jsme se setkali ve směrovací tabulce pouze s přímo **připojenou** (***connected)*** sítí, značenou **C,** nebo **staticky** nastavenou cestou – **S.** Zmíněné tři směrovací protokoly RIP, EIGRP a OSPF mají ve směrovací tabulce před zobrazením sítě zkratky **R**, **D** a **O**.



Obr. 5.1– Výměna směrovacích informací pomocí protokolů

5.2 Příklad topologie se směrovacím protokolem RIP

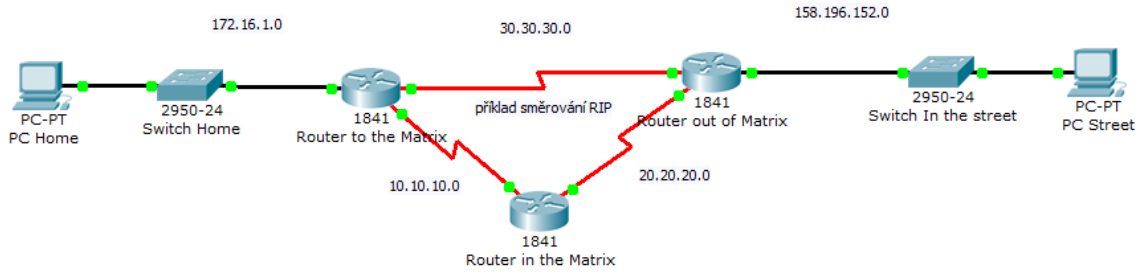
***Routing Information Protocol* (RIP)** je v informatice směrovací protokol umožňující směrovačům (routerům) komunikovat mezi sebou a reagovat na změny topologie počítačové sítě. Ačkoliv tento protokol patří mezi nejstarší doposud používané směrovací protokoly v sítích IP, má stále své uplatnění v menších sítích a to především pro svoji nenáročnou konfiguraci a jednoduchost.

RIP je směrovací protokol typu *distance-vector* (vektor vzdálenosti) využívající Bellmanův-Fordův algoritmus pro určení nejkratší cesty v síti. Metrikou směrování je počet skoků k cílové síti (hop count). Jako ochrana proti směrovacím smyčkám je implementovaný omezený počet směrovačů (hopů) v cestě k cíli, maximální možný počet hopů je 15.

Řešený příklad 5.1 – topologie pro příklad směrovaní pomocí routovacího protokolu RIP

Pro příklad směrovacího protokolu vytvoříme trochu složitější topologii. V případě dvou routerů jsme schopni síť administrovat nastavením statických cest. V případě že přidáme do topologie třetí router, počet statických cest by rapidně narostl. Při přidání jakékoliv další sítě do topologie bychom museli nastavit statickou cestu na zbývajících routerech. Abychom se těmto administrativně náročným úkonům vyhnuli, musíme zvolit směrovací protokol.

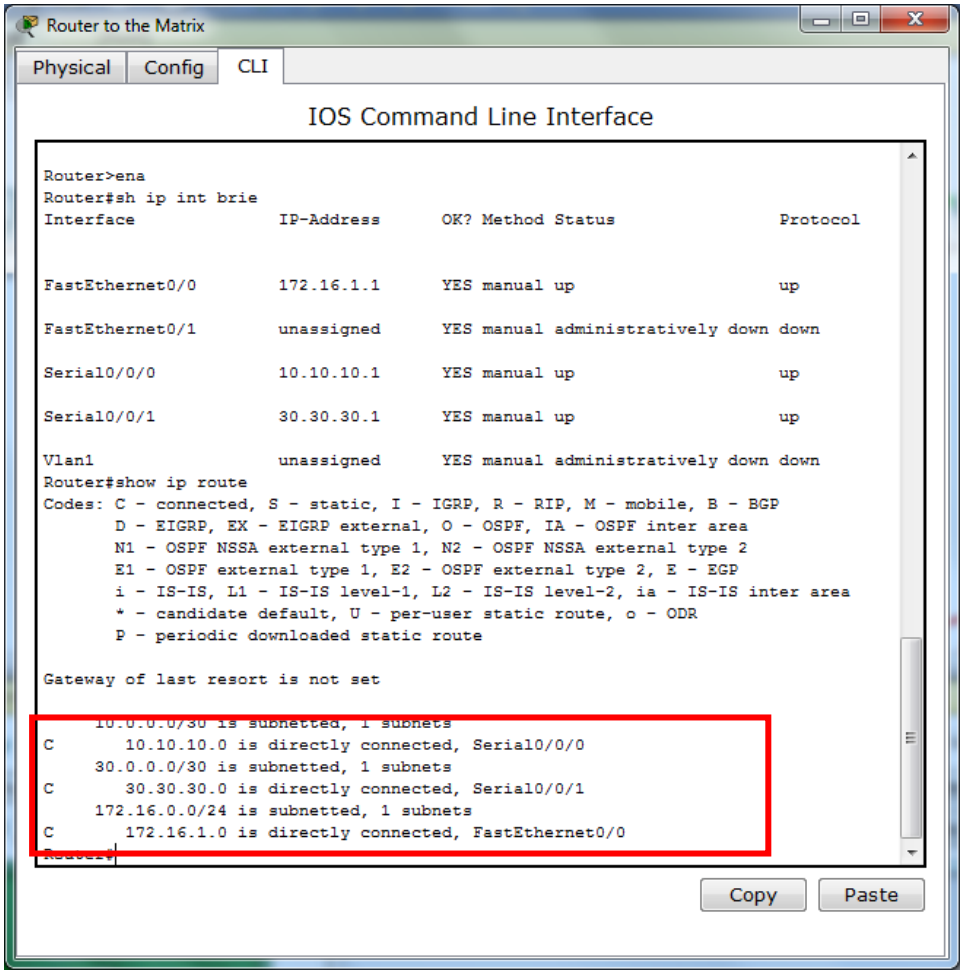
Vytvořená topologie bude obsahovat tři routery, tzn. tři spojovací sítě 10.10.10.0, 20.20.20.0 a 30.30.30.0, krajní routery budou mít svou lokální síť na ethernetovém rozhraní 172.16.1.0 pro levý router a 158.196.152.0 pro pravý router.

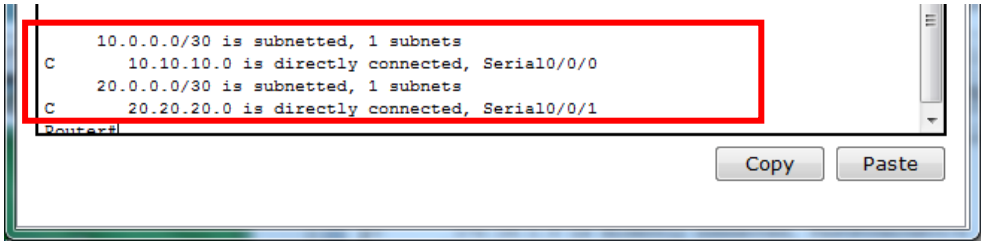


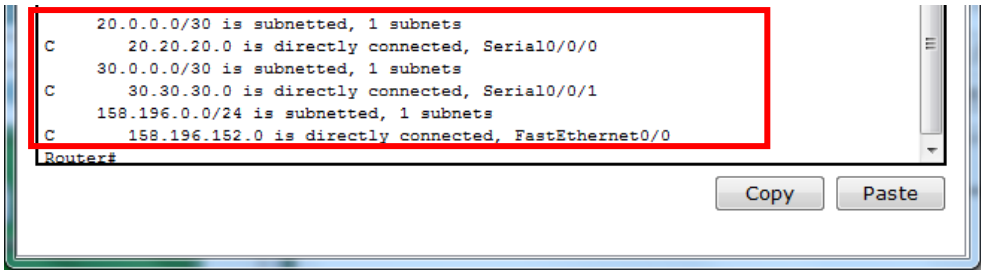
Obr. 5.2 – Topologie pro příklad směrování protokolem RIP.

Řešený příklad 5.2 – směrovací tabulky před nastavením směrovacího protokolu RIP

Při zobrazení směrovacích tabulek příkazem ***show ip route*** *uvidíme přímo připojené sítě (direct connected).*







Obr. 5.3 – Přímo připojené sítě všech routerů v topologii.

Řešený příklad 5.3 – nastavení routovacího protokolu RIP

Na všech routerech nastavíme v konfiguračním módu protokol RIP, příkazem router rip, nastavíme verzi protokolu rip 2 a příkazem network s argumentem přímo připojených sítí vytvoříme seznam sítí, který si routery budou mezi sebou předávat. Verze 2 protokolu rip umí přenášet informace o masce sítě, u verze 1 by všechny sítě pracovali se stejnou maskou.

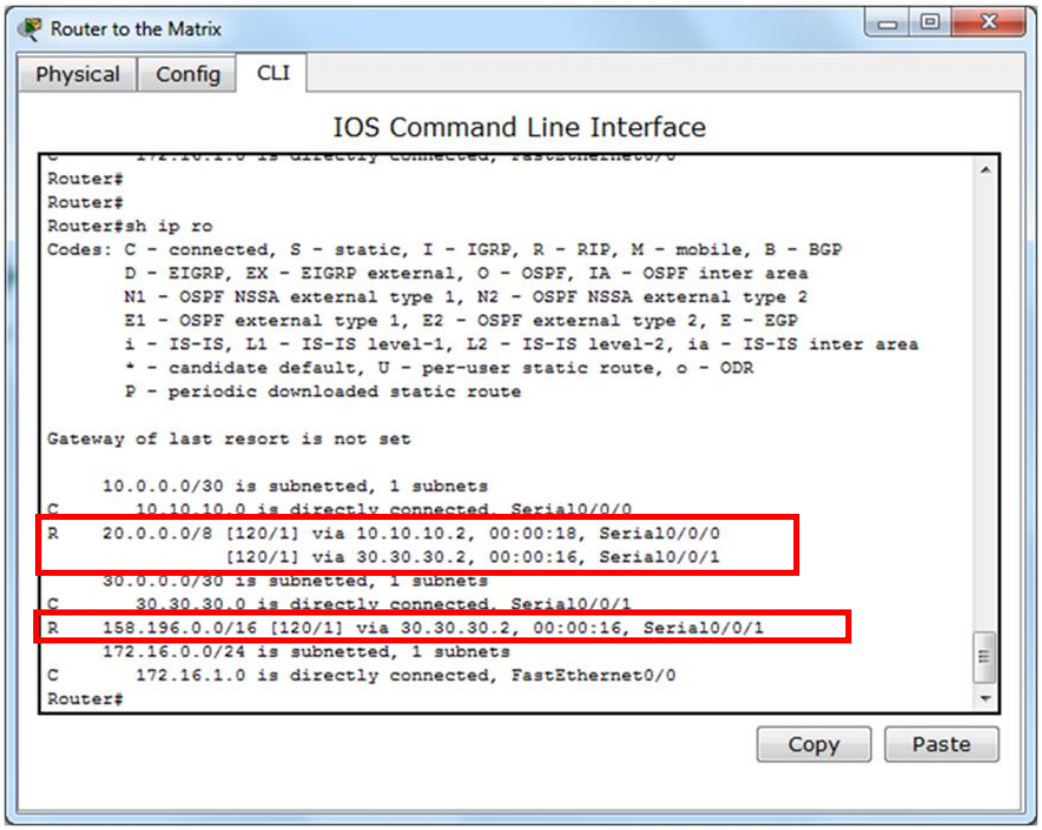
```
router rip
 version 2
 network 10.0.0.0
 network 30.0.0.0
 network 172.16.0.0
```

```
router rip
 version 2
 network 10.0.0.0
 network 20.0.0.0
```

```
router rip
 version 2
 network 20.0.0.0
 network 30.0.0.0
 network 158.196.0.0
```

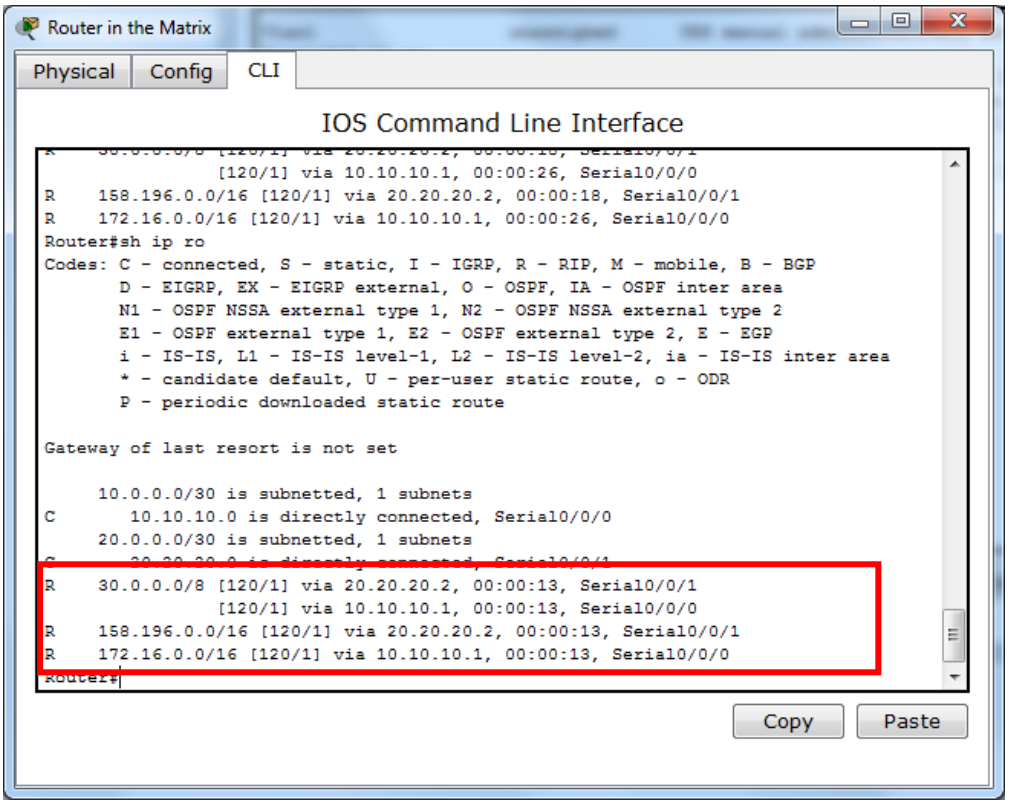
Obr. 5.4 – Nastavení protokolu RIP na všech routerech.

Řešený příklad 5.4 – směrovací tabulky po výměně informací mezi routery pomocí routovacího protokolu RIP

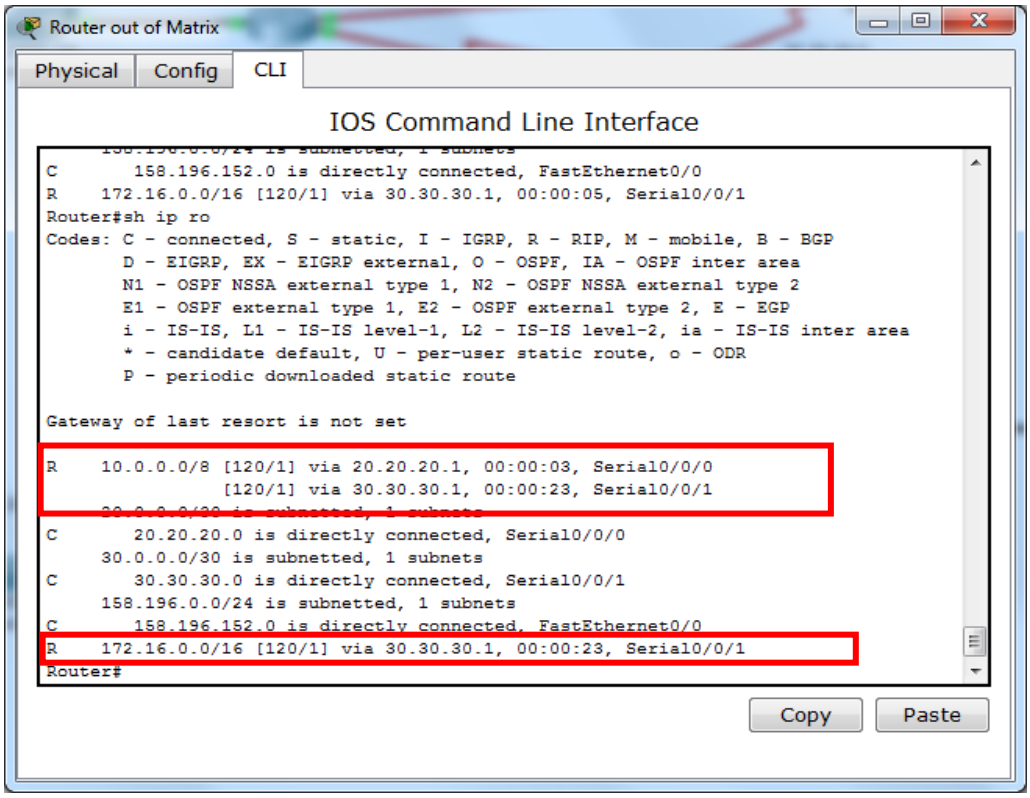


Obr. 5.5 – Směrovací tabulka levého routeru se sítěmi naučenými pomocí protokolu RIP.

Ihned po nastavení protokolu RIP na jednotlivých routerech protokol zajistí výměnu směrovacích tabulek. Sítě, které router doposud neznal a získal od svého souseda tak ve směrovací tabulce zobrazuje pod zkratkou ***R*** *s rozhraním, přes které je nová síť dostupná.*



Obr. 5.6 – Směrovací tabulka spodního routeru se sítěmi naučenými pomocí protokolu RIP.



Obr. 5.7 – Směrovací tabulka pravého routeru se sítěmi naučenými pomocí protokolu RIP.

Ze směrovacích tabulek vidíme, že levý a pravý router získal pomocí protokolu RIP dvě nové sítě. První síť je lokální síť opačného routeru a druhou sítí, kterou nemohl původně znát je spojovací síť opačného routeru se spodním routerem. Spodní router tak samozřejmě získá pomocí protokolu sítě tři: dvě lokální sítě zbylých routerů a jejich spojovací síť.

5.3 Příklad směrovacího protokolu EIGRP

Pokročilejším směrovacím protokolem je ***Enhanced Interior Gateway Routing Protocol*** (*EIGRP*), je nástupcem IGRP, který pracuje s takzvaným beztřídním směrováním (*classless routing*), umožňující vytvoření různě velikých sítí. Také implementuje *Diffusing Update Algoritmus* (*DUAL*), který zlepšuje routování a zabraňuje vytvoření smyček.

Řešený příklad 5.5 – natavení routovacího protokolu EIGRP

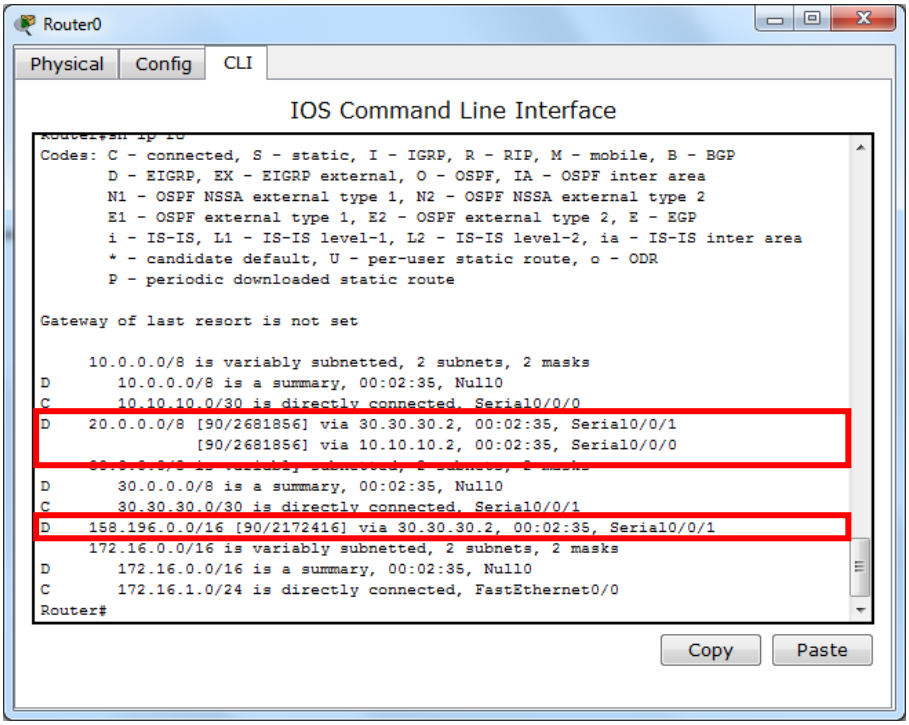
Pokud použijeme routovací protokol EIGRP, musíme na routerech v konfiguračním režimu zvolit tuto sadu nastavení, to znamená, že kromě samotného příkazu ***router eigrp 1****, uvádíme seznam připojených sítí s opačnou (wildcard) maskou sítě.*

```
router eigrp 1                                                    router eigrp 1
 network 172.16.1.0 0.0.0.255 router eigrp 1                       network 20.20.20.0 0.0.0.3
 network 10.10.10.0 0.0.0.3     network 10.10.10.0 0.0.0.3         network 30.30.30.0 0.0.0.3
 network 30.30.30.0 0.0.0.3     network 20.20.20.0 0.0.0.3         network 158.196.152.0 0.0.0.255
```

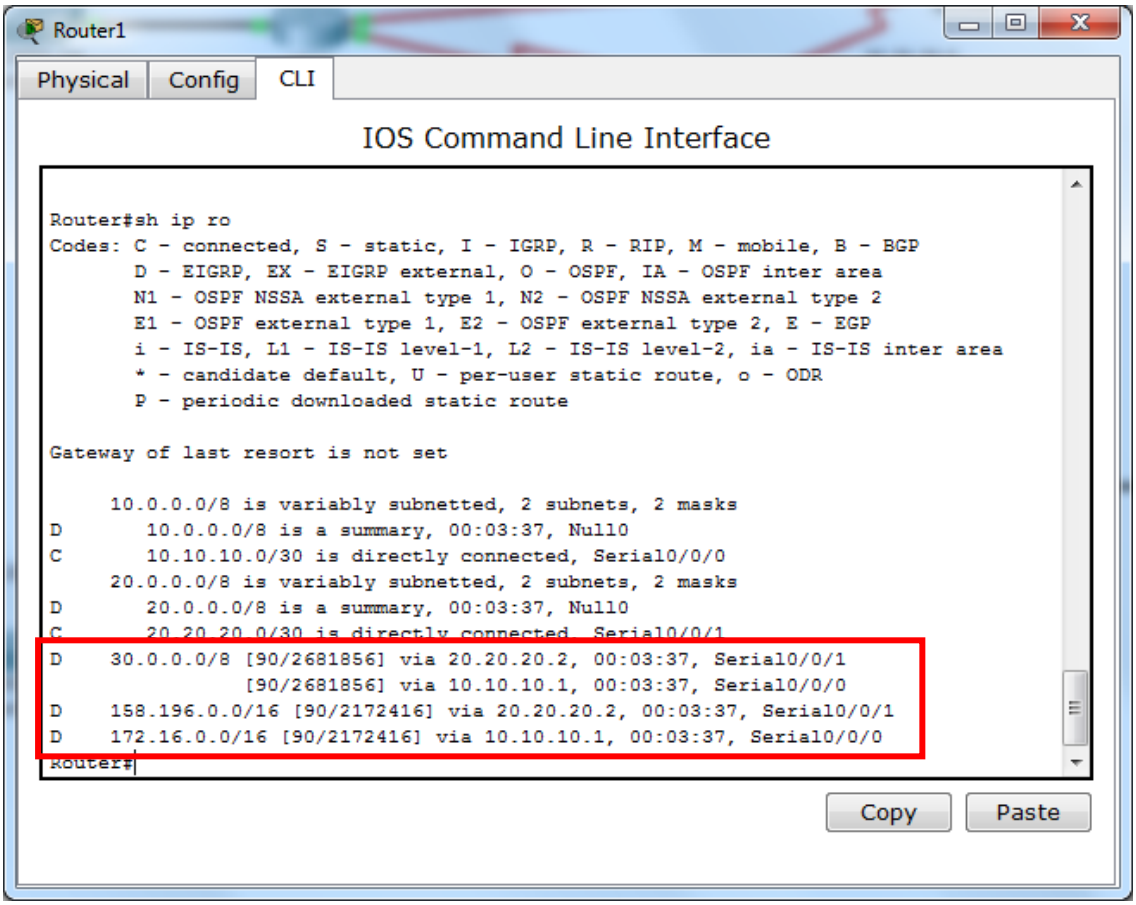
Obr. 5.8 – nastavení protokolu EIGRP.

Řešený příklad 5.6 – směrovací tabulky routovacího protokolu EIGRP

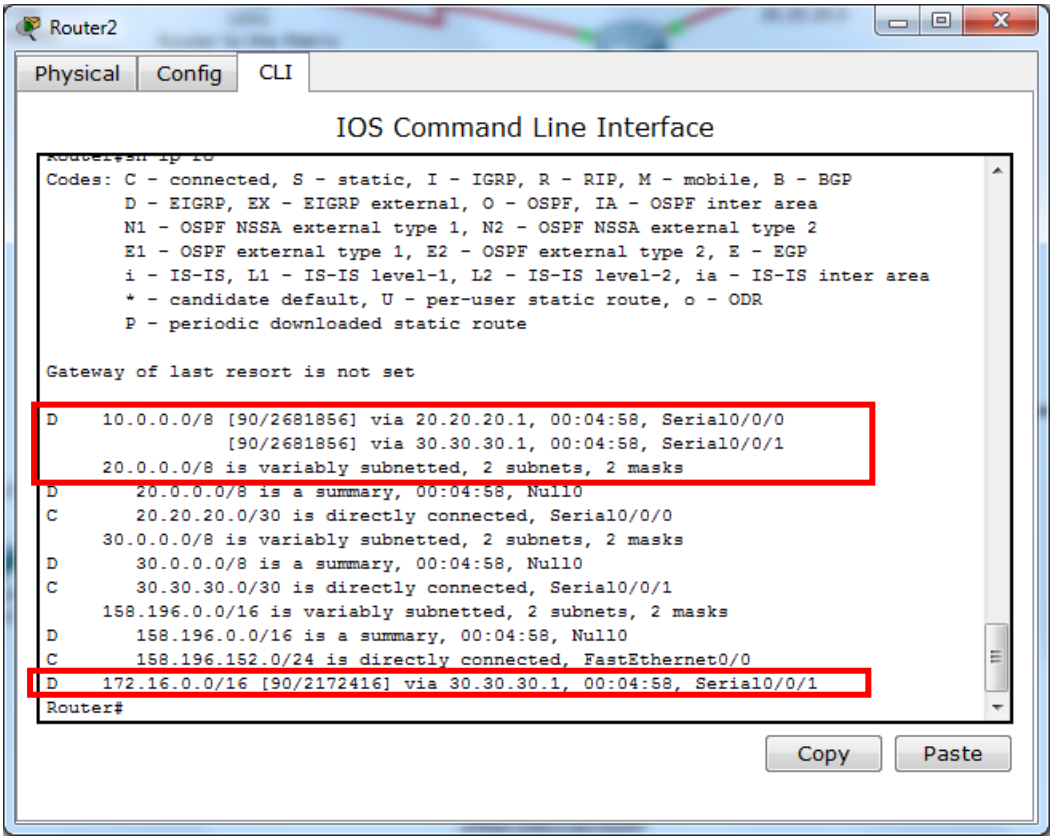
Směrovací tabulky budou mít nyní následující podobu.



Obr. 5.9– Směrovací tabulka levého routeru se sítěmi naučenými pomocí protokolu EIGRP.



Obr. 5.10 – Směrovací tabulka spodního routeru se sítěmi naučenými pomocí EIGRP.



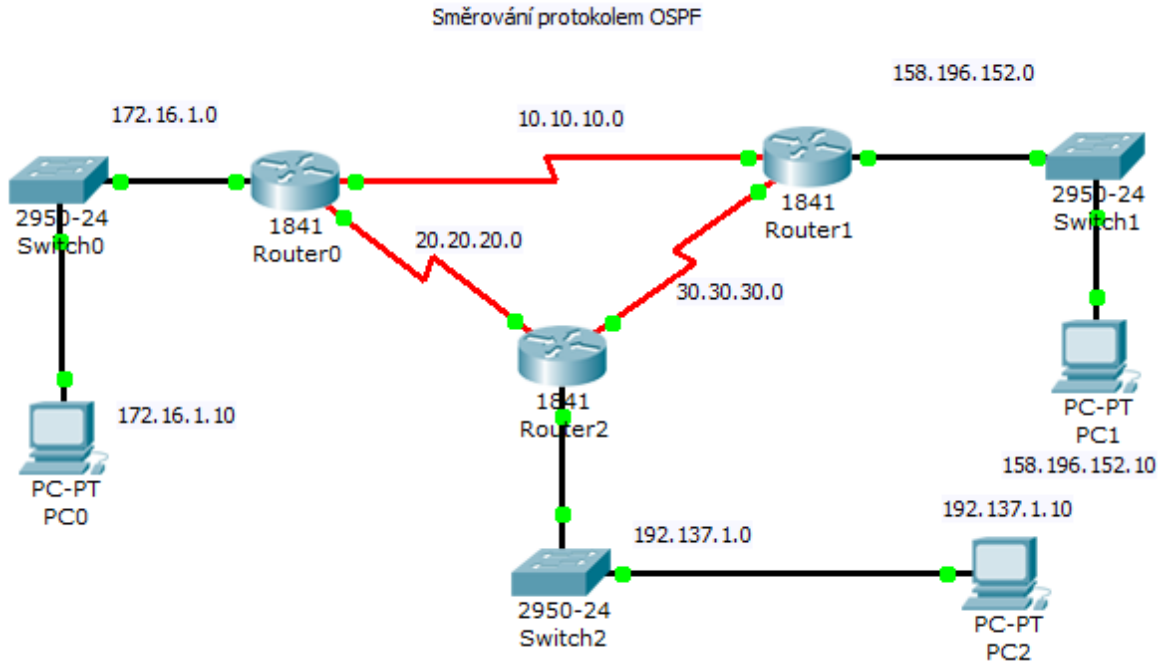
Obr. 5.11 – Směrovací tabulka pravého routeru se sítěmi naučenými pomocí EIGRP.

5.4 Topologie se směrovacím protokolem OSPF

Posledním protokolem, který si vyzkoušíme, bude velice často používaný protokol OSPF. *Open Shortest Path First* (**OSPF**) je adaptivní hierarchický distribuovaný routovací protokol, provádějící změny v routovacích tabulkách na základě změny stavu v síti. Jedná se o nejpoužívanější routovací protokol uvnitř autonomních systémů. Routery, používající tento protokol, si v pravidelných krátkých intervalech zvláštními zprávami (ECHO) kontrolují spojení se svými sousedními routery. Při zjištění jakékoliv změny zasílá oznámení všem routerům v síti, ty si pak podle nové informace přepočítají nové cesty v síti a podle toho upraví routovací tabulky. Výpočet nejkratších cest se provádí Dijkstrovým algoritmem.

Řešený příklad 5.7 – topologie pro příklad směrovaní pomocí routovacího protokolu OSPF

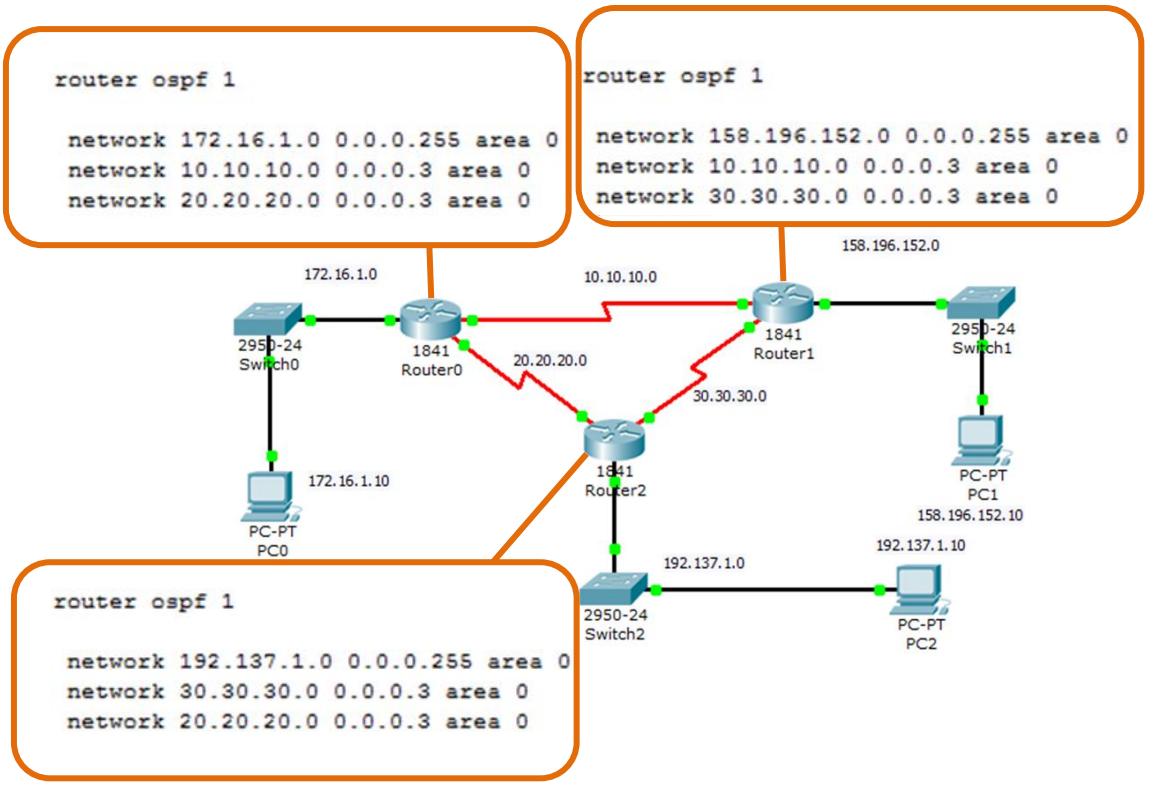
Vytvoříme topologii o třech routerech, z nichž každý bude mít svou lokální síť. Nastavíme spojovací sítě a časování na DCE interfacech Poté nakonfigurujeme ethernetové rozhraní routerů, a na počítačích nastavíme IP adresy, masky a výchozí brány. Poté budeme mít topologii připravenou k nastavení směrovacího protokolu OSPF.



Obr. 5.12 – Topologie pro příklad směrování pomocí OSPF

Řešený příklad 5.8 – nastavení routovacího protokolu OSPF

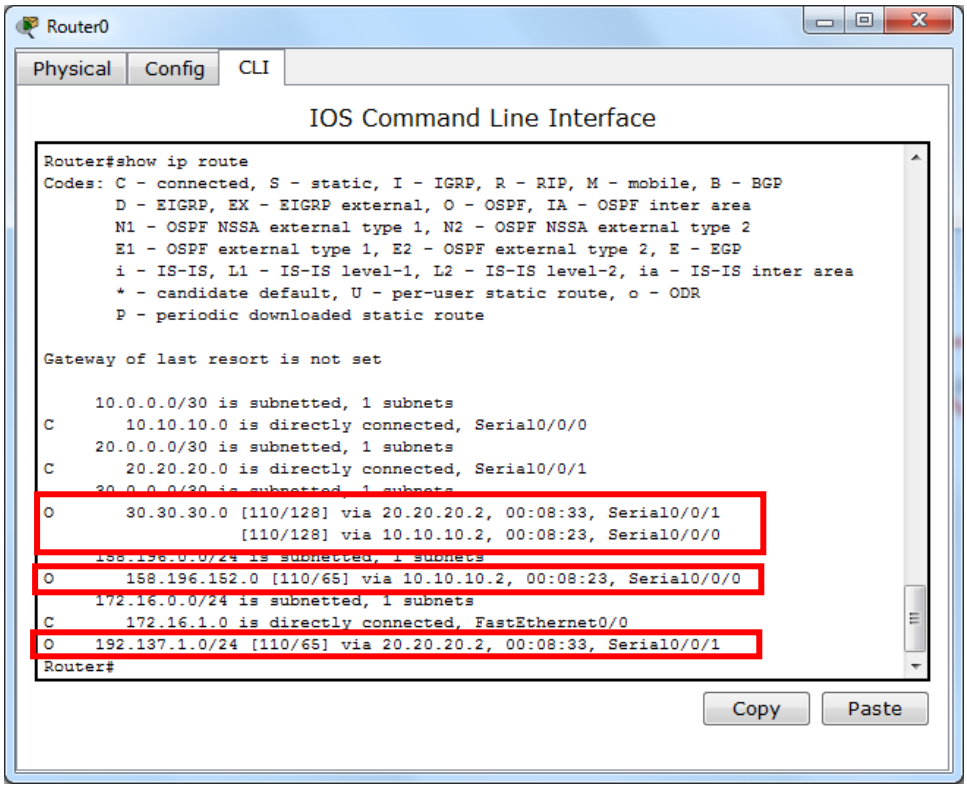
Po základní konfiguraci topologie sítě nastavíme na všech routerech směrovací protokol OSPF. Nejprve použijeme konfiguračním módu příkaz router ospf 1. Jednička je číslo instance směrovacího procesu. Ve složitějších topologiích bychom mohli použít více instancí protokolu OSPF. Poté příkazem network zapíšeme přímo připojené sítě s opačnou tzv. wildcard maskou, tak jako u protokolu EIGRP, a číslem oblasti, obvykle základní páteřní oblast označujeme jako area 0.



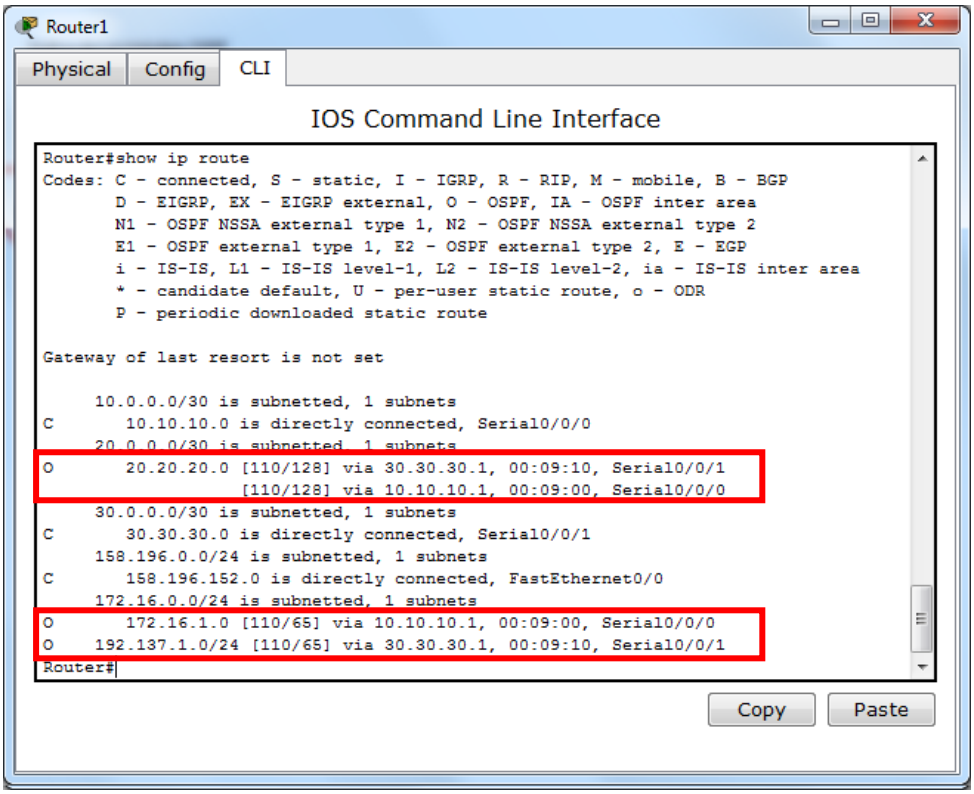
Obr. 5.13– Nastavení směrovacího protokolu OSPF na všech routerech

Řešený příklad 5.9 – směrovací tabulky routerů v topologii

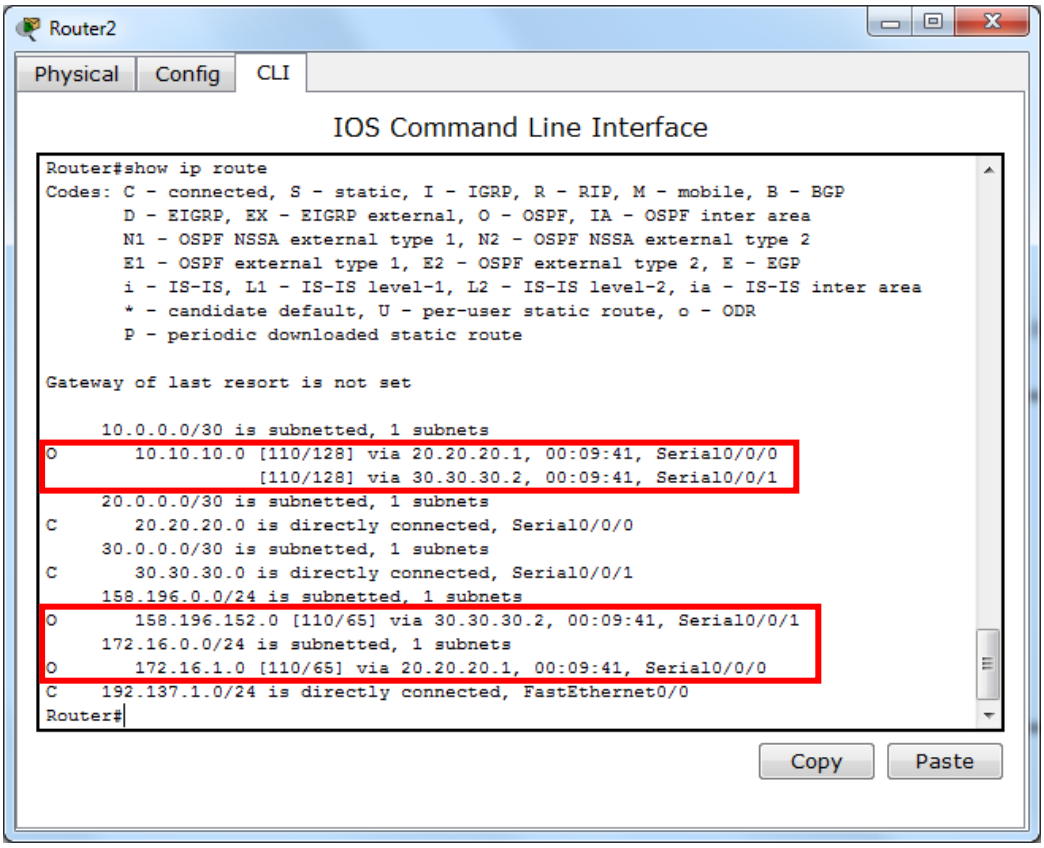
Směrovací tabulky budou mít nyní následující podobu.



Obr. 5.14 – Směrovací tabulka levého routeru s vyznačenými cestami pomocí OSPF



Obr. 5.15 – Směrovací tabulka pravého routeru s vyznačenými cestami pomocí OSPF



Obr. 5.16 – Směrovací tabulka spodního routeru s vyznačenými cestami pomocí OSPF

5.5 Metrika a Administrativní distance a směrovacích protokolů

Každý směrovací protokol potřebuje kritérium, podle kterého posoudí, která z více možných cest do cílové sítě je nejvýhodnější. Různé protokoly používají různá kritéria. Toto kritérium se označuje jako metrika. Například RIP používá „*hop count*“ neboli počet přeskoků mezi routery. Protokol EIGRP využívá kombinaci šířky pásma, zatížení, zpoždění a spolehlivosti linky s pěticí nastavitelných konstant. Obecně platí, čím nižší číslo tím je metrika lepší, pro zajímavost vzoreček výpočtu metriky vypadá takto:

$$metric = \left[K_1 \times bandwidth + \frac{K_2 \times bandwidth}{256 - load} + K_3 \times delay \right] \times \left[\frac{K_5}{reliability + K_4} \right]$$

Defaultní hodnota konstant je K1 = K3 = 1 a K2 = K4 = K5 = 0. Protokol OSPF používá metriku označovanou jako cena (cost). To je číslo v rozsahu 1 až 65535, přiřazené ke každému rozhraní směrovače. Opět čím menší číslo, tím má cesta lepší metriku a bude tedy více preferována. Standardně je ke každému rozhraní přiřazena cena automaticky odvozená z šířky pásma daného rozhraní podle vztahu: **cena = 100000000 / bandwidth v bps.** Např. linka 64kbps bude mít standardně cenu 100000000/64000=1562. Na obrázku 5.17 metrika RIP říká, že k síti 50.0.0 se dostaneme přes jeden router, zatímco do sítě 193.158.193.0 přes routery 2. Pokud by se do této sítě v budoucnu bylo možno dostat přes 1 *hopcount*, tato cesta by dostala přednost a objevila by se ve směrovací tabulce na místo současné cesty. Na obrázcích 5.19 a 5.20 vidíme metriku EIGRP a OSPF.

```
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Serial0/0/0
     40.0.0.0/30 is subnetted, 1 subnets
C       40.40.40.0 is directly connected, Serial0/0/1
R    50.0.0.0/8 [120/1] via 40.40.40.2, 00:00:18, Serial0/0/1
C    192.137.1.0/24 is directly connected, FastEthernet0/0
R    193.158.193.0/24 [120/2] via 40.40.40.2, 00:00:18, Serial0/0/1
Router#
```

Obr. 5.17 – Metrika protokolu RIP je dána počtem „hopů“ tj. počtem routerů do cílové sítě

Protokol	Administrativní distance (AD)
Přímo připojený interface	0
Statická cesta	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
EGP	140

Obr. 5.18 – Administrativní distance síťových cest

Jak vidíme, metrika se u každého protokolu vypočítává jinak a tato čísla mnohdy nejsou porovnatelná, protože jsou počítána z různých kritérií. Pokud tedy budu mít do sítě více cest pomocí více protokolů, nerozhodne o cestě metrika, ale administrativní distance protokolů. To je vlastně číslo dané prioritní tabulkou protokolů. Opět platí, čím nižší číslo, tím vyšší priorita. Nejvyšší prioritu tak má samozřejmě přímo připojený interface, následuje statická cesta. V tabulce na obr. 5.18 vidíme hodnoty AD pro jednotlivé protokoly, což si můžeme ověřit i ve směrovacích tabulkách na obrázku 5.17, 5.19 a 5.20.

```
D    10.0.0.0/8 [90/2681856] via 20.20.20.1, 00:04:58, Serial0/0/0
                [90/2681856] via 30.30.30.1, 00:04:58, Serial0/0/1
     20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       20.0.0.0/8 is a summary, 00:04:58, Null0
C       20.20.20.0/30 is directly connected, Serial0/0/0
     30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       30.0.0.0/8 is a summary, 00:04:58, Null0
C       30.30.30.0/30 is directly connected, Serial0/0/1
     158.196.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       158.196.0.0/16 is a summary, 00:04:58, Null0
C       158.196.152.0/24 is directly connected, FastEthernet0/0
D    172.16.0.0/16 [90/2172416] via 30.30.30.1, 00:04:58, Serial0/0/1
Router#
```

Obr. 5.19 – AD a metrika protokolu EIGRP

```
      10.0.0.0/30 is subnetted, 1 subnets
C        10.10.10.0 is directly connected, Serial0/0/0
      20.0.0.0/30 is subnetted, 1 subnets
O        20.20.20.0 [110/128] via 10.10.10.2, 00:00:09, Serial0/0/0
      30.0.0.0/30 is subnetted, 1 subnets
O        30.30.30.0 [110/192] via 10.10.10.2, 00:00:09, Serial0/0/0
      40.0.0.0/30 is subnetted, 1 subnets
C        40.40.40.0 is directly connected, Serial0/0/1
      50.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R        50.0.0.0/8 [120/1] via 40.40.40.2, 00:00:01, Serial0/0/1
O        50.50.50.0/30 [110/256] via 10.10.10.2, 00:00:09, Serial0/0/0
C     192.137.1.0/24 is directly connected, FastEthernet0/0
O     193.158.193.0/24 [110/193] via 10.10.10.2, 00:00:09, Serial0/0/0
Router#
```

Obr. 5.20 – AD a metrika protokolů RIP a OSPF

Ke kapitole 5 je připravena animace č. 6 a 7

V animaci č. 6 si ukážeme, jakým způsobem se konfiguruje na routeru směrovací protokol. Ukážeme si změnu ve směrovacích tabulkách a ověříme konektivitu mezi vzdálenými sítěmi pomocí pingu. V animaci č. 7 si ukážeme konfiguraci protokolu OSPF s následným ověřením komunikace síťových prvků. V druhé části animace si ukážeme topologii, ve které bude nakonfigurován jak protokol OSPF, tak RIP. Ukážeme si výběr vhodné cesty do vzdálené sítě, rozpojení cesty a následné zaktualizování směrovací tabulky.

Otázky ke kapitole 5

1. Pokud nastavím statickou cestu do sítě, jehož cestu již router zná pomocí protokolu OSPF, dojde k nahrazení této cesty mnou definovanou cestou?
2. Čemu se rovná metrika protokolu EIGRP při zachování výchozích konstant?
3. Jaká wildcard maska patří k maskám 255.255.255.128 a 255.255.0.0 ?

Úlohy k řešení ke kapitole 5

1. Navrhněte topologii sítě se třemi routery, z nichž má každý dvě lokální sítě.
2. Nastavte IP adresy ethernetových interface routeru.
3. Do obou podstítí každého routeru připojte PC a nastavte příslušnou IP adresu, masku a defaultní bránu.
4. Nastavte na všech routerech směrovací protokol RIP.
5. Vyzkoušejte dostupnost všech počítačů mezi sebou.
6. Nastavte na všech routerech směrovací protokol OSPF.
7. Sledujte změny ve směrovacích tabulkách.
8. Nastavte na jednom routeru statickou cestu do sítě sousedního routeru a sledujte změnu ve směrovací tabulce.

Další zdroje

Wendell Odom, Naren Mehta, Rus Healy, *Směrování a přepínání sítí - Autorizovaný výukový průvodce,* 2009, 880 stran, nakladatelství COMPUTER PRESS.

Chcete zvládnout veškerá témata k písemné zkoušce CCIE Routing and Switching 350-001 nebo se dokonale obeznámit s problematikou směrování a přepínání v sítích Cisco? Tato kniha vám pomůže nejen při samostudiu, ale také v běžné praxi administrátora, návrháře sítí či síťového technika.

Barrie Sosinsky, *Mistrovství – počítačové sítě,* 2010, 840 stran, nakladatelství COMPUTER PRESS.

Jste podnikový administrátor, spravujete velkou síť, zajímáte se o síťové protokoly a standardy nebo si propojujete doma počítače a chcete do hloubky rozumět všemu, co se ve vaší síti děje? Tato kompletní příručka vám poslouží jako úplný zdroj informací k teorii i praxi počítačových sítí.

6 ODPOVĚDI NA OTÁZKY

Otázky ke kapitole 1

1. *K čemu slouží příkaz ping?*

Příkaz ping je diagnostickým nástrojem, který kontroluje dostupnost cíle. Je používán jak na koncových, tak na síťových zařízeních. Typické použití je *ping ipaddresa.*

2. *Je nějaký rozdíl mezi paketem a rámcem nebo je to jen podobný termín?*

Z hlediska správné terminologie jde o zásadní rozdíl neboť paket je jednotka na síťové vrstvě, která k segmentu z předchozí transportní vrstvy přidá na začátek hlavičku síťového protokolu, zatímco rámec je ještě níže, a to na úrovni vrstvy síťového rozhraní, protokol zde přibaluje nejen hlavičku ale také zakončení rámce.

Otázky ke kapitole 2

1. *Jakým způsobem bude probíhat síťový provoz na PC, když nenastavíme defaultní bránu?*

   Komunikace bude probíhat pouze v lokální síti, ve které je počítač definován svou ip adresou a maskou, mimo tuto síť již komunikovat nebude moci.

2. *Kterým příkazem přejdu z hierarchicky vyššího konfiguračního režimu do nižšího?*

   Do nižšího režimu vždy přejdeme příkazem **exit**, v případě přechodu z privilegovaného do uživatelského režimu můžeme použít i **disable**.

3. *Mohu v konfiguračním režimu používat příkazy show? Např. show ip route.*

   Ano, ale musíme před tímto příkazem použít slovo **do** *např.* **do show ip int brief,** jinak musíme příkazem **exit** přejít do privilegovaného režimu a tam již příkaz vykonáme.

Otázky ke kapitole 3

1. *Jaký tvar argumentů má příkaz pro nastavení statické cesty?*

   Příkaz má tvar *iproute adresa maska interface*, kde adresa a maska definuje síť a interface přes který do sítě vede cesta.

2. *Co znamená, že zařízení je typu DCE?*

   DTE zařízení je koncové (*Data Terminal Equipment*), naproti tomu je DCE komunikační zařízení (*Data Comuniccation Equipment*). To obvykle poskytuje službu, takže na tomto zařízení se nastavuje synchronizace v našem případě *clockrate*.

3. *Jaké výhody a nevýhody má použití statické cesty?*

   Výhoda statické cesty je její priorita před ostatními cestami a poměrně snadná administrace. Nevýhodou však je, že při změně topologie je cesta stále ve směrovací tabulce, opět se musí ručně zrušit. Při narůstající složitosti topologie je však nastavování cest neefektivní a je třeba tuto práci svěřit směrovacímu protokolu.

Otázky ke kapitole 4

1. *Jak komunikuje DHCP protokol mezi DHCP serverem a koncovým zařízením?*

   Jsou celkem zapotřebí čtyři komunikační fáze,po připojení počítače do sítě počítač vyšle *broadcastový* paket tzv. DHP Discover, který hledá přítomnost DHCP serveru. .Paket tedy dojde na DHCP Server a ten odpoví paketem *DHCP Offer*, který obsahuje nabídku IP adresy, masky sítě, nastavení DNS servru a výchozí brány. Klient dalším požadavkem oznamuje, že s přidělenými údaji souhlasí a na závěr přijde ze serveru potvrzení. Pokud se klient a server na přidělených údajích nedomluví, nebo přijde ze serveru zamítnutí (místo **ACK** přijde paket **NACK**), celý proces se musí opakovat.

2. *Jaké druhy překladu adres se používají v administrátorské praxi?*

   - Network Address Port Translation (*NAPT, PAT*), kdy dochází k mapování čísel portů. Několik strojů pak může sdílet jednu veřejnou IP adresu.
   - NAT (basic NAT, static NAT), umožňující pouze překlad adres, nikoli mapování portů. Tato možnost vyžaduje IP adresu pro každé samostatné spojení.

3. *K čemu slouží DNS?*

   DNS (*Domain Name System*) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Systém DNS umožňuje efektivně udržovat decentralizované databáze doménových jmen a jejich překlad na IP adresy. Stejně tak zajišťuje zpětný překlad IP adresy na doménové jméno.

Otázky ke kapitole 5

1. *Pokud nastavím statickou cestu do sítě, jehož cestu již router zná pomocí protokolu OSPF, dojde k nahrazení této cesty mnou definovanou cestou?*

   Bude rozhodovat AD, takže statická cesta bude mít vždy větší prioritu, proto nahradí současnou cestu, ať už je získaná jakýmkoliv protokolem

2. *Čemu se rovná metrika protokolu EIGRP při zachování výchozích konstant?*

   Pokud K1 = K3 = 1 a K2 = K4 = K5 = 0, tak je poslední součinitel K5/(reliability + K4) ignorován a metrika bude dána součtem **bandwidth + delay**.

3. *Jaká wildcard maska patří k maskám 255.255.255.128 a 255.255.0.0?*

   Opačná masky budou 0.0.0.127 a 0.0.255.255.