Kapitola 33

Navrhování sítí

Existují stovky knih, ve kterých se dozvíte, jak vytvořit tříúrovňovou firemní síť. Tahle kniha však mezi ně nepatří. Spíše vám ukáži, co musíte udělat předtím, než začnete vytvářet vaši síť. Potom vám ukáži některé praktické příklady návrhů sítí.

Nebudou to tedy žádné technické informace, které získáte tím, že se necháte certifikovat. Tyto informace vám pomohou v tom, abyste lépe dělali vaši práci. Tato kapitola je psána převážně s vědomím toho, že budete navrhovat síť zcela od začátku. Přestože se nejedná o častý případ, informace zde uvedené jsou použitelné pro libovolný návrh sítě.

Dokumentace

Dokumentace je prokletím mnoha inženýrů. Nejsem si zcela jist, proč je tomu tak, ale zdá se, že inženýr, který rád píše dokumentaci, je spíše raritou. Psaní je těžká práce (jen si zkuste napsat nějakou knihu!), ovšem výhody jsou značné.

Zdá se, že někteří inženýři věří tomu, že když nashromáždí spousty informací, budou nenahraditelní. V tomhle mi můžete věřit – vy i já jsme nahraditelní. Vlastně jsem si vydělával na živobytí tím, že jsem dokumentoval sítě po propuštění „nenahraditelných" specialistů.

Dobře napsaná dokumentace šetří čas a peníze. Pokud někdo může opravit vaši síť díky tomu, že si přečte vaši dokumentaci, odvedli jste dobrou práci. Pokud vaši síť nemůže opravit nikdo, kromě vás, pak neděláte svoji práci dobře.

Kdykoliv je to možné, dokonce i u malých sítí, byste měli dokumentovat každý detail vaší sítě. To, že jde o malou síť, u které si dokážete zapamatovat všechny IP adresy, ještě neznamená, že by neměla být zdokumentována.

Seznamy požadavků

Jednou z věcí, kterou byste měli provést na začátku každého projektu bez ohledu na to, kolik na něj máte času, je napsat si *seznam požadavků*. Tento dokument by měl obsahovat všechny požadavky na projekt, kterým budete rozumět, stejně jako všechny možné předpoklady pro realizaci projektu. Dokonce i když je požadavkem prostý „návrh nové firemní sítě", zapište si jej a uveďte všechny podmínky pro jeho úspěšnou realizaci.

Po vytvoření vašeho seznamu požadavků jej odešlete všem, kteří jsou do tohoto projektu zapojeni. Mezi adresáty by měl patřit přinejmenším váš šéf. V závislosti na firemní kultuře možná budete chtít tento seznam požadavků adresovat také projektovým manažerům, osobě, která je zodpovědná za financování projektu (sponzor), a všem ostatním osobám zapojeným do jeho realizace. Váš šéf může chtít tento dokument předat dalším stranám, místo abyste jej odeslali přímo vy. Tak či onak, je třeba zveřejnit nějaký dokument, z nějž bude zřejmé, co budete navrhovat a proč.

Psaní seznamu požadavků je jednou z nejdůležitějších věcí, kterou můžete udělat pro to, abyste sami sebe ochránili pro případ, že se rozsah projektu změní.

A ke změně rozsahu projektu jistě dojde. Nepamatuji se na jediný projekt, na kterém jsem pracoval, kdy by se tak nestalo. Změna rozsahu projektů je zkrátka běžnou skutečností.

Například pokud si objednáte linku T1 pro internetovou konektivitu a váš nadřízený vás zklame, protože si nemyslí, že tato linka představuje dostatečnou šířku pásma, měli byste být schopni odkázat se na seznam požadavků, který jste zveřejnili na začátku projektu (a který – doufejme – podpoří vaše rozhodnutí). Díky tomu můžete být klidní, neboť jste odeslali dokument popisující požadavky odpovídající vašemu návrhu. Pokud váš nadřízený o lince T1 nevěděl, pak daný dokument nečetl.

Seznam požadavků nemusí být nijak dlouhý či komplikovaný – vlastně čím jednodušší tento dokument bude, tím je větší šance, že mu lidé porozumí. Všechny body by měly být co možná nejjednodušší (zejména předpoklady). Takhle by mohl seznam požadavků vypadat:

Požadavky:

- Síť musí podporovat 300 uživatelů.

Předpoklady:

- Každý uživatel bude mít jednu pracovní stanici.
- Každá pracovní stanice bude mít pouze jedno ethernetové rozhraní.
- Všechna rozhraní budou podporovat připojení kabelem 1Gb/s Ethernetu.
- Síť nemusí podporovat 1 Gb/s pro všechny uživatele současně.
- Každý uživatel bude mít jeden telefon s podporou jedné telefonní linky.
- Žádné telefony nebudou IP telefony.
- Na síti nebude v brzké budoucnosti provozován VoIP.
- Jeden uživatel bude odpovídat jedné kanceláři.
- Každá kancelář bude obsahovat dva datové konektory a jeden telefonní konektor.
- Veškerá kabeláž bude končit v serverovně.

Pokud váš nadřízený řekne: „Potřebujeme síť, která podporuje 300 uživatelů“, ne vždy chápe souvislosti tohoto prostého sdělení. Vaším úkolem je jednak ujistit se, že ostatní zainteresované osoby mají všechny informace, které potřebují k pochopení toho, co se děje, a jednak si musíte krýt vaše vlastní záda, pokud by někdo nepochopil, co děláte. Pokud zveřejníte všechny vaše předpoklady, váš nadřízený by měl být schopen přečíst si váš dokument a vznést dotazy, které by mohl mít. Třeba ve firmě existuje plán převést v příštím roce telefonní systém na VoIP a vy musíte být s touto skutečností obeznámeni, abyste mohli objednat zařízení, které bude tuto vizi podporovat.

Už jsem se setkal s mnoha projekty, které selhaly proto, že neexistoval žádný seznam požadavků. Také jsem dokazoval (a obhajoval) mnoho pádných argumentů ohledně toho, co bylo řečeno před mnoha měsíci, ale nebylo zapsáno.

Jen na základě toho, že lidé řeknou, že něčemu rozumí, ještě nepředpokládejte, že to udělají, zejména pokud to nejsou „technické“ typy. Jednou jsem pro jistou společnost navrhl důkladný záložní mechanismus internetového připojení. Po instalaci linek DS3 (po 60 denní realizaci) na mě začal zodpovědný manažer, který podepsal objednávku, křičet, protože nechápal, k čemu jsme linky potřebovali. Nikdy jsem si nebyl vědom toho, že návrh nepochopil. Měl jsem za to, že jsme měli

v návrhu jasno, ale jelikož jsem nenapsal seznam požadavků, neexistoval jediný papír, který by to dokazoval.

Tabulky rozvržení portů

První krok, který podnikám při návrhu jakékoliv sítě, je vytvoření seznamu všech zařízení, která budou mít přístup k síti. V případě lokální sítě je třeba zvážit následující okolnosti:

- Kolik uživatelů bude muset síť podporovat?
- Kolik serveru bude muset síť podporovat?
- Kolik tiskáren bude k síti připojeno a kde budou umístěny?
- Jaké budou aplikace běžící po síti? Kolik uživatelů bude s těmito aplikacemi pracovat (HTTP, klientský software, terminály, Citrix)?
- Jaký typ zabezpečení potřebujete?
- Je vyžadována vysoká dostupnost a/nebo cenově přijatelná?
- Jaký procentuální růst se předpokládá?
- Musí být všechna rozhraní gigabitová?
- Bude muset síť podporovat VoIP?
- Budete podporovat jedno fyzické umístění nebo více fyzických umístění (včetně více podlaží v jedné budově)?

Vaším cílem je vytvořit konečný počet všech typů rozhraní pro všechna umístění. Jakmile budete tato čísla znát, můžete se rozhodnout, jaký druh zařízení je třeba objednat. Gigabitové ethernetové přepínače se při nejvyšší hustě portů v dnešních dnech dodávají v násobcích 48. Abyste zjistili, kolik 48portových přepínačů nebo modulů potřebujete, podělte celkový počet požadovaných gigabitových rozhraní číslem 48. Například pokud potřebujete 340 gigabitových rozhraní v jednom umístění, budete potřebovat 340 / 48 = 7,08 modulů (jinými slovy osm modulů).

Při určení počtu portů, které budete potřebovat, nezapomeňte na servery, které nabízí vysokou dostupnost. Mnoho dnešních serverů podporuje propojení více ethernetových rozhraní s jedním nebo dvěma přepínači ve failover páru (tedy v páru s podporou převzetí služeb při selhání spojení). Promluvte si s vašimi systémovými specialisty a zjistěte, co dělají, abyste měli potřebnou představu.

Rovněž byste měli počítat s určitým růstem. Dobrým hrubým odhadem při plánování kapacity je počítat minimálně s 15procentním růstem: 340 × 0,15 = 51. Toto číslo přidejte k počtu aktuálně potřebných rozhraní a poté toto číslo podělte číslem 48, abyste zjistili, kolik modulů budete potřebovat, pokud chcete umožnit růst: 340 + 51 = 411, a 411 / 48 = 8,56. To znamená, že budete potřebovat devět modulů, které poskytnou celkem 432 portů. Devět je liché číslo, což znamená, že jeden přepínač bude obsahovat více modulů než druhý. To ve vašem prostředí může, nebo nemusí vadit, nicméně já osobně mám rád, když všechny strany vypadají stejně. Vždycky je lepší mít příliš mnoho portů než příliš málo portů, tedy pokud to rozpočet umožní. Zaokrouhlením modulů na 5 na každém šasi dostaneme 10 modulů, tedy celkem 480 portů.

Teď máte k dispozici 480 portů a současný požadavek je 340 portů. To umožňuje nárůst o téměř 30 procent. Je možné, že jste na něco zapomněli (tedy alespoň já vždycky na něco zapomenu), takže budete-li mít více prostoru než na 15procentní růst, nebude to na škodu. V případech, jako je tenhle, nezapomenu rezervovat další porty pro případ rozšíření. Ty se budou později vždy hodit.

Další požadavek, na který inženýři často zapomínají, je potřeba trunků mezi přepínači. Přepínače ve failover párech musí být vzájemně propojeny, obvykle vícegigabitovými linkami. Pokud používáte moduly FSM (Firewall Services Modules), měly by pro ně existovat vyhrazené trunky. Moduly CSM (Content Service Modules) by rovněž měly mít své vlastní trunky, stejně jako analyzátor RSPAN, pokud jej budete používat. Pokud budeme počítat s 2Gb/s EtherChannelem pro každý z těchto trunků, právě jste alokovali 16 portů (8 na každé straně).

Pracoval jsem na sítích s velkou šířkou pásma, v nichž každý z těchto trunků vyžadoval 4Gb/s EtherChannely. Návrh, jako je tenhle, by vyžadoval 32 portů (16 na každé straně). To je téměř celý 48portový modul jen pro komunikaci mezi přepínači!

Jakmile zjistíte, kolik portů budete potřebovat, naplánujte zařízení, která budete potřebovat, a zjistěte, jaké funkce budou daná zařízení plnit. Zde jsem se rozhodl, že přepínače 6509 budou použity jako hlavní přepínače a směrovače 2811 budou použity pro internetovou a záložní konektivitu k firemnímu webovému serveru, který se nachází v kolokačním (někdy též hostingovém) centru. Obrázek 33.1 znázorňuje mou tabulku s těmito informacemi.

					Rozhraní			
Název	**Zařízení**	**Funkce**	**Umístění**	**Sloty**	**T1**	**DS3**	**1G**	**10G**
Core-1	6509-E	Hlavní přepínač/směrovač	Rack č. 2	9	0	0	240	0
Core-2	6509-E	Hlavní přepínač/směrovač	Rack č. 3	9	0	0	240	0
Internet	2811	Internetový směrovač	Rack č. 2	1	2	0	2	0
HQ-Colo	2811	Směrovač kolokačního centra	Rack č. 3	1	2	0	2	0

***Obrázek 33.1**: Vzorový seznam zařízení.*

Když teď víte, jaká zařízení budete používat, měli byste každé zařízení určit, abyste přesně věděli, jaký hardware se má objednat. Tento krok vám nesmírně usnadní celý proces návrhu a vytváření sítě. Jakmile budete mít zařízení, můžete rozšířit tabulku o doplnění skutečných sériových čísel jednotlivých součástí. Obrázek 33.2 znázorňuje příklad tabulky pro plánování jednoho z přepínačů 6509, který jsem vybral. Všimněte si, že jsem neuvedl pouze moduly, ale i dodatečnou paměť.

Jakmile budete mít představu o hardwaru, objednání zařízení často spočívá na vedení firmy. Zřejmě budete muset s objednávkou pomoci dodáním seznamu čísel součástí a počtů. Po odeslání objednávky možná budete muset pár týdnů počkat, než zboží dorazí.

Nyní musíte rozplánovat každé rozhraní na každém zařízení. Někomu se to může zdát zbytečné, ale plánování toho, kde bude každé zařízení připojeno, vám později ušetří spoustu nervů. Pokud budete mít plán jako je tenhle, můžete přenechat práci s připojováním zařízení někomu jinému. Tento krok představuje práci na konečné podobě dokumentace, než bude zařízení dodáno.

Pro každé zařízení jsem vytvořil tabulku a někdy i pro každý modul v daném zařízení. Nemusí jít o žádný elaborát. Stačí jednoduchý seznam portů, připojených zařízení a třeba IP adresy či sítě VLAN, které je třeba nakonfigurovat (příklad takového seznamu můžete vidět na obrázku 33.3).

				Rozhraní		
Název	**Zařízení**	**Funkce**	**Sloty**	**10/100/1G**	**GBIC**	**SF-GBIC**
Core-1	**WS-C6509-E**	Hlavní přepínač/směrovač	**9**	**240**	**0**	**4**
Slot 1	WS-X6748-GE-TX	48portový 10/100/1000 FE Blade		48		
Slot 2	WS-X6748-GE-TX	48portový 10/100/1000 FE Blade		48		
Slot 3	WS-X6748-GE-TX	48portový 10/100/1000 FE Blade		48		
Slot 4	WS-X6748-GE-TX	48portový 10/100/1000 FE Blade		48		
Slot 5	WS-SUP720-3B=	Supervisor - 720 Fabric Enabled				2
Slot 6	WS-SUP720-3B=	Supervisor - 720 Fabric Enabled				2
Slot 7	WS-SV C-FWM-1-K9=	Modul FSM (Firewall Switch Module)				
Slot 8						
Slot 9	WS-X6748-GE-TX	48portový 10/100/1000 FE Blade		48		
MSFC Mem	MEM-MSFC2-512MB	Karta MSFC – 512M DRAM				
Sup Mem	MEM-S2-512MB	Modul Sup – 512M DRAM				
Flash Mem	MEM-C6K-CPTFL256M	256M Compact Flash Upgrade				
Ventilátor	WS-C6509-E-FAN	Ventilátoru				
PS č. 1	WS-CAC-3000W-US	3 000W zdroj napájení				
PS č. 2	WS-CAC-3000W-US/2	3 000W zdroj napájení				

Obrázek 33.2: *Podrobnosti k hardwaru hlavního přepínače.*

Fyzický port	VLAN/Trunk/IP	Zařízení	Vzdálené rozhraní
1/1	VLAN 10	Internetový směrovač	F0/0
1/2		Vyhrazeno	
1/3			
1/4			
1/5	VLAN 777	Failover linka 1 modulu FWSM přepínače Core-2	G1/5
1/6	VLAN 777	Failover linka 2 modulu FWSM přepínače Core-2	G1/6

Obrázek 33.3: *Příklad tabulky přiřazení portů.*

Pokud jste naplánovali vaši síť až do této úrovně, jakmile bude zařízení dodáno, zbývá jen je nainstalovat do skříní či stojanu (rack) a propojit zařízení kabelem podle tohoto plánu.

Tabulky IP adres a sítí VLAN

Společně s fyzickým plánováním zařízení a alokací portů je třeba naplánovat rozvržení sítě s protokolem IP a virtuální sítě VLAN. Rád vytvářím poměrně podrobné tabulky s těmito informacemi, stejně jako v případě fyzických zařízení, modulů a portů.

Na obrázku 33.4 jsem rozvrhl své sítě s protokolem IP. Síť s prefixem /23 alokuji pro každou síť VLAN a rovněž rezervuji síť s prefixem /23 nad každou alokací pro budoucí rozšíření.

Pro každou síť s protokolem IP, kterou budu používat, vytvářím tabulku a naplním ji konkrétními informacemi o všech zařízeních v dané síti. Tohle je vynikající cvičení, které vás donutí znovu přemýšlet o každém zařízení, které bude připojeno.

Obrázek 33.5 znázorňuje vzorovou tabulku rozvržení IP adres.

Síť	Maska	VLAN	Popis
10.1.0.0			
10.1.1.0			
10.1.2.0			
10.1.3.0			
10.1.4.0			
10.1.5.0			
10.1.6.0			
10.1.7.0			
10.1.8.0	255.255.254.0	VLAN 10	Internetová demilitarizovaná zóna
10.1.9.0			
10.1.10.0			*vyhrazeno pro rozšíření*
10.1.11.0			*vyhrazeno pro rozšíření*
10.1.12.0	255.255.254.0	VLAN 100	VLAN 100
10.1.13.0			
10.1.14.0			*vyhrazeno pro rozšíření*
10.1.15.0			*vyhrazeno pro rozšíření*

Obrázek 33.4: *Tabulka rozvržení sítě s protokolem IP.*

IP adresa	Maska podsítě	VLAN	Popis
10.1.32.0			Sítě v centrále
10.1.32.1	255.255.254.0	VLAN 130	Výchozí brána (HSRP VIP)
10.1.32.2	255.255.254.0	VLAN 130	Core-1 VLAN 130 IP
10.1.32.3	255.255.254.0	VLAN 130	Core-2 VLAN 130 IP
10.1.32.4	255.255.254.0	VLAN 130	*Vyhrazeno*
10.1.32.5	255.255.254.0	VLAN 130	*Vyhrazeno*
10.1.32.6	255.255.254.0	VLAN 130	*Vyhrazeno*
10.1.32.7	255.255.254.0	VLAN 130	*Vyhrazeno*
10.1.32.8	255.255.254.0	VLAN 130	Barevná tiskárna v Karlově kanceláři
10.1.32.9	255.255.254.0	VLAN 130	Barevná tiskárna v Luciině kanceláři
10.1.32.10	255.255.254.0	VLAN 130	Barevná kopírka č. 1
10.1.32.11	255.255.254.0	VLAN 130	Barevná kopírka č. 2

Obrázek 33.5: *Tabulka rozvržení IP adres.*

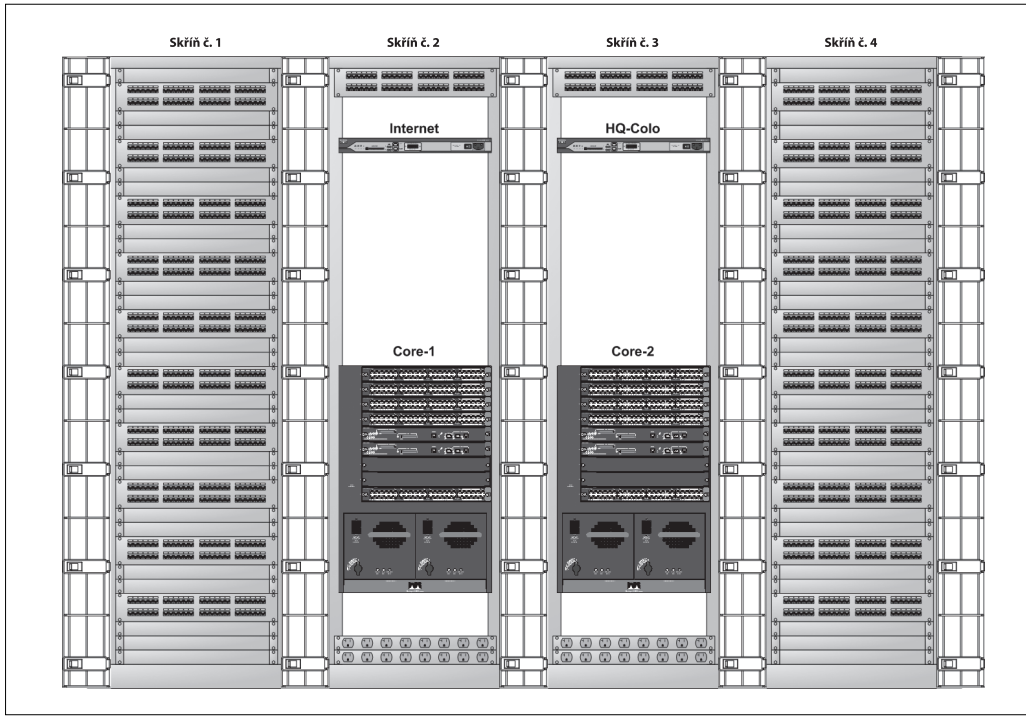
Jakmile budete mít všechny tyto informace zdokumentovány, vytvoření konfigurací by mělo být otázkou lusknutí prsty. A jako bonus navíc, tabulky jsou vynikajícími dokumenty pro danou síť. Mohou být vytištěny a založeny do pořadače nebo je lze někde jednoduše uložit, kde k nim bude snadný přístup.

Po vytvoření sítě doporučuji vytisknout kopii veškeré vámi vytvořené dokumentace. Pokud se cokoliv změní, budete mít zdokumentovaný důkaz stavu sítě v době její implementace.

Projekt rozmístění modulů ve stojanech

Pokud se setkáte s pojmem *projekt rozmístění modulů ve stojanech* (v angl. „bay face layouts“) pak vězte, že jde o diagramy, znázorňující osazení jednotlivých skříní, stojanů (rack) moduly, včetně všech detailů. Pro mě je největší výhodou projektů rozmístění modulů ve stojanech to, že jakmile je jednou vytvořím, můžu instalaci zařízení přenechat někomu jinému, je-li to možné: mohou vybalit

všechny krabice, zkopírovat projekty rozmístění modulů ve stojanech a říci: „Udělejte to podle tohoto projektu." Příklad projektu rozmístění modulů ve stojanech je znázorněn na obrázku 33.6.



Obrázek 33.6: *Projekt rozmístění modulů ve stojanech.*

Existují tři věci, na které inženýři při navrhování nebo plánování osazení skříně zapomenou: napájení, kabely a patch panely. Všechny tyto položky zabírají ve vašich skříních místo.

Špatné požadavky na místo ve skříni mohou být drahou chybou, zejména pokud si pronajímáte kolokační prostor. Projekty rozmístění modulů ve stojanech jsou vynikající kontrolní pojistkou, která zajistí, že budete mít dostatek skříní pro osazení všech zakoupených zařízení.

Požadavky na napájení a chlazení

A teď nastal vhodný okamžik na výpočet požadavků na napájení. Většina prodejců uvádí spotřebu energie dodávaných zařízení na svých webových stránkách. Jednoduše zjistěte, jaký druh napájení dané zařízení vyžaduje (AC/DC, napětí a proud) a jaké jsou potřebné konektory a sečtěte požadavky na každou skříň či stojan (rack). Promluvte si se všemi osobami zodpovědnými za prostředí, v němž budou vaše skříně nebo stojany (rack) umístěny, a ujistěte se, že jsou schopni napájet zařízení, která umístíte do vašich skříní či stojanů (rack).

To, že můžete do skříně nebo stojanu (rack) osadit 40 serverů velikosti 1U, ještě neznamená, že jste schopni zajistit jejich napájení! Výchozím napájením střídavým proudem, instalovaným ve skříni nebo stojanu (rack) v kolokačním centru, jsou často dva 20A AC napájecí moduly. Pokud každý váš server o velikosti 1U spotřebuje 2 A a máte dva zdroje napájení, můžete nainstalovat pouze 10 takových serverů v každé skříni (rack). Pokud chcete přidat další, budete si muset objednat další zdroj napájení.

Nezapomeňte ani na požadavky na chlazení. Společně se specifikací napájení prodejci pro svá zařízení uvádí také hodnoty BTU (British Thermal Unit). Osoba zodpovědná za prostředí, v němž bude dané zařízení nainstalováno, bude rovněž potřebovat znát tyto informace. Třebaže fyzicky můžete nainstalovat dva přepínače 6509s do jedné skříně, nemusí být k dispozici požadované klimatizační systémy, které by byly schopny je ochladit.

Energetické a tepelné hodnoty pro přepínače řady 6500 najdete vyhledáním fráze „6500 power and heat numbers" na webových stránkách společnosti Cisco. Jelikož spotřeba energie a tepelný výkon se různí v závislosti na nainstalovaných modulech, musíte tuto informaci vypočítat pro každou instalaci. Čísla pro přepínač 6509, které jsem specifikoval dříve, jsou uvedena na obrázku 33.7. Podobná tabulka by měla být vytvořena pro každé instalované zařízení.

Zařízení	Slot	Modul	Číslo dílu	Watty	BTU
Core-1 6509E	**Slot 1**	48portový 10/100/1000	WS-X6748-GE-TX	367,50	1 255,01
	Slot 2	48portový 10/100/1000	WS-X6748-GE-TX	367,50	1 255,01
	Slot 3	48portový 10/100/1000	WS-X6748-GE-TX	367,50	1 255,01
	Slot 4	48portový 10/100/1000	WS-X6748-GE-TX	367,50	1 255,01
	Slot 5	Sup-720	WS-SUP720-3B	350,80	1 204,81
	Slot 6	Sup-720	WS-SUP720-3B	350,80	1 204,81
	Slot 7	FWSM	WS-SVC-FWM-1-K9	214,73	733,29
	Slot 8				
	Slot 9	48portový 10/100/1000	WS-X6748-GE-TX	367,50	1 255,01
	Ventilátor	48portový 10/100/1000	WS-C6509-E-FAN	188,00	642,00
		Celkem		**2941,83**	**10 059,96**

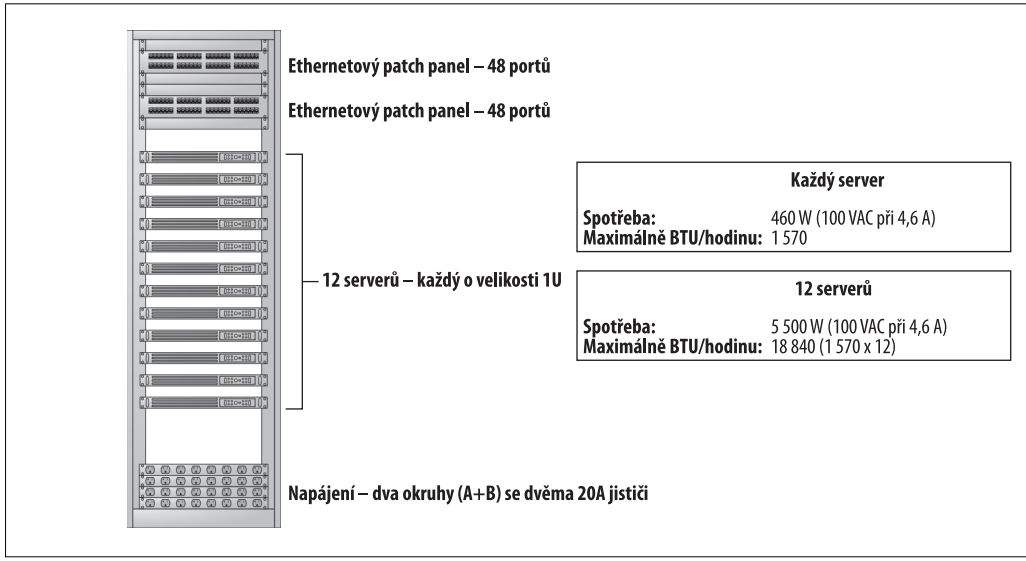
Napájení předpokládá zdroje střídavého proudu

Obrázek 33.7: *Hodnoty napájení a BTU pro přepínač 6509E.*

Nezapomeňte na omezení týkající se počtu zařízení, která mohou být do skříně umístěna. Jako příklad uvedu skříň plnou serverů o velikosti 1U, kterou jsem vytvořil. Specifikace a rozvržení skříně jsou znázorněny na obrázku 33.8. Předpokládejme, že v kolokačním centru, v němž je tato skříň umístěna, platí omezení 20 000 BTU na jednu skříň. Střídavé napájení na jednu skříň je omezeno na dva okruhy s 20A jističem, přičemž každý obsahuje osm zásuvek.

Prozkoumáte-li nejprve servery o velikosti 1U, může se zdát, že jsou velmi efektní, neboť teoreticky jich můžete do jedné skříně (rack) umístit 30 nebo 40. Ovšem v praxi to obvykle možné není. V mém příkladě každý server produkuje maximálně 1 570 BTU za hodinu. (Při plánování byste měli vždy vycházet z maximálních hodnot.) Prostými počty zjistíme, že 12 serverů potenciálně vyprodukuje 18 840 BTU/hodinu. Takže jen na základě samotného tepelného výkonu nemůžeme do jedné skříně umístit více než 12 těchto serverů.

Zaměříme-li se na napájení, omezení budou ještě patrnější. Jelikož každý server spotřebuje 460 wattů (100 V-AC při 4,6 A), měli bychom ke každému napájecímu rozvaděči (tzv. PDU, z angl. Power Distribution Unit) připojit pouze čtyři nebo pět serverů (nikoliv šest). Omezení napájení snadno zjistíte pomocí proudových hodnot. Pokud každý napájecí rozvaděč podporuje pouze 20 A a každý server potřebuje 4,6 A, ke každému napájecímu rozvaděči můžete připojit pouze 4,34 serverů. Podívejte se však pozorněji – specifika uvádí, že server spotřebovává 460 wattů pouze při použití 100 V-AC zdroje. V USA je napětí v elektrické síti 120 V-AC, nikoliv 100 V-AC, takže tato



Obrázek 33.8: *Výpočet počtu serverů, které se vejdou do skříně.*

čísla se trochu změní. Co se stane, změníme-li napětí a watty zůstanou stejné? Pokud W = A × V, pak A =W / V. Takže 460 W dělených 120 V = 3,83 A. Pět serverů, z nichž každý má odběr 3,83 A, dává celkem 19,15 A.

Samozřejmě předpokládáme plné zatížení elektrických obvodů. Mnoho kolokačních center vám neumožní zatížit vaše obvody nad stanovenou hranici (typicky 70 procent). Pokud můžeme zatížit naše obvody pouze na 70 procent, můžeme ke každému napájecímu rozvaděči připojit pouze tři nebo možná čtyři servery. Tudíž i když máme pouze 12 serverů, pokud je každý napájecí rozvaděč schopen snést zátěž 20 A, budeme potřebovat čtyři napájecí rozvaděče.

Jelikož do jedné skříně můžeme umístit pouze 12 serverů (za předpokladu čtyř napájecích rozvaděčů), má smysl mezi nimi ponechat volný prostor. Práce se servery o velikosti 1U může být obtížná, kvůli všem kabelům, které mohou být k těmto serverům připojeny. Jak uvidíte, šest ethernetových rozhraní v každém serveru není nic neobvyklého. Nezapomeňte, že každý server bude obsahovat také konzolové kabely, napájecí kabely a montážní a vázací dráty pro usměrnění celé té změti kabelů. Navíc pokud necháte ve skříni prázdný velký prostor, vedení firmy se bude domnívat, že jej zaplníte, než vám povolí objednat další skříně.

Tipy pro síťové diagramy

Zdá se, že inženýři vytváří své dokumenty tak komplikované, že i oni sami mají problém je vůbec přečíst. Zde jsou některé tipy, které vám pomohou vytvářet dokumentaci tak, že vám k něčemu bude:

V jednoduchosti je krása

Prohlédněte si libovolný nákres v této knize. Všechny jsou navrženy tak, aby vyjádřili jednu představu, čím více sdělení se snažíte nákresem vyjádřit, tím hůře bude srozumitelná.

Oddělte fyzické a logické plánování

Fyzická konektivita je velmi důležitá, ale pokuste se ji oddělit od sítí VLAN, směrování a dalších logických subjektů. Rád vytvářím dva nákresy: jeden pro fyzické porty a druhý se sítěmi VLAN a IP adresami. Při použití přepínaných virtuálních rozhraní platí tento tip dvojnásobně.

Nekřižte čáry

Vždy, když v nákresu překřížíte čáru, bude nákres hůře čitelný. Někdy je to nevyhnutelné, ale snažte se křížení čar omezit na minimum.

Používejte pouze přímé čáry

Pokud zhotovíte nákres, v němž jdou přímé čáry v trochu jiném směru než vodorovném nebo svislém, nákres bude vypadat jako čmáranice sériového vraha. Když věnujete trochu času orientaci všech čar, rozdíl bude markantní. Podobně, čáry nakreslené pod určitým úhlem by měly být nakreslené vždy pod stejným úhlem, je-li to možné.

Používejte náčrtky všude, kde můžete

Pokud jsou v nákresu dvě lokality, nějak je oddělte. Každou lokalitu umístěte do obdélníku (mnoho lidí dává přednost zaobleným obdélníkům). Pomoci může také použití barev, nebo dokonce odstínů šedé.

Vyrovnejte ikony

Pokud je ve vašem nákresu řada ikon, věnujte čas jejich zarovnání podél jedné osy.

Zásady pro pojmenovávání zařízení

Hostitelské názvy by měly být tvořeny tak, aby kdokoliv se základní znalostí sítí mohl určit funkce, které dané zařízení plní. Ovšem zdá se, že mezi lidmi v IT sektoru převládá tendence dávat zařízením co možná nejnepochopitelnější možné názvy. Například zde je skutečný hostitelský název, s nímž jsem se za léta mé praxe v oboru setkal (změnil jsem jméno firmy a podrobnosti, kvůli ochraně provinění): gadnslax1mai750901. Co to má sakra znamenat? Je takový název nutný? Mohu z tohoto hostitelského názvu odvodit použitý systém? A co je důležitější, dokážete to vy?

Na jednom školení týkající se sítě, která obsahovala tyto nic neříkající hostitelské názvy, se jeden ze studentů zeptal, co daný hostitelský název znamená. Nikdo nedokázal odpovědět bez toho, aniž by nahlédl do dokumentu popisujícího rozvržení hostitelského názvu. Hostitelské názvy by neměly vyžadovat žádné pátrání! Zde je vysvětlení dotyčného názvu:

gadnslax1mai750901

gad – název firmy (GAD Technology),

ns – network services (síťové služby),

lax – Los Angeles,

1 – asi jako první, hmm, věc v Los Angeles,

mai – Main Street (Hlavní ulice),

7509 – zařízením je Cisco 7509,

01 – jde o první zařízení 7509 v této lokaci.

Smyslem hostitelských názvů je identifikovat dané zařízení. Hostitelské názvy by měly být snadno zapamatovatelné. Pokud je hostitelský název hůře zapamatovatelný než IP adresa, použití hostitelského názvu je kontraproduktivní.

Pokud je hostitelský název doplněn názvem domény, aby vytvářel *plně kvalifikovaný název domény* (FQDN), výsledný řetězec by měl být stručný a jasný. *sw1.gad.net* je stručný a jasný plně kvalifikovaný název domény, který popisuje první přepínač v doméně poskytovatele sítě *gad*.

Líbí se mi hostitelské názvy, které popisují jednu věc – funkci daného zařízení. Vynikajícím hostitelským názvem je *WAN-Router*. Pro firmy, které mají více lokací, je vhodné přidat lokaci do hostitelského názvu (např. *LAX-WAN-Router*). Zařízení je obvykle instalováno v párech, takže v těchto případech je rovněž dobrým nápadem očíslování zařízení (např. *LAX-WAN-Router-1*). Podle mého názoru je však tento název příliš dlouhý. Skutečnost, že zařízením je směrovač, je ve srovnání s jeho funkcí irelevantní; název *LAX-WAN-1* bude postačující. Pokud chcete použít hierarchie DNS, stejně dobře poslouží také *wan-1.lax.domain.com*.

Každá firma má specifické potřeby. Pokud pracujete u poskytovatele připojení k Internetu, můžete mít zařízení umístěná u mnoha zákazníků. V takovém případě je užitečné zahrnutí jména zákazníka (např. *GAD-WAN-1*). Měli byste odolat nutkání zdokumentovat svoji síť pomocí hostitelských názvů. V hostitelských názvech nepotřebujete uvádět ani sériová čísla zařízení (ano, s tím jsem se opravdu setkal). Samozřejmě, že každý má své vlastní názory na hostitelské názvy, ale mou radou je snažit se o maximální jednoduchost. Po všech uvedených doporučeních lze konstatovat, že ani Lauren není vhodným názvem směrovače. Je to hezké jméno, ale není z něj ani za mák jasná funkce směrovače!

Poté, co jsem vymyslel hostitelské názvy, přidám pro službu DNS před hostitelské názvy také názvy rozhraní. Například rozhraní Serial 0/0/0:1 na směrovači *LAX-WAN-1* by mělo hostitelský název DNS *s0-0-0-1-lax-wan-1* (jelikož DNS může použít pouze pomlčky, nahradím všechna lomítka a dvojtečky pomlčkou). To velmi usnadní použití příkazu traceroute, neboť každý uzel a IP rozhraní v daném uzlu je zřetelně označeno:

```
[gad]$ traceroute switch9.mydomain.com
traceroute to switch9.mydomain.com (10.10.10.10), 30 hops max, 40 byte packets
1  s0-0.router1.mydomain.com 9.854 ms  10.978 ms  11.368 ms
2  f0-1.switch2.mydomain.com 2.340 ms  1.475 ms  1.138 ms
3  g0-0-12.switch9.mydomain.com 1.844 ms  1.430 ms  1.833 ms
```

Návrhy sítí

Nemůžu vám říci, jak byste si měli navrhnout síť. Můžu vám ukázat pár nejčastějších návrhů podnikových a e-commerce sítí a vysvětlit vám, proč jsem se zaměřil právě na tyto návrhy.

Podnikové sítě

Většina sítí je navržena podle schématu klasického *tříúrovňového modelu*. Tříúrovňový model obsahuje úroveň *jádra, distribuce a přístupu*. Tyto úrovně jsou jasně vymezeny a obslouženy různými zařízeními. Obvykle bylo nejpomalejším a nejdražším procesem směrování. Z těchto důvodů se směrování odehrávalo v jádru. Všechny ostatní úrovně byly obvykle přepínány.

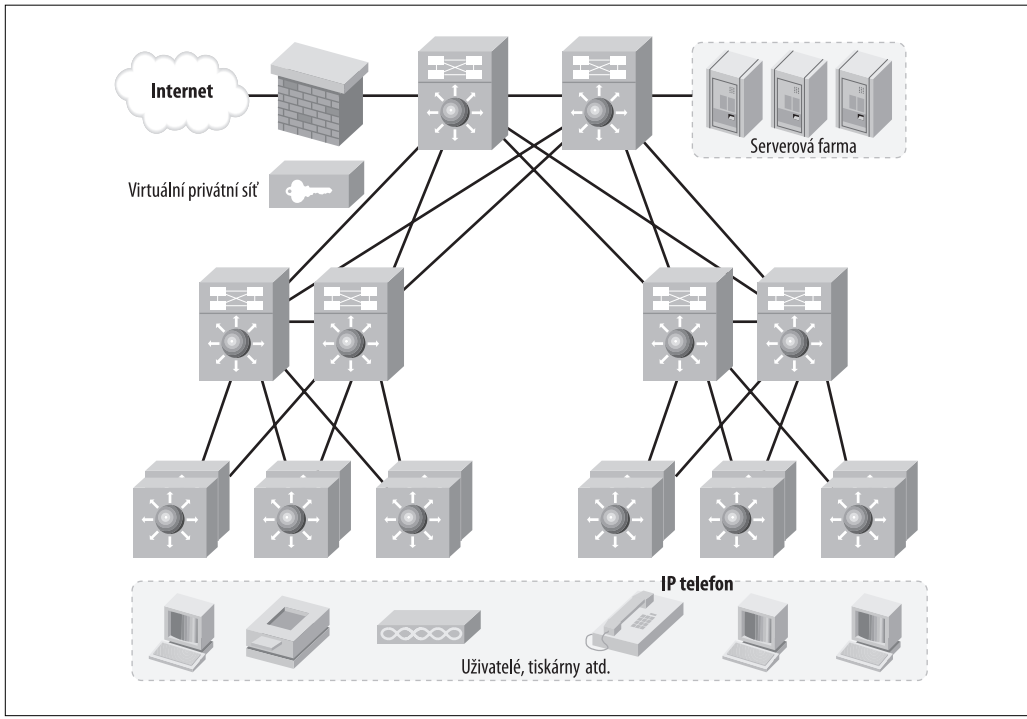
S příchodem levného přepínání na vrstvě 3 je nyní tříúrovňový model pro podnikové sítě často modelem zhroucení (collapsed). Podíváme se nyní na tradiční model tak, jak by mohl být použit dnes, stejně jako na pár modelů se zhrouceným jádrem (collapsed core).

Tříúrovňová architektura

Tříúrovňová architektura, s níž se můžete v učebnicích setkat nejčastěji, je v průmyslu stále nejpoužívanější architekturou. K fyzickému oddělení tří úrovní obvykle dojde tehdy, existuje-li fyzická potřeba tak učinit. Vynikajícím příkladem by mohla být studentská kolej nebo obchodní kampus:

s přepínači jádra (třeba v centrálním umístění), distribučními přepínači v každé budově a přístupovými přepínači blízko k uživatelům v každé budově.

Specifika by závisela na fyzickém rozvržení kampusu. Obrázek 33.9 znázorňuje učebnicovou tříúrovňovou podnikovou síť.



Obrázek 33.9: *Typická tříúrovňová podniková síť.*

Ve spodní části nákresu jsou uživatelé, tiskárny, IP telefony a bezdrátové přístupové body (AP) připojeny k přepínačům přístupové vrstvy. Přepínače přístupové vrstvy jsou připojeny k přepínačům distribuční vrstvy uprostřed. Distribuční přepínače jsou připojeny k horním dvěma přepínačům, které tvoří jádro celé sítě. Internet a serverové farmy jsou na tomto příkladu připojeny k jádru.

Zhroucené jádro – bez distribuce

Sítě se zhrouceným jádrem jsou velmi časté. Často jsem pracoval na Manhattanu, kde jsou velmi časté mrakodrapy. Kancelářské prostory v mrakodrapech jsou obvykle vymezeny podle podlaží. Kabeláž je obvykle vedena z míst na podlaze k centrálnímu umístění na tomtéž podlaží. Podlaží jsou obvykle propojena pomocí okruhů, které vedou mezi dvěma podlažími. Pokud určitá firma sídlí ve více podlažích, kabeláž každého podlaží představuje návrh zhrouceného jádra, neboť možnosti vedení kabelů mezi dvěma podlažími jsou omezené.

Vzhledem k omezenému prostoru na každém podlaží je obvykle potřeba více než dvou vrstev fyzických sítí malá. Nacházejí-li se přepínače jádra na jednom podlaží a přístupové přepínače na zbývajících podlažích, přístupové přepínače mohou fungovat také jako přepínače distribuční vrstvy. Hustota portů obvykle nepředstavuje problém, neboť každé podlaží nezabírá příliš mnoho fyzického

prostoru. Z logického hlediska může být do jádra zhroucena i distribuční vrstva. Logickou distribuční vrstvu nemusíte dokonce vůbec potřebovat. Opět platí, že každé prostředí je jiné.

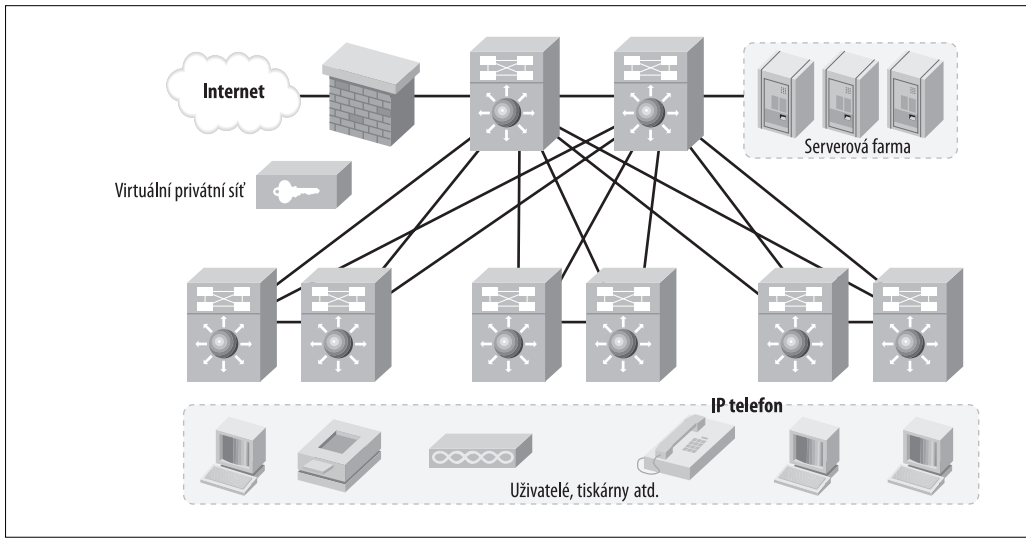
Serverové farmy – kam patří?

Patří servery blíže k uživatelům, které obsluhují, nebo do farmy blíže k jádru? Kam servery ve vaší síti patří, to závisí na tom, jak je vaše síť navržena, a často na typu příslušného serveru. Některé servery by měly být v jádru. Centrální umístění například e-mailových serverů dává smysl. Jiné servery by měly být blíže k uživatelům, které obsluhují. Například v síti univerzitního kampusu by nedávalo smysl umístění účetních serverů do jádra, pokud by bylo celé účetní oddělení umístěno v jedné budově. Pak by opět v každé budově nemuselo existovat místo pro servery.

Hodně záleží také na rozvržení vaší sítě. Mnoho dnešních firem vytváří zcela ploché sítě s modelem jádro/distribuce/přístup zcela včleněných do jednoho páru velkých přepínačů, například Cisco 6509. V takovém případě je vše připojeno ke stejným přepínačům.

Dalším scénářem, s nímž jsem se setkal a který používá tento typ návrhu, je segmentovaná budova. Jedním z projektů, na kterém jsem pracoval, spočíval ve vytvoření nového návrhu sítě pro velký stadión. Stadión byl rozdělen na čtyři segmenty, z nichž každý měl svou vlastní místnost infrastruktury (rozvodnu). Kabely uživatelů byly svedeny do těchto rozvoden a tyto rozvodny byly vzájemně propojeny optickým kabelem.

Obrázek 33.10 znázorňuje příklad sítě se zhrouceným jádrem bez distribuční vrstvy.

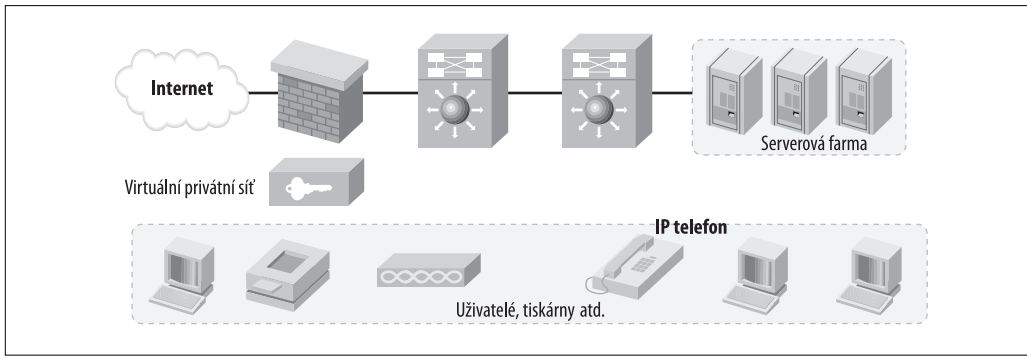


Obrázek 33.10: *Síť se zhrouceným jádrem bez distribuční vrstvy.*

Zhroucené jádro – bez distribuce nebo přístupu

Velmi populární návrh v podnicích, které se nachází uvnitř jedné budovy, je zhroucená síť, v níž jsou pouze přepínače jádra. Podnik se stovkami zaměstnanců, kteří se všichni nachází v jednom umístění, může mít často místnost s počítači umístěnou centrálně vzhledem k danému prostředí.

Pokud ethernetové kabely splní limity týkající se délky vedení použité kabeláže, všechny kabely mohou být vedeny k přepínačům jádra. Pár přepínačů s vysokou hustotou a vysokou dostupností, jako jsou přepínače Cisco 6509, mohou podporovat stovky uživatelů. Návrh takové sítě je znázorněn na obrázku 33.11.



Obrázek 33.11: *Síť se zhrouceným jádrem skládající se pouze z jedné vrstvy.*

Kroky při konfiguraci

Nehodlám zde podrobně procházet kroky při konfiguraci podnikové sítě. Podrobnosti týkající se konfigurace různých zařízení jsou uvedeny na jiných místech této knihy. Místo toho se zaměřím na některé aspekty, které byste měli vzít v potaz při navrhování takové sítě, a pokusím se vás nasměrovat správným směrem. Jako příklad použiji model zhrouceného jádra bez distribuční vrstvy. Pro ilustraci můžete použít obrázek 33.10.

Trunky. Trunky mohou být nezbytné všude, kde dochází k vzájemnému propojení přepínačů. Samozřejmé body jsou mezi dvěma přepínači jádra a linky propojující přístupové přepínače s jádrem. Nezapomeňte ani na linky mezi každým párem přístupových přepínačů.

Vaši síť můžete navrhnout tak, že linky mezi dvěma přepínači jsou linky s protokolem IP, a nikoliv trunky. To platí bezezbytku a mnoha lidem to může usnadnit pochopení sítě. Pokud si vyberte projekt tří vrstev sítě, budete potřebovat méně trunků.

EtherChannely. Rád propojuji své přepínače pomocí minimálně dvou spojení vzájemně svázaných pomocí EtherChannelu. To zajistí určitou odolnost (resilienci) a zvýší šířku pásma mezi přepínači. V závislosti na své síti můžete chtít zvětšit velikost svazků na tři, čtyři nebo ještě více.

Možná máte servery, které rovněž vyžadují EtherChannely. Zkontrolujte svoji skupinu serverů, abyste zjistili, je-li tato funkce vyžadována, a pokud ano, jak by měla být nakonfigurována.

Pokud budete mít ve svých přepínačích jádra moduly, jako jsou moduly FWSM, které vyžadují vyhrazené linky mezi failover páry, možná budete muset navrhnout EtherChannely i pro tyto moduly. Další informace týkající se EtherChannelech najdete v kapitole 7.

Spanning Tree. Určete, které porty budou uživatelskými nebo serverovými porty, a nakonfigurujte je tak, aby podporovaly `spanning-tree portfast`. Nakonfigurujte jeden z přepínačů jádra tak, aby byl kořenovým mostem spaning-tree, a druhý přepínač jádra, aby byl sekundárním kořenovým mostem. Další podrobnosti najdete v kapitole 8.

VTP. Nejsem velkým zastáncem protokolu VTP, zejména v malých sítích, ale i když jej nepoužijete, budete muset nakonfigurovat název domény VTP. Automatické nastavení trunku vyžaduje správné nastavení domény VTP. Další podrobnosti najdete v kapitole 5.

Sítě VLAN. Kolik sítí VLAN budete potřebovat? Nezapomeňte je všechny včas naplánovat. Zde je seznam, který jsem vytvořil při pohledu na obrázek 33.10:

- Internet.
- Internet ve vnitřní síti.
- Serverová farma.
- Uživatelské sítě VLAN.

Včasné plánování vám ušetří rozhodnutí učiněná na poslední chvíli a také čas.

E-commerce webové servery

E-commerce webový server slouží pro prodej zboží a utrácení peněžních prostředků. E-commerce webové servery vyžadují některé funkce, které u jednoduchých webových serverů neexistují. Největším problémem je bezpečnost. Pokud vezmete Linuxový server a rozjedete na něm jednoduchý webový server, starosti si budete muset dělat pouze se zabezpečením tohoto webového serveru. V případě e-commerce webového serveru budete mít pravděpodobně více webových serverů. Každý z těchto webových serverů zřejmě bude muset přistupovat k databázi, která by neměla být přístupná z Internetu. Vlastně tato databáze by neměla být přímo přístupná ani z webových serverů! Spíše by měla existovat vrstva serverů, které zpracují požadavky webových serverů směrované na databázi. Tato vrstva serverů se nazývá *aplikační vrstva*. Nyní si musíte dělat starosti o zabezpečení webových serverů, aplikačních serverů a databázových serverů. Některé z těchto serverů nebo také všechny servery mohou vyžadovat rozdělení zátěže a všechny servery budou vyžadovat správu. Správa může představovat zajímavý problém, neboť jak jsem již řekl, databázové servery by neměly být přístupné z Internetu.

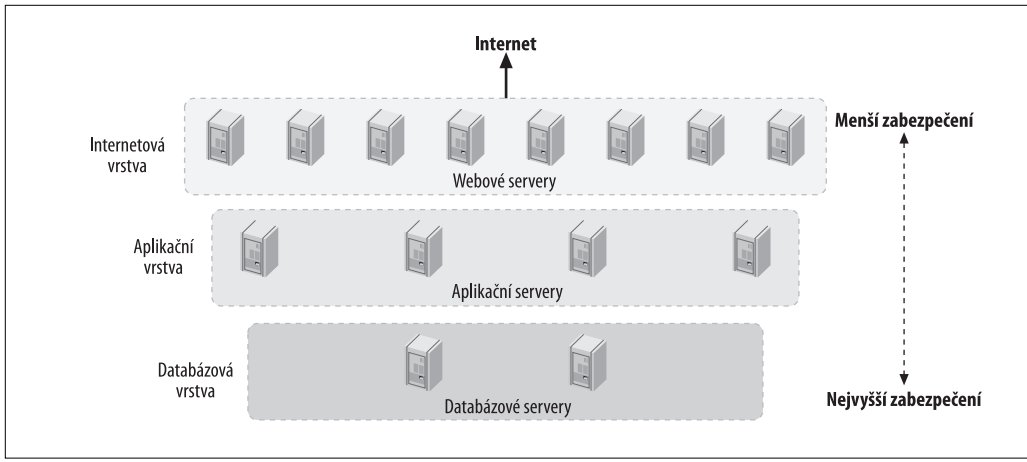
Databázové servery budou obsahovat informace o zákaznících a možná také údaje z kreditních karet. Tyto informace je třeba zabezpečit. Oddělení serverů od Internetu je jedním z nejlepších způsobů bez opr. jak zajistit požadovanou ochranu.

Standardní návrh e-commerce webového serveru se skládá ze tří úrovní. První úroveň obsahuje webové servery, které jsou dosažitelné z Internetu. Tato úroveň se nazývá internetová vrstva. Druhá úroveň obsahuje aplikační servery, které jsou z Internetu obvykle nedosažitelné. Tyto servery mohou komunikovat s webovými servery nacházejícími se nad nimi a s databázovými servery nacházejícími se pod nimi. Nejnižší vrstvou je databázová vrstva, která je přístupná pouze prostřednictvím aplikační vrstvy.

Existuje mnoho způsobů návrhu e-commerce webového serveru. Návrh sítě bude z větší části determinován použitým softwarem a metodami vývojáře. Pracoval jsem na e-commerce webových serverech, které měly pouze dvě vrstvy, zatímco jiné měly čtyři vrstvy. Někdy budou vývojáři trvat na jedné vrstvě. Pokud aplikace jednoduše nepodporuje více vrstev, lámání přes koleno je jen zbytečným plýtváním časem. Nicméně pokud pracujete se servery, které uchovávají údaje o kreditních kartách, ujistěte se, že váš návrh dodržuje standardy asociace PCI (Payment Card Industry) týkající se bezpečnosti.

Internetová vrstva je nejméně bezpečnou vrstvou, neboť je přístupná z Internetu. I když je tato vrstva chráněná firewallem, ke službám na této vrstvě má široká veřejnost přístup. Nejbezpečnější vrstvou je databázová vrstva. Jedinou možností přístupu k databázové vrstvě je prostřednictvím aplikačních serverů. Tyto servery budou obsahovat speciální aplikace, které mohou zpracovat a případně uložit do vyrovnávací paměti informace z databáze pro webové servery.

Tříúrovňová architektura e-commerce serveru je znázorněna na obrázku 33.12. Internetová vrstva obsahuje většinu serverů. Počet serverů se ve spodních vrstvách zpravidla zmenšuje, ačkoliv to neplatí obecně. Například databázová vrstva se může skládat z Oracle clusteru, který by mohl používat mnoho menších serverů.

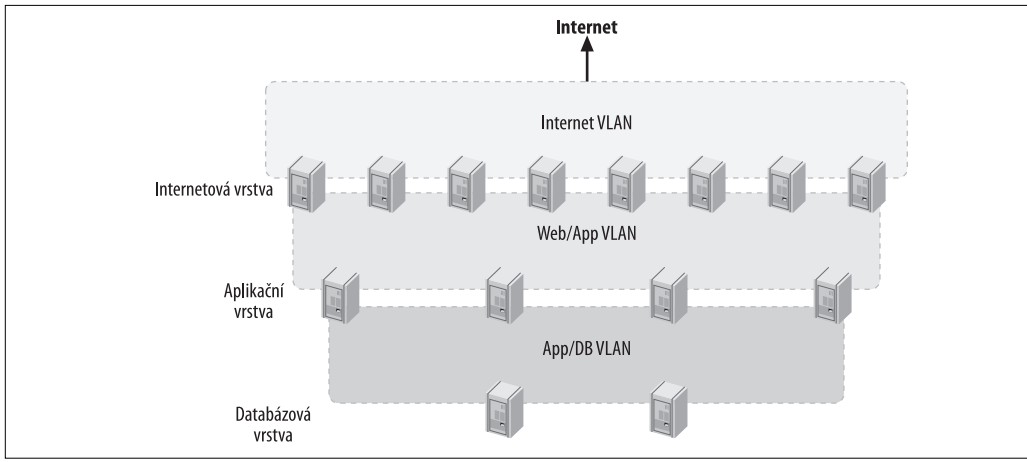


Obrázek 33.12: *Typický tříúrovňový e-commerce webový server.*

Servery na každé úrovni se spojují se servery na sousední úrovni či úrovních. Například aplikační servery mohou mít rozhraní v databázové vrstvě a Internetové vrstvě. Všechny servery mohou mít více rozhraní. V případě sítí s vysokou dostupností mohou servery vyžadovat čtyři rozhraní: dvě pro vyšší úroveň (jedno v každém přepínači) a dvě pro nižší úroveň.

Existují dvě hlavní přípustné metody realizace těchto vrstev. Budu je označovat jako *přemostění* (bridging) a *směrování* (routing). V metodě přemostění platí, že nižší rozhraní horní vrstvy jsou připojena ke stejné síti VLAN jako horní rozhraní dolní vrstvy.

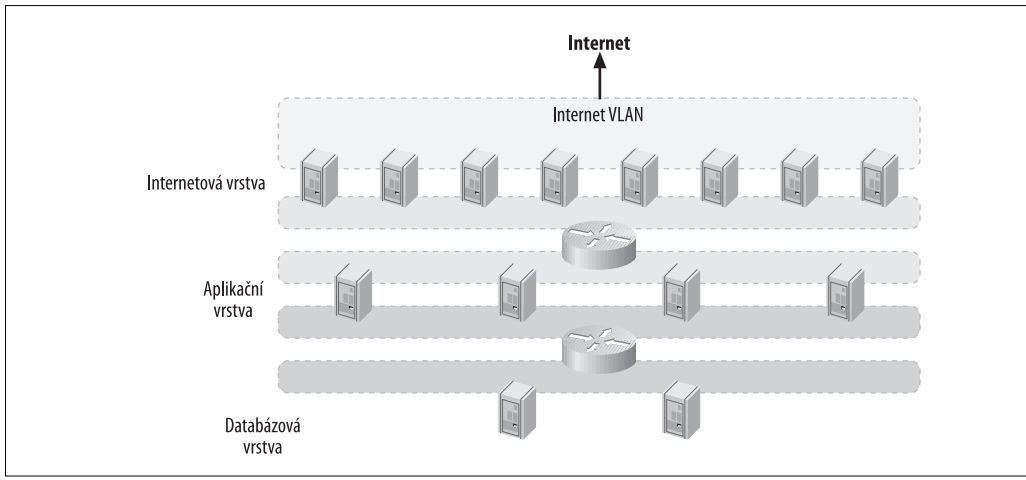
Obrázek 33.13 znázorňuje příklad přemostěného návrhu e-commerce řešení. Výhodami tohoto návrhu jsou jednoduchost a rychlost. Jsou zde pouze tři sítě VLAN a neexistují žádné směrovače nebo firewally oddělující tyto vrstvy. Nevýhodou je nižší bezpečnost, neboť neexistují žádná zařízení



Obrázek 33.13: *Přemostěný tříúrovňový návrh e-commerce řešení.*

oddělující servery v jedné vrstvě od serverů v jiné vrstvě. Severy v přemostěném návrhu potřebují komunikovat pouze se sítěmi, které jsou k nim přímo připojeny. Webové servery jsou jediné servery, které v tomto návrhu potřebují výchozí bránu.

Bezpečnější alternativou k přemostěnému návrhu je směrovaný návrh. Směrování mezi vrstvami umožňuje umístění firewallů mezi vrstvy. Obrázek 33.14 znázorňuje typický směrovaný tříúrovňový návrh e-commerce řešení.



Obrázek 33.14: *Směrovaný tříúrovňový návrh e-commerce řešení.*

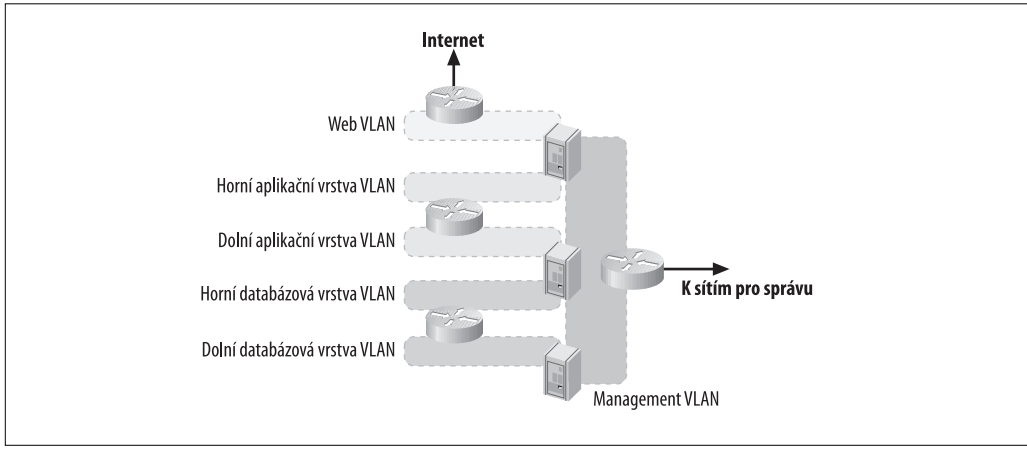
Směrovaný návrh je komplikovanější, neboť v tomto návrhu existuje dvakrát větší počet sítí VLAN, z nichž každá musí mít přepínané virtuální rozhraní nebo logické směrovače oddělující sítě VLAN, servery na každé úrovni musí mít nakonfigurovány výchozí brány nebo příkazy pro směrování. Výhodou směrovaného návrhu je bezpečnost. Jelikož veškerý provoz musí projít směrovačem, směrovač může být firewallem.

Problém obou těchto návrhu spočívá v tom, že neexistuje jednoduchý způsob vzdálené správy serverů. Pokud máte k serverům snadný přístup, tento problém může vyřešit KVM přepínač (Keyboard Video Monitor) v každé skříni (rack). Ovšem e-commerce webové servery jsou typicky hostovány v oddělených kolokačních centrech. V takovém případě jsou možnosti vzdálené správy klíčové.

Vzdálená správa se často provádí pomocí jiné sítě VLAN, která se připojí ke každému serveru a síťovému zařízení daného serveru. Tato síť VLAN pro správu se poté připojí ke směrovači nebo firewallu, který povolí konektivitu k hlavnímu serveru. Obrázek 33.15 znázorňuje příklad takového návrhu.

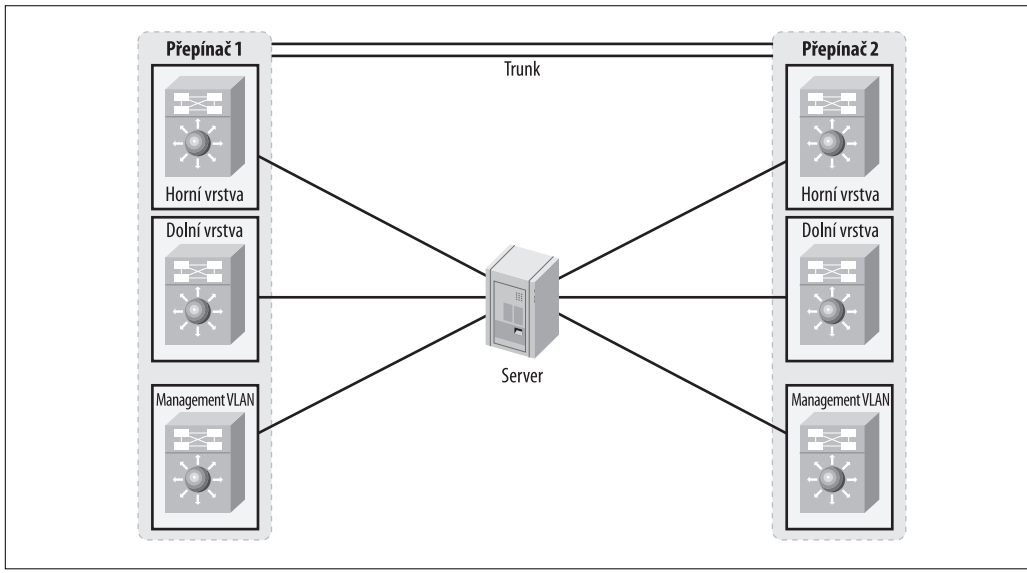
Prošli jste si strastiplnou cestou k zajištění bezpečnosti serverů. Oddělili jste všechny servery do samostatných vrstev a zabránili webovým serverům v komunikaci s databázovými servery. Nyní jste přidali další síť VLAN, která všechny tyto servery propojuje. Pokud si myslíte, že to není dobrý nápad, máte pravdu. Výhody správy sítě převáží nad riziky, ale pouze pokud navrhnete síť správně.

Sítě pro správu by měly být velmi bezpečné. Funkce jako bezpečnost portu a privátní sítě VLAN mohou pomoci zajistit bezpečnost sítě. Žádnému serveru by nemělo být povoleno komunikovat s jiným serverem v síti, s výjimkou záložních serverů a serverů dálkového měření.



Obrázek 33.15: *Síť pro správu e-commerce řešení.*

Problém všech těchto sítí VLAN spočívá v tom, že obvykle se kombinují s návrhem sítě s vysokou dostupností. Pro každou síť VLAN, k níž se musí určitý server připojit, se musí použít dvě ethernetová rozhraní: jedno pro každý z přepínačů v páru s vysokou dostupností. I když se nemusí zdát, že by s tím mohl být nějaký problém, v případě pouhých tří sítí VLAN pro průměrný server je to už šest použitých ethernetových rozhraní. Obrázek 33.16 znázorňuje typický server připojený ke třem sítím VLAN na dvou přepínačích.



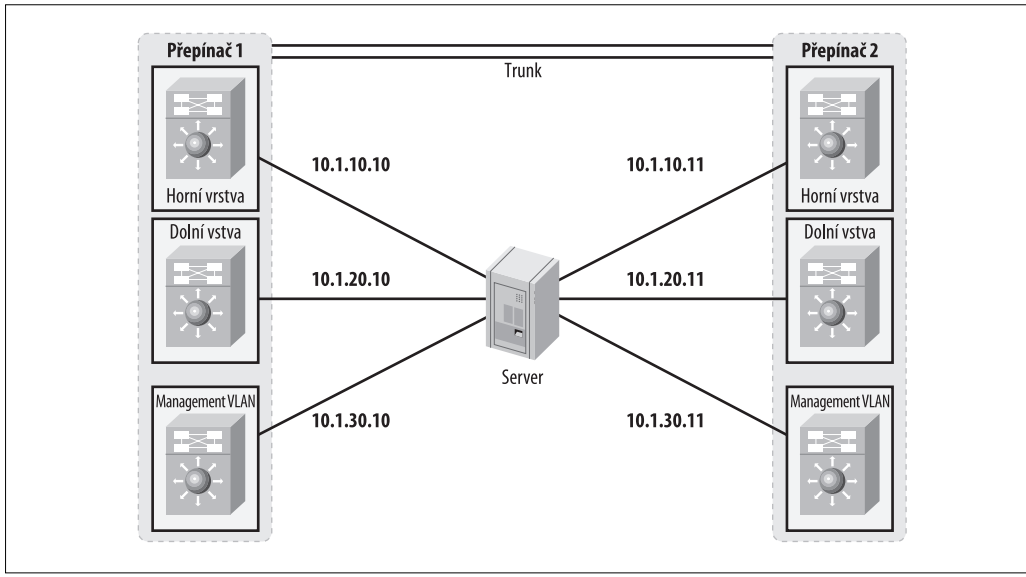
Obrázek 33.16: *Použitá ethernetová rozhraní na serveru.*

Při navrhování sítě, jako je tahle, nezapomeňte úzce spolupracovat s lidmi majícími co do činění se systémem. Existuje celá řada věcí, o nichž byste měli přemýšlet. Zde je jejich stručný výčet:

- Každé rozhraní bude potřebovat IP adresu.

- U některých serverových řešení s vysokou dostupností bude pro každou síť VLAN potřeba třetí IP adresa. Například Solaris IP Multipathing potřebuje kromě jedné virtuální pro každé fyzické rozhraní také virtuální IP adresu pro každou síť VLAN.
- Každá IP adresa, kterou přiřadíte, může vyžadovat DNS položku (včetně virtuálních IP adres).
- Které rozhraní je primární?
- Potřebuje server výchozí bránu? Pokud ano, kam směřuje? Může server podporovat více výchozích nastavení? Jak budou fungovat? Webové servery potřebují výchozí bránu, která směřuje do Internetu. To bude vyžadovat, aby vaše síť VLAN pro správu obsahovala specifické cesty k serverům.
- Kolik fyzických síťových karet v serveru potřebujete, aby tento server podporoval šest ethernetových rozhraní? Ujistěte se, že jich máte dostatek. Dodatečná rozhraní jsou ještě lepší.
- Budou mít servery obě rozhraní v každé síti VLAN aktivní, nebo bude aktivní pouze jedno rozhraní? Některá serverová řešení s vysokou dostupností vyžadují, aby byly přepínače nakonfigurovány určitým způsobem, zatímco jiné vyžadují odlišné konfigurace. Vyzkoušejte je v laboratorním prostředí dříve, než takovou síť vytvoříte.
- Budou vaše servery podporovat vzdálené ethernetové konzoly? Budete pro tento provoz potřebovat vyhrazenou síť?

Při vymýšlení vašeho schématu IP adres je dobrým krokem nechat poslední oktet (nebo oktety) pro každé rozhraní na každém serveru stejné. Jinými slovy, pokud je vaše horní síť 10.1.10.0/24 a vaše dolní síť 10.1.20.0/24, poslední oktet by měl být pro všechny servery v dané síti stejný. Tudíž by horní IP adresa byla 10.1.10.10 a dolní IP adresa by byla 10.1.20.10. Nezapomeňte, že IP adresu musíte přiřadit každému rozhraní, takže poslední oktet by měl být pro všechny přepínače stejný. Obrázek 33.17 znázorňuje, jak by mohlo takové schéma IP adres vypadat.



Obrázek 33.17: *Shodný poslední oktet u více sítí VLAN a přepínačů.*

Malé sítě

Mnoho malých firem nepotřebuje propracované tříúrovňové sítě. Takové firmy mají třeba jen jednu kancelář, nebo dokonce tři, ale kanceláře jsou malé a sítě jsou jednoduché. Dokonce i některé větší firmy nemají nijak propracované sítě. Bez ohledu na velikost nebo složitost sítě by měl být každý aspekt pečlivě zdokumentován.