
KAPITOLA 4

Základy tvorby podsítí

V této kapitole se budeme zabývat následujícími tématy zkoušky ICND1:

- **Adresování v sítích IP (IPv4/IPv6)**
 - Popis fungování a potřeby použití privátního a veřejného adresování IP v sítích protokolu IPv4

V této kapitole navážeme na předchozí kapitolu a budeme zkoumat problematiku adresování IP. Nejdříve ukážeme, jak lze síť IP dělit na podsítě. Bez této klíčové dovednosti nelze zvládnout problematiku sítí obecně. Když nyní víte, o jak důležité téma se jedná, počítejte s tím, že rychlé a přesné dělení sítí na podsítě je poměrně náročné a vyžaduje hodně času na procvičování. Buďte tedy trpěliví a při seznamování s tímto zásadním aspektem sítí se nevzdávejte, dokud si jej dokonale neosvojíte. Rozhodně nežertuji – tato kapitola je natolik důležitá, že byste si ji měli zapsat za uši.

Připravte se tedy na to, že hned ze začátku se do tématu tvorby podsítí IP pustíme hodně zostra. Víím, že následující rada vám bude připadat podivná. Podle mých zkušeností vám ale pomůže, když se před čtením této kapitoly pokusíte zapomenout na vše, co jste se o tvorbě podsítí zatím naučili – zejména pokud jste absolvovali oficiální školení společnosti Cisco nebo Microsoft! Podle mého názoru se jedná o důmyslné mučení, které často způsobuje více škody než užítku, a někdy dokonce zájemce o síť úplně odradí. Ti, kteří odolají a vytrvají, často při dalším studiu tohoto oboru minimálně pochybují o svém zdravém rozumu. Pokud to platí i o vás, můžete se uklidnit. Metoda, pomocí níž problematiku tvorby podsítí vyučuji, je poměrně snadná. Ukážu vám, že se tento náročný úkol dá zvládnout i zcela novým a mnohem jednodušším způsobem.

Jakmile si projdete tuto kapitolu (a zdůrazňuji, že nesmíte vynechat ani dodatečné studijní materiály na konci), dokážete monstrem adresování IP a tvorby podsítí zkrotit. Hlavně se nevzdávejte! Slibuji, že budete opravdu rádi, že jste vydrželi. Jakmile této problematice porozumíte, budete se divit, že vám kdysi připadala tak těžká.

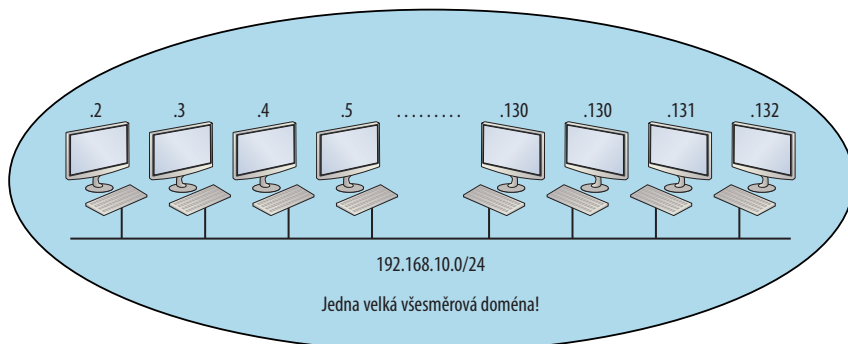


Poznámka

Nejčerstvější aktualizace této kapitoly naleznete na adrese <http://www.lammle.com/forum> nebo na stránce knihy na webu <http://www.sybex.com>.

Základy tvorby podsítí

V kapitole 3, „Úvod do protokolů TCP/IP“, jste se dozvěděli, jak definovat a najít platné rozsahy hostitelů v sítích třídy A, B a C pomocí vypnutí a následného zapnutí všech hostitelských bitů. Tato metoda je velmi dobrá, ale má jeden háček: jak je patrné na obrázku 4.1, definovali jste pouze jednu síť.

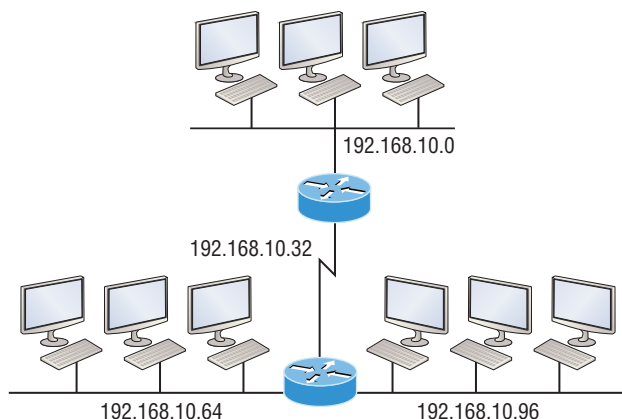


Obrázek 4.1: Jedna síť

Nyní však již víte, že jedna rozsáhlá síť není příliš výhodná (tuto mantru jsme v prvních třech kapitolách mnohokrát opakovali). Jak byste však vyřešili problém s nepraktickou sítí, který je znázorněn na obrázku 4.1? Nebylo by výhodné tuto jednu velkou síťovou adresu rozdělit a vytvořit z ní čtyři lépe zvládnutelné sítě? To si pište, že ano. Abyste to však mohli udělat, musíte použít nechvalně známý trik *tvorby podsítí* (subnetting). Jedná se totiž o nejlepší způsob, jak jednu gigantickou síť rozporcovat na několik menších. Podívejte se na obrázek 4.2, kde se dozvíte, jak to může vypadat.

Co jsou ty adresy 192.168.10.x uvedené na obrázku? To právě vysvětlíme v této kapitole! Ukážeme, jak lze z jedné sítě získat mnoho menších sítí.

Pokračujme nyní tam, kde jsme v kapitole 3 skončili. Budeme pracovat s hostitelskou sekcí (hostitelskými bity) síťové adresy, kde si můžeme půjčit bity k vytvoření podsítí.



Obrázek 4.2: Více propojených sítí

Jak vytvářet podsítě

Chcete-li vytvořit podsítě, v zásadě musíte vzít bity z hostitelské části IP adresy a rezervovat je pro definici adresy podsítě. Je jasné, že v důsledku toho bude k dispozici méně bitů k definování hostitelů, což je potřeba mít neustále na paměti.

Dále v této kapitole projdeme celý proces tvorby podsítí počínaje adresami třídy C. V případě podsítí platí obecné síťové pravidlo: Než se pustíte do vlastní implementace, měli byste určit své aktuální požadavky a nezapomenout ani na plánování budoucího rozvoje.



Poznámka

V první části kapitoly se budeme zabývat třídícím směrováním. Všichni hostitelé (všechny uzly) v síti v tomto případě pracují s přesně stejnou maskou podsítě. Až se později pustíme do masek podsítí s proměnnou délkou (VLSM), rozebereme beztrždní směrování. V tomto prostředí může každý síťový segment používat odlišnou masku podsítě.

Při tvorbě podsítí tedy začneme následujícími třemi kroky:

1. Určíte počet požadovaných síťových ID:
 - Jedno pro každou podsít LAN
 - Jedno pro každé připojení sítě WAN
2. Určíte počet požadovaných hostitelských ID v jedné podsíti:
 - Jedno pro každého hostitele TCP/IP
 - Jedno pro každé rozhraní směrovače
3. Na základě výše uvedených požadavků vytvořte:
 - Jedinečnou masku podsítě pro celou síť
 - Jedinečné ID podsítě pro každý fyzický segment
 - Rozsah hostitelských ID pro každou podsít

Masky podsítí

Aby mohlo schéma adres podsítí fungovat, musí každý počítač v síti „vědět“, které části hostitelské adresy se budou používat ve významu adresy podsítě. Tuto podmínku můžete splnit tak, že každému počítači přiřadíte *masku podsítě* (subnet mask). Masku podsítě je 32bitová hodnota, která zařízení přijímajícímu pakety IP umožňuje rozlišit v IP adrese část se síťovým ID od části s hostitelským ID. Tato 32bitová maska podsítě se skládá z jedniček a nul. Hodnoty 1 přitom reprezentují pozice, které se týkají síťových adres nebo adres podsítí.

Některé sítě se obejdou bez podsítí, a používají tedy výchozí masku podsítě. V zásadě to znamená totéž jako prohlásit, že síť nemá adresu podsítě. Tabulka 4.1 znázorňuje výchozí masky podsítí pro sítě třídy A, B a C.

| Třída | Formát | Výchozí maska podsítě |
|-------|--------------------|-----------------------|
| A | sít.uzel.uzel.uzel | 255.0.0.0 |
| B | sít.sít.uzel.uzel | 255.255.0.0 |
| C | sít.sít.sít.uzel | 255.255.255.0 |

Tabulka 4.1: Výchozí maska podsítě

Na rozhraní lze sice použít jakoukoli masku libovolným způsobem, ale obvykle není vhodné zasahovat do výchozích masek. Jinými slovy: maska podsítě třídy B by neměla mít tvar 255.0.0.0 a někteří hostitelé jej dokonce nedovolí zadat. V současnosti to však většina zařízení umožňuje. V případě sítě třídy A byste neměli měnit první bajt v masce podsítě. Měla by totiž mít minimální hodnotu 255.0.0.0. Podobně není vhodné nastavit hodnotu 255.255.255.255, protože obsahuje samé jedničky, a jedná se tedy o všesměrovou adresu. Masku adresy třídy B začíná hodnotami 255.255.0.0 a na začátku masky třídy C je uvedeno 255.255.255.0. Zejména u zkoušky CCNA není žádný důvod, abyste výchozí hodnoty měnili.



Seznámení s mocninami čísla 2

Při tvorbě podsítí IP je důležité rozumět mocninám čísla 2 a pamatovat si je. U mocnin čísla 2 platí obecné pravidlo: Vidíte-li číslo, které má vpravo nahoře uveden exponent, znamená to, že je potřeba dané číslo vynásobit sebou samým tolikrát, jak určuje příslušný exponent. Zápis 2^3 například znamená $2 \times 2 \times 2$, což se rovná 8. Následuje seznam mocnin čísla 2, který byste se měli naučit:

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8$$

$$2^4 = 16$$

$$2^5 = 32$$

$$2^6 = 64$$

$$2^7 = 128$$

$$2^8 = 256$$

$$2^9 = 512$$

$$2^{10} = 1\ 024$$

$$2^{11} = 2\ 048$$

$$2^{12} = 4\ 096$$

$$2^{13} = 8\ 192$$

$$2^{14} = 16\ 384$$

Lze sice doporučit, abyste si tyto mocniny dvojky zapamatovali, ale není to nezbytné. Stačí si pamatovat, že pracujete s mocninami čísla 2, a každá následná mocnina je proto dvojnásobkem předchozí.

Přítom postupujete takto: Chcete-li zjistit hodnotu 2^9 , vycházíte z toho, že $2^8 = 256$. Proč? Když totiž zdvojnásobíte 2 na osmou (256), dostanete 2^9 (neboli 512). Jestliže potřebujete hodnotu 2^{10} , stačí, když vyjdete od čísla $2^8 = 256$, které vynásobíte dvěma dvakrát.

Můžete také postupovat opačným směrem. Potřebujete-li získat například hodnotu 2^6 , prostě dvakrát vydělíte 256 dvěma: poprvé, abyste dostali 2^7 , a podruhé, abyste dosáhli požadovanou hodnotu 2^6 .

Beztrždní směrování mezi doménami (CIDR)

Další termín, se kterým se musíte seznámit, je *beztrždní směrování mezi doménami* (CIDR – Classless Inter-Domain Routing). Poskytovatelé služeb Internetu (ISP) v praxi pomocí této metody přidělují skupiny adres svým zákazníkům – firmám i domácnostem. Adresy přitom poskytují po blocích určité velikosti. Jedná se o přístup, který brzy podrobněji popíšeme.

Když od ISP dostanete blok adres, vypadá příslušný zápis přibližně takto: 192.168.10.32/28. Z uvedeného formátu lze poznat, jaká je maska podsítě. Notace s lomítkem (/) uvádí, kolik bitů je zapnuto (má hodnotu 1). Teoretická maximální hodnota samozřejmě dosahuje jen /32, protože bajt má 8 bitů a IP adresa sestává ze čtyř bajtů: ($4 \times 8 = 32$). Pamatujte však, že bez ohledu na třídu adres lze největší dostupnou masku podsítě, která je relevantní pro okruhy zkoušky Cisco, zapsat pouze jako /30, protože je nutné ponechat minimálně 2 bity pro hostitelské adresy.

Uvažujte například výchozí masku podsítě třídy A, která má tvar 255.0.0.0. Z toho je zřejmé, že první bajt masky podsítě se skládá ze samých jedniček (1), tj. jedná se o bitovou posloupnost 11111111. S ohledem na notaci s lomítkem je při určení masky potřeba spočítat všechny jedničkové bity. Maska 255.0.0.0 odpovídá zápisu /8, protože obsahuje 8 bitů s hodnotou 1, tj. 8 bitů, které jsou zapnuté.

Výchozí maska třídy B by měla podobu 255.255.0.0, což znamená /16, protože na hodnotu 1 je nastaveno 16 bitů: 11111111.11111111.00000000.00000000.

Tabulka 4.2 shrnuje všechny dostupné masky podsítě a odpovídající notaci CIDR s lomítkem.

| Maska podsítě | Hodnota CIDR |
|---------------|--------------|
| 255.0.0.0 | /8 |
| 255.128.0.0 | /9 |
| 255.192.0.0 | /10 |
| 255.224.0.0 | /11 |
| 255.240.0.0 | /12 |
| 255.248.0.0 | /13 |
| 255.252.0.0 | /14 |
| 255.254.0.0 | /15 |
| 255.255.0.0 | /16 |
| 255.255.128.0 | /17 |

| Maska podsítě | Hodnota CIDR |
|-----------------|--------------|
| 255.255.192.0 | /18 |
| 255.255.224.0 | /19 |
| 255.255.240.0 | /20 |
| 255.255.248.0 | /21 |
| 255.255.252.0 | /22 |
| 255.255.254.0 | /23 |
| 255.255.255.0 | /24 |
| 255.255.255.128 | /25 |
| 255.255.255.192 | /26 |
| 255.255.255.224 | /27 |
| 255.255.255.240 | /28 |
| 255.255.255.248 | /29 |
| 255.255.255.252 | /30 |

Tabulka 4.2: Hodnoty CIDR

Masky /8 až /15 lze použít pouze se síťovými adresami třídy A. Masky /16 až /23 jsou kompatibilní se síťovými adresami třídy A a B. Co se týče masek /24 až /30, uplatňují se u síťových adres tříd A, B i C. Zde leží hlavní důvod, proč většina společností volí síťové adresy třídy A. Vzhledem k tomu, že mohou použít všechny masky podsítě, získávají při návrhu sítě maximální pružnost.



Poznámka

Formát s lomítkem se při konfiguraci směrovačů Cisco nedá použít. Bylo by to příjemné, že? V každém případě je *mimořádně* důležité, abyste znali masky podsítě v notaci s lomítkem (CIDR).

Příkaz IP subnet-zero

Příkaz `IP subnet-zero` sice není nový, ale v minulosti se ve školicích materiálech Cisco ani v okruzích zkoušek neobjevoval. Měli byste však vědět, že v současnosti už společnost Cisco jeho znalost vyžaduje. Tento příkaz umožňuje použít první a poslední podsít v návrhu sítě. Masky třídy C ve tvaru 255.255.255.192 například poskytuje podsítě 64 a 128. Tímto aspektem tvorby podsítí se budeme podrobněji zabývat v další části této kapitoly. Díky příkazu `ip subnet-zero` však nyní můžete pracovat s podsítěmi 0, 64, 128 a 192. Možná to nevypadá jako velký pokrok, ale pro každou použitou masku podsítě tím získáte dvě další podsítě.

K rozhraní příkazového řádku (CLI) se sice dostaneme až v kapitole 6, „Systém Cisco IOS (Internetwork Operating System)“, ale s tímto příkazem byste se měli seznámit již nyní:

```
Router#sh running-config
Building configuration...
Current configuration : 827 bytes
```

```
!
hostname Pod1R1
!
ip subnet-zero
!
```

Z výstupu je patrné, že v tomto směrovači je příkaz `ip subnet-zero` povolen. Společnost Cisco tento příkaz standardně povoluje od verze 12.x svého systému Cisco IOS (současná verze kódu má označení 15.x).

U zkoušky Cisco si nezapomeňte velmi pečlivě přečíst, zda společnost Cisco náhodou nepožaduje, abyste příkaz `ip subnet-zero` *nepoužívali*. V některých případech se s tím můžete setkat.

Tvorba podsítí z adres třídy C

Sít je možné rozdělit na podsítě mnoha různými způsoby. Správná je ta metoda, která je optimální pro konkrétní podmínky. U adresy třídy C je pro definování hostitelů k dispozici pouze 8 bitů. Pamatujte, že bity podsítě začínají vlevo a pokračují směrem doprava, aniž by bylo možné některé bity přeskočit. Z toho vyplývá, že mohou existovat pouze následující masky podsítě třídy C:

| Binary | Decimal | CIDR |
|----------|-------------------|------|
| 00000000 | = 255.255.255.0 | /24 |
| 10000000 | = 255.255.255.128 | /25 |
| 11000000 | = 255.255.255.192 | /26 |
| 11100000 | = 255.255.255.224 | /27 |
| 11110000 | = 255.255.255.240 | /28 |
| 11111000 | = 255.255.255.248 | /29 |
| 11111100 | = 255.255.255.252 | /30 |

Masky /31 ani /32 nelze použít, protože musí zůstat alespoň 2 hostitelské bity k přiřazení IP adres hostitelům. To ale platí pouze zčásti. Masky /32 rozhodně není přípustná nikdy, protože by nezůstaly žádné hostitelské bity. Společnost Cisco však nabízí různé verze systému IOS i operačního systému nových přepínačů Cisco Nexus, které podporují masku /31. Masky /31 leží mimo okruh témat zkoušek CCENT a CCNA, takže se jí v této knize nebudeme zabývat.

V následujícím textu se naučíte mnohem méně namáhavou metodu tvorby podsítí, kterou jsem vám slíbil na začátku kapitoly. Tato metoda značně usnadňuje počítání s velkými čísly. Tomu se nedá odolat, že? Můžete mi totiž věřit, že bez schopnosti rychle a přesně počítat podsítě nemůžete uspět v síťové praxi ani u zkoušky.

Rychlá tvorba podsítí z adresy třídy C

Když jste pro svou síť vybrali možnou masku podsítě a potřebujete určit počet vzniklých podsítí a platných hostitelů a všesměrové adresy podsítě vzniklé na základě masky, stačí odpovědět na pět jednoduchých otázek:

- Kolik podsítí zvolená maska podsítě vytváří?
- Kolik platných hostitelů je k dispozici v každé podsíti?
- Jaké jsou platné podsítě?

- Jaká je všesměrová adresa každé podsítě?
- Jaké jsou platné hostitelské adresy v každé podsíti?

Přítom budete opravdu rádi, že jste se řídili mými radami a věnovali jste čas tomu, abyste si zapamatovali mocniny dvojky. Pokud jste to zatím neudělali, nyní je vhodná doba... Potřebujete-li nápovědu, vraťte se k rámečku „Seznámení s mocninami čísla 2“ v předchozí části této kapitoly. Uvedme si postup, jak najít odpovědi na těchto pět zásadních otázek:

- *Kolik je podsítí?* 2^x = počet podsítí. x je počet maskovaných bitů neboli jedniček. Například v čísle 11000000 udává počet jedničkových bitů 2^2 podsítí. V tomto případě jsou tedy k dispozici 4 podsítě.
- *Kolik je hostitelů v každé podsíti?* $2^y - 2$ = počet hostitelů na jednu podsít. y znamená počet nemaskovaných bitů neboli nul. Například z nul v čísle 11000000 lze spočítat $2^6 - 2$ hostitelů neboli 62 hostitelů v podsíti. Při výpočtu musíte odečíst hodnotu 2 kvůli adrese podsítě a všesměrové adrese, které nepatří mezi platné hostitelské adresy.
- *Jaké jsou platné podsítě?* $256 - \text{maska podsítě} = \text{velikost bloku neboli číslo inkrementu}$. Jako příklad lze uvést masku 255.255.255.192, kde je nutné se zaměřit na čtvrtý oktet (oktet je zajímavý tím, že obsahuje čísla podsítí). Stačí vypočítat rovnici: $256 - 192 = 64$. Bloky masky 192 mají vždy velikost 64. Začněte počítat od nuly v blocích velikosti 64, dokud nedosáhnete hodnoty masky podsítě. Ve čtvrtém oktetu dostáváte podsítě: 0, 64, 128, 192. Nic na tom není, že?
- *Jaká je všesměrová adresa každé podsítě?* Odpověď na tuto otázku je opravdu snadná. V předchozím bodě jsme spočítali, že podsítě mají čísla 0, 64, 128 a 192. Všesměrová adresa je vždy určena číslem, které předchází následující podsít. Podsít 0 má například všesměrovou adresu 63, protože číslo 64 udává další podsít. Podsít 64 má všesměrovou adresu 127, protože pod číslem 128 se skrývá další podsít, atd. Nezapomínejte, že všesměrová adresa poslední podsítě má vždy hodnotu 255.
- *Jaké jsou platné hostitelské adresy?* Platné hostitelské adresy jsou dány čísla mezi podsítěmi. Přítom je nutné vynechat sekvenci samých nul a samých jedniček. Pokud má například podsít číslo 64 a všesměrová adresa se rovná 127, pak platné hostitelské adresy leží v rozsahu 65–126. Platný rozsah *vždy* odpovídá skupině čísel mezi adresou podsítě a všesměrovou adresou.

Pokud to zatím nechápete, neznepokojujte se. Ve skutečnosti to není tak těžké, jak se na první pohled zdá – hlavně vydržte! Chcete-li rozptýlit případné nejasnosti, vyzkoušejte několik následujících praktických příkladů.

Praktické příklady tvorby podsítí: Adresy třídy C

Nyní máte příležitost vyzkoušet si tvorbu podsítí z adres třídy C pomocí právě popsané metody. Je to opravdu efektivní. Začneme první maskou podsítě třídy C a postupně projdeme všechny podsítě, které lze u adres třídy C použít. Jakmile budeme hotovi, ukážeme si, jak snadno lze obdobný postup aplikovat i na adresy třídy A a B.

Praktické cvičení č. 1C: 255.255.255.128 (/25)

Vzhledem k tomu, že 128 lze binárně zapsat jako 10000000, je k dispozici pouze 1 bit pro tvorbu podsítí a 7 bitů pro hostitele. Nyní rozdělíme na podsítě síťovou adresu třídy C 192.168.10.0.

192.168.10.0 = síťová adresa

255.255.255.128 = maska podsítě

Odpovězme si na svých pět základních otázek:

- *Kolik je podsítí?* Číslo 128 má zapnutý 1 bit (10000000), takže odpověď bude $2^1 = 2$.
- *Kolik je hostitelů v každé podsíti?* Vypnuto je 7 hostitelských bitů (10000000). Dostaneme tedy rovnici $2^7 - 2 = 126$ hostitelů. Jakmile zjistíme velikost bloku dané masky, počet hostitelů se vždy rovná velikosti bloku minus 2. Můžeme si ušetřit zbytečné počítání.
- *Jaké jsou platné podsítě?* $256 - 128 = 128$. Pamatujte, že začínáme od nuly a přičítáme velikosti bloku, takže získáme podsítě 0 a 128. Když budete pouze hledat podsítě postupným přičítáním velikosti bloku, nemusíte vůbec provádět kroky 1 a 2. Je zřejmé, že existují dvě podsítě. V předchozím kroku stačí připomenout, že počet hostitelů vždy odpovídá velikosti bloku zmenšené o 2. V tomto případě tedy dostáváme 2 podsítě, z nichž každá obsahuje 126 hostitelů.
- *Jaká je všesměrová adresa každé podsítě?* Číslo těsně předcházející hodnotě další podsítě má zapnuty všechny hostitelské bity a rovná se všesměrové adrese. Po nulové podsíti následuje podsít 128, všesměrová adresa podsítě 0 má tedy hodnotu 127.
- *Jaké jsou platné hostitelské adresy?* Jedná se o čísla mezi adresou podsítě a všesměrovou adresou. Chcete-li najít hostitele, je nejjednodušší napsat adresu podsítě a všesměrovou adresu. Platné hostitelské adresy jsou pak zcela zřejmé. Následující tabulka obsahuje podsítě 0 a 128, platné rozsahy hostitelských adres v každé podsíti a všesměrovou adresu každé z nich:

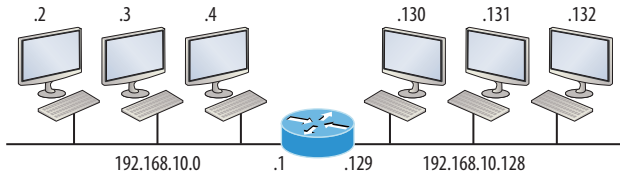
| Podsít | 0 | 128 |
|----------------------------|------------|------------|
| První hostitel | 1 | 129 |
| Poslední hostitel | 126 | 254 |
| Všesměrové vysílání | 127 | 255 |

Z pohledu na masku /25 třídy C je zcela zřejmé, že tvoří dvě podsítě. Proč je to však důležité? Ve skutečnosti to důležité není, ale otázka není správně položena. Místo toho byste se měli ptát, jak s touto informací naložit!

Tato tematika sice nepatří mezi nejzábavnější, ale je skutečně zásadní, takže se snažte udržet pozornost. I nadále budeme pokračovat ve výkladu tvorby podsítí. Klíčem k pochopení tvorby podsítí je porozumět hlavnímu důvodu, proč podsítě vznikají. Předvedeme si to na procesu budování fyzické sítě.

Přidali jsme směrovač znázorněný na obrázku 4.3. Aby tedy mohli hostitelé v naší datové síti komunikovat, potřebují logické schéma síťového adresování. Mohli bychom použít protokol

IPv6, ale prozatím je stále rozšířenější protokol IPv4. Právě tento protokol momentálně probíráme. Budeme se jej tedy držet.



```
Router#show ip route
[výstup je zkrácen]
C 192.168.10.0 is directly connected to Ethernet 0
C 192.168.10.128 is directly connected to Ethernet 1
```

Obrázek 4.3: Implementace logické sítě třídy C s maskou /25

Schéma na obrázku 4.3 zahrnuje dvě fyzické sítě, takže implementujeme logické schéma adresování, které bude zahrnovat dvě logické sítě. Jako vždy je rozumné dívat se dopředu a zvažovat pravděpodobné růstové scénáře – jak krátkodobé, tak dlouhodobé. V tomto případě však vystačíme s maskou /25.

Na obrázku 4.3 je zřejmé, že obě podsítě byly přiřazeny k rozhraní směrovače, který vytváří všesměrové domény a adresuje podsítě. Směrovací tabulku směrovače lze zobrazit příkazem `show ip route`. Všimněte si, že místo jedné velké všesměrové domény nyní existují dvě menší všesměrové domény, přičemž každá z nich může obsahovat až 126 hostitelů. Písmeno `C` ve výstupu směrovače znamená „přímo připojená síť“ (directly connected network). Výstup informuje o tom, že jste vytvořili a implementovali dvě takové sítě se dvěma všesměrovými doménami. Zasloužíte si proto gratulaci. Úspěšně jste rozdělili síť na podsítě podle návrhu sítě. Zkuste to tedy ještě jednou.

Praktické cvičení č. 2C: 255.255.255.192 (/26)

Tentokrát rozdělíme na podsítě síťovou adresu 192.168.10.0 pomocí masky podsítě 255.255.255.192.

192.168.10.0 = síťová adresa

255.255.255.192 = maska podsítě

Odpovězme si na pět základních otázek:

- *Kolik je podsítí?* Číslo 192 má zapnuté 2 bity (11000000), takže odpověď bude $2^2 = 4$ podsítí.
- *Kolik je hostitelů v každé podsíti?* Vypnuto je 6 hostitelských bitů (11000000). Získáváme tedy $2^6 - 2 = 62$ hostitelů. Počet hostitelů vždy odpovídá velikosti bloku minus 2.
- *Jaké jsou platné podsítě?* $256 - 192 = 64$. Pamatujte, že začínáme od nuly a přičítáme velikosti bloku. To znamená, že podsítě budou označeny čísly 0, 64, 128 a 192. Je zřejmé, že bloky mají velikost 64. Existují tedy 4 podsítě, každá po 62 hostitelích.