CISCO

IPv6

Kompletní průvodce nasazením v podnikových sítích

SAMOSTUDIUM

- ✔ Vybudování pilotní sítě
- ✔ Desítky diagramů možných topologií
- ✔ Shrnutí za každou kapitolou

Shannon McFarland
Muninder Sambi
Nikhil Sharma
Sanjay Hooda

CPRESS

Shannon McFarland, Muninder Sambi, Nikhil Sharma, Sanjay Hooda

IPv6
Kompletní průvodce nasazením v podnikových sítích

Computer Press, a. s.
Brno
2011

IPv6
Kompletní průvodce nasazením v podnikových sítích

Shannon McFarland, Muninder Sambi, Nikhil Sharma, Sanjay Hooda

Computer Press, a. s., 2011. Vydání první.

Překlad: Jakub Goner
Jazyková korektura: Martina Mojzesová
Sazba: Petr Klíma
Rejstřík: Daniel Štreit
Komentář na zadní straně obálky: Libor Pácl

Technická spolupráce: Jiří Matoušek, Zuzana Šindlerová, Dagmar Hajdajová
Odpovědný redaktor: Libor Pácl
Technický redaktor: Jiří Matoušek
Produkce: Petr Baláš

Authorized translation from the English language edition, entitled IPV6 FOR ENTERPRISE NETWORKS, 1st Edition, 1587142279 by MCFARLAND, SHANNON; SAMBI, MUNINDER; SHARMA, NIKHIL; HOODA, SANJAY, published by Pearson Education, Inc, publishing as Cisco Press, Copyright © 2011 Cisco Systems, Inc.

Computer Press, a. s.,
Holandská 3, 639 00 Brno

Objednávky knih:
http://knihy.cpress.cz
distribuce@cpress.cz
tel.: 800 555 513

ISBN 978-80-251-3684-3
Prodejní kód: K1973
Vydalo nakladatelství Computer Press, a. s., jako svou 4120. publikaci.

Obsah

KAPITOLA 6

Věnování

Tuto knihu věnuji Lindě, Zackovi a Carterovi. Dostalo se mi velkého požehnání, že jste všichni součástí mého života, a jsem hrdý, že z mých synů vyrostli čestní mladí muži. Děkuji vám, že jste to se mnou po mnoho uplynulých měsíců vydrželi. Rád bych také poděkoval své mámě za její bezpodmínečnou lásku a modlitby a tátovi za jeho povzbuzování, abych se nikdy nepřestal učit. Své tchyni a tchánovi děkuji za to, že přivedli Lindu na tento svět a do mého života – je nejlepší ženou ze všech. Tátovi děkuji za to, že je mým přítelem a rádcem a vždy mi ukazoval, jak je důležitá tvrdá práce.

—Shannon McFarland

Především bych chtěl věnovat tuto knihu svému dědečkovi. Gyani Gurcharan Singh mi byl inspirací jako autor, básník a interpret klasické hudby. Za pevnou podporu během psaní této knihy si zaslouží poděkování celá má rodina: táta (Surinder Singh Sambi), máma (Sukhdev Kaur), můj bratr (dr. Ravinder Singh Sambi), švagrová (Amrit Kaur) a žena (Avnit Kaur). Knihu chci věnovat i své dceři (Japjot), dvojčatům (Kabiru Singhovi a Charanu Kanwalu Singhovi) a mým synovcům (Kanwalovi a Bhanwraovi).

—Muninder Singh Sambi

V prvé řadě chci poděkovat svým rodičům: tátovi (Satbiru Singhovi) a mámě (Indrawati) a ženě (Suman) za jejich podporu při psaní této knihy. Kniha je věnována mým dětem Pulkit a Apoorvě.

—Sanjay Hooda

Chci poděkovat své ženě Parul za její neustávající podporu během celého projektu. Tuto knihu věnuji své dceři Anshi, která mi ukázala, jak malé věci v životě přinášejí skutečné štěstí.

—Nikhil Sharma

Poděkování

Chci poděkovat mnoha lidem, kteří mi během mnoha uplynulých let pomohli získávat znalosti a zkušenosti protokolu IPv6 a podporovali mě, když jsem mu věnoval čas (zejména ze začátku), a také těm, kdo mi poskytovali svou podporu. Patří k nim mí přátelé a cenní pomocníci Freddie Tsao, Steve Pollock, Chris O'Brien a Mark Montanez. Měl jsem štěstí na mnoho skvělých vedoucích, kteří se mnou v uplynulých letech měli značnou trpělivost a nabídli mi účinnou pomoc, zejména ohledně protokolu IPv6. Za všechny jmenuji následující: Todd Truitt, Vince Spina, Kumar Reddy, Mauricio „Mo" Arregoces, Dave Twinam a Mark Webb. Dále bych chtěl poděkovat následujícím pracovníkům společnosti Cisco (dřívějším i současným), kteří mi byli při mém snažení přímo či nepřímo nápomocni: Patrick Grossetete, Chip Popoviciu, Eric Vyncke, Gunter Van de Velde, Tarey Treasure, Darlene Maillet, Angel Shimelish, Chris Jarvis, Gabe Dixon, Tim Szigeti, Mike Herbert, Neil Anderson, Dave West, Darrin Miller, Stephen Orr, Ralph Droms, Salman Asadullah, Yenu Gobena, Tony Hain, Benoit Lourdelet, Eric Levy-Abegnoli, Jim Bailey, Fred Baker a nespočet dalších. Nakonec

chci poděkovat Johnu Spenceovi a Yuriemu Richovi za léta odborných rad a kontroly praktického nasazení protokolu IPv6.

—Shannon McFarland

Poděkování si v prvé řadě zaslouží mí spoluautoři Sanjay Hooda, Nikhil Sharma a Shannon McFarland za kooperaci při psaní knihy. Zvláště chci poděkovat Shannonovi za to, že udržoval naši motivaci a provedl nás některými obtížnějšími tématy.

Děkuji svému rádci a dobrému příteli Sanjayovi Thyamagundaluovi, který mi při psaní této knihy pomáhal.

Rovněž děkuji svému vedoucímu Sachinu Guptovi za jeho podporu a povzbuzování, abych tuto knihu dokončil. Odborní korektoři Jim Bailey a Chip Popoviciu s námi sdíleli své technické zkušenosti protokolu IPv6 a byli k dispozici pokaždé, když jsme s nimi potřebovali konzultovat jejich poznámky.

Nakonec chci poděkovat týmu v nakladatelství Cisco Press, zejména Brettu Bartowovi a Dayně Isleyové, za to, že nás provedli celým procesem tvorby knihy a projevovali trpělivost, když jsme postupně zdokonalovali koncepty jednotlivých kapitol.

—Muninder Singh Sambi

V prvé řadě děkuji svým spoluautorům Muninderovi, Shannonovi a Nikhilovi, kteří mi byli při psaní velmi nápomocni. Dále chci poděkovat svému dobrému příteli Sanjayovi Thyamagundaluovi a svému vedoucímu Vinayovi Parameswarannairovi za jejich podporu při psaní této knihy. Sanjay Thyamagundalu poskytl nejen inspiraci, ale také hluboké postřehy týkající se různých oblastí.

Díky si zaslouží i Brett Bartow, Dayna Isleyová a všichni pracovníci nakladatelství Cisco Press, kteří projevovali značnou trpělivost, když jsme usilovali o dodržení termínů.

—Sanjay Hooda

Na prvním místě chci výslovně poděkovat svému rádci a nejlepšímu příteli Muninderovi Sambimu, který mě uvedl do světa počítačových sítí. Tato kniha by nemohla vzniknout, kdyby nám Sanjay Hooda neposkytl přístup do své laboratoře. Shannon udržoval motivaci celého našeho týmu a ukazoval nám cílovou pásku, která často vypadala příliš vzdálená.

Jsem vděčný svým přátelům, kteří vždy odpověděli na mé volání. Patří k nim Amol Ramakant, Deepinder Babbar, Jagdeep Sagoo a Nitin Chopra.

—Nikhil Sharma

Speciální uznání si zaslouží naši odborní korektoři Chip Popoviciu a Jim Bailey, kteří při korekturách knihy uplatnili své obsáhlé technické znalosti.

Nakonec děkujeme svým fantastickým redaktorům Brettu Bartowovi a Dayně Isleyové a týmu v nakladatelství Cisco Press za jejich podporu, trpělivost a kvalitní práci.

Úvod

O autorech

Shannon McFarland, CCIE č. 5245, je odborník na podnikové konzultace ve společnosti Cisco, který pracuje jako technický konzultant pro podnikové nasazení protokolu IPv6 a návrh datových center. Zaměřuje se přitom na vývoj aplikací a infrastrukturu virtuálních pracovních stanic. V uplynulých šestnácti letech pracoval na rozsáhlých návrzích podnikových areálových sítí, sítí WAN a pobočkových sítí, návrhu a optimalizaci datových center pro operační systémy Microsoft a serverové aplikace a také na návrhu a optimalizaci nasazení infrastruktury virtuálních pracovních stanic. V posledních deseti letech Shannon často po celém světě vystupuje na akcích týkajících se protokolu IPv6 (například na konferenci Cisco Live – dříve Networkers), summitech o IPv6 a dalších oborových událostech. Je autorem mnoha technických dokumentů a podnikových návrhů CVD (Cisco Validated Designs) týkajících se protokolu IPv6, vícesměrového vysílání IP, serveru Microsoft Exchange, prostředí VMware View a dalších aplikací. Přispěl také do mnoha knih nakladatelství Cisco Press. Před svým působením ve společnosti Cisco pracoval jako konzultant pro prodejce VAR (value-added reseller) a rovněž jako síťový technik v oboru zdravotnictví. Shannon žije se svou ženou a dětmi ve městě Castle Rock v Coloradu.

Muninder Sambi, CCIE č. 13915, je vedoucí produktového marketingu platformy Cisco Catalyst 4500/4900. Jako vedoucí produktové řady odpovídá za definice produktových strategií u platforem řad Catalyst 4500 a 4900 s prodeji ve výši mnoha miliard dolarů. Patří k nim architektury produktů nové generace, které slouží pro uživatelský přístup v areálových sítích a serverový přístup v datových centrech. Před nástupem do této funkce hrál Muninder klíčovou roli při definování dlouhodobé strategie softwaru a služeb pro platformy modulárního přepínání Cisco (řady Catalyst 6500 a 4500/4900) včetně zaměření na inovace protokolu IPv6. Některé z těchto inovací umožnily nasazení duální sady protokolů IP v sítích podniků a poskytovatelů služeb. Muninder také patří mezi klíčové členy vývojové rady protokolu IPv6 ve společnosti Cisco. Zastupoval společnost Cisco při mnoha jednáních o návrhu síťové architektury s velkými podnikovými

zákazníky. Během posledních více než dvanácti let pracoval na mnoha návrzích podnikových areálových sítí, sítí WAN a datových center. Před nástupem do společnosti Cisco pracoval Muninder jako síťový konzultant u jednoho z hlavních síťových integrátorů v Indii a odpovídal za návrh a implementaci sítí LAN, WAN a sítí hostovaných datových center. Se svou ženou a dětmi žije ve městě Fremont v Kalifornii.

Nikhil Sharma, CCIE č. 21273, je odborník na technický marketing ve společnosti Cisco, kde odpovídá za definování nových hardwarových i softwarových funkcí produktové řady Catalyst 4500. V posledních deseti letech spolupracoval s různými podnikovými zákazníky na návrhu a řešení potíží velkých a středně velkých areálových sítí a sítí v datových centrech.

Sanjay Hooda, CCIE č. 11737, je technický vedoucí ve společnosti Cisco, kde se zabývá integrovanými systémy a pomáhá definovat architekturu nových produktů. Aktuálně se zaměřuje na vysokou dostupnost a zasílání zpráv v systémech distribuovaného přepínání velkého rozsahu. V průběhu posledních čtrnácti let získal zkušenosti v mnoha oblastech, včetně SCADA (Supervisor Control and Data Acquisition – inspekční řízení a získávání dat), softwarových projektů velkého rozsahu a návrhu podnikových areálových sítí a sítí LAN, WAN a sítí datových center.

O odborných korektorech

Jim Bailey, CCIE č. 5275 (směrování a přepínání; poskytovatel služeb) a CCDE č. 20090008, je technický vedoucí pro AS ve společnosti Cisco Systems, který má v oboru sítí více než osmnáct let praxe. V týmu Advanced Services skupiny Global Government Solutions se soustřeďuje na architekturu, návrh a implementaci rozsáhlých sítí v civilních a vojenských agenturách americké vlády. V posledních pěti letech se specializoval na integraci protokolu IPv6 do těchto sítí.

Ciprian P. Popoviciu, Ph.D., je vedoucím oddělení Cloud and Network 3.0 ve skupině Enterprise Services společnosti Technodyne. Dříve zastával několik vedoucích funkcí ve společnosti Cisco, kde v uplynulých osmi letech úzce spolupracoval se standardizačními orgány a velkými zákazníky po celém světě na vývoji protokolu IPv6 a produktů, strategii a plánování tohoto protokolu a vývoji a nasazení architektury nové generace s podporou protokolu IPv6. Ciprian je spoluautorem dvou často odkazovaných knih o protokolu IPv6 z nakladatelství Cisco Press, čtyř dokumentů RFC a mnoha odborných článků o technologii, strategii a nasazení protokolu IPv6. Je významným členem sdružení IEEE, účastní se práce několika výzkumných poradních komisí a vystupuje na oborových akcích týkajících se protokolu IPv6.

Ikony použité v této knize


PC


Notebook

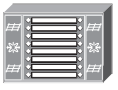

CallManager

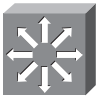

Úložiště FC


Firewall PIX


Směrovač s podporou hlasu


Směrovač


Server blade UCS 5108


Přepínač pro více vrstev

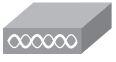

Koncentrátor sítí VPN


Přepínač IntellSwitch


Přepínač pro více služeb


UCS Express


IP telefon


Přístupový bod

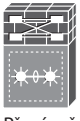

Přepínač

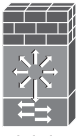

Fabric Interconnect řady 6100


Řadič sítě WLAN


Nexus 5K s integrovaným modulem VSM

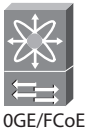

Nexus 4000


Přepínač virtuální vrstvy


Modul služeb firewallu


Přepínač datového centra

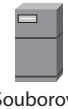

Vzdálený přepínač pro více vrstev


10GE/FCoE


Cisco ASA

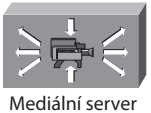

Procesor směrovače nebo přepínače

Procesor směrovače nebo přepínače s Si


Souborový server


Webový server


Smartphone


Mediální server

Typografické konvence

V této knize se při zápisu syntaxe příkazů používají stejné konvence jako v příručce IOS Command Reference (Přehled příkazů systému IOS). Uvedená příručka definuje tyto konvence následovně:

- **Tučné písmo** označuje příkazy a klíčová slova, která se zadávají doslova tak, jak je uvedeno. V ukázkách a výstupech skutečné konfigurace (nikoli v obecné syntaxi příkazů) představuje tučné písmo příkazy, které uživatel zadává ručně (například příkaz show).
- *Kurzíva* zvýrazňuje argumenty, místo kterých se zadávají skutečné hodnoty.
- Svislé čáry (|) oddělují alternativní a vzájemně se vylučující prvky.
- Hranaté závorky ([ ]) označují volitelný prvek.
- Složené závorky ({ }) znamenají požadovanou volbu.
- Složené závorky v hranatých ([{ }]) představují požadovanou volbu uvnitř volitelného prvku.

Zpětná vazba od čtenářů

Nakladatelství a vydavatelství Computer Press, které pro vás tuto knihu přeložilo, stojí o zpětnou vazbu a bude na vaše podněty a dotazy reagovat. Můžete se obrátit na následující adresy:

redakce PC literatury
Computer Press
Spielberk Office Centre
Holandská 3
639 00 Brno

nebo

sefredaktor.pc@cpress.cz

Computer Press neposkytuje rady ani jakýkoli servis pro aplikace třetích stran. Pokud budete mít dotaz k programu, obraťte se prosím na jeho tvůrce.

Errata

Přestože jsme udělali maximum pro to, abychom zajistili přesnost a správnost obsahu, chybám se úplně vyhnout nelze. Pokud v některé z našich knih najdete chybu, budeme rádi, pokud nám ji oznámíte. Ostatní uživatele tak můžete ušetřit frustrace a pomoci nám zlepšit následující vydání této knihy.

Veškerá existující errata zobrazíte na adrese *http://knihy.cpress.cz/K1973* po klepnutí na odkaz Soubory ke stažení.

Úvod k protokolu IPv6

IPv6 (Internet Protocol verze 6) je nová verze protokolu, který se používá při komunikaci všech typů zařízení v Internetu. Protokol IPv6 existuje již mnoho let, ale v současnosti se jeho nasazování v podnicích značně zrychluje. Protokol IPv6 se neustále vyvíjí a vyspívá, protože při praktické implementaci se odhalují mezery samotného protokolu nebo metodologie jeho nasazení.

Podniky po celém světě se s protokolem IPv6 setkávají při nasazení operačních systémů a aplikací, které tento protokol používají automaticky (často i bez vědomí uživatelů nebo správců), nebo protokol IPv6 samy aktivně nasazují z následujících důvodů: kvůli většímu rozsahu adres, rozšíření na rozvíjející se trhy, řešení síťových komplikací při slučování a akvizicích a využití nových možností protokolu při vývoji špičkových koncových bodů a aplikací. Bez ohledu na důvody je zásadně důležité, aby podniky plně rozuměly dostupným možnostem nasazení protokolu IPv6 a při nasazení zvolily radikální, ale dobře promyšlený přístup k plánování a návrhu.

Protokol IP je všudypřítomný. Pokud chce tedy oddělení IT správně naplánovat a nasadit protokol IPv6 v podnikové síti, musí projekt rozdělit podle částí sítě, jako je areálová síť, datové centrum, síť WAN atd., a poté se soustředit na všechna místa, kde se v současnosti používá protokol IPv4. V závislosti na obchodních a technických požadavcích je poté potřeba implementovat protokol IPv6 vedle protokolu IPv4. V některých případech se protokol IPv6 nasazuje v nových oblastech, kde protokol IPv4 není nadále potřebný. Existují také scénáře, kdy protokol IPv6 není potřeba nasadit všude tam, kde slouží protokol IPv4. V této knize rozdělíme podnikovou síť na různé logické části a představíme pokyny návrhu a nasazení, které umožní implementaci protokolu IPv6 v příslušných částech.

Cíle a metody

Nové projekty se v podnicích často komplikují kvůli osobním sporům a jiným netechnickým aspektům. Tato situace mnohdy vede k improvizovanému technickému návrhu a implementaci. Cílem této knihy je poskytnout čtenářům praktickou a vyzkoušenou metodu, jak rozdělit náročný úkol nasazení protokolu IPv6 na zvládnutelné části v závislosti na místech v síti, a nabídnout přitom příklady ověřených konfigurací, které umožňují vybudovat laboratorní, pilotní a produkční síť.

Výklad postupuje poměrně konzistentně od úvodu každé oblasti nasazení přes diagramy s ukázkovými topologiemi (na relevantních místech) až po různé příklady konfigurace, které pomáhají upevnit teoretické koncepce nasazení. Díky této knize dokážete porozumět možnostem nasazení protokolu IPv6 v podniku a zjistíte, jak lze příslušné možnosti nasazení implementovat.

Cílová skupina knihy

Tato kniha je určena pro pracovníky podnikových oddělení IT a partnery nebo konzultanty, kteří poskytují podporu podnikových informačních technologií. Měli byste již ovládat základní koncepce protokolu IPv6 včetně adresování, komunikace sousedních zařízení a směrovačů a směrování. Některé kapitoly sice představují úvod do určitých témat a principů, ale žádná z nich není natolik podrobná, aby mohla začátečníkům v oblasti IPv6 sloužit jako jediný zdroj informací ohledně základního fungování protokolu. Kniha předpokládá, že čtenář má podrobné znalosti síťových technologií, síťového návrhu a praktického nasazení. Kniha vychází z dlouhodobě platných optimálních postupů návrhu společnosti Cisco, které se týkají návrhu sítí vrstvy 2 a vrstvy 3. Nejedná se o úvodní text síťového návrhu ani úvod do protokolu IPv6.

Struktura knihy

Knihu sice můžete přečíst od první do poslední stránky, ale je sestavena tak, aby bylo možné snadno přecházet mezi kapitolami a jejich částmi a vyhledat pouze aktuálně potřebné informace.

Kapitoly 1–4 poskytují úvod do nasazení protokolu v podnicích a obsahují následující úvodní témata:

- **Kapitola 1 „Obchodní důvody pro nasazení protokolu IPv6“** – tato kapitola rozebírá obvyklé obchodní a technické důvody pro nasazení protokolu IPv6 v podniku. Zmiňuje rostoucí trend nasazení protokolu a uvádí běžné příklady jeho použití.
- **Kapitola 2 „Hierarchický návrh sítě“** – tato kapitola poskytuje přehled známého a propracovaného hierarchického modelu návrhu sítí a poskytuje čtenáři základy principů návrhu sítí, na kterých staví další kapitoly knihy.
- **Kapitola 3 „Běžné mechanismy koexistence protokolu IPv6“** – v této kapitole budeme diskutovat několik obvyklých mechanismů koexistence protokolů (také se označují jako přechodové mechanismy), které se používají v podnikovém prostředí. Kapitola představuje duální sadu protokolů, tunely ISATAP, 6to4 a další metody.
- **Kapitola 4 „Síťové služby“** – tato kapitola zkoumá běžné síťové služby, které se používají ve většině implementací protokolu IPv6. Patří k nim vícesměrové vysílání protokolu IPv6, technologie QoS (quality of service) a směrovací protokoly. Další příklady nasazení těchto služeb naleznete ve zbývajících kapitolách knihy.

Kapitoly 5–12 se zaměřují na vlastní nasazení protokolu IPv6 v podnikové síti a mají mnohem techničtější povahu:

- **Kapitola 5 „Plánování nasazení protokolu IPv6“** – tato kapitola poskytuje informace o všeobecných hlediscích před nasazením protokolu IPv6 a fázích nasazení. Kapitola poskytuje systematický pohled na plánování nasazení protokolu IPv6.
- **Kapitola 6 „Nasazení protokolu IPv6 v areálových sítích“** – kapitola se zabývá možnostmi nasazení, které se nejčastěji uplatňují v prostředí areálových sítí. Podrobně rozebírá různé mechanismy koexistence a také konfigurace, které umožňují v areálové

síti úspěšně nasadit protokol IPv6 s vysokou dostupností. Analyzuje také pokročilé technologie, jako je systém virtuálního přepínání Cisco.

- **Kapitola 7 „Nasazení virtualizovaných sítí IPv6“** – tato kapitola diskutuje různá řešení virtualizace sítí, zařízení, pracovních stanic a serverů a poskytuje příklady konfigurace některých uvedených řešení včetně 6PE a 6VPE.
- **Kapitola 8 „Nasazení protokolu IPv6 v sítích WAN a pobočkových sítích“** – tato kapitola nabízí různé scénáře návrhu sítí WAN a pobočkových sítí a uvádí podrobné příklady konfigurace různých zařízení a služeb sítí WAN a pobočkových sítí včetně sítí DMVPN (Dynamic Multipoint VPN) a firewallu Cisco ASA.
- **Kapitola 9 „Nasazení protokolu IPv6 v datovém centru“** – tato kapitola popisuje běžné technologie, služby a produkty v datovém centru a postupuje od společného návrhu směrem k různým konfiguracím, které mohou čtenáři využít ve svém vlastním prostředí. Rozebírá různé produkty určené pro datová centra, jako např. Cisco Nexus 7000, 1000v a MDS 9000 spolu s jinými produkty a technologiemi (Cisco NAM, ASA atd.).
- **Kapitola 10 „Nasazení protokolu IPv6 v sítích VPN pro vzdálený přístup“** – tato kapitola představuje možnosti, jak povolit protokol IPv6 v prostředí sítí VPN pro vzdálený přístup. Uvádí příklady, jak povolit protokol IPv6 ve starší síti VPN (produktech bez podpory tohoto protokolu), a vysvětluje použití řešení Cisco ASA a AnyConnect SSL VPN v prostředí protokolu IPv6.
- **Kapitola 11 „Správa sítí IPv6“** – tato kapitola je zaměřena na běžné komponenty pro správu, které se používají v implementacích protokolu IPv6. K těmto komponentám se řadí aplikace a nástroje pro správu, funkce pro správu a informace správy přenášené protokolem IPv6.
- **Kapitola 12 „Příprava na nasazení: vytvoření laboratoře IPv6 a spuštění pilotního projektu“** – tato kapitola analyzuje nutnost a význam vyhrazené laboratoře a důležitost pilotní fáze nasazení protokolu IPv6. Předkládá praktický a systematický pohled na budování laboratoře, testování aplikací a přechod do pilotního prostředí.

KAPITOLA 1

Obchodní důvody pro nasazení protokolu IPv6

Tato kapitola se zabývá následujícími tématy:

- **Vývoj Internetu a potřeba protokolu IPv6 –** v této části se zaměříme na stávající řešení, která umožňují rozvoj Internetu, a na výhody protokolu IPv6 oproti jiným řešením. Představíme také obchodní důvody pro přechod na protokol IPv6 a projdeme nejčastější dotazy a obavy týkající se tohoto protokolu.
- **Protokol IPv6 a sdružení IETF –** protokol IPv6 se uplatňuje stále více. Standardizační tělesa, jako je sdružení IETF, proto musejí standardizovat jeho funkce, aby byla zajištěna kompatibilita všech síťových a počítačových zařízení.
- **Stav nasazení protokolu IPv6 v podnicích –** mnohé podniky uvažují o přechodu na protokol IPv6 nebo jeho nasazení plánují. Organizace v některých oborech, jako je např. maloobchod, výroba, web 2.0 a IT pro podniky, však mají v přijetí protokolu IPv6 náskok. Zajišťují podporu protokolu IPv6 u svých síťových a výpočetních zařízení a navíc ke komunikaci tímto protokolem přizpůsobují i své obchodní aplikace.

Internet se z interního distribuovaného výpočetního systému používaného v americkém Ministerstvu obrany vyvinul do podoby média, které podnikům umožňuje přicházet s inovacemi a zvyšovat produktivitu při poskytování zboží a služeb svým zákazníkům po celém světě. Celá komunikace je založena na technologii sady protokolů TCP/IP.

Internet sice nepodléhá centralizované správě, ale dohlížejí na něj globální organizace, které se starají o implementaci a správu pravidel fungování klíčových aspektů celého Internetu, jako je adresní prostor IP a systém DNS (Domain Name System). Tyto kritické prvky udržuje a spravuje organizace ICANN (Internet Corporation for Assigned Names and Numbers), která provozuje organizaci IANA (Internet Assigned Numbers Authority). Organizace ICANN/IANA přiřazují jedinečné identifikátory používané v Internetu včetně doménových názvů, IP (Internet Protocol) adres a čísel aplikačních portů.

Další informace jsou k dispozici na následujících adresách:

- ICANN – http://www.icann.org
- IANA – http://www.iana.org

Neziskové sdružení IETF (Internet Engineering Task Force, http://www.ietf.org) standardizuje klíčové protokoly. Využívá přitom technických zkušeností svých volně sdružených členů z celého světa. Příslušné protokoly se používají ve všech produktech, které poskytují síťovou konektivitu. Jednotliví výrobci hardwaru pak nabízejí vlastní uživatelské rozhraní pro konfiguraci a používání těchto protokolů.

Sdružení IETF vyhodnotilo rozvoj protokolu IP s ohledem na adresování. Zaměřilo se na následující hlediska:

- **Vyčerpání adresního prostoru** – sdružení IETF spolu s oborovými partnery z organizace IANA, registru RIR (Regional Internet Registry) a soukromého sektoru předpovídá, že fond veřejných adres protokolu IPv4 bude vyčerpán již v roce 2011.
- **Nárůst velikosti směrovacích tabulek** – metoda klasifikace a přiřazování IP adres pomocí tříd způsobila mimořádné zvětšení směrovacích tabulek směrovačů v páteřních internetových linkách.

V dalších částech kapitoly podrobněji analyzujeme některé potíže související s vyčerpáním IPv4 adres a představíme si dočasná řešení tohoto problému. Poté ukážeme, jak tato situace inspirovala sdružení IETF k vývoji protokolu IPv6.

Vyčerpání IPv4 adres a dočasná řešení

Kvůli nedostatečnému globálnímu adresnímu prostoru protokolu IPv4 musejí hostitelé používat mechanismy, které dovolují překládat interní (privátní) adresní prostor IP na menší adresní prostor (nebo dokonce na jedinou IP adresu) s možností externího směrování. Díky překladu adres NAT (Network Address Translation) může více zařízení v rámci jedné organizace používat lokální privátní adresy (RFC 1918) a přitom sdílet jednu nebo více globálních IPv4 adres k externí komunikaci. Technologie překladu adres NAT sice krátkodobě zpomalila vyčerpávání adresního prostoru IPv4, ale obecně komplikuje obousměrnou komunikaci mezi aplikacemi. Náhradní řešení typu NAT měla tyto dopady:

- Nutnost přizpůsobení bran, firewallů a aplikací, aby se jejich kód dokázal vyrovnat s přítomností překladu adres NAT nebo mechanismu PAT (například díky transparentnosti NAT pomocí protokolu UDP)
- Mapování standardních portů na nestandardní (přesměrování portů)

Vývoj a používání kódů na obcházení překladu adres NAT (STUN, TURN, ICE atd.):

- Vnořené adresy NAT/PAT
- Složitost podpůrné infrastruktury, aplikací a zabezpečení
- Složitost instalace a správy více fondů adres
- Více času, energie a financí na programování a správu náhradních řešení
- Nemožnost jasně identifikovat všechna připojená zařízení v podnikové síti

Poznámka

Senzory, i když jsou zapojeny inline, nemusejí být při zahazování paketů útočníka stoprocentně úspěšné. Než senzor inline začne zahazovat pakety, které odpovídají složené charakteristice, může již útok probíhat, i když jen v neúplné formě. Akce zahazování je u jednoduchých podpisů mnohem efektivnější, protože senzor vystačí s jedinou shodou paketu.

Poznámka

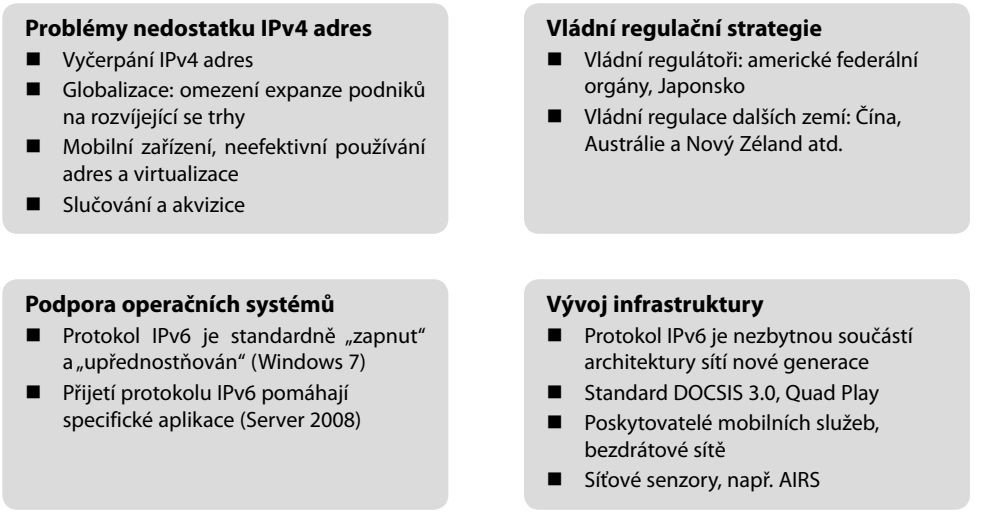
Rozhlas potřeboval k dosažení 50 milionů posluchačů 40 let. Televizi to trvalo 15 let a Internetu stačilo pouhých 5 let!

Protokol IPv6 je navržen jako náhrada protokolu IPv4. Nabízí nepředstavitelně velký počet adres a zároveň přináší snazší správu sítí, transparentnost komunikace mezi koncovými body a funkce pro zvýšení bezpečnosti a mobility, které rozebereme v následující části.

Obchodní důvody pro přechod na IPv6

Protokol IPv6 umožňuje zvýšení zisků, protože podniky mohou používat nové aplikace a rozšířit své podnikání po celém světě. Na přijetí protokolu IPv6 se podílejí čtyři faktory popsané na obrázku 1.1:

- Problémy nedostatku IPv4 adres
- Vládní strategie IT
- Vývoj infrastruktury
- Podpora operačních systémů



Obrázek 1.1: Obchodní důvody pro přechod na IPv6

Následující sekce se zabývají klíčovými tržními důvody, které jsou uvedeny na obrázku 1.1.

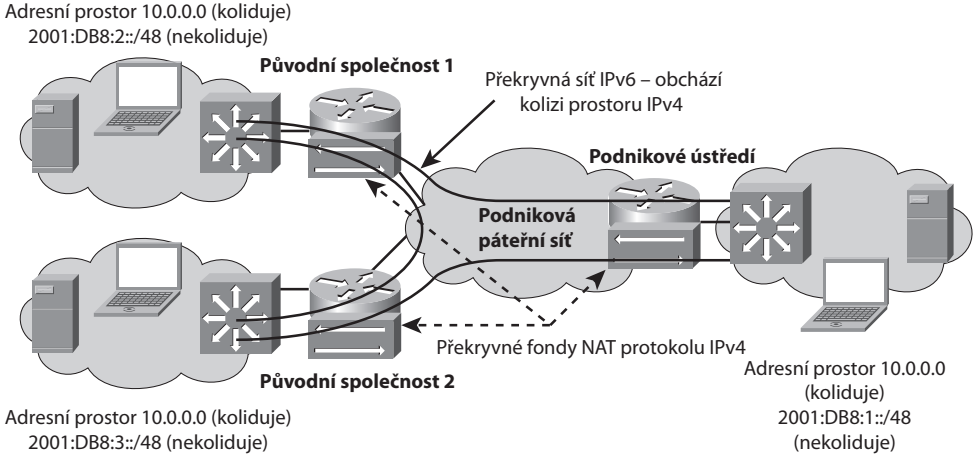
Problémy nedostatku IPv4 adres

K nasazování protokolu IPv6 přispívají následující potíže s IPv4 adresami:

- **Vyčerpání IPv4 adres** – neustále přibývá aplikací a globálních uživatelů, takže vzrůstají nároky na počet IP adres. Zároveň se zvyšuje počet zařízení, která jsou „neustále připojena", jako jsou smartphony, internetová zařízení, připojené automobily, integrované telefonní služby, mediální centra atd. Protokol IPv4 poskytuje 4,2 miliardy ($4{,}294 \times 10^9$) adres. V dnešním globalizovaném a mobilním světě je pouze otázkou času, kdy dojde k úplnému vyčerpání IPv4 adres. Hlavní důvod pro vyčerpání IPv4 adres spočívá v nedostatečné kapacitě původní internetové infrastruktury. Technologie IPv4 však dosáhla svých limitů také kvůli rostoucím požadavkům globalizovaných podniků, značnému rozšíření mobilních zařízení, virtualizaci a slučování či akvizicím firem. Dlouhodobá životnost Internetu proto vyžaduje nasazení nových technologií, jako je protokol IPv6.
- **Globalizace** – všechny podnikové transakce dnes probíhají díky počítačovým sítím. Když korporace rozšiřují svůj záběr na rozvíjející se trhy, musí zároveň růst i celá síť, což vyžaduje přidělení dalších IP adres.
- **Mobilní zařízení** – vzhledem k tomu, že je stále levnější zabudovat do mobilních zařízení poměrně výkonné počítačové čipy, mohou mobilní telefony bez problémů nabízet přístup k Internetu. Tím opět vzrůstají nároky na adresování.
- **Neefektivní používání adres** – organizace, které požádaly o IP adresy v osmdesátých letech a začátkem devadesátých let, často dostaly přiděleno mnohem více adres, než ve skutečnosti potřebovaly. Velké společnosti nebo univerzity například někdy získaly bloky adres třídy A, které obsahují více než 16 milionů IPv4 adres. Některé z těchto alokovaných bloků se nikdy nezačaly používat. Organizace, které je dostaly, se často

zmenšily, zatímco jiné organizace, na které tyto velké bloky nezbyly, se mezitím rozrostly.

- **Virtualizace** – fyzický systém nyní může hostovat mnoho virtuálních systémů. Každý z těchto virtuálních systémů může vyžadovat jednu či více IP adres. Jako příklad lze uvést infrastrukturu VDI (Virtual Desktop Infrastructure) a nasazení systémů HVD (Hosted Virtual Desktop).
- **Slučování a akvizice** – když se jedna společnost sloučí s jinou nebo ji pohltí, dochází často ke konfliktu neboli „kolizi" v privátním schématu adresování IPv4 dle standardu RFC 1918. Obě společnosti mohou například používat stejný adresní prostor 10.x.x.x (jako je znázorněno na obrázku 1.2). Mnoho společností v těchto situacích přechodně nasazuje překryvný fond NAT, kde obě původní firmy mezi sebou komunikují prostřednictvím nepřekrývajícího se adresního prostoru, jako např. 172.16.x.x. Hostitelé v obou původně samostatných společnostech mohou díky tomu komunikovat, dokud není jedna část společnosti přečíslována.



Obrázek 1.2: Překryvný model IPv6 – řešení kolize adres po sloučení firem či akvizici

Protokol IPv6 v tomto scénáři pomáhá zmírnit náklady na řešení kolize adresních prostorů slučovaných firem. Zavádí totiž „překryvnou" síť protokolu IPv6, v níž kritické systémy a hostitelé podporují protokol IPv6 a mohou prostřednictvím této překryvné sítě vzájemně komunikovat. Tímto způsobem lze rychle zajistit konektivitu hostitelů a poskytnout oddělení IT čas, aby buď přečíslovalo adresy v síti IPv4 jedné původní firmy, nebo raději v obou firmách nasadilo síť IPv6 s duální sadou protokolů.

Vládní strategie IT

Mnoho podniků a poskytovatelů služeb po celém světě implementovalo protokol IPv6, aby vyhovělo strategiím IT a podobným programům svých vlád (tj. jedná se o soukromé společnosti, které pracují pro vládní organizace). Vládní nařízení ovlivnilo nasazení protokolu IPv6 v soukromém sektoru například v USA, kde mnoho smluvních dodavatelů ministerstva obrany rychle začalo s plánováním a nasazením protokolu IPv6, aby vyhovělo federálnímu

nařízení o IPv6 z 30. června roku 2008. Kromě toho, že jsou mnohé z těchto společností propojeny se sítěmi federálního úřadu, poskytují také služby a produkty založené na protokolu IP, které budou časem přecházet na verzi IPv6.

Vývoj infrastruktury

Vývoj základní infrastruktury Internetu spolu se změnami v souvisejících oborech, jako je řízení spotřeby a distribuce energie, dospěly do fáze, kdy existující technologie, produkty i protokoly jako IPv4 přestávají stačit. Evoluce technologií inteligentních rozvodných sítí, širokopásmového kabelového připojení a mobilních operátorů znamená, že se nyní k Internetu připojuje stále více zařízení. Ať už se jedná o libovolnou aplikaci nebo technologii, platí, že ke své komunikaci využívá protokol IP nebo jej brzy využívat začne. Protokol IPv4 tyto požadavky nedokáže uspokojit. V každém směru vývoje proto cestu vpřed představuje protokol IPv6.

Podpora operačních systémů

Všechny široce nasazené operační systémy standardně obsahují podporu protokolu IPv6. Tyto operační systémy umožňují používat IPv6 adresy již ve svém výchozím nastavení, což urychluje přijetí protokolu IPv6 v podnikových sítích. K důležitým operačním systémům patří Microsoft Windows 7, Server 2008, Apple Mac OS X a Linux. Mnoho podniků s překvapením zjišťuje, že protokol IPv6 se v jejich sítích již používá, což je způsobeno standardním upřednostňováním protokolu IPv6 před protokolem IPv4. Pracovníci oddělení IT si uvědomují, že se musejí s protokolem IPv6 seznámit a implementovat jej řízeným způsobem. Mohou si tak udržet kontrolu nad jeho chováním a zároveň využít jeho možností.

Shrnutí výhod protokolu IPv6

Tržní impulzy nebo iniciativy často přicházejí zvnějšku podniku a mohou být vynuceny oborovými trendy nebo jinými externími silami (například vyčerpáním internetových IPv4 adres). V jiných případech může podnik usilovat o obchodní či technické výhody. Tabulka 1.1 představuje shrnutí několika hlavních výhod, které mohou podniky získat nasazením protokolu IPv6. O několika z nich už jsme se v této kapitole zmínili a mnoha dalšími se budeme podrobně zabývat v dalších částech knihy.

Nejčastější dotazy týkající se protokolu IPv6

Protokol IPv6 se objevil již před více než deseti lety, ale většina organizací se o něj až donedávna nezajímala. Teprve nyní, když je nedostatek IPv4 adres zřejmý i těm nejzatvrzelejším skeptikům, začíná vzrůstat povědomí o tomto protokolu a zájem o něj.

V následujících částech rozebereme některé často kladené dotazy a mýty, které s protokolem IPv6 souvisejí.

Je protokol IPv6 nezbytným předpokladem podnikového růstu?

Tato otázka je kladena nejčastěji, zejména proto, že většina organizací se v současnosti k Internetu připojuje bez protokolu IPv6. Organizace mohou protokol IPv6 potřebovat ze tří hlavních důvodů:

- Jejich dlouhodobý rozvoj a globální růst vyžaduje větší adresní prostor (nad rámec protokolu IPv4).
- Protokol IPv6 také generuje nové příležitosti a nabízí platformu inovací. Existují celé třídy síťových aplikací, které protokol IPv4 neumožňuje – například telemetrie ve vozidlech, kdy lze do automobilů instalovat miliony senzorů připojených k síti.
- V operačních systémech jako Windows 7 a Linux je podpora protokolu IPv6 standardně zapnuta.

Země vykazující vysoký ekonomický růst jako Indie a Čína, které mají velkou populaci a stále více technicky vzdělaných odborníků, téměř jistě přejdou na protokol IPv6 přímo. Podniky, které chtějí na těchto trzích působit, ale protokol IPv6 přitom samy nepoužívají, budou konkurenčně znevýhodněny.

Tabulka 1.1: Výhody protokolu IPv6

Technické výhody protokolu IPv6	Podrobnosti
Hojnost IP adres	Jedná se o nejzásadnější výhodu protokolu IPv6 oproti verzi IPv4. IPv6 adresu tvoří 128bitové hodnoty místo tradičních 32 bitů v protokolu IPv4. Nový protokol proto poskytuje přibližně 340 bilionů bilionů bilionů globálně směrovatelných adres.
Jednodušší nasazení adres	Každý hostitel, který chce komunikovat se síťovými prostředky, musí mít přiřazenu IP adresu. Tato IP adresa se tradičně přiřazovala ručně nebo získávala pomocí DHCP. Kromě přiřazení adresy ručně a službou DHCP je v protokolu IPv6 standardně dostupná automatická konfigurace adres metodou SLAAC (Stateless Address Autoconfiguration), která urychluje a zjednodušuje nasazení koncových bodů s podporou protokolu IP. Metoda SLAAC často slouží ke konfiguraci zařízení, která nevyžadují interakci s koncovými uživateli. Může se jednat o síťové senzory v automobilech, telemetrická zařízení, výrobní stroje atd. U hostitelů s uživatelským rozhraním, jako jsou pracovní stanice a servery, je nasazení metody SLAAC omezeno chybějícími informacemi DNS v oznámení směrovače. Komunita IETF sepsala experimentální koncept (RFC 5006), který rozšiřuje zprávy oznámení směrovače (zprávy RA) o informace DNS. Standardizační těleso usiluje také o standardy rozšíření RA, které by kromě informací serveru DNS zahrnovaly také možnosti protokolů NTP, BOOTP a DHCP specifické pro dodavatele. V závislosti na implementaci hostitelského operačního systému si aktivovaný síťový adaptér IPv6 přiřadí IP adresu s použitím dobře známého prefixu a vlastní MAC adresy. Nový hostitel mechanismem automatické konfigurace odvodí vlastní adresu z informací, které poskytují sousední směrovače. Spoléhá přitom na protokol označovaný ND (neighbor discovery – zjišťování sousedů). Tato metoda nevyžaduje žádný zásah ze strany správce a není potřeba ani udržovat centrální server přiřazující adresy. To představuje další výhodu oproti protokolu IPv4, kde automatické přidělování adres vyžaduje server DHCP.

Technické výhody protokolu IPv6	Podrobnosti
Integrita síťové konektivity mezi koncovými body	Při použití překladu adres NAT protokolu IPv4 maskuje jediná adresa tisíce adres, které neumožňují směrování. Nelze proto dosáhnout integrity spojení mezi koncovými body. Díky většímu adresnímu prostoru, který poskytuje protokol IPv6, nejsou zařízení typu NAT prakticky nadále potřebná.
Možnost nasazení silnějších bezpečnostních funkcí oproti protokolu IPv4	I když se v současnosti příliš nepoužívají, protokol IPv6 obsahuje integrované bezpečnostní funkce s podporou protokolu IPSec, které umožňují šifrování kontrolních paketů (přilehlé směrovače, zjišťování sousedů) přenášených mezi dvěma nebo více hostiteli. Při šifrování vlastních dat toku se protokol IPv6 spoléhá na stávající mechanismy protokolu IPv4, jako je IPSec.
Zdokonalené rozšiřující hlavičky atributů pro zabezpečení, kvalitu služby a šifrování	Protokol IPv6 obsahuje rozšiřující hlavičky atributů, které nejsou součástí základní hlavičky paketu. Tyto rozšiřující hlavičky se svou unikátní strukturou paketu umožňují využívat šifrování, mobilitu, optimalizované směrování a další funkce. Uvedené hlavičky se v případě potřeby vkládají mezi základní hlavičku IPv6 a datovou část. Základní hlavička IPv6 obsahuje informaci o přítomnosti rozšiřujících hlaviček v poli Next Header (Další hlavička). Tato koncepce značně urychluje předávání paketů ve směrovačích a zvyšuje efektivitu.
Vyšší mobilita	Protokol MIP (Mobile IP) zajišťuje, že původní brána dostane informace o tom, že se hostitel přesunul z jednoho síťového segmentu do jiného. V původní verzi protokolu MIP (založená na IPv4) je nutné veškerý příchozí i odchozí provoz mobilního zařízení přenášet zpět původní (domovské) bráně. Označuje se to jako „trojstranné směrování". V protokolu IPv6 došlo k rozšíření metody MIP, která tyto neefektivní trojstranné přenosy odstraňuje. V protokolu MIPv6 je cizí korespondenční server neustále informován o tom, ve které síti se zařízení nachází a pomocí které brány lze cestující zařízení kontaktovat. Převážná většina paketů prochází přímo mezi mobilním zařízením a stranami, se kterými komunikuje, nikoli přes domovskou adresu zařízení. Tento proces se označuje jako *přímé směrování* (direct routing). Klesají tím náklady a výrazně roste výkon a spolehlivost.
Lepší přidělování prostředků toku díky značkám toku	Protokol IPv6 zachovává všechny atributy kvality služby (QoS) jako Differentiated Services (DiffServ) a Integrated Services (IntServ) z protokolu IPv4. Protokol IPv6 navíc používá 20bajtové pole Flow Label (Značka toku), kde může koncová aplikace definovat přidělení prostředků pro konkrétní aplikaci nebo typ toku. Standardizační orgány sice definovaly konkrétní značky toku protokolu IPv6, ale tuto možnost zatím využívají jen málokteré podnikové aplikace.

Nahradí protokol IPv6 verzi IPv4 kompletně?

Protokoly IPv6 a IPv4 budou souběžně fungovat dlouhou dobu, než celá infrastruktura přejde na výhradní používání protokolu IPv6. Podniky a poskytovatelé služeb značně investovali do protokolu IPv4 a jsou s touto technologií dobře obeznámeni.

Vzhledem k nárůstu nasazení protokolu IPv6 musejí podniky investovat do řešení, která umožní, aby jejich starší sítě hladce a efektivně komunikovaly se sítěmi IPv6. Tímto způsobem zvýší návratnost svých investic. Shrnuto: podniky, které uvažují o přijetí protokolu IPv6, nemusejí svou infrastrukturu IPv4 odepisovat. Místo toho mohou využít přechodové technologie, které zajistí souběžný provoz obou protokolů.

Je protokol IPv6 v porovnání s protokolem IPv4 složitější a náročnější na správu a nasazení?

Větší adresní prostor IP poskytovaný protokolem IPv6 vzbuzuje u síťových návrhářů a správců dojem, že protokol IPv6 je v porovnání s protokolem IPv4 složitější. To je však omyl. Díky rozsáhlému adresnímu prostoru již síťoví architekti nemusejí měnit konfiguraci omezeného adresního prostoru a návrh sítí se tím značně zjednodušuje.

Všechny pomocné protokoly jako DNS fungují v protokolech IPv4 a IPv6 víceméně stejně. Protokol IPv6 kromě toho obsahuje lepší možnosti automatické konfigurace a vícesměrového vysílání (s integrovaným shromaždištěm – rendezvous point), které se oproti protokolu IPv4 implementují snáze.

K dispozici je několik nových pomocných protokolů, jako například MLD (multicast listener discovery) a ND (neighbor discovery), které však převážně nahrazují podobné mechanismy v protokolu IPv4.

S odhlédnutím od hexadecimálního formátu adres protokolu IPv6 lze přidělování adres snáze plánovat a implementovat. Není totiž nadále nutné se zaměřovat na počet hostitelů, ale spíše na počet linek neboli „podsítí", které adresní blok umožňuje přidělit. Z mnoha hledisek je protokol IPv6 pouze starým protokolem IP s vyšším číslem verze. Podobně jako u protokolu IPv4, také protokol IPv6 vyžaduje návrh adresního plánu, který zajišťuje, že budou adresy v síti přirozeně uspořádány.

Aby dokázala funkce protokolu IPv6 využít celá oddělení IT (včetně návrhářů sítí, výpočetních systémů a úložišť, správců, vývojářů aplikací atd.), je nutné investovat do příslušných školení týkajících se této nové technologie.

Umožní protokol IPv6 připojení podnikové sítě k více poskytovatelům služeb?

Před rokem 2007 platily přísně hierarchické zásady přidělování IPv6 adres. Podniky tehdy mohly získat síťové adresy pouze od jediného poskytovatele služeb, aby nedocházelo k překrývání v globální směrovací tabulce.

Roku 2007 se tato pravidla změnila a podniky nyní mohou dostat přiděleny bloky nezávislé na poskytovateli (PI – provider-independent) podobně jako u protokolu IPv4. Když organizace požádá o prostor PI, může dostat adresní prostor IPv6, který není vázán na žádného poskytovatele.

Díky přiděleným adresám nezávislým na poskytovateli mohou podniky i nadále budovat redundantní a spolehlivá řešení obdobná stávajícím architekturám protokolu IPv4.

Odborníci však vyvíjejí mnoho nových prvků a diskutují o změnách zásad, což může ovlivnit připojování k více poskytovatelům u protokolu IPv6. Všechny otázky související s touto problematikou stále nejsou zodpovězeny. Je vhodné sledovat výstupy standardizačních těles a kontaktovat stávající poskytovatele služeb, kteří poskytnou aktuální informace o příslušných změnách.

Nabízí protokol IPv6 vyšší kvalitu služby?

Jediný mechanismus QoS integrovaný do protokolu IPv6 představuje několik polí hlavičky, která mají rozlišovat pakety patřící do různých tříd provozu a identifikovat související pakety jako „tok" (flow). Díky těmto polím hlavičky by měla zařízení typu směrovačů identifikovat toky a typy provozu a snadno v těchto informacích vyhledávat. V praxi jsou tyto prvky hlavičky zcela nepovinné. To znamená, že naprostá většina zařízení neusiluje o nic jiného než o minimální požadovanou úroveň kompatibility.

Protokol IPv4 však obsahuje odpovídající prvky hlavičky, které mají sloužit k podobným účelům. Sotva lze tedy tvrdit, že technologie QoS u protokolu IPv6 je na vyšší úrovni než u protokolu IPv4.

Je protokol IPv6 automaticky bezpečnější než IPv4?

Přesnější by bylo prohlásit, že protokol IPv6 není ani méně, ani více bezpečný než protokol IPv4. Je prostě jiný. Hlavním bezpečnostním mechanismem integrovaným do architektury IPv6 je IPSec. Každá implementace protokolu IPv6 založená na dokumentech RFC a kompatibilní se standardy musí podporovat zabezpečení IPSec. Povolení nebo zapnutí této funkce však není povinné. Integrace šifrování vede k mylnému závěru, že protokol IPv6 je automaticky bezpečnější než verze IPv4. Platí však, že nový protokol i nadále vyžaduje pečlivou implementaci a poučené systémové a síťové správce.

Snižuje chybějící podpora překladu adres NAT v protokolu IPv6 jeho bezpečnost?

Názor, že překlad adres NAT posiluje bezpečnost, je z větší části mýtem. Metoda NAT má řešit nedostatek IPv4 adres. Vzhledem k tomu, že protokol IPv6 žádným nedostatkem netrpí, sítě IPv6 překlad adres NAT nepotřebují. Pokud někdo považuje NAT za bezpečnostní mechanismus, může to chápat jako snížení bezpečnosti protokolu IPv6 v porovnání s IPv4. Překlad adres NAT však žádné účinné zabezpečení neposkytuje. Koncepce „bezpečnosti díky skrývání" je převážně překonaná. Naprostá většina útoků totiž nevyužívá metody založené na přímém IP směrování z Internetu do vnitřní podnikové sítě, ale jedná se spíše o útoky na vrstvách 4–7. Návrh protokolu IPv6 usiluje o to, aby byl překlad adres NAT zbytečný. Standard RFC 4864 pak přichází s koncepcí LNP (Local Network Protection) založené na protokolu IPv6. Tato technologie přitom poskytuje minimálně stejné bezpečnostní výhody jako překlad adres NAT.

Protokol IPv6 a sdružení IETF

Sdružení IETF již od roku 1995 aktivně pracuje na vývoji konceptů a standardů týkajících se protokolu IPv6. Scházejí se přitom pracovní skupiny, které působí v těchto oblastech:

- Aplikace
- Internet
- Provoz a správa
- Aplikace fungující v reálném čase a infrastruktura

- Směrování
- Zabezpečení
- Transport

Aktivitu na poli standardizace protokolu IPv6 vyvíjejí zejména skupiny zaměřené na Internet, provoz a správu a transport. Tyto skupiny byly a často dosud jsou velmi činné při vývoji standardů týkajících se adresování, nasazení, správy, přechodu na protokol IPv6 a jeho zabezpečení. U implementací protokolu IPv6 a souvisejících prvků architektury je zásadně důležité, aby odpovídaly standardům, což zajišťuje kompatibilitu zařízení od různých dodavatelů.

Sdružení IETF publikuje mnoho konceptů a standardů RFC, které jsou často aktualizovány. Chcete-li být na změny protokolu IPv6 připraveni, měli byste výstupy sdružení IETF a jiných standardizačních těles pečlivě analyzovat. Další informace naleznete na webu http://www.ietf.org.

Kromě sdružení IETF existuje také program organizace IPv6 Forum s logem IPv6 Ready, které certifikuje, že infrastruktura IT (sítě, počítače a úložiště) dodržuje standardy IPv6 a umožňuje interoperabilitu. Uvedený program slouží hlavně ke zvýšení důvěry uživatelů v protokol IPv6, který je již k dispozici a připraven k použití. Komise IPv6 Ready Logo Committee definuje požadavky testů, které kontrolují soulad se standardy a interoperabilitu. Dodavatelé pak v těchto testech mohou získat certifikát, že jejich produkty jsou připraveny na protokol IPv6. Další podrobnosti o logu IPv6 Ready a certifikovaných produktech naleznete na adrese http://www.ipv6ready.org.

Stav nasazení protokolu IPv6 v podnicích

Po více než patnácti letech zastoupení ve standardizačních orgánech a deseti letech vývoje v současnosti protokol IPv6 přijalo mnoho velkých poskytovatelů služeb a podniků. IPv6 je nyní robustní a vyspělý protokol, který umožňuje modernizovat staré aplikace a vyvíjet nové. Protokol IPv6 se prosazuje v mnoha vertikálních oborech (viz tabulku 1.2).

Tabulka 1.2: Nasazení protokolu IPv6 v rámci vertikálních trhů

Vertikální trh	Příklady
Vyšší vzdělávání a výzkum	Vývoj senzorů
	Mediální služby
	Kolaborace
	Mobilita
Výroba	Integrovaná zařízení
	Průmyslový Ethernet
	Komponenty s podporou IP

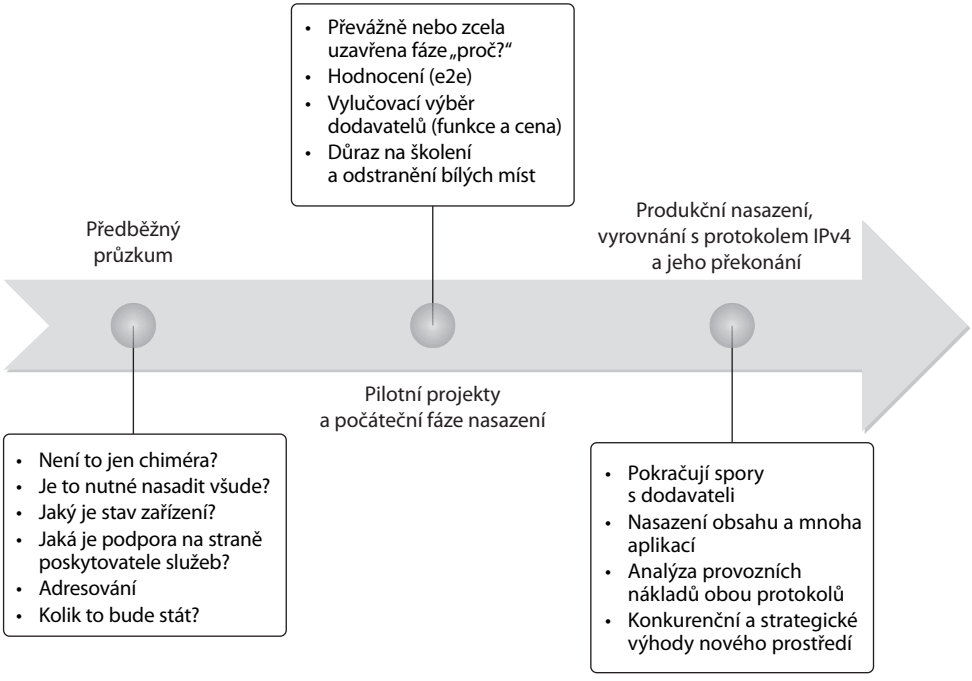
Vertikální trh	Příklady
Vláda (státní a veřejný sektor)	Ministerstvo obrany USA
	Síť WIN-T (Warfighter Information Network-Tactical)
	Systém FCS (Future Combat System)
	Systém JTRS (Joint Tactical Radio System)
	Technologie GIG-BE (Global Information Grid Bandwidth Expansion)
Doprava	Telematika
	Řízení dopravy
	Hotspoty
	Přepravní služby
Finance	Slučování a akvizice – překryvné sítě
Zdravotní péče	Domácí péče
	Bezdrátové sledování inventáře
	Vyšetřování
	Mobilita
Spotřebitel	Set-top boxy
	Internetové hry
	Jednoúčelová zařízení
	Zvuk a video
	Bezpečnostní sledování
Rozvodné podniky	SmartGrid
	Služby IP po rozvodech elektřiny

Protokol IPv6 se zpočátku používal pouze v oblastech výzkumu a prodeje, kde vznikly jeho první praktické implementace. Od té doby proniká protokol IPv6 na všechny oborové trhy. V některých případech se přitom jedná o specifické případy nasazení, jako například sítě senzorů, robotické paže či udržování stálého prostředí. Jindy se tento protokol používá stejným způsobem bez ohledu na obor.

Většinu podniků lze zařadit do jedné ze tří kategorií, které jsou znázorněny na obrázku 1.3.

První kategorie se často označuje jako fáze předběžného průzkumu. Podnik zde analyzuje, zda protokol IPv6 skutečně funguje, jaké má výhody, jak zapadá do podnikového prostředí, jaké mezery zaplňuje a jaké budou náklady na jeho nasazení. V této fázi je nutné seznámit podnikové vedení s významem protokolu IPv6, který umožní dosáhnout proměnlivých podnikových cílů. Technické oddělení IT se ve fázi předběžného výzkumu musí seznámit s principy protokolu IPv6 a s tím, jak jeho fungování závisí na stávající infrastruktuře. Přitom se využívají pracovní skupiny, školení a praktické instalace. Mnohé podniky v této fázi zatím nevědí, zda je pro ně protokol IPv6 relevantní.

Druhá kategorie představuje fázi pilotních projektů a počátečního nasazení. Většina otázek již byla zodpovězena nebo alespoň padlo rozhodnutí o tom, že protokol IPv6 bude nasazen bez ohledu na to, zda k tomu existují jednoznačné obchodní důvody. Nasazení protokolu IPv6 bez jasného ekonomického zdůvodnění se často přirovnává k „přípravě domu na neznámého hosta“. Mnoho techniků, kteří zažili počáteční fáze rozvoje technologií VoIP a IP telefono-



Obrázek 1.3: Kategorie přijetí v podnicích

vání si vzpomínají, že nebyli dostatečně připraveni na související zásadní posun paradigmatu a jejich sítě neposkytovaly vysokou dostupnost (alespoň na úrovni nutné pro přenos hlasu) a dostatečnou kvalitu služby. Při investování času, energie a finančních prostředků do protokolu IPv6 bez definovaných obchodních požadavků je mnohdy nutné se připravit na neznámé. V této fázi probíhají pečlivější hodnocení, začínají školení a dochází ke komunikaci s dodavateli produktů, které nejsou kompatibilní s protokolem IPv6.

Poslední třetí kategorie odpovídá produkční fázi, kdy podnik usiluje o špičkové produkční nasazení protokolu IPv6. V této etapě probíhá rychlý přesun většiny nebo dokonce všech prvků infrastruktury IT na protokol IPv6. Cílem je dosáhnout stejné funkční úrovně jako u protokolu IPv4 nebo minimálně natolik kvalitních služeb, které nebudou narušovat činnost podniku. Podnik se ještě v této fázi může zabývat nekompatibilními produkty nebo dodavateli, ale většina podobných případů je již vyřešena výměnou dodavatelů, kteří nemají jasný plán. Podnik se vrací ke standardnímu fungování, ale zároveň se soustřeďuje na to, aby využil aplikace a služby s podporou protokolu IPv6 jako svou konkurenční výhodu.

V celém procesu probíhá neustálé vzdělávání v technických i obchodních aspektech. V každé fázi je pak potřeba zajistit, že budou všechny zainteresované skupiny směřovat za společným cílem.

Přijetí protokolu IPv6 se často setkávalo s potížemi. Podniky jej totiž nechtěly nasazovat vzhledem k tomu, že podporu protokolu IPv6 poskytovala jen malá část produktů a většina poskytovatelů služeb nezajistila nasazení protokolu IPv6 ve svých přípojných bodech. Poskytovatelé služeb neposkytovali podporu proto, že se na ni podniky nedotazovaly, případ-

ně proto, že ji většina produktů neumožňovala. Dodavatelé pak nevyvíjeli produkty kompatibilní s tímto protokolem, protože o ně nežádali podnikoví zákazníci ani poskytovatelé služeb. Jednalo se (a někde stále jedná) o začarovaný kruh, který mohou přerušit pouze inovátoři a vůdčí osobnosti, které udělají první krok.

Z hlediska poskytovatelů obsahu patří mezi propagátory nasazení protokolu IPv6 společnost Google, která spustila program zpřístupnění svých služeb pomocí protokolu IPv6: http://www.google.com/ipv6. Mnoho poskytovatelů obsahu a významných webů již nabízí podporu protokolu IPv6 pro hostitele, kteří je tímto protokolem dokáží kontaktovat. K těmto webům patří Google (vyhledávání a služba Gmail), YouTube, Netflix, Comcast a Facebook.

Navzdory názorům odborných časopisů, blogů, dodavatelů a různých skeptiků platí, že podniky již s nasazováním protokolu IPv6 začaly a v současnosti v tom pokračují. Mnoho společností se nasazováním protokolu IPv6 nechlubí, což vede k mylnému dojmu, že se nic neděje. Společnosti často zavádění protokolu IPv6 utajují buď z bezpečnostních důvodů (neznají všechny vektory útoků a nemají zatím k dispozici dostatečná bezpečnostní opatření), nebo z důvodů finančních. Diskuzi těchto aspektů a rozbor důležitých hledisek nasazení protokolu IPv6 naleznete v dalších kapitolách této knihy.

Shrnutí

IPv6 je internetový protokol nové generace, který překonává omezení adres v protokolu IPv4 a zcela odstraňuje nebo výrazně redukuje výskyt situací, kdy je nutné použít překlad adres NAT či mechanismus PAT. Hlavní důvod pro přijetí protokolu IPv6 spočívá v mimořádném počtu adres, který poskytuje. Firmy se tak mohou bezproblémově rozvíjet a lze vyvíjet nové internetové aplikace.

Sdružení IETF a další organizace nadále vyhodnocují možná řešení a připravují koncepty a standardy RFC, aby byla zajištěna interoperabilita hostitelů s podporou protokolu IPv6.

Většina poskytovatelů služeb a obsahu spolu s mnoha podniky nasazení protokolu IPv6 ve své síťové infrastruktuře plánuje, realizuje nebo tento protokol již nasadila, aby dokázala držet krok s novými aplikacemi.

Cílem této knihy je poskytnout podnikům a poskytovatelům služeb koncepční rámec, který jim pomůže při hladkém přechodu na protokol IPv6 pomocí existujících technologií. Kniha také popisuje způsoby, jak lze protokol IPv6 integrovat do stávající podnikové infrastruktury.

Další odkazy

Poznámky v této kapitole často zmiňují, že je nutné kompletně porozumět technologickým aspektům protokolu IPv6. Při implementaci protokolu IPv6 je nutné zohlednit mnoho aspektů návrhu včetně zabezpečení, kvality služby, dostupnosti, správy, školení IT a podpory aplikací.

Následuje přehled vybraných zdrojů informací, které obsahují další podrobnosti o protokolu IPv6, doporučeních společnosti Cisco pro návrháře, produktech a řešeních a dění v oboru:

Aoun, C. a E. Davies. RFC 4966, „Reasons to Move the Network Address Translator Protocol Translator (NAT-PT) to Historic Status“ (Důvody, proč nadále považovat překlad protokolů – NAT-PT – za historickou záležitost). http://www.rfc-editor.org/rfc/rfc4966.txt.

Cerf, Vinton G. „A Decade of Internet Evolution“ (Deset let vývoje Internetu). http://bit.ly/cNzjga.

Curran, J. RFC 5211, „An Internet Transition Plan“ (Plán přechodu Internetu na protokol IPv6). http://www.rfc-editor.org/rfc/rfc5211.txt.

IANA: http://www.iana.org.

ICANN: http://www.icann.org.

IETF: http://www.ietf.org.

IETF Behavior Engineering for Hindrance Avoidance (behave) drafts (Koncepty IETF týkající se obcházení komunikačních překážek): https://datatracker.ietf.org/wg/behave.

IPv6 address report (Zpráva o adresování IPv6): http://www.potaroo.net/tools/ipv4.

Jeong, J., S. Park, L. Beloeil a S. Madanapalli. RFC 5006, „IPv6 Router Advertisement Option for DNS Configuration“ (Možnost oznámení směrovače IPv6 v konfiguraci DNS). http://www.rfc-editor.org/rfc/rfc5006.txt.

Rekhter, Y., B. Moskowitz, D. Karrenberg, J. de Groot a E. Lear. RFC 1918, „Address Allocation for Private Internets“ (Přidělování adres v privátních sítích). http://www.rfc-editor.org/rfc/rfc1918.txt.

Van de Velde, Hain, Droms, Carpenter a Klein. RFC 4864, „Local Network Protection for IPv6“ (Ochrana lokální sítě protokolu IPv6). http://www.rfc-editor.org/rfc/rfc4864.txt.

KAPITOLA 2

Hierarchický návrh sítě

Tato kapitola se zabývá následujícími tématy:

- **Principy návrhu sítí** – v této části rozebereme tři základní aspekty návrhu podnikových sítí: modularita, hierarchie a odolnost. V dalších částech uvedené koncepce rozšíříme na jednotlivé bloky podnikové sítě. Poté přejdeme k podrobnostem jednotlivých modulů.
- **Návrh jádra podnikové sítě** – v této části analyzujeme význam jádra sítě a ukážeme si, jakými hledisky se řídí jeho návrh.
- **Návrh podnikové areálové sítě** – v této části si představíme různé možnosti návrhu areálové sítě pro přístupově-distribuční bloky.
- **Návrh podnikových síťových služeb** – v této části vysvětlíme význam síťových služeb, když podniky přecházejí od nativního nasazení protokolu IPv4 k návrhu s duální sadou protokolů IPv4/IPv6.
- **Návrh sítě podnikového datového centra** – v této části prozkoumáme návrh sítí, které se instalují v datových centrech, a síťové funkce nakonfigurované na jednotlivých vrstvách. Budeme se také zabývat návrhy sítí SAN.
- **Návrh podnikové hraniční sítě** – v této části budeme diskutovat návrh a služby podnikové hraniční sítě, která zahrnuje agregaci WAN v ústředí, přístup k Internetu a pobočkovou síť.

První počítačové sítě využívaly plochou topologii, kam byla zařízení přidávána podle potřeby. Tyto ploché síťové topologie se snáze navrhovaly, implementovaly a spravovaly – za předpokladu, že počet síťových zařízení zůstával poměrně nízký. Když se k těmto sítím připojovalo stále více hostitelů, komplikovalo se řešení síťových problémů, protože chyby nebylo možné izolovat. Návrh těchto plochých sítích se také příliš nehodil k připojování velkého počtu hostitelů.

Vzhledem k problémům s plochými sítěmi prošly podniky několika fázemi návrhu sítí, které jim jednak umožnily škálování sítě spolu s růstem podniku, ale zároveň poskytly možnost izolace problematických domén. V důsledku tohoto vývoje návrhy sítí postupně zvyšovaly svou modularitu, hierarchičnost a odolnost. Tyto tři koncepce se nadále staly základem každého kvalitního návrhu sítě.

V této kapitole analyzujeme všechny tři pilíře dobrého návrhu sítě – modularitu, hierarchičnost i odolnost – a rozšíříme tyto koncepce i na segmentování podnikové sítě do menších stavebních bloků včetně jádra podnikové sítě, areálové sítě, síťových služeb, datového centra a hraniční sítě (zahrnuje připojení k Internetu, vzdálený přístup, síť WAN a připojení poboček). Kapitola rovněž rozebírá hlediska návrhu všech uvedených stavebních kamenů. Návrháři a architekti sítí tak mohou pečlivě zkontrolovat jednotlivé varianty návrhu a aplikovat tyto návrhové principy na vlastní návrhy podnikových sítí. Kapitola také poskytuje základní informace o různých síťových službách, které dále rozvíjí kapitola 4, „Síťové služby".

Principy návrhu sítí

Podnikové aplikace se v průběhu uplynulých let vyvinuly od nejjednodušších forem typu klient-server až po interaktivnější služby. Tyto aplikace nyní využívají technologie jako hlas, video a bezdrátový přístup. Přechod na kolaborativní a interaktivní aplikace znamenal výrazný posun v nárocích kladených na podnikové sítě. Proměnlivé podnikové prostředí nyní vyžaduje, aby podniková síť poskytovala tyto funkce:

- **Uživatelský dojem z kolaborativních aplikací** – stále častěji se využívají aplikace pro spolupráci, komunikaci v reálném čase, jednotné přihlášení a mobilitu. Mezi priority návrhu těchto aplikací patří snadné a příjemné používání.
- **Podpora rozmanitých typů koncových uživatelských zařízení** – podniky kromě tradičních osobních počítačů (PC) a IP telefonů stále častěji využívají bezdrátová zařízení (včetně notebooků a smartphonů s podporou Wi-Fi) a terminálů typu tenkých klientů.
- **Odolnost sítě a rychlejší konvergence** – podnikové procesy, které se přizpůsobují globalizaci a fungují 24 hodin denně 365 dní v roce, vyžadují odolnou síťovou infrastrukturu, která zajišťuje přístup k obchodním aplikacím i během upgradu či výpadku sítě.
- **Komplexní bezpečnost** – v uplynulých letech vzrostl počet a složitost bezpečnostních hrozeb. Zabezpečení sítě se proto musí vyvíjet a přizpůsobit distribuovaným a dynamickým aplikacím. Vzhledem k rozvoji obchodních kontaktů je nutné zajistit pružný přístup partnerů a hostů.

Podniková síť tvoří infrastrukturu, která propojuje koncové uživatele a zařízení. Její rozsah může být omezen na jediné patro budovy, více pater jedné budovy nebo na více budov rozmístěných ve větším areálu. Síť představuje vysokorychlostní předivo, které poskytuje základní konektivitu a nabízí sadu odolných, bezpečných a snadno řiditelných síťových služeb, které jsou potřebné k provozu klíčových podnikových aplikací. Při návrhu podnikové sítě je nutné zohlednit tři principy:

- Modularita
- Hierarchičnost
- Odolnost

Jednotlivé principy popíšeme v následujících částech kapitoly.

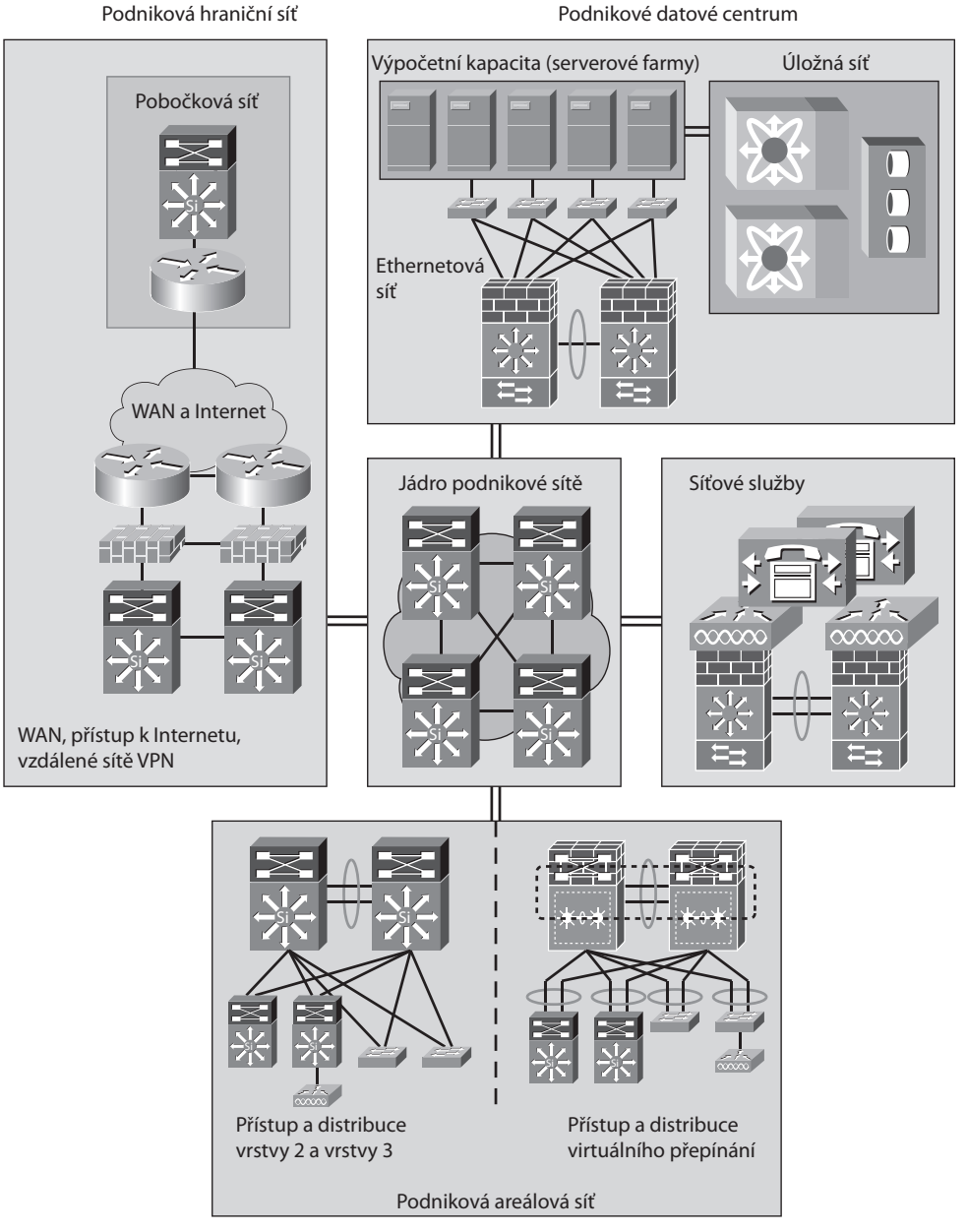
Modularita

Modularita patří mezi základní principy strukturované sítě. Definuje podnikovou síť jako množinu více stavebních kamenů, které jsou systematicky navrženy samostatně. Tam, kde je to vhodné, pak aplikuje hierarchickou strukturu a redundantnost.

Modulárnější návrh sítě sestává z nezávislých síťových bloků, které poskytují určitou funkci nebo sadu funkcí. Výpadek, upgrade nebo jiná změna jednoho modulu se proto projeví pouze v rámci jeho hranic. V modulárním návrhu sítě lze síťové služby volit s ohledem na jednotlivé moduly, ale jejich funkčnost je potřeba ověřit v rámci celkového návrhu sítě. Jak je patrné z obrázku 2.1, skládá se návrh podnikové sítě z následujících modulů:

- **Jádro podnikové sítě** – modul jádra podnikové sítě představuje páteř sítě, která propojuje moduly areálové sítě, datového centra, hraniční sítě a síťových služeb. Bez jádra sítě by všechny ostatní moduly zůstaly izolované. Jádro proto musí poskytovat své služby nepřetržitě. Návrh vrstvy jádra by měl zahrnovat dostatečnou úroveň redundance a odolnosti proti selhání, aby bylo v případě selhání síťové komponenty zajištěno neprodleně obnovení toku dat. Spolu s odolností proti selhání by měl návrh jádra sítě rovněž poskytovat rychlou konvergenci a vyrovnávání zatížení, což umožní optimální využití všech síťových prvků v rámci jádra.
- **Podniková areálová síť** – modul areálové sítě obsahuje všechny síťové prvky potřebné pro nezávislou činnost. Zabezpečuje síťovou konektivitu mezi koncovými uživateli, zařízeními a jádrem podnikové sítě. Tento modul lze dále rozložit na více vrstev s ohledem na požadovanou funkčnost a služby. Podnik může mít ve stejném geografickém umístění i více areálových bloků, pokud to vyžaduje počet uživatelů v dané lokalitě.
- **Podnikové datové centrum** – modul datového centra se skládá ze tří klíčových prvků. Jedná se o počítače (servery), síťová zařízení (ethernetové přepínače) a úložiště (Fibre Channel). Modul datového centra obsahuje výkonná výpočetní zařízení ve formě serverových farem, které hostují podnikové aplikace. Tyto serverové farmy se obvykle připojují jak k ethernetové přepínané infrastruktuře, tak k úložné síti Fibre Channel, ačkoli v současnosti vzrůstá obliba technologií jednotného připojení úložiště, jako je FCoE (Fibre Channel over Ethernet). Síť datového centra uživatelům poskytuje připojení k podnikovým aplikacím, které fungují na serverových farmách. Úložná síť může zahrnovat přepínače Fibre Channel, které propojují hostitele Fibre Channel, zařízení iSCSI serverových farem nebo produkty s podporou řešení Cisco Unified Fabric, které sjednocuje sítě Fibre Channel a Ethernet do stejné infrastruktury.
- **Podniková hraniční síť** – modul podnikové hraniční sítě zahrnuje připojení k Internetu, síť VPN pro vzdálený přístup a moduly sítě WAN, které podnik připojují k síti poskytovatele služeb. Podniková hraniční síť obsahuje všechny síťové prvky, které umožňují efektivní a zabezpečenou komunikaci mezi podnikovým areálem a vzdálenými pobočkami, obchodními partnery, mobilními uživateli a Internetem. Modul hraniční sítě agreguje konektivitu z různých vzdálených poboček, filtruje provoz a směruje jej do podnikového areálu.

- **Síťové služby** – modul síťových služeb představuje relativně nový prvek koncepce podnikové sítě. Modul síťových služeb obsahuje služby IPv4 i IPv6, které jsou potřebné pro jednotnou komunikaci, mobilitu a autentizaci uživatelů. Většina podniků obvykle nedefinuje vyhrazený blok síťových služeb, které jsou místo toho dobře integrovány do



Obrázek 2.1: Příklad modulárního návrhu sítě

datového centra. Modul síťových služeb však nabízí značnou výhodu podnikům, které nasazují protokol IPv6, ale nemohou ihned plně implementovat síť s duální sadou protokolů IPv4/IPv6. Tyto podniky potřebují dočasně vybudovat překryvnou síť jako dočasné řešení, které propojí hostitele IPv6 pomocí sítě bez podpory tohoto protokolu. Jsou-li tyto služby konsolidovány do jediného modulu síťových služeb, nemusí architekti během migrace na duální sadu protokolů navrhovat v síti mnoho tunelů.

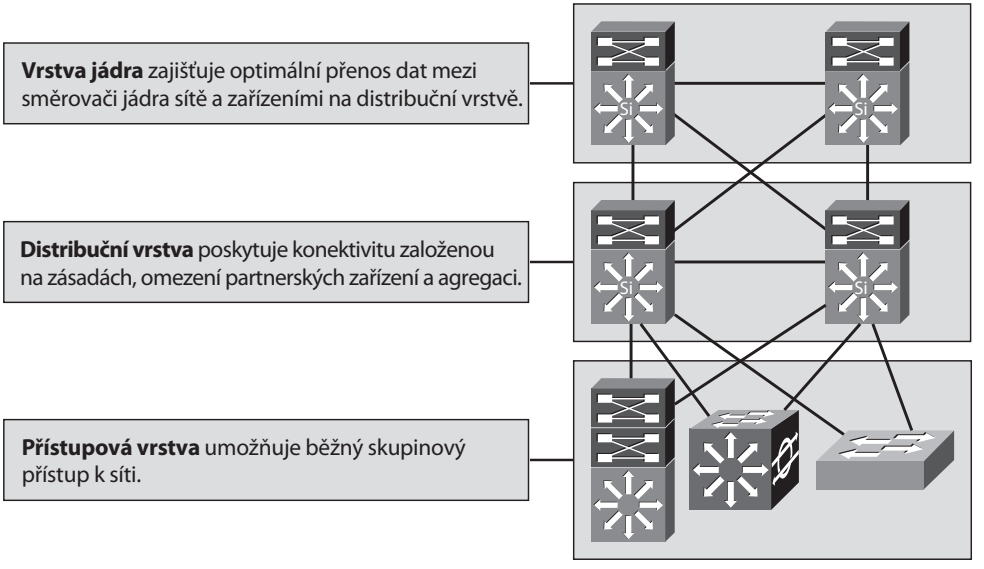
Menší stavební bloky modulárního návrhu sítě se snadno spravují a poskytují následující výhody:

- **Snadná správa** – díky modulárnímu návrhu sítě je možné každý modul spravovat samostatně a využít specializované nástroje pro správu všech síťových prvků v jednotlivých modulech. Nezávislé funkce v jednotlivých modulech umožňují zachovat možnost správy každého modulu.
- **Izolace chyb a řešení potíží** – tyto funkční moduly poskytují hranice, které lze sladit s funkčními jednotkami nebo podpůrnými podnikovými strukturami.
- **Lepší pružnost** – modularita usnadňuje změny při upgradech síťových zařízení. Nároky na upgrade zůstávají omezeny na malou podmnožinu zařízení nebo uživatelský segment, který vyžaduje rozšíření funkcí.
- **Nižší provozní výdaje** – moduly dělí síť na menší součásti, které jsou jednodušší a přehlednější. Jednoduchost pomáhá urychlit implementaci návrhu a zkracuje školení uživatelů sítě. Díky jasné a nepřekrývající se funkčnosti každé vrstvy lze síťový návrh snadno zkontrolovat.
- **Zjednodušený výběr produktů** – modularita dovoluje mapovat nákup konkrétního síťového zařízení na příslušnou síťovou vrstvu, takže není potřeba utrácet finanční prostředky za zbytečné funkce.

Vzhledem k tomu, že moduly jsou na sobě nezávislé, projeví se výpadek, upgrade nebo jiná změna jednoho modulu pouze v rámci jeho hranic.

Hierarchičnost

Hierarchičnost patří mezi hlavní pilíře dobrého návrhu sítě. Návrh sítě každého modulu, které byly uvedeny v předchozích odstavcích, musí zahrnovat hierarchičnost a odolnost. Podnikové prostředí a jeho komunikační kanály se musejí neustále vyvíjet. Návrh sítě proto musí být dostatečně pružný, aby dovoloval zapojení nových zařízení a aplikací či zvýšení kapacity bez zásadního přebudování. Tato pružnost návrhu sítě se vyvinula při přechodu od tradičních plochých sítí k hierarchické topologii s diskrétními vrstvami, kde má každá vrstva konkrétní roli. Síťový architekt tak může zvolit správnou platformu a povolit požadované funkce na příslušné vrstvě. Tyto vrstvy mají funkční vlastnosti a poskytují hranice chybových domén. Každá vrstva se vyznačuje jedinečnými funkcemi a samostatnými moduly, které poskytují síťové služby.



Obrázek 2.2: Hierarchický návrh sítě

Typická podniková areálová síť sestává ze tří vrstev (viz obrázek 2.2):

- **Vrstva jádra** (core layer) zajišťuje optimální přenos dat mezi lokálními sítěmi a propojuje různé prostředky distribuční vrstvy. Poskytuje také konektivitu prostředkům datového centra a přístup k Internetu prostřednictvím hraniční sítě.
- **Distribuční vrstva** (distribution layer) propojuje síťové služby s přístupovou vrstvou a implementuje zásady týkající se zabezpečení, vyrovnávání zařízení provozu a směrování.
- **Přístupová vrstva** (access layer) zajišťuje konektivitu pro koncové uživatele a zařízení.

Hierarchický návrh sítě poskytuje mnoho výhod, i když je vytvoření takového návrhu v porovnání s plochou topologií sítě poměrně drahé. Tyto výhody rozšiřují funkčnost sítě a model díky nim lépe splňuje cíle návrhu. Hierarchický návrh sítě přináší následující hlavní výhody:

- **Škálovatelnost** – díky hierarchickému návrhu sítě mohou síťoví architekti snáze replikovat libovolné moduly při růstu podnikové sítě. Jak je patrné na předchozích modelech, návrhy sítí, které nevyužívají model se třemi vrstvami, se často vyznačují omezenou škálovatelností. Hierarchický model může mít sice také svá omezení, ale oddělení funkcí v rámci sítě poskytuje přirozené růstové body, aniž by to výrazně ovlivnilo jiné části sítě.
- **Pružnost** – strukturovaný hierarchický návrh ze své podstaty poskytuje vysoký stupeň pružnosti. Umožňuje totiž fázové nebo postupné změny každého modulu v síti nezávisle na jiných modulech. Změny transportu na vrstvě jádra lze provést nezávisle na distribuční vrstvě. Změny návrhu či kapacity distribuční vrstvy lze pak implementovat fázovým či postupným způsobem. V rámci celkového hierarchického návrhu je

do architektury zařazen také modul služeb, který zejména umožňuje implementovat služby kontrolovaným způsobem. Při hierarchickém návrhu sítě je potřeba zohlednit hlavně tyto oblasti:

- **Pružnost řídicí úrovně** – umožňuje migraci mezi protokoly vrstvy 2 (STP) a vrstvy 3 (směrování).
- **Pružnost úrovně předávání** – podporuje nasazení a použití protokolu IPv6 souběžně s protokolem IPv4.
- **Pružnost uživatelských skupin** – nabízí síťový přístup a související služby v síti na podporu správy včetně akvizic, partnerství nebo outsourcingu podnikových funkcí.
- **Pružnost správy a řízení provozu** – vývoj kolaborativních aplikací vyžaduje, aby návrhy areálových sítí poskytovaly jednodušší metody monitorování toku a řešení příslušných potíží.
- **Pružná bezpečnostní architektura** – bezpečnostní architektura by se měla přizpůsobovat proměnlivým schématům provozu, jaké generují nově nasazované aplikace.

- **Snazší implementace** – vzhledem k tomu, že hierarchický model dělí síť na logické a fyzické sekce, mohou architekti snáze zavádět síťové prvky bez narušení stávající infrastruktury. V návrhu areálové sítě lze například nasadit a připojit k distribuční vrstvě nové přístupové přepínače, aniž by došlo k narušení činnosti stávajících přístupových přepínačů a uživatelů, kteří jsou k nim připojeni.
- **Snazší řešení potíží** – hierarchický návrh sítě usnadňuje řešení problémů se sítí, protože chyby jsou izolovány do jediné domény. Smyčka ve směrování v distribučním bloku například ovlivní pouze připojené přístupové přepínače a nikoli jiné distribuční bloky.
- **Snadná správa a plánování kapacity** – v hierarchickém modelu se obvykle lépe plánuje kapacita, protože požadavky na kapacitu se zpravidla zvyšují při přenosu dat směrem do jádra sítě. Díky všem dalším výhodám se hierarchicky navržené sítě většinou snáze spravují. Správu sítě vesměs zjednodušují předvídatelné toky dat, škálovatelnost, nezávislé implementace a jednodušší řešení potíží.

V částech o podnikové areálové síti a datovém centru se třemi vrstvami hierarchického modelu budeme zabývat podrobněji.

Odolnost

Kromě budování modulárního a hierarchického návrhu sítě je důležité, aby síťoví architekti při každém kroku návrhu sítě zohlednili také její odolnost. Integrovaná odolnost, kdy se v návrhu nevyskytují jediné body selhání, představuje klíč při zajištění vysoké dostupnosti a nepřerušeného fungování podniku. Je nutné zkoordinovat funkce odolnosti v návrhu přepínačů, linek a sítě v rámci všech modulů a vrstev zmíněných výše. Zapojením redundantních supervizorů do přístupové vrstvy lze například zabezpečit nepřerušené fungování podniku i v případě výpadku aktivního supervizoru. Díky tomu se výpadek nijak neprojeví na síťové konvergenci v distribuční vrstvě (u nasazení vrstvy 2 i směrovaného přístupu).

Integrace odolnosti do návrhu může vyžadovat použití nových funkcí, ale často stačí zvolit správnou implementaci hierarchie a příslušným způsobem nakonfigurovat základní topologie vrstvy 2 a vrstvy 3.

V následujících sekcích s ohledem na tři základní principy, tj. modularitu, hierarchičnost a odolnost, rozebereme návrhy sítě pro každý z odlišných modulů: jádro podnikové sítě, podnikovou areálovou síť, podnikové síťové služby, podnikové datové centrum a podnikovou hraniční síť (síť WAN v ústředí, přístup k Internetu a pobočkovou síť).

Návrh jádra podnikové sítě

Vrstva jádra je nejjednodušší, ale má zásadní význam. Tvoří páteř celé sítě. Jádro musí poskytovat vysokou spolehlivost a zajistit co nejrychlejší přepínání velkých objemů provozu. Nabízí omezenou sadu služeb a vyznačuje se vysokou dostupností, kterou zajišťují redundantní zařízení a odpovídající konfigurace. Díky tomu lze upgradovat software a měnit hardware bez narušení činnosti podnikových aplikací. Jádro poskytuje modul směrování vrstvy 3, který obsluhuje příchozí i odchozí provoz podnikové sítě. Směrování má kritický význam pro jádro datového centra a při jeho konfiguraci je nutné využít robustní bezpečnostní mechanismus, aby nedocházelo k propojení s nevhodnými partnery, injekcím nesprávných tras a neobjevovaly se smyčky ve směrování. Prevence tohoto problému vyžaduje, aby vrstva jádra měla tyto vlastnosti:

- Autentizace partnerů směrování
- Filtrování trasy
- Protokolování změn sousedů
- Ochrana proti falšování: jednosměrové RPF (uRPF) a omezování rychlosti

Tabulka 2.1 uvádí několik pokynů, které lze při návrhu jádra sítě využít.

Tabulka 2.1: Správné a chybné postupy návrhu vrstvy jádra

Ano	Ne
Navrhujte jádro s ohledem na vysokou spolehlivost. Zvažte využití technologií 10gigabitového a gigabitového Ethernetu v konfiguracích port-channel, které poskytují vysokou rychlost a redundanci.	Používejte softwarové funkce, protože mohou potenciálně zpomalit provoz.
Navrhujte zařízení vrstvy jádra tak, aby dosahovala nízké latence.	Podporujte přístup pracovních skupin na vrstvě jádra.
Používejte směrovací protokoly s rychlou konvergencí.	Snažte se při přidávání nových uzlů jádra zvýšit výkon pomocí upgradů hardwaru či softwaru.

Návrh podnikové areálové sítě

Architektura areálové sítě vychází ze dvou základních bloků neboli modulů, které jsou propojeny prostřednictvím jádra sítě:

- Distribuční vrstva
- Přístupová vrstva

Obě vrstvy podrobně popíšeme v následujících částech kapitoly.

Distribuční vrstva

Distribuční vrstva propojuje přepínače přístupové vrstvy s jádrem sítě. Velká podniková areálová síť může v závislosti na počtu níže připojených přístupových přepínačů obsahovat jeden nebo více distribučních přepínačů. Optimální postupy doporučují nepřekračovat 20 přepínačů přístupové vrstvy připojených k jediné distribuční vrstvě. Jedná se hlavně o omezení řídicí úrovně distribuční vrstvy bez ohledu na to, zda se jedná o návrh vrstvy 2 nebo směrovaného přístupu. Distribuční vrstvu lze v současnosti konfigurovat pomocí tří základních návrhových variant:

- Návrh přístupu vrstvy 2
- Návrh směrovaného přístupu
- Návrh virtuálního přepínače

Návrh přístupu vrstvy 2

Přístup vrstvy 2 představuje tradiční návrh přístupu a distribuce v areálové síti, kde jsou všechny přístupové přepínače nakonfigurovány v režimu předávání vrstvy 2. Distribuční přepínače pak fungují k oddělení vrstev 2 a 3. V tomto konkrétním návrhu slouží přepínače distribuční vrstvy jako výchozí brány pro koncové hostitele.

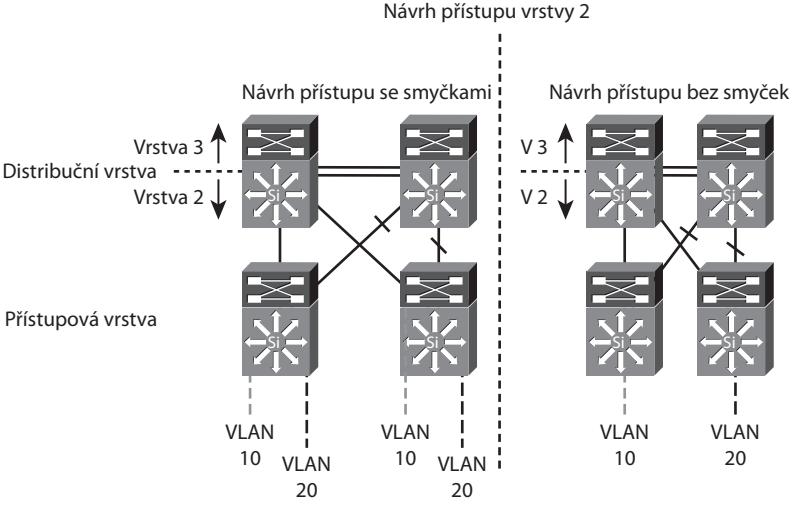
Trunkové linky založené na síti VLAN rozšiřují podsítě od distribučních přepínačů směrem dolů na přístupovou vrstvu. V přepínačích distribuční vrstvy funguje protokol redundance prvního přeskoku, jako např. HSRP (Hot Standby Router Protocol) nebo GLBP (Gateway Load Balancing Protocol), spolu se směrovacím protokolem, který zajišťuje vzestupné směrování do jádra areálové sítě. V přístupových portech a linkách mezi přepínači je podle potřeby nakonfigurována jedna verze protokolu STP (Spanning Tree) s některou variantou zvyšující zabezpečení (jako např. Loopguard, Rootguard a BPDUGuard). Tyto technologie a funkce jsou sice při nasazení v areálové síti zásadně důležité, nezávisí na protokolu IPv6, a proto se jimi nebudeme podrobně zabývat.

Návrh přístupu vrstvy 2 má dvě základní podoby (jak je znázorněno na obrázku 2.3), které se primárně liší jen v tom, jak jsou definovány sítě VLAN:

- **Návrh se smyčkami** – jsou nakonfigurovány sítě VLAN typu 1:N, které překonávají více přístupových přepínačů. Všechny tyto rozšířené sítě VLAN proto mají topologii kostry grafu sítě nebo se smyčkami vrstvy 2.
- **Návrh V (neboli bez smyček)** – tento návrh sleduje aktuální optimální postupy při návrhu více vrstev a definuje unikátní síť VLAN pro každý přístupový přepínač. Odstranění smyček z topologie přináší různé výhody. Patří k nim vyrovnávání zatíže-

ní odchozích připojení jednotlivých zařízení pomocí protokolu GLBP, nižší závislost na protokolu STP při zotavení sítě, omezení rizika všesměrových bouří a možnost vyhnout se záplavám jednosměrového vysílání (podobné potíže s návrhem souvisejí s nesymetrickými topologiemi předávání vrstvy 2 a 3).

Podrobnostmi koncepce a konfigurace všech uvedených návrhů se budeme zabývat v kapitole 6, „Nasazení protokolu IPv6 v areálových sítích".



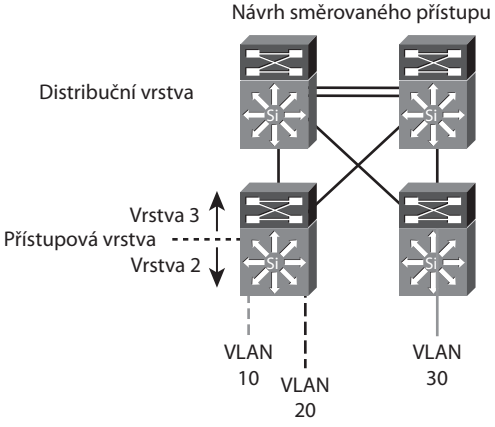
Obrázek 2.3: Návrh přístupu vrstvy 2

Návrh směrovaného přístupu

Alternativní konfigurace k tradičnímu modelu s více vrstvami distribučních bloků vypadá tak, že přístupový přepínač funguje jako úplný uzel směrování vrstvy 3 (poskytuje přepínání vrstev 2 i 3) a místo přístupu k distribučním odchozím trunkovým linkám vrstvy 2 jsou k dispozici dvoubodové směrované linky vrstvy 3. Tato alternativní konfigurace, ve které se přechod mezi vrstvami 2 a 3 přesunuje z distribučního přepínače na přístupový přepínač (viz obrázek 2.4), vypadá jako zásadní změna návrhu, ale ve skutečnosti se jedná o rozšíření optimálního přístupu k návrhu s více vrstvami. Podrobnostmi koncepce a konfigurace všech uvedených návrhů se budeme zabývat v kapitole 6.

Návrh směrovaného přístupu poskytuje díky využití přístupu vrstvy 2 k distribučním odchozím linkám několik výhod oproti návrhu s více vrstvami:

- Poskytuje běžné koncové nástroje pro řešení potíží (např. ping a traceroute), používá jediný řídicí protokol (buď EIGRP – Enhanced IGRP, nebo OSPF – Open Shortest Path First) a odstraňuje požadavek na funkce jako HSRP.
- V mnoha prostředích se sice jedná o vhodný návrh, ale nelze jej využít všude, protože sítě VLAN nemohou přesahovat přes více přístupových přepínačů.



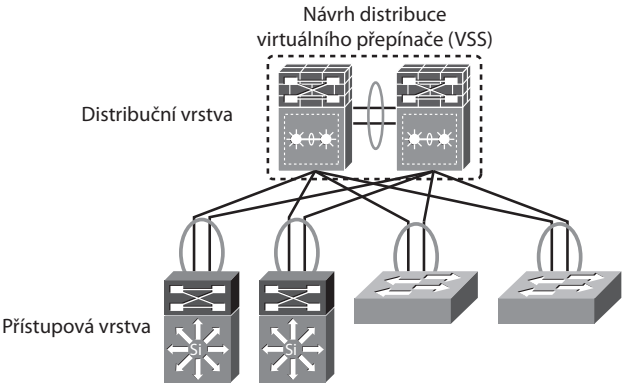
Obrázek 2.4: Návrh směrovaného přístupu

Vzhledem k tomu, že návrhy směrovaného přístupu poskytují další výhody, přinášejí také určité potíže:

- Implementace návrhu směrovaného přístupu vyžaduje pečlivé plánování a návrh, aby se nevyskytly smyčky směrování. Je také nezbytné provést vhodnou sumarizaci tras, aby bylo možné zajistit škálování síťového návrhu při přidávání nových uživatelů a přepínačů přístupové vrstvy do sítě.
- V případě návrhu vrstvy 2 je možné podsítě snadno rozšířit přes více přepínačů přístupové vrstvy, které propojují stejnou distribuční vrstvu. U návrhu směrovaného přístupu může rozšíření stejné podsítě přes dva přístupové přepínače způsobit překrývání adres, což může být problematické. Návrhář sítě pak musí pečlivě implementovat podsítě a sumarizaci tras na distribuční vrstvě.
- Implementace směrovaného přístupu může být drahá, protože poskytování funkcí vrstvy 3 může vyžadovat odlišný hardware a software na každé přístupové vrstvě.

Distribuční blok systému virtuálního přepínání

Návrh distribučního bloku systému virtuálního přepínání (VSS – Virtual Switching System), který je znázorněn na obrázku 2.5, se zásadně liší od typického návrhu přístupu vrstvy 2 nebo vrstvy 3. V minulosti se připojovalo více přístupových přepínačů ke dvěma redundantním distribučním přepínačům a konfigurace síťových řídicích protokolů (jako např. HSRP a 802.1D Spanning Tree) rozhodovala o tom, jak přepínače předávají provoz každým z odchozích připojení a jak se síť zotavuje v případě výpadku přepínače či linky. Když se objevila koncepce virtuálního přepínače, lze dvojici distribučních přepínačů nyní nakonfigurovat tak, aby fungovaly jako jediný logický přepínač.



Obrázek 2.5: Návrh distribučního bloku systému virtuálního přepínání

Transformací redundantních fyzických distribučních přepínačů do jediného logického přepínače se zásadně mění síťová topologie. V jiných návrzích bloků přístupu a distribuce je přístupový přepínač nakonfigurován se dvěma odchozími připojeními ke dvěma distribučním přepínačům a vyžaduje řídicí protokol, který rozhoduje o výběru použitého odchozího připojení. V implementaci VSS má přístupový přepínač jedinou logickou vzestupnou linku typu MEC (Multichassis EtherChannel), která je připojena k jedinému distribučnímu přepínači. Architekturou VSS se budeme podrobněji zabývat v kapitole 6.

Porovnání návrhů distribučních bloků

Každý ze tří návrhů bloků přístupu a distribuce sice nabízí prakticky použitelný přístup, ale návrhy s virtuálním přepínačem a směrovaným přístupem se vyznačují výhodami oproti tradičnímu přístupu s více vrstvami. Tyto novější návrhy se od klasického přístupu s více vrstvami liší celkovou jednodušší konfigurací a provozem sítě, vyrovnáváním zatížení pro jednotlivé toky v obou směrech a rychlejší konvergencí. Srovnání těchto tří variant návrhu naleznete v tabulce 2.2.

Tabulka 2.2: Porovnání modelů návrhu distribuovaných bloků

Funkce	Návrh přístupu vrstvy 2	Směrovaný přístup	Virtuální přepínač
Protokoly řídicí úrovně přístupu a distribuce	Spanning Tree (PVST+, Rapid-PVST+ nebo MST)	EIGRP nebo OSPF	PAgP, LACP
Přístupové přepínače přemosťující síť VLAN	Podporováno (vyžaduje smyčky STP na vrstvě 2)	Ne	Podporováno
Hranice vrstvy 3	Distribuce	Přístup	Distribuce
Protokol FHRP	Požadováno HSRP, GLBP, VRRP	Nepovinné	Nepovinné
Vyrovnání zatížení jednotlivých toků z přístupové do distribuční vrstvy	Ne	Ano – ECMP (Equal Cost Multipath)	Ano – MEC
Konvergence	900 ms až 50 sekund (závisí na topologii STP a vyladění FHRP)	50 až 600 ms	50 až 600 ms

Přístupová vrstva

Přístupová vrstva slouží jako kontaktní rozhraní neboli hranice podnikové sítě. Na této vrstvě se k síti připojují koncová zařízení. Přístupová vrstva také představuje první místo, kde lze inicializovat síťové služby. Jako příklad zařízení, která je možné připojit k přístupové vrstvě, lze uvést počítače, servery, IP telefony, bezdrátové přístupové body, kamery a další zařízení PoE/PoE+. Tabulka 2.3 shrnuje některé služby poskytované přepínačem přístupové vrstvy.

Návrh podnikových síťových služeb

Modul síťových služeb představuje relativně nový prvek návrhu areálové sítě. Když začínají návrháři areálové sítě uvažovat o migraci na prostředí s duální sadou protokolů IPv4/IPv6 a nadále integrují pokročilejší zařízení technologie Unified Communications, musejí se vypořádat s několika problémy. Je nutné zajistit hladkou integraci těchto služeb do areálové sítě a zároveň poskytnout příslušnou úroveň správy provozních změn a izolaci chyb. Návrh areálové sítě také musí zůstat pružný a škálovatelný. Služby IPv6 je například možné nasadit pomocí přechodné překryvné sítě založené na tunelech, která umožňuje zařízením protokolu IPv6 tunelovat data přes části areálové sítě, které zatím protokol IPv6 nepodporují. Tento přechodný přístup umožní rychlejší zavedení nových služeb, aniž by to vyžadovalo změnu režimu celé sítě. Do modulu služeb se doporučuje umístit například tyto služby:

- **Centralizované bezdrátové řadiče** – tyto řadiče připojují a řídí přístupové body v rámci celého areálu.
- **Centralizované ukončování tunelů IPv6 protokolu ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) z podnikové areálové sítě do modulu síťových služeb** – tímto způsobem vzniká přísně řízená tunelová síť, která překrývá stávající síť. Podobně jako u všech tunelových technologií platí, že navázání více tunelů protokolu ISATAP k různým síťovým segmentům značně komplikuje správu a řešení potíží se sítí.
- **Služby Unified Communications (Cisco Unified Communications Manager, brány)** – kvůli zajištění služeb Unified Communications nasazují podniky správce volání a jiná zařízení hlasové brány do bloku služeb, což zajišťuje jejich centralizovanou správu.
- **Brány zásad** – brány zásad poskytují autentizaci a autorizaci uživatelů spolu s funkcemi řízení přístupu k síti. Běžné brány zásad zahrnují funkce serverů AAA (authentication, authorization, accounting), serverů řízení přístupu (ACS) a profilerů řízení přístupu k síti.