Vypracování českých výukových materiálů pro kurz CCNA3 R&S Scaling Networks

Martin Trebatický

Bakalářská práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin Trebatický**
Osobní číslo:	**A12068**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Forma studia:	**prezenční**
Téma práce:	**Vypracování českých výukových materiálů pro kurz CCNA3 R&S Scaling Networks**
Téma anglicky:	**Developing Czech Teaching Materials for the CCNA3 R&S Scaling Networks Course**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Objasněte základní pojmy používané v protokolech OSPF, EIGRP, STP, VTP, DHCP a DNS pod protokoly IPv4 a IPv6.**
3. **Vytvořte český vyukový materiál pro kurz CCNA3 R&S Škálování sítí z aktuální verze anglických podkladů webu Cisco akademie.**
4. **Vytvořte českou prezentaci v PowerPointu pro přednášky z uvedeného předmětu.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Online Curriculum: Scaling Networks. Cisco Networking Academy [online]. [cit. 2017-01-30]. Dostupné z: https://www.netacad.com/**
2. **EMPSON, Scott. CCNP routing and switching portable command guide. 2nd edition. Indianapolis: Cisco Press, 2014, 391 p. ISBN 978-1-58714-434-9.**
3. **LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-80-251-2359-1.**
4. **CISCO NETWORKING ACADEMY na VUT v Brně FIT: Kurz CCNA Routing and Switching 3 [online]. Page last modified on June 28, 2016 [cit. 2017-01-30]. Dostupné z: http://netacad.fit.vutbr.cz/index.php?n=CCNA.Explor3**
5. **SOSINSKY, Barrie A. Mistrovství - počítačové sítě [vše, co potřebujete vědět o správě sítí]. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.**

Vedoucí bakalářské práce:	**Ing. Miroslav Matýsek, Ph.D.** Ústav počítačových a komunikačních systémů
Datum zadání bakalářské práce:	**24. února 2017**
Termín odevzdání bakalářské práce:	**24. května 2017**

Ve Zlíně dne 24. února 2017

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

Jméno, příjmení: Martin Trebatický

Název bakalářské/diplomové práce: Vypracování českých výukových materiálů pro kurz CCNA3 R&S Scaling Networks

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 22. 5. 2017

Trebatický
.....
podpis diplomanta

ABSTRAKT

Cílem práce, bylo vytvořit překlad anglických výukových materiálu kurzu CCNA 3 R&S Škálování Sítí, pro výuku a usnadnění porozumění pro studenty. Po zpracování teoretických základů, obsahujících témat, bylo úlohou přeložit celý obsah kurzu. Výsledkem práce je, kompletní překlad v Českém jazyce a prezentace do výuky, vytvořena podle chronologického obsahu kurzu.

Klíčová slova: Cisco, Směrování, Přepínání, Síťová komunikace, Škálování sítí

ABSTRACT

The goal of this work, was creating a translation of english studying course materials CCNA 3 R&S Scaling Networks, for teaching and facilitate understanding of students. After processing the theoreticall basics of themes included, was a task, translate the course at all. The result of my work, is complete translation in Czech language and presentation for teacher, created by according to chronological content of course.

Keywords: Cisco, Routing, Switching, Network comunication, Scaling networks

OBSAH

ÚVOD

Různé firmy a podniky spoléhají stále víc, na své infrastruktury sítí. Protože s rostoucí firmou se také zvyšují veškeré náklady a požadavky sítě. Podnik, je to velké uživatelské prostředí s mnoha uživateli, lokacemi a systémy. Tím pádem, musí podniková síť, podporovat různé typy síťového provozu ve více pobočkách, nebo obchodních jednotkách. Podpora je potřebná hlavně v centralizaci administrativního řízení, při konvergování přenosů, kritických aplikacích a kvůli obchodním potřebám.

Každý podnik si dnes, ve své podnikové síti, na vysokou úroveň spolehlivosti sítě. Časté, nebo i jen občasné výpadky, způsobují ztráty nejen příjmů a dat, ale i zákazníků. Proto se v podnikových sítích používají přísnější normy. Je to kvůli velkým objemům provozu. Aby se spolehlivosti dostálo, funkce redundantních napájecích zdrojů a převzetí služby pří selhání, udržují síť v provozu.

Prvním krokem ke správně fungující síti, je hierarchický návrh, aby se provoz nerozšiřoval do jiných částí sítě. K organizaci se používá třívrstvý hierarchický model návrhu sítě. Každá jeho vrstva je navržena tak, aby splňovala specifické funkce. Přístupová vrstva poskytuje připojení uživatelům, distribuční vrstva, zase předává provoz z jedné lokální sítě do druhé. Třetí vrstva, jádrová, slouží jako páteřní vrstva. Provoz začne v přístupové vrstvě a pokračuje ostatními, pokud je funkcionalita těchto vrstev požadována.

Návrhář sítě, si musí promyslet strategii, jak síť navrhnout, aby byla k dispozici s cílem jejího efektivního a snadného škálování. Je všeobecně odporučeno, aby bylo použito rozšířitelné modulární zařízení, kvůli přidání nových funkcí a zařízení, bez nutnosti nákladné modernizace. Především je potřeba zvolit správné moduly, u kterých je možnost modifikace a modernizace, bez ovlivnění ostatních funkčních oblastí.

Následně po zvolení správných zařízení a modulů, je vytvoření strategie variabilního adresování IPv4, nebo Ipv6. Pečlivou přípravou adresace, se eliminuje potřeba změn a problémů s novými uživateli. Pak nastává otázka správného výběru zařízení. Podle odporučení, je dobré použít směrovače, nebo vícevrstvé přepínače, čili zařízení 3. vrstvy, pro filtrování a omezení provozu v jádru sítě.

Tyto základní kroky a požadavky, by stačili k základní funkcionalitě sítě. Jenomže velké podnikové sítě mají pokročilejší požadavky pro návrh. Tím se dostáváme k velkému počtu koncových uživatelů a náročnosti na velikost sítě. Proto síťový návrháři, používají tyto metody, nebo kroky k vylepšení sítě velkého rozsahu. Spolehlivost se dá zaručit, implementací redundantního spojení mezi zařízeními přístupové a jádrové vrstvy, nebo víceméně prioritně

mezi kritickými zařízeními. Implementaci více spojení, je možné pomocí agregace linek, nebo vybalancováním zatížení cest se stejnými náklady. Agregací více spojení do konfigurace EtherChannel, má za následek, zvýšení dostupnosti pásma. Dalším krokem by mohlo být implementování bezdrátového připojení. To by zaručilo mobilitu a možnosti expanze celé sítě.

Asi nejdůležitějším krokem, by bylo použití škálovatelného směrovacího protokolu a implementace jeho funkcí. Tyto funkce zabezpečují izolovanou aktualizaci směrování a minimalizují velikost směrovacích tabulek. Proto jsou nejčastěji používány dynamické směrovací protokoly OSPF a EIGRP. Jsou výborně využitelné, ve velkých škálovatelných sítích a poskytují robustnost a bezpečnost všech aspektů směrovací domény.

Pro spolehlivé pracování sítě, je taky potřeba operační sytém, k řízení všech parametrů. Společnost Cisco, používá ve svých zařízeních Cisco IOS. Je důležité zvolit si správnou verzi IOS pro všechny svoje zařízení v síti. Pak už stačí jenom zakoupit licenci a práce může začít.

Praktická část obsahuje překlad celého kurzu CCNA 3 Škálování Sítí, s interaktivními pomůckami a různými aktivitami. Pro lepší přehled v tématech, je potřeba použití interaktivních materiálů z originálního znění kurzu, s přeloženým obsahem v této práci.

I. TEORETICKÁ ČÁST

1 SPANNING TREE PROTOCOL

1.1 Redundance a smyčky v sítí

Pro mnoho organizací, je dostupnost jejich sítě zásadní, a redundance je velice důležitou součástí návrhu sítě. Hlavně kvůli prevenci narušení síťových služeb. Redundance lze docílit instalací duplicitních zařízení, nebo redundantními cestami. Ty nabízejí alternativní trasy pro fyzické údaje. Redundantní cesty se vytvářejí, z důležitosti vysoké dostupnosti linky. Když teda dojde k výpadku jedné linky, nebo zařízení, fungování sítě zabezpečí alternativní cesta, která slouží jako záloha. Jenomže, tyto cesty můžou způsobit logické smyčky na 2. vrstvě. Smyčky můžou způsobit několik problémů, počínaje broadcastovou bouří, problémy z konektivitou, nestabilitu tabulky MAC adres a několikanásobné doručení.

Smyčky v síti vznikají ze dvou důvodů. Jedním je neodborná manipulace, či chyba obsluhy. Ale to jsou spíš náhodné situace. Tím druhým a důležitějším jsou, redundance linek, jako záloha a vyvážení zatížení. Vyvažování zatížení, je případ využití redundantních linek, pro zvýšení výkonu a využití všech linek zároveň.

Z důvodu prevence proti těmhle problémům, je nutné použit protokol STP [3].

1.1.1 Broadcastová Bouře/Vysílací Bouře

Je nejčastějším problémem v běžné LAN síti, kde existuje smyčka. Z principu přepínačů, dochází k tomuto efektu, protože na 2. vrstvě OSI modelu, není funkce TTL (Time to Live), která by ukončila kolování broadcastových rámců, po určené době. To znamená, že šíří v síti více broadcastových rámců, než můžou aktivní prvky zpracovat. Když tento efekt nastane, většinou to končí úplným zahlcením sítě. Tím pádem, není dostupná žádná šířka pásma pro autorizovaný přenos a síť není dostupná pro datovou komunikaci.

Dalším důsledkem bouře, může být selháním koncového zařízení, kvůli požadavkům na zpracování vysokého provozního zatížení. Děje se to proto, že vysílání je směrováno ze všech portů přepínače a všechny připojená zařízení musí zpracovávat veškerý vysílaný provoz, který nekonečně zaplavuje celou smyčkovou síť. Vysílací bouře, může vzniknout během pár vteřin, kvůli pravidelnému vysílání rámců [1],[3].

1.2 STP

Protokol STP, odstraňuje smyčky 2. vrstvy, pokud jsou použity mezi linkami, které jsou redundantní. Dělá to pomocí mechanismu pro zákaz redundantní cesty, pokud je to nutné, jako například při objevení chyby. Jinak řečeno, vyhledává nejkratší cestu mezi dvěma přepínači. Na výpočty nejkratší cesty, používá STA (Spanning Tree Algorithm), algoritmus pro vytvoření databáze síťové topologie a na základě určitých parametrů, ruší redundantní spoje. To znamená, že blokuje porty a ty potom nevysílají žádná data a všechna přijatá zahodí. Když se přeruší některá linka, pokusí se vytvořit alternativní cestu, odblokováním zakázaného portu. STP je dynamický protokol, takže má schopnost rekonfigurace, aby zabránil vzniku smyček. Princip fungování spočívá, ve vytváření virtuální topologie, která neobsahuje smyčky, na fyzické topologii, která smyčky obsahovat může [1].

Protokol STP je původní verze IEEE-802.1D a byl nahrazen protokolem RSTP(Rapid Spanning Tree Protocol). Oba Protokoly sdílejí většinu stejné terminologie a metody odstraňování smyček v síti. Ale od původní verze se objevilo pár různých typů STP:

- **RSTP** - vylepšeni STP, poskytuje rychlejší konvergenci
- **PVST+** - vylepšení STP, poskytuje samostatnou instanci pro každou VLAN v síti
- **Rapid PVST+** - vylepšení RSTP s rychlejší konvergencí
- **MSTP** – mapuje více LAN do jedné instance (až 16 instancí RSTP)

1.3 STA

STP a RSTP používají algoritmus STA, k určování portů k zablokování. Blokováním redundantních cest, je rozhodující, aby se zabránilo vzniknutí smyček v síti. Fyzicky ale cesty stále existují, ale jsou zakázány. V případě selhání cesty, STA přepočítá hodnoty a odblokuje potřebné porty, k aktivaci redundantní cesty.

Princip STA spočívá v označení jednoho přepínače jako kořenového mostu a používá ho k referenci pro výpočty všech cest. Výběr tohoto přepínače, probíhá volebním procesem. Proces vybírá ze všech přepínačů, které si vyměňují BPDU a pomocí informací z těchto rámců určuje přepínač z nejnižším BID (Bridge ID). Ten, který má nejnižší BID, se automaticky stává kořenovým mostem. BPDU je rámec vyměňován mezi přepínači. Každý rámec obsahuje BID odesílatele. Jeho hodnota obsahuje hodnotu priority, MAC adresu odesílatele a rozšířené ID systému. Jejich kombinací se určuje hodnota BID [1].

Při posílání rámců BPDU, mezi přepínači, sousední přepínače ve vysílací doméně, si přečtou BID a pokud zjistí, že kořenový identifikátor souseda je nižší, identifikuje ho jako kořenový

můstek. Pak se vyšlou nové BPDU, k ostatním připojeným přepínačům v doméně a ten s nejnižším BID je kořenovým můstkem pro celou instanci [12].

Hned po zjištění kořenového mostu, vypočítá STA nejkratší cestu k němu. A začne určovat, které porty se mají zablokovat. Bere v úvahu i cenu cesty a portů. Cena celkové trasy, se vypočítá součtem cen portů, spojených z jejími rychlostmi, podél celé trasy ke kořenovému mostu. Vybírá se cesta z nejnižší cenou. Po zjištění nejlepších cest, přidělí role všem zúčastněným portům. Role portu, určuje jeho vztah ke kořenovému můstku, a zda má povolen přenos dat. Role portů jsou:

- Zvolí se kořenový můstek
- Určí se kořenové porty – porty z nejnižší cenou, ve stavu vysílání
- Následují určené porty – porty, který patří do topologie, připojují segment a jsou ve stavu vysílání
- Ostatní se nastaví na neurčené – jsou redundantními cestami, ale blokovány

Když jsou role portů určeny, určuje se nejlepší cesta ke kořenovému můstku. Ta se určuje součtem cen jednotlivých portů podél celé cesty. Výchozí ceny portů jsou definovány jejich operační rychlostí. Preferována je cesta z nejnižší cenou a všechny ostatní jsou blokovány.

Kořenový můstek (bridge), má pár důležitých vlastností. Kromě toho že má nejnižší BID v sítí, všechny jeho porty jsou určené a ve stavu předávání. Můstek je kořen celého stromu, takže všechny akce a rozhodnutí, se dělají z jeho pohledu. Proto je nejlepší zajistit, aby Kořenový můstek byl nejvýkonnějším zařízením v topologii [1], [9].

1.3.1 Vyvažování Zatížení STP

Protokol STP se používá k vyvažování zatížení provozu na trunk portech. Pokud máme více redundantních trunk linek mezi přepínači, jedna linka je blokována a komunikuje jenom druhá. Protože obě linky mají stejné BID kořenového můstku, blokování portu se volí podle ID portu (PID) odesílatele. PID, je 16 bitová hodnota a skládá se z indexu portu a jeho priority. Priorita je vy výchozí hodnotě 128, ale je možnost manuálního nastavení. Port z nižší hodnotou PID, má vyšší prioritu a použije se na komunikaci. Druhý je zablokován, kvůli vzniku smyček.

Jiná metoda vyvažování zátěže, spočívá ve využití ceny cesty. Je možné, že trunk linky jsou zapojeny do různých přepínačů, takže cena cesty se určuje podle rychlosti linky. Cena se dá taky zadat manuálně, a větší prioritu má cesta z nižší cenou.

1.3.2 Konvergence a Rozšíření STP

Při změnách topologie, například připojení/odpojení zařízení, nebo portu, si porty přepínače projdou několika stavy. Přepínaná síť je konvergovaná v momentu, kdy všechny porty přepínačů jsou ve stavu vysílání, nebo blokování. Je to vlastně čas, za který port projde ze stavu blokování do stavu vysílání. Stavy portů jsou:

- **Blokování** – nevysílá, přijímá jenom BPDU
- **Naslouchání** – jen posílá a přijímá BPDU
- **Učení se** – posílá a přijímá BPDU, učí se z nich MAC adresy
- **Vysílání** – vše posílá a přijímá

Kvůli zvětšení rychlosti konvergence a bezpečnosti, společnost Cisco vytvořila řadu rozšíření. Nejužívanější rozšíření jsou:

- **PortFast** – port nastavený jako PortFast, nemusí projít cyklem stavů portu, ale přejde rovnou do stavu vysílání. Je to možné jen na portu, kde nemůže dojít ke smyčce.
- **UplinkFast** – použití hlavně na přístupové vrstvě celého přepínače. Při selhání kořenové linky, odblokuje záložní linku a zajistí expresní přepnutí do stavu vysílání. Vynechá přitom stavy Naslouchání a Učení.
- **STP Ochrana** – ochrání síť, před zvolením nesprávného kořenového můstku. Vynucuje si nastavení portu na Určený, a pokud by se měl stát kořenovým portem, zablokuje ho.
- **Ochrana BPDU** – chrání port na koncové stanici. Když projde BPDU rámec tímto portem, tak ho vypne.
- **Filtr BPDU** - filtruje provoz STP na koncových portech. Zabrání přijímání a odesílání BPDU rámců [1], [12].

1.4 Rapid STP

RSTP nahradil protokol STP, kvůli vylepšením rychlosti konvergence. STP má moc velký čas konvergence (30-50s), proti RSTP, který to zvládne za pár sekund. Patří do normy IEEE 802.1d. Terminologie a příkazy se moc nemění, ale pár vylepšení se najde:

- Použití formátu BPDUv2.
- Všechny přepínače generují a posílají BPDU na všechny porty.
- Posílání Nabídky a Souhlasu mezi sousedy.
- Definuje se typ linky, pro rychlý přechod do stavu vysílání.

- Změna rolí portů.
- Změna stavů portů.

U RSTP přibyla jedna role portu:

- Kořenové Porty - porty nejblíže ke kořenovému můstku
- Určené Porty – všechny nekořenové porty, ale přenos dat mají povolen
- Alternativní a záložní Porty – nakonfigurovány k blokování, využity v případě potřeby
- Zakázané Porty – port, který je vypnutý

A navíc se určuje typ portu, nebo linky:

- Point-to-point – spojení bodu z bodem, linka je plně duplexní
- Koncový – port, nebo linka, připojuje koncová zařízení
- Sdílený – sdílená linka s polovičním duplexem

1.5 Vylepšení STP a RSTP

1.5.1 PVST+

Známe tři verze vycházející z originální verze STP, 802.1D:

- **CST (**Common Spanning Tree) – použití jedné instance STP pro všechny VLAN. Šetří procesor, protože vypočítává pouze jednu instanci. Nemůže sdílet zatížení provozu, takže jeden Uplink, blokuje všechny VLAN.
- **PVST** (Per-VLAN Spanning Tree) – poskytuje samostatnou instanci pro každou VLAN a vylepšuje flexibilitu. Potřebuje trunk porty, kvůli ISL zapouzdření. Není kompatibilní s CST.
- **PVST+** (Per-VLAN Spanning Tree Plus) – je kompatibilní s CST i PVST. Podporuje obojí zapouzdření, ISL a taky 802.1Q. Je použitý jako výchozí mód, většiny platforem Cisco. V PVST+ dokážeme nastavit parametry tak, že se zvolí víc kořenových můstků, pro polovinu VLAN jeden a druhý pro zůstatek. To zvyšuje redundanci v síti [1].

Vlastnosti PVST+:

- Může nastat optimální vyvážení zátěže.
- Při velkém počtu VLAN, můžou nastat značné ztráty cyklů procesoru, u všech přepínačů.
- Zlehčuje cesty vysílací doménou bez smyčky

PVST+ se určuje, přes informace získané výměnou rámců BPDU mezi přepínači. Každý zúčastněný port, přechází přes pět možných stavů a tři časovače BPDU, které zajišťují, že se během vytváření STP, nevytvoří žádné smyčky.

Stavy portů PVST+:

- **Blokování** – nepodílí se na předávání rámců. Obdrží jen BPDU, aby určil polohu a ID kořenového můstku.
- **Poslouchání** – poslouchá, aby určil cestu ke kořenu. Vysílá vlastní BPDU, k informaci, že se připravuje k aktivní účasti v topologii.
- **Učení** – učí se MAC adresy, připravuje se na předávání rámců a naplňuje tabulku MAC adres
- **Vysílání** – port posílá data, odesílá a přijímá BPDU rámce.
- **Zakázáno** – administrativně deaktivován, neúčastní se komunikace.

Postup PVST+, pro zajištění topologie sítě bez logických smyček:

- **Zvolí se kořenový můstek** – přepínač z nejnižším ID, všechny porty jsou Určené.
- **Volí se kořenový port, nekořenových můstků** – je to cesta z nejnižší cenou, ke kořenovému můstku. Obvyklý stav portů je Vysílání.
- **Volí se Určený port každého segmentu** – tento port se volí na každé lince, pro každou VLAN. Je vybírán na přepínači, z nejnižší cenou cesty ke kořenu. Obvykle ve stavu vysílání.
- **Ostatní porty jsou alternativní** – obvykle jsou blokovány, aby nepřerušili topologii, ale zpracovávají přijaté BPDU rámce.

1.5.2 Rapid PVST+

- **MST** (Multiple Spanning Tree) – vychází z normy IEEE 802.1s, je rychlý jako RSTP a mapuje několik VLAN do jedné instance STP.
- **RPVST+** - Je jednou z implementací RSTP protokolu a je to proprietární protokol. Vychází z normy IEEE 802.1w. Pro každou VLAN v síti, běží RSTP zvlášť.

RPVST+ je vylepšením původního standardu IEEE 802.1d. Terminologie STP 802.1w, zůstává v podstatě stejná jako v původním standardu 802.1d. Takže zkušení uživatelé, by neměli mít problém z konfigurací nového protokolu. Zachovává se i zpětná kompatibilita z původním standardem. Je to preferovaný protokol zabraňování smyček 2. vrstvy přepínané sítě.

Je to implementace RSTP, od společnosti Cisco na bázi VLAN. To znamená, že pro každou VLAN běží nezávislá instance. Neexistují v něm blokované porty, ale definuje stav, jako vyřazení, učení a předávání.

RPVST+, urychluje přepočet, při změnách topologie sítě 2. vrstvy. Konvergence je dosažitelná, v několika málo stovkách milisekund, samozřejmě ve správně nakonfigurované síti. Porty nakonfigurovány jako alternativní, nebo zálohovací, se dokáží změnit do stavu předávání, bez čekání na konvergenci sítě.

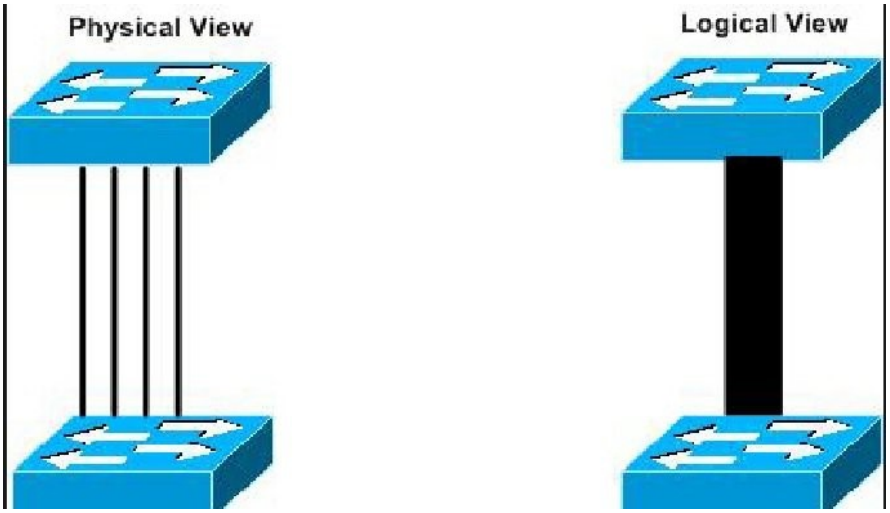
Používá rámce BPDU verze 2. RSTP odešle BPDU rámec a načítá bajt značky, trochu jiným způsobem. Informace portu se můžou stát ihned zastaralými, pokud nepřijmou za tři časové doby (2s), nějaké Hello pakety. BPDU se používají jako mechanismus udržování, tři po sobě vynechané rámce BPDU, indikují ztracení spojení [1], [9].

2 AGREGACE LINEK

2.1 EtherChannel

Agregace linky, je schopnost vytvoření jednoho logického spojení přes více fyzických propojení mezi dvěma zařízeními, čím se zvýší šířka pásma. Tak se umožní sdílení zatížení fyzických linek. Jiná forma, než blokace linek u STP. V přepínaných sítích se používá forma agregace nazývaná EtherChannel.

Fyzický a Logický pohled na agregaci linek



Obr. 1. Fyzický a Logický pohled na agregaci linek [13]

Používají se existující porty přepínače, protože není nutnost rychlejší a dražší linky. Je zobrazen, jako jedno logické rozhraní, proto může zajistit, konfigurace celé linky, namísto každého jednotlivého portu. Konfigurace této linky, využívá balance zatížení mezi linkami, které jsou součástí stejného EtherChannelu [12].

Může se implementovat jedna nebo více metod, v závislosti na hardwarové platformě. Metody zahrnují vyvažování zatížení zdrojové a cílové MAC adresace, nebo IP adresace. Vyvažování zátěže, závisí na zvoleném algoritmu, protože se určuje, přes které fyzické rozhraní odejdou data. Pokud dojde k selhání linky, datová komunikace se přesune na jiné, funkční fyzické rozhraní. Výchozí metoda pro vyrovnání zatížení je podle zdrojové MAC adresy, ale nastavit lze IP adresu, nebo XOR operaci [1].

Tato technologie se značně rozšířila, protože dokáže řešit problémy s datovou propustností do páteřní sítě a obcházet nejčastější poruchy na trase. EtherChannel může vzniknout z dvou až osmi fyzických rozhraní, které musí mít stejnou rychlost a typ, musí být plně duplexní

přiřazeny do stejné VLAN, nebo trunk linky. EtherChannel nejde vytvořit mezi porty různých přepínačů, to znamená, že každý člen musí být na stejném přepínači. Maximální počet podporovaných kanálů je až 128 EtherChannelů, v závislosti na použité platformě. Pozor na typy rozhraní, nelze je smíchat. Například Gigabit a Fast Ethernet rozhraní nemohou být smíchána [4].

V konfiguraci můžeme určit, jak se má řešit přiřazování k fyzickému rozhraní. Je to možné dvěma metodami. Tou první je manuální nastavení hodnoty, z níž se počítá hash, jehož výsledkem je hodnota 0-7 a ta určí port k použití. Další metodou je dynamická agregace z použitím agregačního protokolu. Přepínače Cisco, podporují dva dynamické agregační protokoly. EtherChannel může být vytvořen dynamickým vyjednáváním, se sousedními přepínači, za pomoci jednoho z těchto protokolů:

- **PAgP** – Portový agregační protokol, Cisco proprietární.
- **LACP** – Protokol řízení agregace linky, standard IEEE, původně definován 802.3ad.

2.2 Port Aggregation Protocol

Protokol PAgP pomáhá při automatické tvorbě EtherChannelu. Linka konfigurována protokolem PAgP, posílá pakety mezi porty a vyjednávají o vzniku kanálu. Pokud protokol identifikuje správnou linku, seskupí porty a vytvoří EtherChannel, který pak přidá do STP jako jeden port. PAgP zajistí, že všechny porty mají stejný typ konfigurace. Také řídí EtherChannel, zkontroluje konzistenci konfigurace a spravuje přidávání a selhávání linek mezi dvěma přepínači. To znamená, že zajišťuje, aby linky byly kompatibilní a v případě nutnosti, také povolení spojení [1].

PAgP funguje ve třech režimech:

- **Zapnuto** – Nutí rozhraní ke kanálu bez funkce PAgP. Rozhraní pakety nevyměňují.
- **Žádoucí** (Desirable) – Režim nastaví rozhraní v aktivním stavu vyjednávání, které pak iniciuje vyjednávání z jinými rozhraními, zasíláním PAgP paketů
- **Auto** – Režim nastaví rozhraní v pasivním stavu vyjednávání, které pak reaguje na pakety PAgP a přijímá je, ale nezakládá vyjednávání.

Režimy musí být kompatibilní na obou stranách. Kanál se zformuje jen, když jsou režimy:

- **Žádoucí a Žádoucí** – oba iniciují vyjednávání
- **Žádoucí a Auto** – jeden je iniciátor a druhý přijímá
- **Auto a Auto** – na obou stranách není iniciátor, kanál se nezformuje

2.3 Link Aggregation Control Protocol

Protokol LACP, umožňuje připojit několik fyzických portů, k vytvoření jednoho logického kanálu. LACP, odesílá pakety k partnerovi a může ho přepnout k vyjednávání automatického balíčku. Používá se pro usnadnění EtherChannelu, v prostředí více dodavatelů.

LACP požaduje:

- Podporu EtherChannel na všech ethernetových rozhraních
- Rychlost a duplex – každé rozhraní ze stejnou rychlostí a stejným duplexním režimem
- Všechny rozhraní, musí být přiřazeny v jedné VLAN, nebo trunk lince
- Povolený rozsah je stejný pro všechny VLAN

EtherChannel umožňuje, aby v jednom logickém spojení, může být až osm redundantních linek. Používání pouze jednoho spojení, využije jenom polovinu z dostupné šířky pásma.

Dělá podobnou funkci, jako PAgP a poskytuje stejné výhody při vyjednávání. Pomáhá s vytvářením spojení EtherChannel, zjišťováním konfigurací každé strany. Ujistí se, že jsou kompatibilní a v případě nutnosti, je možné zapnutí linky [12].

Režimy LACP jsou:

- **Zapnuto** – nevyměňuje LACP pakety a nutí rozhraní na kanál bez LACP
- **Aktivní** – režim nastaví port na aktivní vyjednávací stav, iniciuje vyjednávání s jinými porty odesíláním LACP paketů
- **Pasivní** – režim nastaví port na pasivní vyjednávací stav, reaguje na LACP pakety a přijímá, ale vyjednávání nezaloží

Režimy musí být kompatibilní na obou stranách, aby se kanál zformoval:

- **Aktivní a Aktivní** – oba iniciují vyjednávání
- **Aktivní a Pasivní** – jeden je iniciátor a druhý přijímá
- **Pasivní a Pasivní** – žádný iniciátor, kanál se nezformuje

3 WIRRELES LOCAL AREA NETWORK

3.1 Přehled WLAN

Nároky na sítě, se neustále zvětšují a proto se za použití správných technologií, může síť rozšiřovat podle potřeb každé organizace. Stále důležitějším aspektem rozšíření připojení přístupové vrstvy sítě je, pomocí bezdrátového připojení. To poskytuje mnoho výhod, jako velkou flexibilitu, snížení nákladů na provoz, schopnost růstu a přizpůsobení se měnícím se požadavkům sítě, firmy a koncových uživatelů. Lidé jsou připojeni pomocí mnoha moderních zařízení, jako PC, notebooky a chytré telefony. V podnikovém prostředí, je nejdůležitější, bezdrátová lokální síť WLAN.

Výhodou WLAN je velká flexibilita, produktivita, menší náklady, přizpůsobitelnost a schopnost růstu. Odstranění kabeláže, solidní rychlosti, mobilita a rychlejší výsledky, jsou dalšími výhodami bezdrátových sítí [6].

3.2 Komunikace WLAN

Bezdrátové sítě se rozdělují na:

- **WPAN** Bezdrátové osobní sítě – rozsah několik metrů, Bluetooth a přímé připojení Wi-Fi
- **WLAN** Bezdrátové sítě LAN – rozsah několik set metrů, domy a firmy
- **WWAN** Bezdrátová širokopásmová síť – rozsah v km, metropolitní oblast

Wi-Fi je WLAN standard IEEE 802.11, používaný pro poskytnutí přístupu k síti, běžným domácím a firemním uživatelům. Zahrnuje přenos dat, hlasu a videa do vzdálenosti až 300 metrů [1].

Všechny bezdrátové zařízení pracují v oblasti rádiových vln elektromagnetického spektra. Přidělování spektra rádiových frekvencí (RF), reguluje unie ITU-R. Pásma frekvencí jsou silně regulována a používají se pro nouzové aplikace a situace. WLAN pracují v lékařském pásmu ISM 2,4 GHz a nelicencované národní informační struktuře UNII 5GHz [12].

Vysílače a přijímače bezdrátových zařízení sítě LAN, jsou naladěny na specifické frekvence rozsahu RF. Sítě 802.11 mají přiděleny tyto frekvenční pásma:

- 2,4 GHz 802.11b/g/n/ad
- 5 GHz 802.11a/n/ac/ad
- 60 GHz 802.11ad

Přehled implementací standardu 802.11

Standard	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva
IEEE 802.11	1997	2,4	2	DSSS a FHSS
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM
IEEE 802.11n	2009	2.4 nebo 5	600	MIMO a OFDM
IEEE 802.11y	2008	3,7	54	
IEEE 802.11ac	2013	5	1000	MU – MIMO
IEEE 802.11ad	2014	2,4 , 5 , a 60	7000	

Obr. 2. Přehled implementací standardu 802.11

3.3 Komponenty

Abyste mohli komunikovat bezdrátově, je potřeba bezdrátové síťové karty NIC. Ta potřebuje k funkčnosti potřebný softwarový ovladač, rádiový přijímač/vysílač naladěny na stejné frekvence a plnou funkčnost. Navíc je potřeba bezdrátového směrovače, nebo přístupového bodu pro koncové uživatele.

Domácí bezdrátový směrovač slouží jako:

- **AP Přístupový bod** – bezdrátový přístup pro 802.11a/b/g/n/ac
- **Přepínač** – 4 porty, plně duplexní přepínač, pro připojení kabelových zařízení
- **Směrovač** – výchozí brána pro připojení k jiným síťovým infrastrukturám

Tyto směrovače poskytují i pokročilé funkce, jako vysokorychlostní přístup, adresaci IPv6, QoS a USB porty.

Bezdrátoví klienti používají svou NIC, k objevení nedalekých AP, které inzerují svoje SSID. Klienti se pokouší spojit a autentizovat s AP. Po ověření, mají uživatelé přístup k síti [7].

AP můžou být:

- **Autonomní AP** – zařízení konfigurováno přes Cisco CLI. Užitečné v situacích, kdy je potřeba jenom pár přístupových bodů. Domácí směrovač je skvělým příkladem, protože má celou svoji konfiguraci, uloženou v sobě. Víc AP se kontroluje použitím bezdrátových doménových služeb WDS.
- **AP založeny na řídících jednotkách** – jsou závislá od serveru, nevyžadují počáteční konfiguraci. Používají se větších sítích, kde je více AP. Každý nový přidaný přístupový bod, je automaticky konfigurován a spravován řídícím zařízením sítě WLAN [7].

Mnoho přístupových bodů, si vyžaduje použití externích antén, aby se staly plně funkčními jednotkami. Vyhovující antény, vyvinula společnost Cisco, speciálně pro 802.11. Cisco přístupové body používají:

- **Všesměrové antény** – Poskytují pokrytí 360 stupňů a nejlepší použití je v otevřených prostorách, chodbách a kancelářích.
- **Směrové antény** – Zaměřují rádiový signál v určeném směru. Tím poskytují zvýšený signál ve směru, kam je anténa natočená. Signál v ostatních směrech se stává slabším.
- **Yagi antény** – Používají se k rozšíření rozsahu venkovních AP v určitém směru [6].

3.4 Topologie

WLAN můžou využívat různé, síťové topologie. 802.11, má dva hlavní režimy topologie:

- **Ad hoc** – Připojování 2 zařízení, bez pomoci infrastruktury (například Bluetooth a Wi-Fi Direct). Komunikace peer-to-peer, bez použití AP nebo směrovače. Označuje se jako IBSS.
- **Režim Infrastruktury** – Pokud se bezdrátové zařízení připojí, přes AP v síti WLAN, tak se AP připojuje k síťové infrastruktuře pomocí DS, kabelovým distribučním systémem. Skládá se z několika komponent a poskytuje podporu klientům WLAN. Skládá se z dvou bloků topologie, BSS a ESS [1].

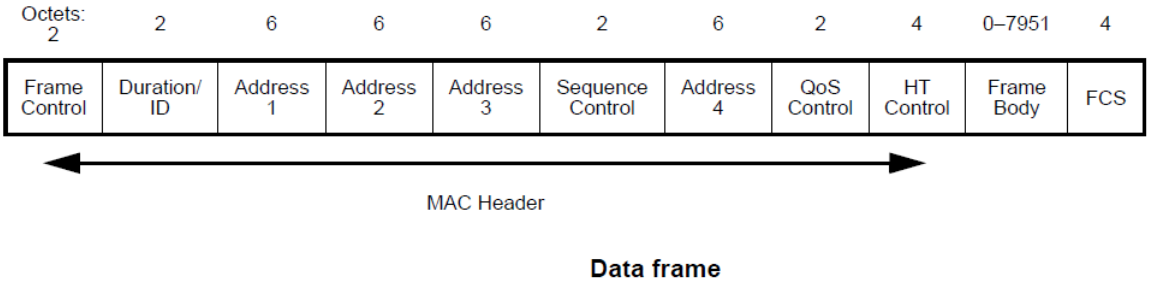
Základní servisní sada BSS – skládá se z jednoho AP, který propojuje všechny bezdrátové klienty. Všichni klienti v Oblasti základních služeb (BSA), komunikují, pokud jsou v téhle oblasti skutečného pokrytí. Když ji opustí, už komunikovat nemůžou. K identifikaci každé BSS, se používá MAC adresa 2. vrstvy, nazývá se Identifikátor sady základních služeb, BSSID [12].

Rozšířená servisní sada ESS – může spojovat dvě nebo více BSS, pokud poskytují slabé pokrytí. Spájejí se do ESS přes společný distribuční systém DS. Klienti z jednoho BSA, můžou komunikovat z klienty z jiných oblastí pokrytí, ale v rámci toho samého ESS. Každý systém je identifikován identifikátorem SSID a každý BSS v něm, jako BSSID. Lze taky stupňovat úroveň přístupu. Vlastně jednu buňku ESS, tvoří jeden AP a k němu připojení klienti [12].

3.5 Bezdrátový rámec 802.11

Formát bezdrátového rámce 802.11, je podobný tomu ethernetovému, ale obsahuje víc polí.

Rámec 802.11



Obr. 3. Rámec 802.11 [14]

Kontrola rámce – určuje typ rámce a má více podpolí

Doba trvání – doba potřebná k přijmu přenosu dalšího rámce

Adresa 1 – MAC adresa přijímatele

Adresa 2 – MAC adresa vysílače

Adresa 3 – MAC adresa cíle

Kontrola sekvencí – podřízené číslo sekvence a podpoložky fragmentu

Adresa 4 – většinou chybí, používá se při Ad hoc

Užitečné zatížení – data pro přenos

FCS – sekvence kontroly rámce, řídí chyby 2. vrstvy [11] [14]

3.6 Proces Připojení

Proces připojení klienta, je klíčovou součástí. Proces se nazývá skenování a může být ve dvou režimech.

Pasivní – AP periodickou inzercí svých majákových rámců, umožňuje zjistit klientům, které sítě a AP jsou v oblasti k dispozici a k použití.

Aktivní – klienti musí znát SSID, pak zahájí proces požadavkem sondy na víc kanálů. Požadavek sondy má SSID a podporovaný standard.

Autentifikace standardu 802.11 má dvě metody:

Otevřená autentizace – Používá se tam, kde není bezpečnost tak důležitá a poskytuje připojení k libovolnému AP. Klient chce ověřit a AP reaguje souhlasem.

Autentizace sdíleného klíče – Potřeba použít klíč, který je předem sdílený mezi AP a klientem [7].

3.7 Bezpečnost

Se zavedením bezdrátové sítě, se zvýšili nároky na bezpečnost. Díky moderním technologiím, nemusí útočník vstoupit do budovy, aby se připojil. O to víc, klienti, kteří mají v ochraně svých dat svá živobytí, dbají na zvýšenou bezpečnost.

K napadení bezdrátové sítě může dojít náhodně, nebo cíleně. Hrozby pro tyto sítě spočívají v útočnících s bezdrátovým přístupem, nepřátelských AP, zachycování dat a DoS útoky [6].

WLAN se zabezpečují proti vetřelcům a ochranou svých dat, těmito metodami:

- **Maskování SSID** – AP můžou deaktivovat rámce signálu SSID, ale musí ho manuálně identifikovat.
- **Filtrování MAC adres** – povolení přístupu na základě MAC adresy klienta.

I tak to není dostatečná ochrana, proto se bezdrátová síť zabezpečuje ověřovacími a šifrovacími systémy. Zavedeny byly dva typy autentizace, Otevřeného systému a Sdíleného klíče. Ověřování pomocí sdíleného klíče, poskytuje mechanismy jako WEP, WPA a WPA2, kvůli ověření a šifrování dat. Heslo musí být předem sdíleno.

WEP (Wired Equivalent Privacy) – poskytuje ochranu jako kabelové připojení. Data jsou šifrována metodou RC4 a statickým klíčem, což usnadňuje nabourání.

WPA (Wi-Fi Protected Access) – používá WEP, ale se silnějším šifrováním dat, TKIP (Temporary Key Integrity Protocol). Ten mění klíč pro každý paket.

WPA2/IEEE802.11i – průmyslový standard, k šifrování používá AES (Advanced Encryption Standard), nyní asi nejsilnější šifrovací protokol.

WPA a WPA2, používají tyto metody šifrování dat:

- **TKIP** – šifrovací metoda používaná WPA. Má podporu pro starší zařízení WLAN, protože řeší nedostatky WEP.
- **AES** – metoda používaná WPA2. Provádí stejné funkce jako TKIP, ale s mnohem silnějším šifrováním. Je to tím, že používá režim Počítání znaků a protokol CCMP [1], [6], [7].

4 OPEN SHORTEST PATH FIRST

4.1 Jedno-Oblastní Protokol OSPF

Aby v podnikové sítě mohli směrovače mezi sebou komunikovat, protože jejich hierarchické návrhy jsou škálovatelné pro velké sítě, tak používají pokročilejší protokoly stabilní linky. Jedním z protokolů stabilní linky je OSPF – Otevření Nejkratší Cesty jako První. Výborně funguje ve velkých hierarchických sítích, kde je důležitá rychlá konvergence. Je velice populární, hlavně kvůli ladění v mnoha ohledech. A navíc podporuje dvouvrstvý hierarchický návrh, což je nazýváno více oblastní OSFP [3].

Je to běžně implementovaný protokol, vyvinut jako náhrada za RIP. Má významné výhody, hlavně nabízí rychlejší konvergenci a nasazení v sítích velkých měřítek. Funkce a vlastnosti protokolu OSPF jsou:

- Je to beztřídní protokol, s podporou variabilního adresování.
- Používá Dijkstrův algoritmus pro výpočet nejkratší cesty – SPF.
- Udržuje směrovací tabulky.
- Velké sítě může rozdělit do oblastí – tím se sníží výpočet SPF, zmenší se směrovací tabulky a LSU (Link-state Update).
- Smyčkám předchází, pomocí databáze stavů linek. LSDB je stejná pro všechny směrovače, synchronizuje se pomocí zaplavení LSA. Její pomocí se tvoří směrovací tabulky.
- Je možnost použití manuální sumarizace, pro zmenšení směrovacích tabulek. Automatické ne.
- Updaty směrování se posílají, v případě potřeby.
- Je bezpečný, protože používá ověřování zpráv MD5.
- Používá protokol IP 89, takže si sám detekuje a opravuje chyby.
- Sousedství navazuje posíláním Hello paketů, každých 10 vteřin. Pak musí mít oba sousedi společné parametry.
- LSA se odesílají každých 30 minut, nebo při změnách. Šíří se zaplavováním.
- ID směrovače OSPF, je nejvyšší aktivní IP adresa směrovače.
- DR/BDR – volba podle priority, nebo ID směrovače. Probíhá jenom ve více oblastních sítích. Pokud selže zástupce DR, zvolí se BDR, jako nový DR [1].

4.2 Více přístupová síť OSPF

OSPF definuje pět typů sítí:

- **Pont-to-Point** – Dva směrovače, jedna společná linka.
- **BMA** (Broadcast Multiacces) – Propojení více směrovačů přes síť Ethernet.
- **NBMA** (Non-Broadcast Multiaccess) – Propojení více směrovačů, bez vysílání broadcastu.
- **Point-to-Multipoint** – Propojení více směrovačů, propojených v topologii rozbočovače a paprsků, přes NBMA.
- **Virtuální propojení** – Propojení vzdálených oblastí OSPF do oblasti páteře [12].

Více přístupová síť (multiaccess), je síť s více zařízeními na stejném médiu, se sdílenou komunikací. Všechny zařízení a multicast rámce jsou vidět. Tyto sítě vytvářejí zaplavení LSA rámci. Buď tím, že vytváří více přidružení z každým směrovačem, to by znamenalo nadměrný počet LSA v stejné síti. Druhá možnost, je rozsáhlé zaplavení LSA. Kdy směrovače nadměrně zaplavují svoje LSU při inicializaci [9].

Reklamní rámce LSA mají více typů, každý z nich obsahuje specifické informace. OSPF musí podporovat prvních pět typů LSA. Tyto typy jsou:

- **Typ 1** – informace o směrovači a přímo připojených rozhraních, pouze v rámci oblasti
- **Typ 2** – informace o síti LAN a směrovačích v ní, pouze v oblasti, generované DR
- **Typ 3** – sumarizace, pochází s ABR, sítě dostupné mimo oblast
- **Typ 4** - sumarizace ASBR, pocházejí z ABR pro ASBR
- **Typ 5** – informace o externích cestách, pochází s ASBR, externí autonomní systém
- **Typ 6** – multicast informace
- **Typ 7** – jiná rozšíření - NSSA

V sítích s více přístupy, se počet sousedů a zaplavení rámci LSA, řeší určeným směrovačem. DR se volí, jako sběrný a distribuční bod pro LSA. Záložní směrovač BDR, naslouchá komunikaci, a když selže DR, je vybrán jako nový. Ostatní směrovače, pokud nejsou DR a BDR, stávají se DROTHER. Volba směrovačů je založena, buď na prioritě, nebo ID. Priorita může být číslo v rozsahu od 1 do 255. Čím vyšší priorita, tím pravděpodobnější zvolení. Je-li hodnota priority 0, směrovač se nemůže stát DR. Výchozí hodnota priority směrovače, je nastavena na 1 [2], [9].

4.3 Více Oblastní OSPF

Příliš mnoho směrovačů, moc zatěžuje procesor a vytváří velikou databázi linek LSDB, protože pokrývá záznamy celé topologie a udržuje je pro každou síť v oblasti. Velká oblast způsobuje taky velikou směrovací tabulku. Ve výchozím nastavení OSPF, se sumarizace tras nedělá, a proto je směrovací tabulka velmi rozsáhlá. To znamená taky, že se provádí časté výpočty SPF. Ten přepočítává trasy a aktualizuje tabulku, protože se událi změny v topologii [1].

Proto se rozsáhlé sítě rozdělují na více oblastí. Oblast 0, je hlavní oblast, nazývaná oblast páteře. Všechny ostatní oblasti se připojují k ní. Více oblastní hierarchicko-topologické OSPF mají pár výhod:

Menší směrovací tabulky – Mezi oblastmi se sumarizují trasy, proto je ve směrovací tabulce méně položek.

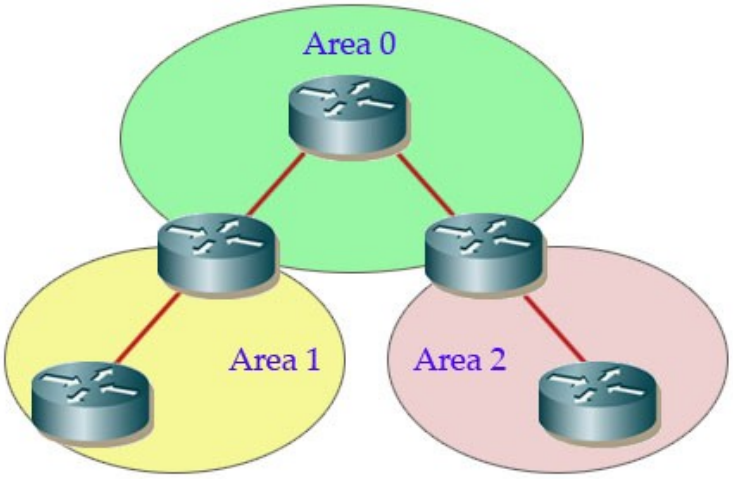
Menší režie aktualizací – Snižuje požadavky na paměť a zpracování, protože je méně směrovačů, vyměňujících LSA.

Menší frekvence výpočtů SPF – Lokalizuje dopad změn topologie v oblasti, protože zaplavení LSA se zastaví na její hranici [1].

Typy oblastí v OSPF jsou:

- **Standartní oblast** – přijímá updaty, sumarizované a externí cesty
- **Páteřní oblast** – propojuje všechny ostatní oblasti, má stejné vlastnosti jako standartní. Vždy je to Area 0/Oblast 0.
- **Stub oblast** – nepřímá trasy z ostatních autonomních systémů.
- **Totálně Stub Oblast** – nepřijímá sumarizované trasy mimo oblast. Cisco proprietární.
- **Not-so-stubby oblast NSSA** – importuje některé externí trasy typu 7 a převádí je na typ 5 [12].

Více oblastí protokolu OSPF



Obr. 4. Více oblastí protokolu OSPF

Typy směrovačů používaných v OSPF je víc a každý má své vlastnosti:

- **ABR (Area Border Router)** – Hraniční směrovač oblasti. Rozhraní má ve více oblastech a pro každou oblast samostatnou LSDB. Připojuje oblasti k páteři.
- **ASBR (Autonomous System Border Router)** – Má rozhraní ve více autonomních systémech, distribuuje cesty z jiných. Redistribuce se objevuje, když ASBR spojuje různé směrovací domény.
- **Interní směrovač** – Pouze v jedné oblasti.
- **Páteřní směrovač** – Aspoň jedno rozhraní v Oblasti 0 [1].

K rozpoznávání položek směrovací tabulky, nám slouží několik deskriptorů. Trasy IPv4jsou identifikovány pomocí těchto deskriptorů:

O – Směrovače typu 1 a 2 LSA, popisují detaily v rámci oblasti. Znamená to, že trasa je uvnitř oblasti.

O IA – Po obdržení souhrnných LSA na ABR směrovači, se přidají do LSDB a generuje do místní oblasti. Když se přijímá externí LSA, přidá se do LSDB a zaplavuje se s nimi celá oblast. Označení indikuje trasy interakce.

O E1 nebo **OE2** – Externí LSA ve směrovací tabulce, jako vnější cesta E1 a externí cesta E2 [10], [12].

4.4 Sumarizace tras OSPF

Sumarizace tras, udržuje směrovací tabulky malé. Jedná se o sumarizaci několika cest do jedné, pak propagované do oblasti páteře. Pomáhá také zvýšit stabilitu sítě, snižováním zbytečného zaplavování LSA rámci.

Shrnutí tras, lze nakonfigurovat pouze na ABR, nebo ASBR. Ty propagují souhrnnou trasu. Souhrnná trasa je typu 5.

Shrnutí trasy je možné dvěma způsoby:

Sumarizace trasy vnitřní oblasti – vyskytuje se na ABR a zahrnuje trasy z každé oblasti. Nevztahuje se na externí trasy.

Sumarizace Externí trasy – prostřednictvím redistribuce tras, pouze na ASBR [9].

5 ENHANCED INTERIOR GATEWAY ROUTING PROTOKOL

5.1 Přehled Protokolu EIGRP

Síťový technik, má při návrhu sítě, na výběr z více možností. Jeho plán musí zohledňovat, pokrytí, velikost provozu, náklady, výběr správných zařízení a samozřejmě směrovacího protokolu sítě. Dalším velice populárním směrovacím protokolem je EIGRP – Směrovací Protokol Rozšíření Vnitřní Brány. Ačkoli, je na pohled relativně lehký ke konfiguraci, jeho možnosti a funkce jsou velmi rozsáhlé a robustní.

EIGRP je pokročilý, distanční vektorový směrovací protokol, který používá více směrovacích tabulek, k řízení procesu směrování a obsahuje mnohé funkce, které nejsou k dispozici v jiných směrovacích protokolech. Používá se ve velkých, více protokolových sítích, na zařízeních Cisco [2].

Výchozí administrativní vzdálenosti pro EIGRP, jsou 90 pro cesty vnitřní a 170 pro cesty externí. Také využívá protokolově závislé moduly, k podpoře protokolů IPv4 a IPv6.

DUAL (Diffusing Update Based Algorithm) - Rozptylující Aktualizační Algoritmus, nachází se ve středu protokolu. Základní kámen protokolu EIGRP, který zaručuje bezproblémové a záložní cesty v celé doméně směrování. Uchovává všechny záložní trasy, aby se v případe potřeby mohli rychle přizpůsobit.

Sousední přidružení – Vytváření vztahů s přímo propojenými směrovači, také povolených s EIGRP. Přidružení se používají ke sledování stavu sousedů.

RTP (Reliable Transport Protocol) – jedinečný pro EIGRP a poskytuje dodávky paketů sousedům. RTP a sledování sousedů nastavuje stupeň DUAL.

Částečné a ohraničené aktualizace – Položky nestárnou. Částečné obsahují jenom informace o změnách trasy. Ohraničené, šíří částečné aktualizace směrovačům, které ovlivňují změny. Tím se minimalizuje šířka pásma.

Podporuje rovnoměrné a nerovnoměrné balancování zatížení cen [1], [8].

EIGRP používá pět různých typů paketů. Jsou odesílány spolehlivým a nespolehlivým přenosem. Mohou být odesílány jako unicast a multicast, pomocí protokolu RTP.

- **Hello Pakety** – Používá se k objevení sousedů a udržení sousedních přidružení. Odesílány jako multicast s nespolehlivým doručením, každých pět sekund. Směrovač

předpokládá obdržení Hello paketů od souseda, pokud jo, trasy zůstávají životaschopnými. Používá se časovač zadržení, pro určení doby čekání k obdržení dalšího paketu, k prohlášení že je soused nedosažitelný.

- **Aktualizační pakety** – Propagují sousedům informace o směrování. Odesílány jako unicast i multicast, se spolehlivým doručením, pouze v případě potřeby. To znamená, že posílá přírůstkové aktualizace pouze při změně stavu cíle.
- **Potvrzovací pakety** (ACK) – Potvrzují přijetí zprávy, odeslané spolehlivým doručením. Odesílány jako unicast, s nespolehlivým doručením. Je to vlastně Hello paket bez jakýchkoli dat.
- **Dotazové pakety** – Dotazují se tras od sousedů. Odesílány jako unicast i multicast, se spolehlivým dodáním.
- **Pakety odpovědí** – Odpověď na dotaz EIGRP. Odesílány jako unicast, se spolehlivým doručením [8].

5.2 Metrika

Kompozitní metrika ve výchozím nastavení EIGRP, používá tyto hodnoty pro výpočet preferované cesty do sítě:

- **Šířka pásma (BW)** – Nejpomalejší šířka pásma, ze všech rozhraní, od zdroje k cíli.
- **Zpoždění (DLY)** – Součet všech zpoždění po cestě.
- **Spolehlivost (Reliability)** – Nejhorší spolehlivost mezi cílovou destinací a zdrojem. Spolehlivost rozhraní se počítá jako zlomek 255.
- **Zatížení (Txload/Rxload)** – Nejhorší zatížení na lince mezi zdrojem a cílem. Počítá se na základě šířky pásma a rychlosti paketů. Vysílání a zatížení, se počíta jako zlomek 255.

EIGRP používá, kompozitní metrický vzorec, složený z hodnot K1 až K5. K1 a K3, identifikují šířku pásma a zpoždění, s výchozími hodnotami 1. K2 je zatížení, K4 s K5, představují spolehlivost a jsou nastaveny na 0 [1].

Výpočet metriky směrovací tabulky, pro výběr nejlepších cest, dělá EIGRP automaticky. Postup je následovný:

- Určí se linka z nejmenší šířkou pásma (Například 1 000 000 kb/s).

- Určí se hodnota zpoždění pro každé rozhraní na cestě do cíle. Spočítají se všechna zpoždění a vydělí 10.
- EIGRP používá 32 bitovou hodnotu, ale číslo vyjde jako 24 bitové. Proto se násobí 256 a rozšíří se na 32 [10].

5.3 DUAL

Tomuto algoritmu se jinak říká i srdce protokolu EIGRP. Používá několik důležitých termínů, které jsou v centru mechanismu vyhnutí se smyčkám:

- **Successor (Nástupce)** – Nástupcem se volí sousední směrovač, který přesměrovává pakety a je cestou z nejnižší cenou cesty do cíle. IP adresa nástupce, je v tabulce hned za slovem via (přes). Tabulky obsahují, jenom nejlepší cestu nástupce.
- **Dosažitelná vzdálenost (FD)** – Nejnižší vypočítaná metrika dosažení cíle. V tabulce je uvedena jako druhé číslo v závorkách.
- **Dosažitelný nástupce (FS)** – Záložní cesty, jenž dokáží rychle konvergovat topologii, bez překomponování. Je to vlastně soused, z cestou beze smyček a splňuje realizovatelnou podmínku FC.
- **Ohlášená vzdálenost (RD)** a **Reklamní vzdálenost (AD)** – Jednoduše vzdálenost souseda ke stejnému cíli.
- **Realizovatelná podmínka (FC)** – Podmínka je splněna, pokud RD souseda je menší, než vzdálenost do cíle. Je-li menší, trasa je bez smyček.

DUAL se používá na získání volné smyčky, během výpočtu cesty. Tím se umožní synchronizace všech směrovačů, kterých se týkají změny topologie. Poskytuje to rychlejší konvergenci, než u jiných protokolů.

Rozhodováni výpočtů cest DUAL algoritmu, provádí FSM (Finite State Machine), což je model složený z tří položek. Konečný počet stavů, přechody mezi stavy a operace. FSM sleduje všechny cesty a vybírá tu z nejnižší cenou, která bude vložena do směrovací tabulky. Pokud selže, nebo neexistuje žádné FS, tak DUAL uvede síť do aktivního stavu a dotáže se sousedům o nového nástupce [1], [2], [8].

5.4 Sumarizace cest EIGRP

Automatická Sumarizace

Zakázaní, nebo povolení automatické sumarizace cest, je jedna z nejběžnějších metod ladění. Protože umožňuje směrovači seskupovat sítě a propagovat je, jako jednu skupinu, pomocí jedné sumarizované cesty. Následkem je snížení počtu položek v aktualizacích směrování a ve směrovacích tabulkách. To vede k snížení využití šířky pásma a rychlejšímu hledání v tabulkách. Standardně je automatické shrnutí deaktivováno [8].

Manuální Sumarizace

Protože protokol EIGRP, je beztřídní a obsahuje masku podsítě v aktualizacích, v manuálním shrnutí se můžou vyskytnout trasy supernet. Je to agregace několika hlavních adres sítě.

Postup manuální sumarizace je:

Napíšou se sítě v binárním kódu. Sumarizovaná maska podsítě, se hledá porovnáváním bitů zleva doprava. Hledají se odpovídající bity, když narazíte na neodpovídající je konec. Spočítá se počet odpovídajících bitů zleva a to určuje masku podsítě shrnuté trasy. Tím se rapidně zredukuje počet celkových tras ve směrovacích tabulkách a taky se vyžaduje menší využití šířky pásma.

Sumarizované trasy se propagují do sítě, pomocí redistribuce. Redistribuované cesty se identifikují:

- **D** – Cesta naučená z aktualizace EIGRP.
- * - Kandidát na výchozí trasu.
- **EX** – Externí trasa EIGRP, nebo statická trasa mimo doménu směrování.
- **170** – Administrativní vzdálenost externí trasy [1], [8].

5.5 Autentifikace EIGRP

Kvůli ohrožení směrovačů, nebo koncových uživatelů, se pro bezpečnost používá, autentizace směrovacích protokolů pomocí algoritmu MD5. Aby se směrovač ujistil, že je všechno z důvěryhodného zdroje, používá tři složky:

- Šifrovací algoritmus
- Klíč algoritmu, sdílený jen směrovači
- Obsah samotného paketu

MD5 zajišťuje, komunikují jen směrovače z předem sdíleným klíčem a proces ověřování začne tím, že se vytvoří klíčenka a aspoň jeden klíč. Zadá se ID klíče v rozsahu od 0 do 2 147 483 647. ID klíče musí být stejné ve všech směrovačích. Zadá se klíčenka, něco jako heslo, i to musí být stejné, pro správné ověření [8].

Porovnání vlastností směrovacích protokolů

	Distance Vector				Link State	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Speed Convergence	Slow	Slow	Slow	Fast	Fast	Fast
Scalability - Size of Network	Small	Small	Small	Large	Large	Large
Use of VLSM	No	Yes	No	Yes	Yes	Yes
Resource Usage	Low	Low	Low	Medium	High	High
Implemenation and Maintenance	Simple	Simple	Simple	Complex	Complex	Complex

Obr. 5. Porovnání vlastností směrovacích protokolů

6 CISCO INTERNETWORK OPERATING SYSTEM

6.1 Úvod

Produkty společnosti Cisco, jsou mimořádně rozmanité. Každá organizace, podnik, nebo zákazník, si vybírá z velmi širokého spektra síťových zařízení, k rozvážnému určení ideální kombinace pro svou síť. Při výběru, je nutné zvažovat modernizaci, proto je velmi důležité vybrat si ten správný obraz IOS – Internetový Operační Systém, se správnou sadou funkcí a verzí. Ty si každý zákazník může zvolit, podle svých specifických potřeb. Operační systém je používaný jenom ve směrovačích a přepínačích Cisco. Je to vlastně balíček, pevně integrovaných funkcí směrování, přepínání, propojování a telekomunikace [12].

6.2 Vydání Softwaru Cisco IOS

IOS podporuje velké množství funkcí a technologií. Pro vyhovění požadavků trhu, je software organizován do rodiny vydání softwarových vlaků. Rodina obsahuje několik verzí IOS a ty:

- Sdílejí kódovou základnu
- Používají se na příslušné platformy HW
- Překrýváni pokrytí podpory

Při vydání softwaru, spolu sním, existují další verze, vytvořené pro implementaci nových funkcí a oprav některých chyb. Ty se označují jako vlaky. Vlak IOS, se používá k dodávce verzí se společnou kódovou základnou. Může obsahovat víc vydání [5].

6.2.1 Vlaky Cisco IOS 12.4

Rodina vydání softwaru 12.4, má dva vlaky. Hlavní vlak 12.4 a vlak 12.4T. Hlavní vlak přijímá opravy softwaru s cílem zvýšení kvality. Označují se taky jako vydání údržby (MD). Hlavní vlak je vždy spojen z vlakem technologickým (T vlakem). T vlak, přijímá nové funkce podpory softwaru a hardwaru, spolu z opravami, které má i hlavní vlak. 12.4T je označován za vydání včasného nasazení (ED).

Číslování vlaků 12.4, používá schéma:

- **Hlavní vlak** – číslo vlaku, ID údržby a ID obnovení – například 12.4 (21a)
- **T vlak** – číslo vlaku, ID údržby, ID vlaku a ID obnovení – například 12.4 (20) T1

Číslo v závorce, indikuje o kolikáté, obnovení se jedná. Obnovení je proces obdržení údržby, oprav a funkcí.

6.2.2 Vlaky Cisco IOS 15.0

Poskytují několik vylepšení:

- Nová podpora hardwaru a funkcí
- Nové předvídatelné vydání a obnovení
- Proaktivní principy podpory vydání
- Zjednodušené číslování

Používá se jiný model vydáním jako u 12.4. Hlavní vlak 15 a T vlak, mají prodloužené vydání údržby EM a standartní údržbu T. Hlavní vlaky, jsou označovány, jako M vlaky. EM obsahuje funkce a podporu hardwaru. Nový model vydání Cisco IOS zahrnuje, funkce dědičnosti z 12.4, vydávány dva až tři krát ročně. A vydání obnovy údržby M a T, má jenom opravy chyb [1], [9].

Číslování vlaků 15.0:

- **Vydání EM** – Pro dlouhodobou údržbu. Hlavní vlak obsahuje funkce z předchozích verzích, plus přírůstková vylepšení nových funkcí a podpory. Příklad číslování, 15.0(1)M1, je první obnova údržby.
- **Vydání T** – Pro krátké verze aplikací, aby se tolik nečekalo na EM. Poskytuje pravidelné opravy chyb a kritickou opravu podpory chybových sítí. Příklad číslování, 15.1(1)T1, je první obnovení údržby [1].

6.3 Licencování Cisco IOS

Vydání softwaru Cisco IOS 15.0, obsahuje nové sady funkcí pro platformy, zjednodušující výběr obrazu. Technologické balíčky funkcí, jsou povoleny v univerzálním obrazu, za pomoci licenčních klíčů k aktivaci. Licence jsou podporovány na platformách Cisco ISR G2.

Technologické balíčky, které jsou k dispozici:

- IP Base – předpoklad k instalaci ostatních balíčků
- Data
- Unified Communications (UC)
- Bezpečnost (SEC)

Proces Licencování:

Krok 1 – Zakoupení balíčku nebo funkce – Při zakoupení softwaru, obdržíte certifikát, který obsahuje licenční klíč pro aktivaci produktu PAK a důležité informace o licenční smlouvě. PAK slouží, jako potvrzení k získání licence. Je to 11 místní alfanumerický klíč od společnosti Cisco.

Krok 2 – Získání licence – Získání licenčního souboru, pro aktivaci softwaru. Dá se získat, přes aplikaci CLM, což je správce licencí Cisco. Nebo se dá získat registrací na webovém portálu společnosti Cisco. Obě možnosti vyžadují číslo PAK a jedinečné ID zařízení UDI. Během nákupu se obdrží PAK a UDI je kombinací PID produktu a sériového čísla zařízení SN.

Krok 3 – Instalace licence – K nainstalování se použije příkaz ***license install url-lokace-uložení***, a pak jak se znovu načte směrovač, je licence aktivována [1], [9], [12].

II. PRAKTICKÁ ČÁST

7 KAPITOLA 0 – PŘEDSTAVENÍ KURZU

Škálování sítí [1]

7.1 Škálování Sítí

7.1.1 Zpráva Pro Studenta

7.1.1.1 Vítejte

Vítejte v kurzu CCNA R&S Škálování Sítí. Cílem tohoto kurzu je seznámit vás se základními koncepcemi a technologiemi sítí. Tyto on-line studijní materiály vám pomůžou při rozvíjení dovedností potřebných pro plánování a implementaci malých sítí v celé řade aplikací. Specifické dovednosti v jednotlivých kapitolách jsou popsány na začátku každé kapitoly.

Můžete použít svůj chytrý telefon, tablet, notebook nebo stolní počítač k přístupu ke svému kurzu, účastnit se diskusí se svým instruktorem, prohlížet své známky, číst nebo zkoumat text a prakticky používat interaktivní média. Avšak, některé média jsou složité a musí být prohlíženy na počítači, stejně jako činnosti Packet Traceru, kvízů a zkoušek.

7.1.1.2 Globální komunita

Když se účastníte v Síťové Akademii, tak se zapojíte do globální komunity, které spojili společné cíle a technologie. Školy, vysoké školy, univerzity, a jiné subjekty ve více než 160 zemích, které se programu účastní. Vizualizace globální komunity Síťové Akademie je k dispozici na http://www.netacad.com.

Podívejte se na oficiální stránce Cisco Networking Academy na Facebooku a LinkedIn. Na facebookové stránce se můžete setkat a spolupracovat s ostatními studenty Síťové Akademie z celého světa. LinkedIN stránky Síťové akademie Cisco vás spojí z nabídkami práce a můžete vidět, jak jiní efektivně komunikují o svých dovednostech.

7.1.1.3 Víc než jen informace

Výukové prostředí NetSpace je důležitou součástí celkové zkušenosti z kurzu pro studenty a instruktory v Síťové Akademii. Tyto on-line materiály kurzu zahrnují studijní text a související interaktivní média, simulační aktivity Packet Traceru, laboratoře s reálným vybavením, vzdálený přístup k laboratořím a mnoho různých druhů kvízů. Všechny tyto materiály poskytují důležitou zpětnou vazbu, která vám pomůže zhodnotit své pokroky v celém průběhu kurzu.

Materiál v tomhle kurzu zahrnuje širokou škálu technologií, které usnadňují, jak lidi pracují, žijí, hrají si a učí se komunikovat prostřednictvím zvuku, videa a jiných dat. Sítě a internet mají vliv na lidi různě v různých částech světa. I když jsme pracovali s instruktory z celého světa, abychom vytvořili tyto materiály, protože je velmi důležité spolupracovat se svým instruktorem a spolužáky, aby se materiál v tomto kurzu vztahoval na vaši místní situaci.

7.1.1.4 Praxe vede k mistrovství

V typické lekci, po učení o tématu poprvé, si budete kontrolovat znalosti z některými položkami interaktivních médií. Pokud se najdou nové příkazy k učení, budete je praktikovat s pomocí kontrole syntaxe, před použitím příkazů na konfiguraci nebo potížemi ze sítí v Packet Traceru, síťového simulačního nástroje. Dále budete dělat praktické aktivity na reálném vybavení ve třídách, nebo k nim vzdáleně přistupovat přes internet.

Packet Tracer může také poskytovat dodatečné trénování kdykoliv, tím že vytvoříte své vlastní aktivity nebo budete chtít soutěžně otestovat své dovednosti se spolužáky v hrách pro více hráčů. Bohatou zpětnou vazbu o dovednostech, které jste schopni prokázat u testů a závěrečné zkoušky vám zprostředkuje posouzení vašich dovedností v integračních laboratořích Packet Traceru.

7.1.1.5 Mysl otevřená doširoka

Důležitým cílem v oblasti vzdělávání je obohatit vás, studenty, tím že rozšíříme vaše znalosti a jak je realizovat. Je důležité si uvědomit, že instruktážní materiály i instruktor můžou celý proces jenom usnadnit. Je nutné učinit závazek sami sobě, učit se novým věcem. Následující stránky obsahují několik návrhů, které vám pomůžou s učením a přípravou na přechod svých dovedností na pracoviště.

7.1.1.6 Prozkoumejte svět sítí

Packet Tracer je síťový nástroj pro výuku, který podporuje širokou škálu fyzických a logických simulací. Také poskytuje vizualizaci nástrojů, které vám pomohou pochopit vnitřní fungování sítě.

Předem vyrobené aktivity, které poskytují širokou škálu zkušeností, se skládají ze simulací sítí, her, aktivit a různých výzev. Tyto nástroje vám pomohou rozvíjet porozumění toho, jak fungují toky dat v síti.

7.1.1.7 Vytvořte si vlastní světy

V Packet Traceru můžete také vytvořit své vlastní pokusy a scénáře pro vytváření sítí. Doufáme, že v průběhu času zvážíte jeho použití – a to nejen pro využití předpřipravených aktivit, ale také, abyste se stali autory, objevovateli a experimentátoři.

On-line studijní materiály mají v sobě aktivity Packet Traceru, které se spustí na počítačích s operačním systémem Windows. Samozřejmě jen když je nainstalovaný. Tato integrace může také pracovat na jiných operačních systémech používajících emulaci Windows.

7.1.1.8 Přehled kurzu

Cílem tohoto kurzu je architektura, komponenty a operace směrovačů a přepínačů ve větších a víc komplexnějších sítích. Naučíte se jak nakonfigurovat směrovače a přepínače pro pokročilé funkce. Budete schopni provést následující kroky:

Konfigurovat a řešit problémy DHCP a DNS operací pro IPv4 a IPv6

Popsat operace a výhody protokolu STP

Konfigurovat a řešit problémy operací STP

Popsat operace a výhody agregace linek a Cisco VLAN Trunk Protokolu (VTP)

Konfigurovat a řešit problémy VTP, STP a RSTP

Konfigurovat a řešit problémy základních operací směrovačů v komplexních sítích pro IPv4 a IPv6

Konfigurovat a řešit problémy pokročilých operací směrovačů a implementace RIP, OSPF a EIGRP směrovacích protokolů pro IPv4 a IPv6

Spravovat Cisco IOS licencování softwarů a konfiguračních souborů

Na konci tohoto kurzu budete schopni nakonfigurovat a řešit problémy směrovačů a přepínačů a řešit běžné problémy s OSPF, EIGRP, STP a VTP protokoly v obou IPv4 i IPv6 sítích. Taky budete schopni rozvíjet svoje znalosti a dovednosti, potřebné k implementaci DHCP a DNS operací v síti.

8 KAPITOLA 1 – PŘEDSTAVENÍ DO ŠKÁLOVÁNÍ SÍTÍ

8.1 Představení do škálování sítí

8.1.1 Úvod

8.1.1.1 Úvod

Jako firma roste, tak rostou i její síťové požadavky. Podniky spoléhají na síťovou infrastrukturu, která poskytuje kritické služby. Síťové výpadky mohou vést ke ztrátě příjmů a ztracení zákazníky. Síťoví návrháři musí navrhnout a postavit podnikovou síť, která je škálovatelná a vysoce dostupná.

Tato kapitola popisuje strategie, které mohou být použity k systematickému návrhu vysoce funkční sítě, jako je hierarchický návrh sítě modelu Cisco Enterprise Architecture a vhodným výběrem zařízení. Cíle návrhu sítě jsou omezit počet přístrojů ovlivněných selháním jednoho síťového zařízení, předložit plán a cestu pro růst a vytvořit spolehlivou síť.

8.1.1.2 Aktivita cvičení – Síť podle vzhledu

Váš zaměstnavatel otevírá novou pobočku.

Vy jste byl přeložen k jedné síti jako její správce, kde vaším úkolem bude navrhnout a udržovat novou pobočkovou síť.

Správci sítě v ostatních odvětvích použily Cisco třívrstvého hierarchického modelu při navrhování svých sítí. Vy rozhodnete použít stejný přístup.

Chcete-li získat představu o tom, jak používat hierarchický model, tak můžete udělat pro zlepšení procesu návrhu výzkum na toto téma.

8.2 Implementace Návrhu Sítě

8.2.1 Hierarchický návrh sítě

8.2.1.1 Potřeba škálování sítí

Podniky stále více spoléhají na jejich síťové infrastruktury, na schopnost zajistit kritické služby. Jako podniky rostou a vyvíjejí se, tak najmou více zaměstnanců, otevřou pobočky a

expandují na světové trhy. Tyto změny přímo ovlivňují požadavky na síť. Velké podnikatelské prostředí s mnoha uživateli, lokacemi a systémy je označována jako podnik. Podniková síť je síť, která se používá k podpoře obchodních podniků.

Po kliknutím na tlačítko Přehrát na obrázku se zobrazí animace malé sítě expandující do podnikové sítě.

Podnikové sítě musí podporovat výměnu různých typů síťového provozu, včetně datových souborů, e-mailů, IP telefonie a video aplikace pro více obchodních jednotek.

Všechny podnikové sítě musí:

- Podporovat kritické aplikace
- Podporovat konvergování síťových přenosů
- Podporovat rozmanité obchodní potřeby
- Poskytovat centralizované administrativní řízení

8.2.1.2 Zařízení obchodního podniku

Uživatelé očekávají, že podnikové sítě, jako je například znázorněno na obrázku, budou aktivní 99,999 procent času. Výpadky v podnikové síti zabraňují podniku vykonávat běžné denní aktivity, což může vést ke ztrátě příjmů, zákazníků, dat a možností.

Chcete-li získat tuto úroveň spolehlivosti, vysoká úroveň, zařízení podnikových tříd jsou běžně instalována v podnikové síti. Je navržena a vyrobena tak, že má přísnější normy než zařízení nižší úrovně, ve firemních zařízeních se pohybují velké objemy síťového provozu.

Zařízení podnikové třídy je navrženo kvůli spolehlivosti, s funkcemi jako jsou redundantní napájecí zdroje a schopnost převzetí služeb při selhání. Možnost převzetí služeb při selhání je schopnost zařízení přejít z nefunkčního modulu, služby či zařízení k fungujícímu provozu s jednou malou nebo žádnou přestávkou.

Zakoupení a instalace zařízení podnikové třídy nutně neodstraňuje potřebu správného návrhu sítě.

8.2.1.3 Hierarchický návrh sítě

Pro optimalizaci šířky pásma v podnikové síti, je potřeba zorganizovat tuto síť tak, že provoz zůstane místní a není zbytečně rozšířen do jiných částí sítě. Použitím třívrstvého hierarchického modelu návrhu si pomáháme organizovat síť.

Tento model rozděluje funkce sítě do třech odlišných vrstev, jak je znázorněno na obrázku 1:

- Přístupová vrstva
- Distribuční vrstva
- Jádrová vrstva

Každá vrstva je navržena tak, aby splňovala specifické funkce.

Přístupová vrstva poskytuje připojení pro uživatele. Distribuční vrstva se používá, aby předala provoz z jedné lokální sítě do druhé. Nakonec, jádrová vrstva představuje vysokorychlostní páteřní vrstvu mezi rozptýlenými sítěmi. Provoz uživatelů začíná v přístupové vrstvě a prochází ostatními vrstvami, pokud je funkcionalita těchto vrstev vyžadována.

I přesto, že hierarchický model má tři vrstvy, některé menší podnikové sítě můžou implementovat dvoustupňový hierarchický návrh. Ve dvoustupňové hierarchické konstrukci, jádrové a distribuční vrstvy jsou sloučeny do jedné vrstvy, což snižuje náklady a složitost, jak je znázorněno na obrázku 2.

8.2.1.4 Cisco podniková architektura

Cisco podniková architektura rozděluje síť do funkčních komponentů při zachování jádrové, distribuční a přístupové vrstvy. Jak ukazuje obrázek, primární moduly Cisco podnikové architektury zahrnují:

- Podnikový kampus
- Podniková hrana
- Hrana poskytovatele služeb
- Dálkový

Podnikový kampus

Podnikový kampus se skládá z celého areálu infrastruktury tak, aby zahrnoval přístupovou, distribuční a jádrovou vrstvu. Modul přístupové vrstvy obsahuje přepínače 2 nebo 3 vrstvy, aby poskytoval požadovanou hustotu portů. Implementace VLAN a dálkových napojení na distribuční vrstvě budovy dochází zde. Redundance do přepínačů distribuční vrstvy budovy je důležitá. Modul distribuční vrstvy zahrnuje přístup budovy za pomoci zařízení 3 vrstvy. Směrování, řízení přístupu, a QoS jsou prováděny na tomto modulu distribuční vrstvy. Modul jádrové vrstvy zajišťuje vysokorychlostní propojenost mezi moduly distribuční vrstvy,

serverových datových farmách a podnikovou hranu. Redundance, rychlá konvergence a odolnost proti chybám je to na co se zaměřujeme při návrhu v tomto modulu.

Kromě těchto modulů, Podnikový kampus může obsahovat další sub-moduly, jako jsou:

- **Serverová farma a centrum datových modulů** - Tato oblast poskytuje vysokorychlostní připojení a ochranu pro servery. Je velmi důležité zajistit bezpečnost, redundanci a odolnost proti chybám. Systémy pro správu sítě monitorují výkon sledováním zařízení a dostupnosti sítě.
- **Moduly služeb** - Tato oblast poskytuje přístup ke všem službám, jako jsou služby IP telefonie, služby bezdrátového ovladače a sjednocené služby.

Podniková hrana

Podniková hrana se skládá z Internetu, modulů VPN a WAN spojující podnikovou a síť poskytovatele služeb. Tento modul rozšiřuje služby podniku do vzdálených sítí a umožňuje, aby podnik mohl využívat Internet a partnerské zdroje. Poskytuje QoS, vyztuženou politiku, úrovně služeb a zabezpečení.

Hrana poskytovatele služeb

Hrana poskytovatele služeb poskytuje Internet, veřejné telefonní sítě (PSTN) a služby WAN.

Všechna data, která vstupují nebo opouští podnikovou kompozitní síťový model (ECNM) prochází všechna zařízení elektronického sběru dat. To je bod, aby všechny pakety mohli být vyšetřeny a udělat rozhodnutí, zda by paketu mělo být povoleno vstoupit do podnikové sítě. Systémy detekce průniku (IDS) a systém prevence průniku (IPS) lze konfigurovat také na podnikové hrany k ochraně proti škodlivým aktivitám.

8.2.1.5 Poruchové domény

Dobře navržená síť řídí nejen provoz, ale také omezuje rozsah selhání domén. Chybná doména je oblast sítě, která je ovlivněna, když kritické zařízení nebo síťová služba vykazuje problémy.

Funkce zařízení, která původně určí selhání má vliv na selhání domény. Například nefunkční přepínač na síťovém segmentu běžně ovlivňuje pouze počítače jen na tomto segmentu. Nicméně, v případě, že směrovač selže, ten který připojuje tento segment pro ostatní, má dopad mnohem větší.

Použití redundantních linek a spolehlivému vybavení podnikové třídy se minimalizuje možnost narušení v síti. Menší selhání domén, snižuje dopad výpadku na produktivitu společnosti. Také se zjednoduší proces řešení problémů, a to tím, že se zkracují prostoje pro všechny uživatele.

Na obrázku klikněte na jednotlivá síťová zařízení pro zobrazení příslušné domény selhání.

Omezení rozsahu selhání domén

Vzhledem k tomu, že selhání v jádrové vrstvě sítě, může mít potenciálně velký dopad, tak se síťový návrhář často se zaměřuje svoje úsilí, aby se zabránilo selháním. Toto úsilí může značně zvýšit náklady na realizaci sítě. V hierarchickém modelu návrhu, je nejjednodušší a obvykle nejméně nákladné řídit velikost domény selhání v distribuční vrstvě. V distribuční vrstvě, mohou být chyby sítě obsaženy na menší oblasti a tak ovlivňovat méně uživatelů. Při použití zařízení 3 vrstvy v distribuční vrstvě, každý směrovač funguje jako brána pro omezený počet uživatelů přístupové vrstvy.

Nasazení bloku přepínačů

Směrovače, nebo vícevrstvé přepínače, jsou obvykle rozmístěny ve dvojicích s přepínači přístupové vrstvy a jsou rovnoměrně rozdělený mezi nimi. Tato konfigurace se odporučuje pro bloky přepínačů budovy nebo jednoho oddělení. Každý blok přepínačů působí nezávisle na ostatních. V důsledku toho, selhání jednoho zařízení nezpůsobí pád sítě. I selhání celého bloku přepínačů nemá vliv na nějak významný počet koncových uživatelů.

8.2.2 Rozšiřování sítě

8.2.2.1 Návrh pro škálovatelnost

Chcete-li podporovat podnikovou síť, návrhář si musí vytvořit strategii s cílem umožnit síti být k dispozici a efektivně a snadno škálovat. V základním provedení strategie sítě jsou zahrnuty následující doporučení:

- Použijte rozšiřitelné, modulární zařízení nebo úzkou skupinu zařízení, které lze snadno upgradovat pro zvýšení schopnosti. Moduly zařízení mohou být přidány do stávajících zařízení na podporu nových funkcí a zařízení, aniž by bylo nutné velké modernizace technologií. Některá zařízení mohou být integrovány do skupiny, ale chovají se jako jedno zařízení a to přináší zjednodušení řízení a konfigurace.
- Navrhnout hierarchickou síť, aby zahrnovala moduly, které mohou být přidány, modernizovány a modifikovány podle potřeby, aniž by to ovlivnilo návrh ostatních

funkčních oblastí sítě. Například vytvořit separátní přístupovou vrstvu, která může být rozšířena bez ovlivnění distribuční a jádrové vrstvy sítě podniku.

- Vytvoření strategie adresování IPv4 nebo IPv6, která je hierarchická. Pečlivé plánování IPv4 adresace eliminuje potřebu znovu řešit adresaci sítě pro podporu dalších uživatelů a služeb.
- Vyberte si směrovače nebo vícevrstvé přepínače s cílem omezit vysílání a filtrovat jiný nežádoucí provoz na síti. Používejte zařízení 3 vrstvy pro filtrování a omezení provozu v jádru sítě.

Jak je znázorněno na obrázku, mezi pokročilejší požadavky na návrh sítě patří:

- Implementace redundantního spojení v síti mezi kritickými zařízeními a mezi zařízeními přístupové a jádrové vrstvy.
- Implementace více spojení mezi zařízeními, buď s Agregací linek (EtherChannel) nebo balance zatížení stejné ceny a tím zvětšit šířku pásma. Kombinování více ethernetových linek do jediné zatížené balancované konfigurace EtherChannelu, to má za následek zvýšení dostupnosti šířky pásma. Implementace Etherchannelu lze použít při rozpočtových omezeních zakazujících obstarání vysokorychlostních rozhraní a běžící vlákno.
- Implementace bezdrátového připojení s cílem umožnit mobilitu a expanzi.
- Použitím škálovatelného směrovacího protokolu a implementací funkcí v tomto směrovacím protokolu a pro izolaci aktualizace směrování a minimalizaci velikosti směrovací tabulky.

8.2.2.2 Plánování redundance

Implementace redundance

U mnoha organizací má dostupnost sítě zásadní význam pro podporu podnikatelských potřeb. Redundance je důležitou součástí návrhu sítě kvůli prevenci narušení síťových služeb tím, že minimalizuje možnost selhání jediného bodu. Jedním ze způsobů, kterým se provádí redundance je instalace duplicitních zařízení a poskytování služeb zotavení se pro kritická zařízení.

Jiný způsob, kterým se provádí redundance, jsou redundantní cesty, jak je znázorněno na obrázku. Redundantní cesty nabízejí alternativní cesty pro fyzické údaje, které procházejí sítí. Redundantní cesty v přepínané síti podporují vysokou dostupnost. Nicméně, v důsledku

operací přepínačů, redundantní cesty v přepínané Ethernetové sítí můžou způsobit logické smyčky na vrstvy 2. Z tohoto důvodu je nutno použít Spanning Tree Protocol STP (STP).

STP odstraňuje smyčky 2 vrstvy, jsou-li redundantní linky použity mezi přepínači. Je to tím, že poskytuje mechanismus pro zákaz redundantní cesty v přepínané síti, dokud to není nutné, jako když se objeví chyby. STP je otevřený standardní protokol, který se používá v přepínaném prostředí pro vytvoření logické topologie bez smyček.

Další podrobnosti o redundanci sítě LAN a operacích STP jsou zahrnuty v kapitole s názvem "Redundance LAN".

8.2.2.3 Zvětšování šířky pásma

Implementace EtherChannelu

V hierarchickém návrhu sítě, některé linky mezi přístupovými a distribučními přepínači můžou potřebovat zpracovávat větší množství provozu, než ostatní linky. Jak se provoz z více linek sbíhá do jednoho, odchozího spojení je možné, že linka se stane zúženou cestou. Agregace linek umožňuje správci zvýšit množství šířky pásma mezi zařízeními tím, že vytvoří jednu logickou linku, která se skládá z několika fyzických linek. EtherChannel je forma agregace linek používané v přepínaných sítích, jak je znázorněno na obrázku.

EtherChannel používá existujících portů přepínače, protože dodatečné náklady na modernizaci linky na rychlejší a dražší spojení nejsou nutné. Je viděn jako jedno logické spojení pomocí Etherchannel rozhraní. Většina konfiguračních úloh se dělá na tomhle rozhraní, namísto na každém jednotlivém portu a to zajistí konzistenci konfigurace celé linky. Nakonec, konfigurace využívá balance zatížení mezi linkami, které jsou součástí téže EtherChannelu a v závislosti na hardwarové platformě, může být implementována jedna nebo více metod na balanci zatížení.

Operace a konfigurace nalezněte v kapitole Agregace linek

8.2.2.4 Rozšíření přístupové vrstvy

Implementace bezdrátového připojení

Tato síť musí být navržena tak, aby bylo možné rozšířit síťový přístup osob a zařízení, podle individuální potřeby. Stále důležitějším aspektem rozšíření konektivity přístupové vrstvy je prostřednictvím bezdrátového připojení. Poskytování bezdrátového připojení nám nabízí mnoho výhod, jako je zvýšení flexibility, snížení nákladů a schopnost růst a přizpůsobit se měnícím se požadavkům sítě a firmy.

Chcete-li komunikovat bezdrátově, koncová zařízení vyžadují bezdrátovou síťovou kartu, která zahrnuje rádiový vysílač / přijímač a potřebný softwarový ovladač, aby byla funkční. Navíc je vyžadován bezdrátový směrovač nebo bezdrátový přístupový bod (AP) pro uživatele k připojení, jak je znázorněno na obrázku.

Existuje mnoho úvah při realizaci bezdrátové sítě, jako typy bezdrátových zařízení pro použití, bezdrátové pokrytí požadavků, pozorování rušení a bezpečnostní úvahy.

Operace a implementace bezdrátového provozu budou pokryty podrobněji v kapitole s názvem "Bezdrátové sítě LAN".

8.2.2.5 Jemné doladění směrovacích protokolů

Správa směrované sítě

Podnikové sítě a poskytovatele služeb internetu často používají více pokročilejších protokolů, jako je například protokoly stabilní linky, protože jejich hierarchické návrhy mají možnosti škálování pro velké sítě.

Směrovací protokol stabilní linky jako OSPF – Otevření Nejkratší Cesty jako První, jak je znázorněno na obrázku 1, funguje dobře pro větší hierarchické sítě, kde je rychlá konvergence důležitá. OSPF směrovače vytvářejí a udržují přilehlého nebo přilehlé sousedy, s jinými připojenými OSPF směrovači. Když směrovač zahájí přilehlost se sousedy, začíná výměna aktualizací stabilní linky. Směrovače dosáhnou plnou úroveň přilehlosti, když jsou synchronizovány přehledy jejich databáze stabilní linky. S OSPF, aktualizace stabilní linky stavu jsou zaslány, hned jak dojde ke změnám v síti.

OSPF je populární směrovací protokol stabilní linky, který lze doladit v mnoha ohledech. V kapitole s názvem "Úprava a řešení problémů Single-Area OSPF" se bude týkat některé z pokročilejších funkcí konfigurace OSPF a řešení problémů.

Navíc, OSPF podporuje dvouvrstvý hierarchický návrh, nebo multi-area OSPF, jak je znázorněno na obrázku 2. Všechny sítě OSPF začínají oblastí Area 0, nazývané také páteřní oblast. Vzhledem k tomu, že se síť rozšíří, může být vytvořeny jiné, nepáteřní oblasti. Všechny nepáteřní oblasti se musí připojit přímo na Area 0. V kapitole s názvem "Multiarea OSPF" si představíme výhody, operace, provoz a konfiguraci Multi-area OSPF.

Další populární směrovací protokol pro větší sítě je EIGRP – Rozšíření Vnitřní Brány Směrovací Protokol. Cisco vyvinula EIGRP jako proprietární vzdálenostní vektorový směrovací protokol s rozšířenými schopnostmi. Ačkoli konfigurace je relativně jednoduchá, uskutečněné funkce a možnosti jsou rozsáhlé a robustní. Například, používá více tabulek pro řízení

procesu směrování, jak je znázorněno na obrázku 3. EIGRP obsahuje mnoho funkcí, které nejsou k dispozici v jiných směrovacích protokolech. Je to vynikající volba pro velké, víc-protokolové sítě, které primárně využívají Cisco zařízení.

V kapitole s názvem "EIGRP" představíme provoz a konfiguraci směrovacího protokolu, zatímco kapitola s názvem "EIGRP Pokročilá konfigurace a řešení problémů" zahrnuje některé další pokročilé možnosti konfigurace EIGRP.

8.3 Výběr Síťových Zařízení

8.3.1 Hardware přepínačů

8.3.1.1 Platformy přepínačů

Při návrhu sítě, je důležité vybrat správný hardware pro splnění současných požadavků sítě, jakožto i umožnit rozšíření sítě. V rámci podnikové sítě, oba přepínače i směrovače hrají klíčovou roli v komunikaci po síti.

Existuje pět kategorií přepínačů pro podnikové sítě, jak je znázorněno na obrázku 1:

Kampusové LAN přepínače - Chcete-li škálovat výkon v podnikové LAN síti, existuje jádro, distribuce, přístup a kompaktní přepínače. Tyto přepínací platformy se liší od přepínačů bez větráku s osmi pevnými porty na 13 čepelové přepínače, které podporují stovky portů. Mezi Kampusové LAN přepínací platformy patří Cisco 2960, 3560, 3750, 3850, 4500, 6500 a 6800 Series.

Cloud-řízené přepínače - Cisco Meraki cloud-řízené přístupové přepínače umožňují virtuální stohování přepínačů. Monitorují a konfigurují tisíce portů přepínače přes internet, bez zásahu IT personálu na místě.

Přepínače datových center - datové centrum by mělo být postaveno na bázi přepínačů, které podporují škálovatelnost infrastruktury, provozní kontinuitu a flexibilitu dopravy. Pod přepínací platformy datových center patří přepínače série Cisco Nexus a přepínačů série Cisco Catalyst 6500.

Poskytovatel služeb přepínače - poskytovatelé služeb přepínače spadají do dvou kategorií: agregační přepínače a přístupové Ethernet přepínače. Agregační přepínače jsou předními Ethernetovými přepínači, které shromažďují informace o provozu na okraji sítě. Poskytovatelé služeb Ethernet přístupových přepínačů jsou vybaveny možnosti aplikace inteligence, sjednocených služeb, virtualizace, integrovaného zabezpečení a zjednodušené správy.

Virtuální sítě - Sítě jsou stále víc virtualizované. Cisco Nexus virtuální síťové přepínací platformy poskytují bezpečné multi-najímatelné služby, přidáním virtualizační inteligence technologii datového centra sítě.

Při výběru přepínače, musí správci sítě determinovat přepínač podle tvarových faktorů. To zahrnuje fixní konfiguraci (obrázek 2), modulární konfigurace (obrázek 3), stohovatelný (obrázek 4), nebo ne-stohovatelný. Tloušťka přepínače, která je vyjádřena v počtem regálových jednotek, je také důležitá pro přepínače, které jsou namontovány v regálu. Například, fixní konfigurační přepínače jsou zobrazeny na obrázku 2, mají tloušťku 1 regálové jednotky (1U).

Kromě těchto úvah, Obrázek 5 ukazuje ostatní běžné obchodní úvahy při výběru přepínacího zařízení.

8.3.1.2 Hustota portů

Hustota portů přepínače se vztahuje na počet portů, které jsou k dispozici na jednom přepínači. Obrázek ukazuje hustotu portů pro tři různé přepínače.

Fixní konfigurace přepínače obvykle podporuje až 48 portů na jednom zařízení. Mají možnosti až pro čtyři další porty pro malé zásuvné zařízení form-factor (SFP). Vysoká hustota portů umožňuje lepší využití omezeného prostoru a síly. Jsou-li dva přepínače, které každý obsahují 24 portů, tak by měli být schopny podporovat až 46 zařízení, protože alespoň jeden port na přepínači je ztracen s připojením každého přepínače na zbývající části sítě. Kromě toho jsou zapotřebí dvě elektrické zásuvky. Alternativně, má-li jeden přepínač 48 portů, tak 47 zařízení může být podporováno, ale pouze s jedním portem použitým pro připojení přepínače ke zbytku sítě a pouze v jedné zásuvky potřebné na to, aby se přizpůsobil jeden přepínač.

Modulární přepínače můžou podporovat velmi vysokou hustotu portů, když přidáme více linkových karet přepínacích portů. Například některé Catalyst 6500 přepínače můžou podporovat více než 1000 portové přepínače.

V rozsáhlých podnikových sítích, které podporují tisíce síťových zařízení, si vyžadují vysokou hustotou modulárních přepínačů pro co nejlepší využití prostoru a výkonu. Bez použití modulárního přepínače s vysokou hustotou, by síť potřebovala mnoho přepínačů s fixní konfigurací přizpůsobit pro počet zařízení, která potřebují přístup k síti. Tento přístup může spotřebovat mnoho energie a spoustu úložného prostoru.

Síťový návrhář musí také zvážit otázku uplinku úzkých linek. Řada fixních konfiguračních přepínačů může spotřebovat mnoho dalších portů pro agregaci šířky pásma mezi přepínači, za účelem dosažení cílového výkonu. S jediným modulárním přepínačem, šířka pásma agregací je mnohem menší problém, protože šasi desky, která je propojí, může poskytnout potřebnou šířku pásma, aby se zařízení připojená k linkovým kartám portů přepínače, mohli přizpůsobit.

8.3.1.3 Hodnocení odesílání

Hodnocení odesílaní, definuje možnosti zpracování přepínačů dle ratingu, kolik dat dokáže přepínač zpracovat za sekundu. Produktové linie přepínačů se zařazují podle hodnocení odesílání, jak je znázorněno na obrázku. Přepínače Vstupní-úrovně mají nižší hodnocení než přepínače na podnikové úrovni. Tato hodnocení jsou důležitá a je potřeba je vzít v úvahu při výběru přepínače. V případě, že je hodnocení odesílání přepínače příliš nízké, nemůže zajistit plnou rychlost kabelu při komunikaci napříč všemi svými porty. Rychlost kabelu je rychlost přenosu dat, kterou je každý Ethernetový port na přepínači schopen dosáhnout. Rychlost přenosu dat může být 100 MB/s, 1 Gb/s, 10 Gb/s nebo 100 Gb/s.

Například, typický 48 portový gigabitový přepínač pracuje na plné rychlosti kabelu a generuje 48 Gb/s provozu. Pokud přepínač podporuje pouze rychlost odesílání 32 Gb/s, tak nemůže běžet v plné rychlosti kabelu napříč všemi porty současně. Naštěstí přístupová vrstva přepínačů obvykle nepracuje v plné rychlosti kabelu, protože je fyzicky omezována svými up-linky do distribuční vrstvy. To znamená, že méně nákladné přepínače, z nižším výkonem lze použít v přístupové vrstvě a dražší, výkonnější přepínače lze použít při distribučních a jádrových vrstvách, kde míra hodnocení odesílání má větší vliv na výkon sítě.

8.3.1.4 Power over Ethernet (PoE)

PoE přepínač umožňuje dodávky energie do zařízení přes existující ethernetové kabeláže. Tuto funkci lze použít přes IP telefony a některé bezdrátové přístupové body. Kliknutím na zvýrazněné ikony na obrázku 1, zobrazíte PoE porty na každém zařízení.

PoE umožňuje větší flexibilitu při instalaci bezdrátových přístupových bodů a IP telefonů, což jim umožňuje je instalovat kdekoliv, kde je ethernetový kabel. Správce sítě by měl zjistit, zda jsou funkce požadovány, protože přepínače co podporují PoE, jsou drahé.

Relativně nové Cisco Catalyst 2960-C a 3560-C kompaktní přepínače podporují PoE projdi-přes. PoE projdi-přes umožňuje správci sítě napájení, zařízeních připojených k přepínači,

stejně jako samotný přepínač tím, že odebírá energii z určitých up-stream přepínačů. Kliknutím na ikonu zobrazíte na obrázku 2 Cisco Catalyst 2960-C.

8.3.1.5 Vícevrstvé přepínání

Vícevrstvé přepínače jsou typicky rozmístěny v jádrových a distribučních vrstvách organizace přepínané sítě. Vícevrstvé přepínače jsou charakteristické svou schopností vybudovat směrovací tabulky, podporovat několik směrovacích protokolů a odesílat IP pakety rychlostí blízké rychlosti odesílání 2 vrstvy. Vícevrstvé přepínače často podporují specializovaný hardware, jako jsou aplikačně specifické integrované obvody (ASIC). ASIC spolu s vyhrazenými softwarovými datovými strukturami efektivněji odesílají IP pakety, nezávisle na CPU.

Teď je trend tvořit síť, jako prostředí čistě podle 3 vrstvy. Když byly poprvé použity přepínače v sítích, žádný z nich nepodporoval směrování. Nyní, téměř všechny přepínače podporují směrování. Je pravděpodobné, že brzy budou podporovat všechny přepínače, protože náklady se přitom snižují ve srovnání s jinými omezeními, které obsahují procesor směrování. Nakonec termín vícevrstvý přepínač bude zbytečný.

Jak je znázorněno na obrázku, přepínače Catalyst 2960 znázorňují přechod na čisté prostředí 3 vrstvy. S verzemi IOS před 15. x, tyto přepínače podporují pouze jedno aktivní přepínací virtuální rozhraní (SVI). S IOS 15. x, tyto přepínače nyní podporují více aktivních SVI. To znamená, že na přepínač se může vzdáleně přistupovat prostřednictvím více IP adres v odlišných sítích.

8.3.2 Hardware Směrovače

8.3.2.1 Požadavky směrovače

V distribuční vrstvě podnikové sítě, je vyžadováno směrování. Bez směrovacího procesu, nemohou pakety opustit lokální síť.

Směrovače hrají klíčovou roli při vytváření sítí propojení více oblastí v rámci podnikové sítě, které poskytují redundantní cesty, a připojení ISP na internetu. Směrovače můžou také působit jako překladatelé mezi různými typy médií a protokolů. Například směrovač může přijímat pakety z Ethernetové sítě a znovu je zapouzdřit pro dopravu přes Sériovou síť.

Směrovače používají síťové části cílové adresy IP pro směrování paketů do správného místa určení. Vybírají alternativní cestu, pokud linka spadne, nebo když je provoz přetížen.

Všichni hostitelé v lokální síti, specifikují IP adresu lokálního rozhraní směrovače v jejich IP konfiguraci. Toto rozhraní směrovače je výchozí brána.

Směrovače slouží také k dalším prospěšným funkcím:

- Poskytovat broadcast vysílání
- Připojení vzdálených lokací
- Skupiny uživatelů řadí logicky podle aplikace nebo oddělení
- Poskytují zvýšenou bezpečnost

Klepněte na každou zvýrazněnou oblast v obrázku pro další informace o funkcích směrovačů. S podnikem a ISP, se schopnost efektivně směrovat a obnovovat v případě selhání síťové linky, stala rozhodující při doručování paketů na místo jejich určení.

8.3.2.2 Směrovače Cisco

Jak se síť stále rozrůstá, je důležité vybrat správné směrovače, ke splnění svých požadavků. Jak je znázorněno na obrázku, existují tři kategorie směrovačů:

Větevní směrovače - Větevní směrovače optimalizují větevní služby na jediné platformě, zatímco zároveň přináší optimální zážitek napříč větevní a WAN infrastruktury. Maximalizuje se dostupnost služby na větvi, teda si vyžaduje sítě určené pro 24x7x365 provozuschopnosti. Vysoce dostupné větevní sítě musí zajistit rychlé zotavení z typických chyb, při minimalizaci nebo eliminaci dopadu na službu a poskytnout jednoduchou konfiguraci a správu sítě.

Směrovače okraje sítě - směrovače na okraji sítě umožňují okraji sítě dodávat vysoce výkonné, vysoce bezpečné a spolehlivé služby, které spojují kampus, datová centra a větevní sítě. Zákazníci očekávají vysoce kvalitní multimediální zážitek a více typů obsahu, než kdykoliv předtím. Zákazníci chtějí interaktivitu, personalizaci, mobilitu a ovládání pro veškerý obsah. Také chtějí mít přístup k obsahu kdykoli a kdekoli si oni vyberou, přes libovolné zařízení, ať už doma, nebo v práci, nebo na cestách. Směrovače okraje sítě musí přinést zvýšení kvality služeb, nonstop video a mobilní schopnosti.

Směrovače poskytovatele služeb – tyto směrovače se liší portfoliem služeb a zvyšují výnosy tím, že poskytují end-to-end škálovatelná řešení a účastnické služby. Provozovatelé musí optimalizovat operace, snížit náklady a zlepšit škálovatelnost a flexibilitu, dodávat příštím generacím internetové zkušenosti napříč všemi zařízeními a lokacemi. Tyto systémy jsou navrženy ke zjednodušení organizace, zvýšení výkonu a rozmístění dodávek síťových služeb.

8.3.2.3 Hardware směrovače

Směrovače také přicházejí v mnoha různých variantách, jak je znázorněno na obrázku. Správci sítě v podnikovém prostředí by měly být schopny podporovat různé směrovače, od malých stolních směrovačů až po plné stojanové jednotky nebo čepelové modely.

Směrovače mohou být také zařazeny do kategorie fixní nebo modulární konfigurace. S fixní konfigurací, je požadované rozhraní směrovače vestavěné. Modulární směrovače přicházejí s více sloty, které umožňují správci sítě změnu rozhraní na směrovači. Jako příklad lze uvést, Cisco 1841 směrovač, který je dodáván se dvěma Fast Ethernetovými RJ-45 vestavěnými rozhraními a dvěma sloty, které mohou přijmout mnoho různých modulů síťového rozhraní. Směrovače přicházejí s řadou různých rozhraní, jako je například Fast Ethernet, Gigabit Ethernet, sériové a optického vlákno.

8.3.3 Správa Zařízení

8.3.3.1 Správa souborů IOS a Licencování

S tak širokým výběrem síťových zařízení produktové řady Cisco, z kterých lze vybírat, může organizace pečlivě určit ideální kombinaci, aby vyhovovala všem potřebám jednotlivých zaměstnanců a zákazníků.

Při výběru nebo modernizaci zařízení Cisco IOS, je důležité vybrat si ten správný IOS obraz se správnou sadou funkcí a verzí. IOS se týká balíku směrování, přepínání, zabezpečení a dalších internetových technologií, které jsou integrovány do jediného multitasking operačního systému. Je-li nový přístroj dodán, je dodán s předinstalovaným obrazem softwaru a odpovídajícími trvalými licencemi pro balíky a sady funkcí dle specifických potřeb zákazníka.

Pro směrovače, počínaje softwarem Cisco IOS vydaným ve verzi 15.0, Cisco upravil proces umožnění nových technologií v rámci sad funkcí IOS, jak je znázorněno na obrázku.

8.3.3.2 Vnitřní versus vnější řízení

Bez ohledu na to, jak je síťové zařízení Cisco IOS implementováno, existují dva způsoby připojení PC k tomuto síťovému zařízení pro konfiguraci a monitorování úkolů. Tyto metody zahrnují řízení vnější a vnitřní, jak je znázorněno na obrázku.

Vnější řízení se používá pro prvotní konfiguraci, nebo pokud připojení k síti není k dispozici. Konfigurace pomocí vnějšího řízení vyžaduje:

- Přímé napojení na konzoli nebo AUX portem
- Emulace terminálu klientem

Vnitřní řízení se používá ke sledování a provádění změn konfigurace síťového zařízení přes síťové připojení. Konfigurace pomocí vnitřního řízení vyžaduje:

- Alespoň jedno síťové rozhraní na zařízení, které má být funkční a připojené
- Telnet, SSH nebo HTTP pro přístup k zařízení Cisco

8.3.3.3 Základní příkazy směrovače

Základní konfigurace směrovače obsahuje název hostitele pro identifikaci, heslo pro zabezpečení, přiřazení IP adres rozhraním pro připojení a základní směrování. Obrázek 1 ukazuje příkazy zadané k tomu, aby fungoval směrovač s OSPF. Ověřit a uložit změny konfigurace můžeme pomocí příkazu ***copy running-config startup-config***. Obrázek 2 ukazuje výsledky příkazů konfigurace, které byly zadány na obrázku 1. Chcete-li vymazat konfiguraci směrovače, použijte příkaz ***erase startup-config*** a pak příkaz pro obnovu - ***reload***.

8.3.3.4 Základní příkazy směrovače pro zobrazení

Zde jsou některé z nejčastěji používaných IOS příkazů k zobrazení a ověření provozního stavu směrovače a sním související funkcionalitu sítě. Tyto příkazy jsou rozděleny do několika kategorií.

Související ze směrováním:

show ip protocols - zobrazí informace o nakonfigurovaných směrovacích protokolech. Pokud je OSPF nakonfigurováno tak, že zahrnuje ID OSPF procesu, ID směrovače, propagaci zesíťovaného směrovače, že sousedé dostávají aktualizace od něj a výchozí administrativní vzdálenost je pro OSPF - 110. (Obrázek 1)

show ip route - Zobrazuje informace ze směrovací tabulky, včetně: směrovacích kódů, známých sítích, administrativních vzdálenostech a metriky, jak se trasy naučili, další skok, statické trasy a výchozí trasy. (Obrázek 2)

show ip OSPF neighbor - zobrazuje informace o OSPF sousedech, kteří byly získáni, včetně ID směrovače souseda, jeho priority, stavu (Full = sousednost byla zformovaná), IP adresu a lokální rozhraní, které se dozvěděl od souseda. (Obrázek 3)

Související z rozhraním:

show interfaces - Zobrazí rozhraní s řádkem o stavu protokolu, šířce pásma, zpoždění, spolehlivosti, zapouzdření, duplexu, a I / O statistik. Pokud je zadán bez zvláštního označení rozhraní, zobrazí se všechna rozhraní. Jsou-li konkrétní rozhraní stanovena po provedení příkazu, budou zobrazeny pouze informace o tomto rozhraní. (Obrázek 4)

show ip interfaces - Zobrazí informace o rozhraní, včetně: stavu protokolu, IP adresy, je-li pomocná adresa nakonfigurována a zda je ACL povolen na rozhraní. Pokud je zadán bez zvláštního označení rozhraní, zobrazí se všechna rozhraní. Jsou-li konkrétní rozhraní stanovena po provedení příkazu, budou zobrazeny pouze informace o tomto rozhraní. (Obrázek 5)

show ip interface brief - Zobrazí všechna rozhraní s informacemi o IP adresaci a rozhraní a řade stavů protokolů. (Obrázek 6)

show protocols - Zobrazí informace o směrovacím protokolu, který je povolen a o stavu protokolu na rozhraních. (Obrázek 7)

Ostatní příkazy související z připojením zahrnují příkaz show CDP neighbors (Obrázek 8). Tento příkaz zobrazí informace o přímo připojených zařízeních, včetně ID zařízení, místním rozhraním je zařízení připojeno k, schopnosti (R = směrovač, S = přepínač), platformě a ID portu vzdáleného zařízení.

8.3.3.5 Základní příkazy přepínače

Základní konfigurace přepínače zahrnuje název hostitele pro identifikaci, heslo pro zabezpečení a přiřazení IP adres pro připojení. Vnitřní přístup přepínače si vyžaduje mít IP adresu. Obrázek 1 ukazuje příkazy zadané k tomu, aby přepínač fungoval.

Obrázek 2 ukazuje výsledky konfiguračních příkazů, které byly zadány na obrázku 1. Ověření a uložení konfigurace přepínače se provádí pomocí příkazu ***copy running-config startup-config.*** Chcete-li vymazat nastavení přepínače, použijte příkaz ***erase startup-config*** a pak příkaz pro obnovu - ***reload***. Může být také nutné vymazat jakékoliv informace o VLAN pomocí příkazu ***delete*** flash: vlan.dat. Když jsou konfigurace přepínačů na místě, zobrazíme konfigurace s pomocí příkazu ***show running-config***.

8.3.3.6 Základní příkazy přepínače pro zobrazování

Přepínače využívají společné IOS příkazy pro konfiguraci, pro kontrolu připojení a zobrazení aktuálního stavu přepínače. Klikněte na tlačítko 1 až 4 pro ukázkové výstupy příkazů a důležité informace, které správce může z nich shromažďovat.

Související z rozhraním a porty:

show port-security - Zobrazí všechny porty s aktivní bezpečností. K prozkoumání konkrétního rozhraní, obsahují ID rozhraní. Informace obsažené ve výstupu: maximální povolené adresy, aktuální počet, počet narušení bezpečnosti a opatření, která mají být přijata. (Obr 1)

show port-security address - Zobraz všechny bezpeční MAC adresy nakonfigurované na všech přepínacích rozhraních. (Obrázek 2)

show interfaces - Zobrazí jeden nebo všechny rozhraní s řádkem o stavu protokolu, šířce pásma, zpoždění, spolehlivosti, zapouzdření, duplexu, a I/O statistik. (Obrázek 3)

show mac-address-table - Zobrazí všechny MAC adresy, které se přepínač již naučil, jak se tyto adresy naučil (dynamická/statická), číslo portu a VLAN přiřazenou k portu. (Obr 4)

Stejně jako směrovač, přepínač také podporuje příkaz ***show CDP neighbors***.

8.3.4 Shrnutí

8.3.4.1 Shrnutí

Hierarchický model návrhu sítí rozděluje síťovou funkcionalitu do přístupové vrstvy, distribuční vrstvy a jádrové vrstvy. Cisco Podniková Architektura dále rozděluje síť do funkčních komponentů.

Dobře navržená síť ovládá provoz a omezuje rozsah selhání domén. Směrovače a vícevrstvé přepínače mohou být nasazeny ve dvojicích tak, že selhání jednoho zařízení nezpůsobí přerušení služby.

Návrh sítě by měl zahrnovat strategii adresování IP, škálovatelné a rychle se zužující směrovací protokoly, vhodné protokoly 2 vrstvy a modulární nebo cluster zařízení, které lze snadno upgradovat pro zvýšení kapacity.

Server mission-critical by měl mít připojen ke dvěma různým přepínačům přístupové vrstvy. Měl by mít redundantní moduly, je-li to možné, a záložní zdroj energie. Může být vhodné, zajistit více připojení k jednomu nebo více ISP.

Síťový návrhář by měl určit směrovač z příslušné kategorie: větevní směrovače, síťové okrajové směrovače nebo směrovače poskytovatele služeb. Je důležité, aby také nasadil vhodný typ přepínače pro danou sadu požadavků, spínacích funkcí a technických údajů, a očekávaného provozního proudu.

9 KAPITOLA 2 – REDUNDANCE LAN

9.1 Redundance LAN

9.1.1 Úvod

9.1.1.1 Úvod

Síťová redundance je klíčem k zachování spolehlivosti sítě. Více fyzických linek mezi zařízeními poskytuje redundantní cesty. Síť pak může pokračovat v činnosti, i když jediná linka nebo port selhali. Redundantní linky mohou také sdílet provozní zátěž a zvýšit kapacitu.

Více cest musí být řízeno tak, aby smyčky 2 vrstvy nebyli vytvořeny. Nejlepší cesty jsou vybrány a alternativní cesta by měla být okamžitě k dispozici, když primární cesta selže. Spanning Tree Protokoly se používají ke správě redundance 2 vrstvy.

Redundantní zařízení, jako jsou vícevrstvé přepínače nebo směrovače, poskytují pro klienta možnost použít alternativní výchozí bránu, když primární výchozí brána selže. Klient nyní může mít více cest na více než jednu možnou výchozí bránu. Redundantní protokoly prvního skoku se používají ke správě, jak se klientovi přiřazuje výchozí brána a aby bylo možné použít alternativní výchozí bránu, která by měla být použita, když primární výchozí brána selže.

Tato kapitola je zaměřena na protokoly používané ke správě těchto forem redundance. Pokrývá také některé z možných redundantních problémů a jejich příznaky.

9.1.1.2 Aktivita – Bouřlivý provoz

Je to váš první den v práci jako správce sítě pro malé až středně velké firmy. Předchozí správce sítě náhle odešel a upgrade sítě zabral místo v podnikání.

Během upgradu byl přidán nový přepínač. Vzhledem k inovaci, mnozí zaměstnanci si stěžuje, že mají problémy s přístupem k internetu a serverům v síti. Ve skutečnosti většina z nich se nemůže připojit k síti vůbec. Váš podnikový vás manažer požádá, abyste okamžitě prošetřili to, co by mohlo být příčinou těchto problémů s připojením a zpožděním.

Takže se podíváte na zařízení pracující ve vaší síti v hlavním distribučním zařízení v budově. Všimněte si, že topologie sítě se zdá být vizuálně správné a že kabely byly správně zapojeny, směrovače a přepínače jsou zapnuté a funkční a přepínače jsou spojeny dohromady, tak aby poskytovali zálohování nebo redundanci.

Nicméně, jedna věc, kterou uděláte je oznámení, že všechny indikátory stavů přepínačů jsou permanentně blikající ve velmi rychlém tempu do té míry, že téměř jeví jako stále svítící. Myslíte si, že jste našli problém s konektivitou, s kterým bojují vaši zaměstnanci.

Používat internet k výzkumu STP. Jak budete hledat, dělejte si poznámky a popište:

- Broadcastovou bouřku
- Přepínací smyčky
- Účel STP
- Variace STP

Dokončete otázky, které doprovázejí soubor PDF pro tuto aktivitu. Uložte svou práci a buďte připraveni sdílet své odpovědi s třídou.

9.2 Koncepty Spanning Tree

9.2.1 Účel Spanning Tree

9.2.1.1 Redundance v 1 a 2 vrstvě OSI modelu

Třístupňový hierarchický návrh sítě, který využívá jak jádro, tak distribuční a přístupovou vrstvu s redundancí, se snaží eliminovat i jediný bod selhání v síti. Několik kabelových tras mezi přepínači poskytuje fyzickou redundanci v přepínané síti. To zvyšuje její spolehlivost a dostupnost. Když, máme alternativní fyzické cesty pro data procházející sítí, umožňuje tak přístup uživatelů k síťovým zdrojům a to navzdory přerušení cesty.

Kliknutím na tlačítko Play na obrázku 1 zobrazíte animaci o redundanci sítě.

PC1 komunikuje s PC4 přes redundantní síťovou topologii

Je-li narušeno propojení sítí, mezi přepínači S1 a S2, cesta mezi PC1 a PC4 je automaticky upravena tak, aby kompenzovala narušení.

Když dojde k obnovení síťového připojení mezi přepínači S1 a S2, tak se cesta pak upraví kvůli směrování přímo z S2 na S1 , a dostaneme se na PC4.

Pro mnoho organizací, má dostupnost sítě zásadní význam při podpoře podnikatelských potřeb. Proto, dizajn síťové infrastruktury je zásadním prvkem podnikání. Redundance cest zajišťuje potřebnou dostupnost více síťových služeb, eliminací možností i jen jediného bodu selhání.

Poznámka: Redundance 1 OSI vrstvy je znázorněno použitím více linek a zařízení, ale je potřeba více, než jen fyzické plánování, taktéž je nutné k dokončení nastavení celé sítě. Pro fungování redundance systematickým způsobem, je také zapotřebí použití protokolů 2. OSI vrstvy, jako je například STP.

Redundance je důležitou součástí hierarchického návrhu, pro prevenci narušení služeb sítě pro uživatele. Redundantní sítě vyžadují přidání fyzické cesty, ale logická redundance musí být také součástí návrhu. Nicméně, redundantní cesty v přepínané ethernetové síti může vyvolat jak fyzické, tak i logické smyčky 2. vrstvy.

Logická smyčky 2. vrstvy můžou nastat v důsledku přirozeného fungování přepínačů. Konkrétně se jedná o procesu učení a napře dování. Když existuje více cest mezi dvěma zařízeními v síti, a není tam žádná jiná implementace STP na přepínačích, dojde k smyčkám 2. vrstvy. Smyčky 2. vrstvy můžou mít za následek tři základní problémy uvedené na obrázku 2.

9.2.1.2 Problémy s redundancí 1. vrstvy: Nestabilita databáze MAC

Ethernetové rámce nemají atribut času (TTL). V důsledku toho, pokud neexistuje žádný mechanismus umožňující zablokovat další šíření těchto rámců na přepínané síti, pokračují v šíření mezi přepínači nekonečně nebo do přerušení spojení a tím přeruší smyčku. Toto pokračující šíření mezi přepínači může mít za následek nestabilitu databáze MAC. To může nastat v důsledku přenosu vysílacích rámců.

Vysílací rámce jsou předávány na všechny přepínací porty, s výjimkou původního vstupního portu. Tím je zajištěno, že všechna zařízení ve vysílací doméně, budou moci přijmout rámec. Pokud existuje více než jedna cesta k odeslání rámce, může dojít k nekonečné smyčce. Když k smyčce dojde, je možné, že se tabulka MAC adres na přepínači bude neustále měnit s aktualizacemi z vysílacích rámců, což vede k nestabilitě databáze MAC.

Klepnutím na tlačítko Přehrát na obrázku zobrazíte animaci. Když animace zastaví, přečtěte si text vlevo od topologie. Po krátké pauze bude animace pokračovat.

V animaci:

PC1 posílá vysílací rámec do S2. S2 přijímá vysílací rámec na F0/11. Když S2 přijímá tento rámec, aktualizuje svou tabulku MAC adres pro záznam, že PC1 je k dispozici na portu F0/11.

Vzhledem k tomu, že je vysílacím rámcem, S2 předává rámec ze všech portů, včetně Trunk1 a Trunk2. Když vysílací rámec přichází na S3 a S1, přepínače si aktualizují své tabulky MAC adres, což naznačuje, že PC1 je k dispozici na portu F0/1 na S1 a na portu F0/2 na S3.

Vzhledem k tomu, že se jedná o vysílací rámec, S3 a S1 ho předávají na všechny porty, s výjimkou portu pro vstup. S3 posílá vysílací rámec z PC1 na S1. S1 posílá vysílací rámec z PC1 do S3. Každý přepínač aktualizuje svou tabulku MAC adres s nesprávným portem pro PC1.

Každý přepínač posílá vysílací rámec ze všech jeho portů, s výjimkou vstupního portu, což má za následek, že oba přepínače posílají rámec na S2.

Když S2 přijímá vysílací rámce ze S3 a S1, tabulka MAC adres je aktualizována s posledním záznamem přijatým od ostatních dvou přepínačů.

Tento proces se opakuje znovu a znovu, dokud není smyčka přerušena fyzickým odpojením spojů, které ji vytvářejí, nebo vypnutím některého z přepínačů ve smyčce. Tím dochází, k vysokému zatížení CPU u všech přepínačů zachycených ve smyčce. Vzhledem k tomu, že stejné rámce jsou stále předávány mezi všemi přepínači ve smyčce, procesor přepínače musí zpracovávat mnoho dat. To zpomaluje jeho výkon při spuštění legitimního provozu.

Hostitel zachycen v síťové smyčce není přístupný jiným hostitelům v síti. Navíc, kvůli neustálým změnám v tabulce MAC adres, přepínač neví, z jakého portu bude posílat unicast rámce (rámec, který je posílaný jen jednomu přijímateli). Ve výše uvedeném příkladu, mají přepínače uvedené nesprávné porty pro PC1. Jakýkoli unicast rámec určený pro PC1, cestuje ve smyčce po celé síti, stejně jako vysílací rámce. Stále více rámců, které se přemisťují po síti, nakonec vytvoří vysílací bouři.

9.2.1.3 Problémy s redundancí 1. vrstvy: Vysílací bouře

Vysílací bouře nastane, když je v smyčce 2. vrstvy zaznamenáno tolik vysílacích rámců, že se spotřebuje veškerá dostupná šířka pásma. V důsledku toho není dostupná žádná šířka pásma pro legitimní přenos a síť nebude dostupná pro datovou komunikaci. Jedná se o účinné odmítnutí služby (DoS).

Vysílací bouře je nevyhnutelná ve smyčkové síti. Jelikož více zařízení vysílá po síti více vysílání, dojde ke zvýšení provozu a to spotřebovává zdroje. To nakonec vytvoří vysílací bouřku, která způsobí selhání sítě.

Existují další důsledky vysílacích bouří. Vzhledem k tomu, že vysílání je směrováno z každého portu přepínače, všechna připojená zařízení musí zpracovávat veškerý vysílaný provoz,

který nekonečně zaplavuje celou síťovou smyčku. To může způsobit selhání koncového zařízení kvůli požadavkům na zpracování, které jsou potřebné k udržení tak vysokého provozního zatížení na NIC.

Klepnutím na tlačítko Přehrát na obrázku zobrazíte animaci vysílací bouře. Když se animace zastaví, přečtěte si text vpravo od topologie. Po krátké pauze bude animace pokračovat.

V animaci:

- PC1 pošle vysílací rámec na smyčkovou síť.
- Vysílací rámec se pohybuje ve smyčce všech propojených přepínačů v síti.
- PC4 vysílá také vysílací rámec do smyčkové sítě.
- Vysílací rámec PC4 je zachycen ve smyčce mezi všemi propojenými přepínači, stejně jako vysílací rámec PC1.

Jelikož více zařízení vysílá po síti více vysílání, dojde ke zvýšení provozu a to spotřebovává zdroje. To nakonec vytvoří vysílací bouřku, která způsobí selhání sítě.

Když je síť plně nasycená vysílacím přenosem, který je mezi jednotlivými přepínači ve smyčce, nová komunikace přepadne, protože ji nelze zpracovat.

Vysílací bouře se může vyvinout během několika sekund, protože zařízení připojená k síti pravidelně vysílají vysílací rámce, například jako požadavky ARP. Výsledkem je, že při vytvoření smyčky se přepínaná síť rychle sníží.

9.2.1.4 Problémy s redundancí 1. vrstvy: Duplikace unicast rámců

Vysílací rámce nejsou jediným typem rámců, které jsou ovlivněny smyčkami. Jednotlivé rámce odesílané do smyčkové sítě mohou mít za následek duplicitní rámce přicházející do cílového zařízení.

Klepnutím na tlačítko Přehrát na obrázku zobrazíte animaci o tomto problému. Když animace zastaví, přečtěte si text vpravo od topologie. Po krátké pauze bude animace pokračovat.

V animaci:

- PC1 pošle unicast rámec určený pro PC4.
- S2 nemá záznam o vstupu pro PC4 ve své MAC tabulce. Při pokusu o nalezení PC4 zaplní unicast rámec všechny porty přepínače, s výjimkou portu, který obdržel provoz.
- Rámec přichází na přepínače S1 a S3.
- S1 má záznam vstupu MAC adresy pro PC4, takže předává rámec mimo PC4.

- S3 má záznam vstupu v tabulce MAC adres pro PC4, takže předává unicast rámec z Trunk3 na S1.
- S1 obdrží duplicitní rámec a posune unicast rámec na PC4.
- PC4 nyní obdržel stejný rámec dvakrát.

Většina protokolů v horní vrstvě není určena k rozpoznání duplicitních přenosů. Obecně platí, že protokoly, které využívají mechanismus číslování sekvencí, předpokládají, že přenos selhal a že pořadové číslo bylo recyklováno pro další komunikační relaci. Jiné protokoly se pokusí předat duplicitní přenos k příslušnému protokolu vyšší vrstvy, který má být zpracován a případně vyřazen.

LAN protokoly 2. vrstvy, jako je Ethernet, postrádají mechanismus pro rozpoznání a odstranění nekonečných smyčkových rámců. Některé protokoly 3. vrstvy implementují mechanismus TTL, který omezuje počet opakování přenosu paketů síťovým zařízením 3. vrstvy. Zařízení s 2. vrstvou tento mechanismus nemají, proto nepřetržitě a opakovaně přenášejí smyčkovou komunikaci. STP, mechanizmus 2. vrstvy pro vyhnutí se smyčkám, byl vyvinut pro řešení těchto problémů.

Chcete-li zabránit vzniku těchto problémů v redundantní síti, musí být na přepínačích povolen jen určitý typ STP. Ten je ve výchozím nastavení povolen na přepínačích společnosti Cisco, aby se zabránilo tomu, že se objeví smyčky 2. vrstvy.

9.2.2.1 STA – Spanning Tree Algoritmus: Úvod

Redundance zvyšuje dostupnost síťové topologie tím, že chrání síť před i jediným bodem selhání, například selhání síťového kabelu nebo přepínače. Když do návrhu vložíme fyzickou redundanci, objeví se smyčky a duplicitní rámce. Smyčky a duplicitní rámce mají vážné důsledky pro přepínanou síť. Pro řešení těchto problémů byl vyvinut protokol STP.

STP zajišťuje, že existuje pouze jedna logická cesta mezi všemi cílovými destinacemi v síti, záměrným blokováním redundantních cest, které by mohly způsobit smyčku. Port je považován za zablokovaný, pokud uživatelům brání v přístupu nebo opuštění tohoto portu. Nezahrnuje rámce datových jednotek protokolu BPDU, které používají STP k zabránění smyček. Blokování redundantních cest je rozhodující pro zabránění vzniku smyček v síti. Fyzické cesty stále existují k poskytnutí redundance, ale tyto cesty jsou zakázány, aby se zabránilo vzniku smyček. Je-li cesta nutná, ke kompenzaci selhání síťového kabelu nebo přepínače, STP přepočítá cesty a odblokuje potřebné porty, aby umožnila aktivování cesty redundantní.

Klepnutím na tlačítko Přehrát na obrázku 1 zobrazíte STP v akci.

V příkladu jsou všechny přepínače vybaveny funkcí STP:

- PC1 vysílá vysílání do sítě.
- S2 je konfigurován s protokolem STP má nastavený port pro Trunk2 na blokovací stav. Blokovací stav zabraňuje použití portů pro předávání uživatelských dat, což zabraňuje vzniku smyček. S2 předává vysílací rámec ze všech přepínacích portů, s výjimkou původního portu z PC1 a portu pro Trunk2.
- S1 přijímá vysílací rámec a vysílá všechny jeho přepínací porty, kde dosáhne PC4 a S3. S3 posune rámec z portu Trunk2 a S2 rámec vypustí. Tak je zabráněno smyčce 2. vrstvy.

Klepnutím na tlačítko Přehrát na obrázku 2 zobrazíte přepočítání STP, pokud dojde k poruše.

Služba STP zabraňuje vzniku smyček konfigurací cesty bez smyčky v síti pomocí strategicky umístěných portů "zablokování". Spínače se systémem STP jsou schopny kompenzovat poruchy dynamickým odblokováním dříve zablokovaných portů a umožňujícím provozu procházet alternativními cestami.

Dosud jsme používali termín Spanning Tree Protocol a zkratku STP. Ale použití těchto výrazů může být zavádějící. Mnozí profesionálové jej obecně používají k odkazům na různé

implementace STP, jako je protokol Rapid Spanning Tree (RSTP) a protokol Multiple Spanning Tree Protocol (MSTP). Abychom mohli správně komunikovat o koncepcích STP, je důležité odkazovat se na konkrétní implementaci nebo na standard v kontextu. Nejnovější dokumentace IEEE o STP (IEEE-802-1D-2004) říká: " že STP byla nyní nahrazena protokolem Rapid Spanning Tree Protocol (RSTP)." IEEE používá "STP" k odkazu na původní implementaci a "RSTP" pro popis verze specifikované v IEEE-802.1D-2004. V tomto učebním plánu, kde je původním protokolem kontext diskuse, se používá výraz "původní 802.1D spanning tree", aby se zabránilo záměně. Vzhledem k tomu, že tyto dva protokoly sdílejí většinu stejné v terminologii a metodách pro cestu bez smyček, bude primární zaměření na stávající standard a vlastní implementace společnosti Cisco STP a RSTP.

Poznámka: STP je založen na algoritmu, který vynalezl Radia Perlman při práci v Digital Equipment Corporation a ho publikoval v dokumentu z roku 1985 "Algoritmus pro distribuovaný výpočet STP v rozšířené LAN síti".

9.2.2.2 STA: Role portů

IEEE 802.1D STP a RSTP používají algoritmus STA, k určení, které porty přepínačů v síti musí být zablokovány, aby se zabránilo vzniku smyček. STA označuje jeden přepínač jako kořenový most a používá ho jako referenční bod pro výpočty všech cest. Na obrázku je kořenový most (přepínač S1) vybrán volebním procesem. Všechny přepínače, které se účastní výměnných stanic BPDU STP, určují, který přepínač má v síti nejnižší identifikační číslo mostu (BID). Přepínač s nejnižším BID se automaticky stává kořenovým mostem pro výpočty STA.

Poznámka: Pro jednoduchost předpokládejte, dokud není uvedeno jinak, že všechny porty všech přepínačů jsou přiřazeny k VLAN 1. Každý přepínač má jedinečnou MAC adresu přidruženou k VLAN 1.

BPDU je schránka zasílání zpráv vyměňovaná přepínači pro STP. Každá BPDU obsahuje BID identifikující přepínač, který odeslal BPDU. Hodnota BID obsahuje hodnotu priority, MAC adresu odesílacího přepínače a volitelnou rozšířenou ID systému. Nejnižší hodnota BID je určena kombinací těchto tří polí.

Po zjištění kořenového mostu vypočítá STA nejkratší cestu k němu. Každý přepínač používá STA k určení portů, které budou blokovány. Zatímco STA určuje nejlepší cesty ke kořenovému mostu, pro všechny přepínací porty v rozhlasové doméně, je zabráněno přenosu dat přes síť. STA při určování, které porty se mají zablokovat, bere v úvahu náklady na cestu i

port. Náklady na cestu se vypočítávají pomocí hodnot nákladů portu spojených s rychlostmi portu, pro každý port přepínače podél dané cesty. Součet hodnot nákladů portu určuje celkové náklady na cestu ke kořenovému mostu. Pokud je k dispozici více než jedna cesta, STA vybírá cestu s nejnižšími náklady.

Když STA zjistil, které cesty jsou nejvhodnější, vzhledem ke každému přepínači, přidělí role portů zúčastněným portům přepínače. Role portu popisuje, jejich vztah v síti ke kořenovému můstku, a zda jsou povoleny přenosy vpřed:

Kořenové porty - jsou porty přepínače nejblíže ke kořenovému můstku. Na obrázku je kořenový port na S2 F0/1 konfigurován pro trunk linku mezi S2 a S1. Kořenový port na S3 je na F0/1, který je nakonfigurován pro trunk linku mezi S3 a S1. Kořenové porty jsou vybrány na základě každého přepínače.

Určené porty - všechny nekořenové porty, které mají stále povolení pro přenos po síti. Na obrázku jsou porty přepínačů (F0/1 a F0/2) na S1 označeny jako určené porty. S2 má také svůj port F0/2 konfigurovaný jako určený port. Určené porty jsou vybrány na bázi trunku. Je-li jeden konec trunk linky kořenový port, pak druhý konec je určený port. Všechny porty na kořenovém můstku jsou určené porty.

Alternativní a záložní porty - alternativní porty a záložní porty jsou nakonfigurovány tak, aby byly blokovány, aby se zabránilo smyčkám. Na obrázku STA konfiguroval port F0/2 na S3 v alternativní roli. Port F0/2 na S3 je ve stavu blokování. Alternativní porty jsou vybírány pouze na trunkových linkách, kde žádný z nich není kořenovým portem. Všimněte si, že je zablokován pouze jeden konec trunk linky. To umožňuje rychlejší přechod do stavu předávání v případě potřeby. (Blokovací porty přicházejí do hry pouze tehdy, když dva porty na stejném přepínači poskytují redundantní propojení přes síť.)

Zakázané porty - Zakázaný port je port přepínače, který je vypnutý.

Poznámka: Zobrazované role portů jsou definované serverem RSTP. Role původně definovaná stanicí 802.1D STP pro alternativní a záložní porty nebyla určena.

9.2.2.3 STA: Kořenový můstek

Jak je znázorněno na obrázku 1, každá instance STP (Přepínaná LAN nebo vysílací doména) má přepínač označený jako kořenový můstek. Kořenový můstek slouží jako referenční bod pro všechny výpočty, které určují, které redundantní cesty se blokují.

Volební proces určuje, který přepínač se stává kořenovým můstkem.

Obrázek 2 zobrazuje pole BID. BID se skládá z hodnoty priority, rozšířeného ID systému a MAC adresy přepínače.

Ve volebním procesu se účastní všechny přepínače ve vysílací doméně. Po zapnutí přepínače začne vysílat rámce BPDU každé dvě sekundy. Tyto BPDU rámce obsahují BID přepínače a kořenové ID.

Když přepínače posílají své rámce BPDU, sousední přepínače ve vysílací doméně přečtou informace o kořenových ID z rámců BPDU. Pokud je kořenový identifikátor z BPDU přijat, je nižší než kořenový identifikátor na přijímacím přepínači, pak přijímající přepínač aktualizuje svůj kořenový identifikátor a identifikuje sousední přepínač jako kořenový můstek. Nicméně, nemusí to být sousední přepínač. Může to být jakýkoli jiný přepínač ve vysílací doméně. Přepínač pak vyšle nové rámce BPDU s nižším kořenovým ID k ostatním přilehlým přepínačům. Nakonec, přepínač s nejnižším BID je identifikován jako kořenový můstek pro instanci STP.

Pro každou instanci je vybrán kořenový můstek. Je možné mít několik odlišných kořenových mostů. Pokud jsou všechny porty všech přepínačů členy VLAN 1, existuje pouze jedna instance. Rozšířené ID systému hraje roli v tom, jak jsou určovány všechny instance.

9.2.2.4 STA: Cena cesty

Pokud byl kořenový můstek zvolen pro instanci STP, STA zahájí proces určování nejlepších cest ke kořenovému můstku ze všech cílů vysílací domény. Informace o cestě se určují součtem jednotlivých cen portů podél cesty od cíle ke kořenovému můstku. Každý "cíl" je ve skutečnosti port přepínače.

Výchozí ceny portů jsou definovány rychlostí, s kterou daný port operuje. Jak je znázorněno na obrázku 1, 10Gb/s ethernetové porty mají cenu portu 2, 1Gb/s porty mají cenu portu 4, 100Mb/s porty mají cenu portu 19 a 10Mb/s porty mají cenu portu 100.

Poznámka: Vzhledem k tomu, že se novější a rychlejší ethernetové technologie dostanou na trh, hodnoty cen cest se mohou změnit tak, aby odpovídaly různým rychlostem, které jsou k dispozici. Nelineární čísla v tabulce zahrnují některé vylepšení staršího standardu. Hodnoty byly již změněny, aby vyhovovaly standardu 10Gb/s. Pro ilustraci pokračujících změn spojených s vysokorychlostní sítí, přepínače Catalyst 4500 a 6500 podporují metodu s větší cenou cesty; Například 10Gb/s má cenu cestu 2000, 100Gb/s má cenu cesty 200 a 1Tb/s má cenu cesty 20.

Přestože porty přepínačů mají s sebou přidružené výchozí ceny portů, jsou taky konfigurovatelné. Schopnost konfigurovat jednotlivé ceny portů poskytuje administrátorovi flexibilitu, aby ručně řídil cesty ke kořenovému můstku.

Chcete-li konfigurovat cenu portu rozhraní (jak je znázorněno na obrázku 2), zadejte příkaz v konfiguračním módu rozhraní spanning-tree cost hodnota. Hodnota může být mezi 1 a 200 000 000.

V tomto příkladu byl port přepínače F0/1 nakonfigurován s hodnotou portu 25 pomocí příkazu ***spanning-tree cost 25*** na rozhraní F0/1.

Chcete-li obnovit cenu portu na výchozí hodnotu 19, zadejte příkaz ***no spanning-tree cost***.

Cena cesty se rovná součtu všech cen portů podél cesty ke kořenovému můstku (viz obrázek 3). Cesta s nejnižšími náklady se stává preferovanou a všechny ostatní redundantní cesty jsou blokovány. V příkladu je cena cesty 19, od S2 ke kořenovému můstku S1 přes cestu 1 (to na základě individuálních cen portů specifikovaných IEEE), zatímco cena cesty přes cestu 2 je 38. Protože cesta 1 má nižší celkovou cenu cesty ke kořenovému můstku, je preferována. STP konfiguruje redundantní cestu, která má být blokována, což zabraňuje vzniku smyčky.

Chcete-li ověřit cenu portu a cesty ke kořenovému můstku, zadejte příkaz ***spanning-tree*** (jak ukazuje obrázek 4). Pole Cost (cena) v horní části výstupu je celková cena cesty ke kořenovému můstku. Tato hodnota se mění v závislosti na počtu portů přepínače, které se musí dostat ke kořenovému můstku. Ve výstupu je každé rozhraní také identifikováno s individuální cenou portu 19.

9.2.2.5 Rozhodnutí rolí portů pro RSTP

V příkladu, přepínač S1 je kořenový můstek. Přepínače S2 a S3 mají kořenové porty konfigurované pro porty připojující se zpět k S1.

Poté, co přepínač určil, který z jeho portů je nakonfigurován v roli kořenového portu, musí také rozhodnout, které porty mají určenou a alternativní roli.

Kořenový můstek automaticky konfiguruje všechny porty přepínače v určené roli. Jiné přepínače v topologii konfigurují své nekořenové porty jako určené nebo alternativní.

Určené porty jsou konfigurovány pro všechny segmenty LAN. Pokud jsou dva přepínače připojeny ke stejnému segmentu sítě LAN a kořenové porty již byly definovány, musí se oba

dva přepínače rozhodnout, který port má být nakonfigurovaný jako určený port a který zůstane alternativním portem.

Přepínače na segmentu LAN si vyměňují rámce BPDU, které obsahují BID přepínače. Obecně platí, že přepínač s nižším BID má svůj port nakonfigurován jako určený, zatímco přepínač s vyšším BID má svůj port nakonfigurovaný jako alternativní. Mějte však na paměti, že první prioritou je nejnižší cena cesty ke kořenovému můstku a že BID odesílatele se používá pouze v případě, že náklady na port jsou stejné.

Každý přepínač určuje role portů, které jsou přiřazeny každému z nich, čímž vytvoří bez smyčkový STP.

Obrázky 1 až 7 ilustrují způsob určení rolí portů.

9.2.2.6 Rozhodnutí rolí portů pro RSTP

Při určování kořenového portu přepínače, přepínač porovnává ceny všech portů přepínačů účastnících se STP. Portu přepínače s nejnižší celkovou cenou cesty ke kořenovému můstku je automaticky přiřazena role kořenového portu, protože je nejblíže kořenovému můstku. V síťové topologii přepínačů mají všechny nekořenové můstky přepínačů jeden vybraný kořenový port a tento port poskytuje nejnižší cestu zpět ke kořenovému můstku.

Poznámka: Přepínač, který nebyl určen jako kořenový můstek síťové topologie, bude mít definovaný pouze jeden kořenový port.

Obrázek ukazuje topologii se čtyřmi přepínači. Z hlediska rolí portů F0/1 na přepínači S3 a portu F0/3 na přepínači S4 byly tyto porty vybrány jako kořenové porty, protože mají pro své příslušné přepínače nejnižší ceny cesty ke kořenovému můstku.

S2 má dva portové porty F0/1 a F0/2 se stejnými cenami cest ke kořenovému můstku. V tomto případě budou ID mostů sousedních přepínačů, S3 a S4, použity k přerušení vazby. Toto je známé jako BID odesílatele. S3 má BID 24577.5555.5555.5555 a S4 má BID 24577.1111.1111.1111. Protože S4 má nižší BID, port F0/1 na S2, připojený k S4 bude kořenovým portem.

Poznámka: Hodnoty BID nejsou na obrázku zobrazeny.

Dále musí být na sdílených segmentech vybrány určené porty. S2 a S3 se připojují ke stejnému segmentu LAN, a proto si vyměňují rámce BPDU. STP určuje, zda bude port S2 F0/2 nebo F0/2 na S3 určeným portem pro sdílený segment. Přepínač s nejnižší cenou cesty ke

kořenovému můstku, bude mít svůj port jako určený port. Port F0/2 na S3 má nižší cenu cesty ke kořenovému můstku, takže to bude určený port pro tento segment.

S2 a S4 procházejí obdobným procesem pro svůj sdílený segment. Port S4 F0/1 má nižší cenu cesty ke kořenovému můstku a stává se určeným portem v tomto sdíleném segmentu.

Všechny role STP portů byly přiřazeny, kromě portu F0/2 na S2. Port F0/1 byl již vybrán jako kořenový port pro tento přepínač. Vzhledem k tomu, že port F0/2 na S3 je určeným portem pro tento segment, port S2 F0/2 se stane portem alternativním.

Určený port je port, který odesílá a přijímá přenos z tohoto segmentu do kořenového mostu. To je nejlepší port na tomto segmentu směrem ke kořenovému můstku. Alternativní port nebude odesílat nebo přijímat přenos na daném segmentu. Toto je část smyčkové prevence STP.

9.2.2.7 Formát rámce BPDU

STA závisí na výměně BPDU rámců, kvůli určení kořenového můstku. Rámec BPDU obsahuje 12 odlišných polí, které předávají informace o cestě a prioritě použité k určení kořenového můstku a cest ke kořenovému můstku.

Klepnutím na pole BPDU na obrázku 1 zobrazíte podrobnosti.

- První čtyři pole určují protokol, verzi, typ zprávy a příznaky stavů.
- Následující čtyři pole se používají k identifikaci kořenového můstku a cen cest ke kořenovému můstku.
- Poslední čtyři pole jsou všechna políčka časovače, která určují, jak často jsou odesílány zprávy BPDU a jak dlouho jsou informace získané procesem BPDU zachovány.

Obrázek 2 ukazuje rámec BPDU, který byl zachycen pomocí Wireshark. V příkladu obsahuje rámec BPDU více polí, než bylo dříve popsáno. Zpráva BPDU je zapouzdřena do ethernetového rámce, když je přenášena po celé síti. Záhlaví 802.3 označuje zdrojové a cílové adresy rámce BPDU. Tento snímek má cílovou MAC adresu 01: 80: C2: 00: 00: 00, což je adresa více směrového vysílání pro skupinu STP. Je-li rámec adresován touto MAC adresou, každý přepínač, který je nakonfigurován pro STP, přijímá a přečte informace z tohoto rámce. Všechna ostatní zařízení v síti rámec nezohledňují.

V příkladu jsou kořenové ID a BID shodné v zachyceném rámci BPDU. To znamená, že rámec byl zachycen z kořenového můstku. Časovače jsou nastaveny na výchozí hodnoty.

9.2.2.8 Šíření a zpracování 802.1D BPDU

Každý přepínač ve vysílací doméně původně předpokládá, že je kořenovým můstkem pro instanci STP, takže odeslané rámce BPDU obsahují BID místního přepínače jako kořenový identifikátor. Ve výchozím nastavení jsou rámce BPDU odeslány každé dvě sekundy po spuštění přepínače. Výchozí hodnota časovače Hello je určená v rámci BPDU je dvě sekundy. Každý přepínač uchovává místní informace o svém vlastním BID, kořenovém ID a cenu cesty ke kořenu

Když sousední přepínače obdrží rámec BPDU, porovnávají se kořenový identifikátor z rámce BPDU s lokálním kořenovým identifikátorem. Je-li kořenový identifikátor v BPDU nižší než místní kořenový identifikátor, přepínač aktualizuje místní kořenové ID a ID v jeho BPDU zprávách. Tyto zprávy označují nový kořenový můstek v síti. Vzdálenost ke kořenovému můstku je také indikována aktualizací cen cest. Například pokud by byla BPDU přijata na Fast Ethernet portu přepínače, cena cesty by se zvýšila o 19. Pokud je místní kořenový identifikátor nižší než kořenový identifikátor přijatý v rámci BPDU, rámec je vyřazen.

Po aktualizaci kořenového ID pro identifikaci nového kořenového můstku, obsahují všechny následující rámce BPDU odeslané z tohoto přepínače nové kořenové ID a aktualizované ceny cest. Tímto způsobem mohou všechny ostatní sousední přepínače vidět nejnižší identifikační kořen po celou dobu. Vzhledem k tomu, že rámce BPDU procházejí mezi dalšími přilehlými přepínači, ceny cest se neustále aktualizují, aby se ukázala celková cena cesty ke kořenovému můstku. Každý přepínač v STP využívá své cesty k určení nejlepší možné cesty ke kořenovému můstku.

Následující část shrnuje proces BPDU:

Poznámka: Priorita je rozhodujícím faktorem pro výběr kořenového můstku. Pokud jsou priority všech přepínačů stejné, zařízení s nejnižší MAC adresou se stává kořenovým můstkem.

- Každý přepínač se označuje jako kořenový můstek. S2 předává rámce BPDU ze všech portů přepínače. (Obrázek 1)
- Když S3 obdrží BPDU z přepínače S2, S3 porovná svůj kořenový identifikátor s rámcem BPDU, který obdržel. Priority jsou stejné, takže přepínač je nucen prozkoumat část MAC adresy a zjistit, která MAC adresa má nižší hodnotu. S2 má nižší

hodnotu adresy MAC, takže S3 aktualizuje své kořenové ID s kořenovým identifikátorem S2. V tomto bodě S3 považuje S2 za kořenový můstek. (Obrázek 2)

- S1 porovnává jeho kořenový identifikátor s identifikátorem v přijatém rámci BPDU, identifikuje jeho místní kořenový identifikátor jako nižší hodnotu a vyřadí BPDU ze S2. (Obrázek 3)
- S3 odesílá rámce BPDU a kořenový identifikátor obsažený v rámečku BPDU je s S2. (Obr. 4)
- S2 obdrží rámec BPDU a odmítne jej po ověření, že kořenový identifikátor v BPDU odpovídá jeho místnímu kořenovému ID. (Obrázek 5)
- S1 odstraňuje rámec BPDU přijatý od S3, protože S1 má nižší hodnotu priority v kořenovém identifikátoru. (Obr. 6)
- S1 vysílá své rámce BPDU. (Obrázek 7)
- S3 identifikuje kořenový identifikátor v rámci BPDU jako nižší hodnotu, a proto aktualizuje hodnoty svých kořenových ID, což naznačuje, že S1 je nyní kořenovým můstkem. (Postavení 8)
- S2 identifikuje kořenový identifikátor v rámci BPDU jako nižší hodnotu a proto aktualizuje hodnoty kořenových ID, což naznačuje, že S1 je nyní kořenovým můstkem. (Obrázek 9)

9.2.2.9 Rozšířené ID systému

ID můstku (BID) se používá k určení kořenového můstku v síti. Pole BID rámce BPDU obsahuje tři samostatná pole:

- Priorita můstku
- Rozšířené ID systému
- MAC adresa

Každé pole se používá při volbě kořenového můstku.

Priorita můstku

Priorita můstku je přizpůsobitelná hodnota, která může být použita k ovlivnění toho, který přepínač se stane kořenovým můstkem. Přepínač s nejnižší prioritou, ten z nejnižším BID, se stává kořenovým můstkem, protože má přednost nižší hodnota priority. Chcete-li například zajistit, že určitý přepínač byl vždy kořenovým můstkem, nastavte prioritu na nižší hodnotu než ostatní přepínače v síti. Výchozí hodnota priority pro všechny přepínače Cisco je 32768. Rozsah je 0 až 61440 v přírůstcích 4096. Platné hodnoty priorit jsou 0, 4096, 8192,

12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 a 61440. Všechny ostatní hodnoty jsou zamítnuty. Priorita můstku 0 má přednost před všemi ostatními prioritami.

Rozšířené ID systému

Včasné implementace IEEE 802.1D byly navrženy pro sítě, které nepoužívaly VLAN. Ve všech přepínačích byl společný STP. Z tohoto důvodu by u starších přepínačů Cisco mohlo být rozšířené ID systému vynecháno v rámcích BPDU. Vzhledem k tomu, že VLAN se staly běžnými pro segmentaci síťové infrastruktury, byla rozšířena technologie 802.1D, která zahrnuje podporu pro VLAN, což vyžaduje, aby VLAN ID bylo zahrnuto do rámce BPDU. VLAN informace jsou zahrnuty do rámce BPDU pomocí rozšířeného ID systému. Všechny novější přepínače obsahují standardně rozšířené ID systému.

Jak je znázorněno na obrázku 1, pole s prioritou můstku má délku 2 bajty nebo 16 bitů. 4bitové se používají pro prioritu můstku a 12bitové se používají pro rozšířené ID systému, který identifikuje VLAN účastnící se tohoto konkrétního procesu STP. Použitím těchto 12 bitů, pro rozšířené ID systému, se snižuje priorita mostu na 4 bity. Tento proces si vyhrazuje 12 nejdůležitějších bitů pro VLAN ID a zůstávající 4 bity pro prioritu můstku. To vysvětluje, proč může být priorita můstku konfigurována pouze v násobcích 4096 nebo 2 ^ 12. Pokud jsou vzdálenější bity 0001, je priorita mostu 4096. Pokud jsou vzdálené zůstávající bity 1111, tak je priorita můstku 61440 (= 15 x 4096). Přepínače řady Catalyst 2960 a 3560 neumožňují konfiguraci priority můstku 65536 (= 16 x 4096), protože se předpokládá použití pátého bitu, který není k dispozici kvůli použití rozšířeného ID systému.

Rozšířená hodnota ID systému je přidána k prioritní hodnotě můstku v BID k určení priority a VLAN rámce BPDU.

Pokud jsou dva přepínače konfigurovány se stejnou prioritou a mají stejný rozšířený systémový identifikátor, bude mít přepínač mající MAC adresu s nejnižší hexadecimální hodnotou nižší BID. Zpočátku jsou všechny přepínače konfigurovány se stejnou hodnotou výchozí priority. Adresa MAC je rozhodujícím faktorem, který přepínač se stane kořenovým můstkem. Aby bylo zajištěno, že rozhodnutí o kořenovém můstku nejlépe vyhovuje požadavkům sítě, doporučuje se, aby správce nakonfiguroval požadovaný přepínač kořenového mostu s nižší prioritou. To také zajišťuje, že přidání nových přepínačů do sítě nespustí nové volby STP, které mohou narušit síťovou komunikaci při výběru nového kořenového můstku. Po-

kud jsou všechny přepínače konfigurovány se stejnou prioritou, jako u všech přepínačů udržovaných ve výchozí konfiguraci s prioritou 32768, MAC adresa se stává rozhodujícím faktorem, který přepínač se stává kořenovým můstkem, jak je znázorněno na obrázku 3.

Poznámka: V příkladu je priorita všech přepínačů 32769. Hodnota je založena na výchozí prioritě 32768 a přiřazení k VLAN 1 přidružené ke každému přepínači (32768 + 1).

MAC adresa s nejnižší hexadecimální hodnotou se považuje za preferovaný kořenový most. V příkladu má S2 nejnižší hodnotu pro svou MAC adresu a je proto označena jako kořenový můstek pro danou instanci STP.

9.3 Různé druhy STP

9.3.1 Přehled

9.3.1.1 Typy STP

Od vydání původního protokolu IEEE 802.1D se objevilo několik odrůd STP.

Různé typy STP zahrnují:

STP - Jedná se o původní verzi IEEE 802.1D (802.1D-1998 a starší), která poskytuje síťovou smyčku v síti s nadbytečnými vazbami. Common Spanning Tree (CST) předpokládá jednu instanci STP pro celou přemosťovanou síť, bez ohledu na počet VLAN.

PVST + - Toto je vylepšení služby Cisco STP, které poskytuje samostatnou instanci 802.1D pro každou VLAN nakonfigurovanou v síti. Samostatná instance podporuje PortFast, UplinkFast, BackboneFast, BPDU ochranu, filtr BPDU, ochranu kořenů a ochranu smyčky.

802.1D-2004 - Jedná se o aktualizovanou verzi standardu STP zahrnující IEEE 802.1w.

Protokol Rapid Spanning Tree Protocol (RSTP) nebo IEEE 802.1w - Jedná se o vývoj STP, který poskytuje rychlejší konvergenci.

Rapid PVST + - Jedná se o vylepšení technologie RSTP společnosti Cisco, která používá systém PVST +. Rapid PVST + poskytuje samostatnou instanci 802,1w na VLAN. Samostatná instance podporuje platformu PortFast, ochranu BPDU, filtr BPDU, ochranu kořenů a ochranu proti smyčce.

Multiple Spanning Tree Protocol (MSTP) - Jedná se o standard IEEE inspirovaný dřívější implementací Cisco Multiple Instance STP (MISTP). MSTP mapuje více VLAN do stejné

instance. Implementace MSTP společnosti Cisco je MST, která poskytuje až 16 instancí RSTP a kombinuje mnoho VLAN se stejnou fyzickou a logickou topologií do společné instance RSTP. Každá instance podporuje PortFast, ochranu BPDU, filtr BPDU, ochranu kořenů a ochranu proti smyčce.

Profesionální síťový personál, jehož úkoly zahrnuje správu spínačů, může být vyžadován, aby rozhodl, který typ třeba implementovat.

9.3.1.2 Charakteristika STP protokolů

Jedná se o vlastnosti různých protokolů STP. Slova z kurzivou označují, přesný protokol STP, který je vlastní Cisco nebo je to standardní implementace IEEE:

- **STP** - předpokládá jednu instanci IEEE 802.1D STP pro celou přemosťovanou síť, bez ohledu na počet VLAN. Protože existuje pouze jedna instance, požadavky na CPU a paměť pro tuto verzi jsou nižší než u ostatních protokolů. Protože je však pouze jedna instance, existuje pouze jeden kořenový můstek a jeden strom. Provoz pro všechny VLAN proudí přes stejnou cestu, což může vést k neoptimálním dopravním tokům. Z důvodu omezení 802.1D se tato verze pomalu sbližuje.
- **PVST +** - vylepšení technologie STP od Cisco, které poskytuje samostatnou instanci implementující 802.1D pro každou VLAN, která je nakonfigurována v síti. Rychlost konvergence je podobná původnímu STP. Samostatná instance podporuje PortFast, UplinkFast, BackboneFast, BPDU ochranu, filtr BPDU, ochranu kořenů a ochranu smyčky. Role portů jsou definovány stejně jako v RSTP. Vytvoření instance pro každou VLAN zvyšuje požadavky na procesor a paměť, ale umožňuje kořenové můstky typu VLAN. Tato konstrukce umožňuje optimalizaci STP pro provoz každé VLAN. Konvergence této verze je podobná konvergenci 802.1D. Konvergence je však pro každou VLAN.
- **RSTP (nebo IEEE 802.1w)** - Vývoj STP, který poskytuje rychlejší konvergenci než původní implementace 802.1D. Tato verze řeší mnoho problémů konvergence, ale protože stále poskytuje jednu instanci protokolu STP, neřeší problémy s neoptimálním provozním tokem. Pro podporu této rychlejší konvergence, jsou požadavky na využití procesoru, a paměti této verze vyšší než u CST, ale nižší než u aplikací Rapid PVST +.

- **Rapid PVST +** - Vylepšení RSTP od společnosti Cisco, které využívá technologii PVST +. Poskytuje samostatnou instanci 802.1w pro každou VLAN. Samostatná instance podporuje platformu PortFast, ochranu BPDU, filtr BPDU, ochranu kořenů a ochranu proti smyčce. Tato verze se zabývá otázkami konvergence a neoptimálními problémy s dopravním tokem. Tato verze však má nejvyšší požadavky na CPU a paměť.
- **MSTP** - standard IEEE 802.1s a byl inspirován dřívější implementací MISTP společnosti Cisco. Chcete-li snížit počet požadovaných instancí protokolu STP, MSTP zmapuje více VLAN, které mají stejné požadavky na tok dat do stejné instance.
- **MST** - Implementace MSTP společnosti Cisco, která poskytuje až 16 instancí RSTP (802.1w) a kombinuje mnoho VLAN se stejnou fyzickou a logickou topologií do společné instance RSTP. Každá instance podporuje PortFast, ochranu BPDU, filtr BPDU, ochranu kořenů a ochranu proti smyčce. Požadavky na CPU a paměť této verze jsou nižší než požadavky na Rapid PVST +, ale vyšší než u RSTP.

Výchozí režim pro přepínače Cisco Catalyst je PVST +, který je povolen na všech portech. PVST + má po změně topologie mnohem pomalejší konvergenci než Rapid PVST +.

Poznámka: Novější přepínače Cisco s novějšími verzemi IOS, jako jsou přepínače Catalyst 2960 s IOS 15.0, ve výchozím nastavení spouštějí PVST +. Nové přepínače zahrnují mnoho specifikací IEEE 802.1D-2004, jako jsou alternativní porty, namísto bývalých neoznačených portů. Nové přepínače však musí být konfigurovány explicitně pro rychlý režim STP, aby bylo možné spustit protokol RSTP.

9.3.2 PVST+

9.3.2.1 Přehled PVST+

Původní standard IEEE 802.1D který definuje CST, který přebírá pouze jednu instanci STP pro celou spínanou síť, bez ohledu na počet VLAN. Síť provozovaná CST má tyto vlastnosti:

- Není možné sdílení zatížení. Jeden uplink musí blokovat všechny VLAN.
- CPU je ušetřeno. Musí být vypočítána pouze jedna instance STP.

Společnost Cisco vyvinula systém PVST +, aby síť mohla spustit nezávislou instanci implementace technologie IEEE 802.1D pro každou síť VLAN. U zařízení PVST + je možné, aby jeden trunk port na přepínači zablokoval VLAN při posílaní do dalších VLAN. PVST + lze použít k implementaci vyvažování zatížení 2. vrstvy. Přepínače v prostředí PVST+, vyžadují

vyšší proces procesoru a taky spotřebu pásma BPDU, než tradiční implementace STP. Protože každá VLAN provozuje samostatnou instanci STP.

V prostředí PVST +, lze nastavit parametry tak, že polovina VLAN bude posílat na každý trunkový uplink. Na obrázku je port F0/3 na S2 předávající port pro VLAN 20 a F0/2 na S2 je port pro předávání do VLAN 10. To je dosaženo konfigurací jednoho přepínače, který má být vybrán jako kořenový můstek pro polovinu VLAN v síti a druhý přepínač, aby byl zvolen jako kořenový můstek pro druhou polovinu VLAN. Na obrázku je S3 kořenovým můstkem pro VLAN 20 a S1 je kořenový můstek pro VLAN 10. Více kořenových můstků STP na VLAN zvyšuje redundanci v síti.

Sítě provozující PVST + mají tyto vlastnosti:

- Může dojít k optimálnímu vyvažování zátěže.
- Jedna STP instance pro každou udržovanou VLAN může znamenat značné ztráty procesorových cyklů u všech přepínačů v síti (kromě šířky pásma, která se používá pro každou instanci k odeslání vlastního BPDU). To bude problematické pouze v případě, že je nakonfigurován velký počet VLAN.

9.3.2.2 Stavy portů a operace PVST+

STP usnadňuje cestu bez logické smyčky v celé vysílací doméně. Je určen prostřednictvím informací získaných výměnou rámců BPDU mezi propojenými přepínači. Pro usnadnění výuky logického STP, každý port přepínače přechází přes pět možných stavů portů a tři časovače BPDU.

STP je určen okamžitě po ukončení spuštění přepínače. Pokud port přepínače přechází přímo z blokovacího stavu do stavu předávání, bez informací o celé topologii během přechodu, může port dočasně vytvořit datovou smyčku. Z tohoto důvodu STP uvádí pět stavů portů. PVST + taky používá pět stavů portů. Obrázek popisuje stavy portů, které zajišťují, že během vytváření logického STP nebudou vytvořeny žádné smyčky:

Blokování - port je alternativní a nepodílí se na předávání rámců. Port obdrží rámce BPDU pro určení polohy a kořenového ID kořenového můstku, a které role by měl každý port přepínače předpokládat v konečné, aktivní topologii STP.

Poslech - Poslouchá pro určení cesty ke kořenu. STP zjistil, že port se může podílet na předávání rámců podle rámců BPDU, které přepínač získal. Port přepínače přijímá rámce BPDU, vysílá vlastní rámce BPDU a informuje přilehlé přepínače, že port se připravuje k účasti v aktivní topologii.

Učení - Učí se MAC adresy. Port se připravuje na účast v předávání rámců a začne naplňovat tabulku MAC adres.

Předávání - port je považován za součást aktivní topologie. Posílá datové rámce, odesílá a přijímá rámce BPDU.

Zakázáno - Port 2. vrstvy se nepodílí na STP a nepředává rámce. Vypnutý stav je nastaven, když je port přepínače administrativně deaktivován.

Všimněte si, že počet portů v každém z různých stavů (blokování, poslech, učení nebo předávání) lze zobrazit pomocí příkazu ***spanning-tree summary***.

Pro každou VLAN v přepínané síti provádí PVST + čtyři kroky pro zajištění topologie logické sítě bez smyčky:

Volí se jeden kořenový můstek - Pouze jeden přepínač může fungovat jako kořenový můstek (pro danou VLAN). Kořenový můstek je přepínačem s nejnižším ID můstku. Na kořenovém můstku jsou všechny porty označeny jako určené porty (žádné kořenové).

Vybírá se kořenový port na každém nekořenovém můstku - PVST + vytvoří jeden kořenový port na každém nekořenovém můstku pro každou VLAN. Kořenový port, je cesta z nejnižší cenou, z nekořenového můstku ke kořenovému, což označuje směr cesty k můstku kořenovému. Kořenové porty jsou obvykle ve stavu předávání.

Vybírá se určený port v každém segmentu - na každé lince PVST + vytvoří jeden určený port pro každou VLAN. Určený port je vybrán na přepínači, který má cestu z nejnižší cenou ke kořenovému můstku. Určené porty jsou obvykle v režimu předávání a předávají provoz v segmentu.

Zbývající porty v přepínané síti jsou alternativní porty - alternativní porty obvykle zůstávají v blokovacím stavu, aby logicky přerušily topologii smyčky. Pokud je port v blokovacím stavu, nepředává přenos, ale může stále zpracovávat přijaté zprávy BPDU.

9.3.2.3 Rozšířené systémové ID a PVST+ operace

V prostředí PVST +, rozšířené ID systému zajišťuje, že každý přepínač má jedinečné BID pro každou VLAN.

Například výchozí hodnota BID pro VLAN 2 bude 32770 (priorita 32768 plus rozšířený systémový identifikátor o 2). Pokud nebyla nakonfigurována žádná priorita, každý přepínač má stejnou výchozí prioritu a volba kořenu pro každou VLAN je založena na MAC adrese. Tato metoda je náhodný způsob výběru kořenového můstku.

Existují situace, kdy správce může chtít určitý přepínač vybrat jako kořenový můstek. Může se jednat o nejrůznější důvody, včetně toho, že přepínač je umístěn více v centru návrhu LAN, přepínač má vyšší procesní výkon nebo má dálkově jednodušší přístup a správu. Chcete-li manipulovat s volbami kořenového můstku, přiřaďte nižší prioritu přepínači, který chcete zvolit jako kořenový můstek pro požadovanou VLAN.

9.3.3 Rapid PVST+

9.3.3.1 Přehled Rapid PVST+

RSTP (IEEE 802.1w) je vylepšení původního standardu 802.1D a je začleněn do standardu IEEE 802.1D-2004. Terminologie STP 802.1w zůstává v zásadě stejná jako původní terminologie IEEE 802.1D STP. Většina parametrů zůstala nezměněna, takže uživatelé, kteří STP znají, mohou snadno nakonfigurovat nový protokol. Rapid PVST + je implementace produktu RSTP společnosti Cisco na bázi VLAN. Pro každou VLAN běží nezávislá instance RSTP.

Obrázek ukazuje síť se systémem RSTP. S1 je kořenový můstek se dvěma určenými porty ve stavu předávání. RSTP podporuje nový typ portu. Port F0/3 na S2 je alternativní ve stavu vyřazování. Všimněte si, že neexistují blokovací porty. RSTP nemá blokující stav, ale definuje stav portů jako vyřazení, učení nebo předávání.

RSTP urychluje přepočet STP při změně topologie sítě 2. vrstvy. Může dosáhnout mnohem rychlejší konvergence v správně nakonfigurované síti, někdy v několika málo stovkách milisekund. Definuje typ portů a jejich stav. Je-li port nakonfigurován jako alternativní nebo zálohovací, může se okamžitě změnit do stav předávání, aniž by čekal na konvergenci sítě. Následující text stručně popisuje vlastnosti RSTP:

- RSTP je preferovaný protokol při zabraňování smyčkám 2. vrstvy v prostředí přepínané sítě. Mnoho rozdílů bylo vytvořeno při vylepšeních od společnosti Cisco od původního 802.1D. Tato vylepšení, jako jsou BPDU nesoucí a odesílající informace o rolích portů pouze na sousední přepínače, nevyžadují žádnou další konfiguraci a zpravidla budou fungovat lépe než dřívější verze. Nyní jsou transparentní a integrovány do operací protokolu.
- Vylepšení vlastností od společnosti Cisco z původní 802.1D, jako například UplinkFast a BackboneFast, nejsou kompatibilní s protokolem RSTP.

- RSTP (802.1w) nahrazuje původní 802.1D při zachování zpětné kompatibility. Hodně z původní terminologie 802.1D zůstala a většina parametrů zůstává nezměněna. Navíc je 802.1w schopen se vrátit zpět do starší verze 802.1D, aby spolupracoval se staršími přepínači na bázi portů. Například algoritmus RSTP volí kořenový můstek přesně stejným způsobem jako původní 802.1D.
- RSTP uchovává stejný formát BPDU jako původní IEEE 802.1D, s výjimkou toho, že pole verze je nastaveno na hodnotu 2 označující RSTP a pole příznaků používá všech 8 bitů.
- RSTP je schopen aktivně potvrdit, že port může bezpečně přejít do stavu předávání, aniž by musel spoléhat na konfiguraci časovače.

9.2.5.2 BPDU rámce pro RSTP

RSTP používá BPDU typu 2 a verze 2. Původní 802.1D STP používá typ 0, verze 0. Přepínač se systémem RSTP však může komunikovat přímo s přepínačem, který používá původní 802.1D STP. RSTP odešle BPDU a načítá bajt značky trochu jiným způsobem než v původním 802.1D:

- Informace portu o protokolu mohou být okamžitě zastaralé, pokud nebudou přijímány Hello pakety za tři po sobě jdoucí časy (standardně 6 sekund) nebo pokud vyprší maximální časový limit.
- BPDU se používají jako udržovací mechanismus. Tři následně vynechané BPDU rámce indikují ztracenou spojitost mezi můstkem a jeho sousedním kořenem nebo určeným můstkem. Rychlé stárnutí informací umožňuje rychlé zjištění selhání.

Poznámka: Stejně jako STP, tak přepínač RSTP odešle BPDU se svými aktuálními informacemi každé časové období Hello (dvě sekundy ve výchozím nastavení), i když přepínač RSTP neobdrží BPDU z kořenového můstku.

Jak je znázorněno na obrázku, RSTP používá příznakový bajt verze 2:

- Bity 0 a 7 se používají pro změnu a potvrzení topologie. Jsou v původním 802.1D.
- Bity 1 a 6 se používají pro proces návrhu dohody (pro rychlou konvergenci).
- Bity 2 až 5 zakódují roli a stav portu.
- Bity 4 a 5 se používají ke kódování role portu pomocí dvoubitového kódu.

9.2.5.3 Hraniční porty

Hraniční port RSTP je port přepínače, který nikdy není určen k připojení k jinému přepínači. Okamžitě přechází do stavu předávání, když je to povoleno.

Koncept hraničního portu RSTP odpovídá funkci PVST +, PortFast. Hraniční port je přímo připojen ke koncové stanici a předpokládá se, že k němu není připojeno žádné zařízení. Hraniční porty by měly okamžitě přejít do stavu předávání, čímž přeskočí časově náročný počáteční stavy portů 802.1D, poslech a učení.

Implementace Cisco RSTP (Rapid PVST +) udržuje klíčové slovo PortFast pomocí příkazu ***spanning-tree portfast*** pro konfiguraci hraničního portu. To dělá přechod, z STP na RSTP bezproblémový.

Obrázek 1 ukazuje příklady portů, které mohou být konfigurovány jako hraniční. Obrázek 2 ukazuje příklady portů, které hraniční nejsou.

Poznámka: Konfigurace hraničního portu, který se má připojit k jinému přepínači, se nedoporučuje. Může to mít negativní následky pro RSTP, protože může dojít k dočasné smyčce, což pravděpodobně zpomalí konvergenci.

9.2.5.4 Typy propojení

Typ propojení poskytuje kategorizaci pro každý port účastnící se RSTP pomocí duplex módu. V závislosti na tom, co je připojeno ke každému portu, lze identifikovat dva různé typy propojení:

- **Point-to-Point -** Port pracující v režimu plně duplexního připojení typicky spojuje přepínače a je kandidátem na rychlý přechod do stavu předávání.
- **Sdílené -** port pracující v polo-duplexním režimu spojuje přepínač s rozbočovačem, který připojuje více zařízení.

Na obrázku klikněte na každé propojení a dozvíte se informace o typech propojení.

Typ propojení může určit, zda je port schopný okamžitě přejít do stavu předávání, pokud jsou splněny určité podmínky. Tyto podmínky se liší u hraničních a nehraničních portů. Nehraniční porty jsou rozděleny do dvou typů: point-to-point a sdílené. Typ propojení je automaticky určen, ale může být potlačen konfigurací explicitního portu pomocí příkazu ***spanning-tree link type parameter***. Mezi funkce role portů, pokud jde o typy propojení, patří následující:

- Připojení hraničních portů a point-to-point jsou kandidáty na rychlý přechod do stavu předávání. Před přidáním parametru typu propojení však musí RSTP určit roli portu.
- Kořenové porty nepoužívají parametr typu propojení. Kořenové porty umožňují rychlý přechod do stavu předávání, jakmile je port synchronizován.
- Alternativní a záložní porty ve většině případů nepoužívají parametr typu propojení.
- Určené porty nejvíce využívají parametr typu propojení. Rychlý přechod do stavu předávání určeného portu nastane, pouze pokud je parametr typu propojení nastaven na point-to-point.

9.4 Konfigurace STP

9.4.1 Konfigurace PVST+

9.4.1.1 Catalyst 2960 – Základní konfigurace

Tabulka zobrazuje základní konfiguraci STP pro Cisco Catalyst 2960 sériový přepínač. Všimnete si, že jako základní mód STP je nastaven na PVST+.

9.4.1.2 Konfigurace a Verifikace ID můstku

Pokud správce chce, aby se určitý přepínač stal kořenovým můstkem, musí být hodnota priority můstku upravena, aby se ujistil, že je nižší než hodnoty priorit můstků všech ostatních přepínačů v síti. Existují dvě různé metody konfigurace hodnot priority můstku na přepínači Cisco Catalyst.

Metoda 1

Abyste zajistili, že přepínač má nejnižší hodnotu priority můstku, použijte primární příkaz ***spanning-tree vlan vlan-id root primary*** v globálním konfiguračním módu. Priorita přepínače je nastavena na předdefinovanou hodnotu 24 576 nebo na nejvyšší násobek 4 096, menší než nejnižší priorita můstku zjištěná v síti.

Pokud je požadován alternativní kořenový můstek, použijte příkaz v globálním konfiguračním módu ***spanning-tree vlan vlan-id root secondary***. Tento příkaz nastaví prioritu přechodu na předdefinovanou hodnotu 28 672. To zajišťuje, že alternativní přepínač se stane kořenovým můstkem, pokud selže primární. Předpokládá se, že ostatní přepínače v síti mají výchozí hodnotu priority 32 768.

Na obrázku 1, S1 byl vybrán jako primární kořenový můstek pomocí příkazu ***spanning-tree vlan 1 root primary*** a S2 byl nakonfigurován jako sekundární kořenový můstek pomocí příkazu ***spanning-tree vlan 1 root secondary***.

Metoda 2

Další metodou pro konfiguraci hodnoty priority můstku je příkaz v globálním konfiguračním módu, ***spanning-tree vlan vlan-id priority***. Tento příkaz dává podrobnější kontrolu nad prioritní hodnotou můstku. Hodnota priority je konfigurována v krocích po 4,096 mezi 0 a 61,440.

V příkladu byl S3 určen, s prioritní hodnotou můstku 24,576 pomocí příkazu ***spanning tree vlan 1 priority 24576***.

Chcete-li ověřit prioritu můstku přepínače, použijte příkaz ***show spanning-tree***. Na obrázku 2 je priorita přepínače nastavena na 24 576. Všimněte si také, že přepínač je určen jako kořenový můstek pro instanci STP.

Pro konfiguraci přepínačů S1, S2 a S3 použijte Kontrolu syntaxe (Syntax Checker) na obrázku 3. Pomocí druhé metody, popsané výše, nakonfigurujte S3 ručně s nastavením priority na 24 576 pro VLAN 1. Pomocí metody 1 nakonfigurujte S2 jako sekundární kořenový můstek pro VLAN 1 a nakonfigurujte S1 jako primární kořen pro VLAN 1. Ověřte konfiguraci pomocí příkazu ***show spanning-tree*** na S1.

9.4.1.3 PortFast a Ochrana BPDU

PortFast je Cisco funkce pro prostředí PVST +. Je-li port přepínače konfigurován pomocí PortFast, tento port se okamžitě přepne ze stavu blokování do stavu předávání, obejde přitom obvyklé přechodové stavy 802.1D STP (stavy poslechu a učení). PortFast můžete používat na přístupových portech, abyste umožnili těmto zařízením, okamžitě se připojit k síti, než aby čekali na to, až protokol IEEE 802.1D STP konverguje na každou VLAN. Přístupové porty jsou porty, které jsou připojeny k jedné pracovní stanici nebo k serveru.

V platné konfiguraci PortFast, by nikdy neměly být přijímány BPDU, protože by to znamenalo, že k portu je připojen jiný můstek nebo přepínač, což může způsobit smyčku. Přepínače Cisco podporují funkci zvanou Ochrana BPDU. Když je aktivována, nastaví port do porušeného/vyřazeného stavu BPDU. Tím bude port vypnutý. Funkce ochrany BPDU poskytují bezpečnou odpověď na neplatné konfigurace, protože musíte rozhraní znovu ručně spustit zpět do provozu.

PortFast technologie je užitečná pro protokol DHCP. Bez PortFastu může počítač odeslat požadavek DHCP ještě předtím, než je port ve stavu předávání, odmítnutím hostitele od získání použitelné IP adresy a dalších informací. Protože PortFast okamžitě změní stav na předávání, PC vždy získá použitelnou adresu IP.

Poznámka: Vzhledem k tomu, že účelem je minimalizovat čas, který musí přístupové porty čekat, až se STP na konverguje, měl by být použit pouze na přístupové porty. Pokud povolíte PortFast na portu připojeném k jinému přepínači, riskujete vytvoření smyčky.

Chcete-li nakonfigurovat PortFast na portu přepínače, zadejte příkaz pro konfiguraci rozhraní ***spanning-tree portfast*** na každé rozhraní, které chcete, jak je znázorněno na obrázku 2. Příkaz v globálním konfiguračním módu, ***spanning-tree portfast default***, umožňuje konfiguraci na všech ne-trunkových rozhraních.

Chcete-li konfigurovat ochranu BPDU na přístupovém portu 2. vrstvy, použijte příkaz ***spanning-tree bpduguard enable***. Příkaz ***spanning-tree portfast bpduguard default*** umožňuje ochranu BPDU na všech PortFast portech.

Chcete-li ověřit, zda je PortFast a BPDU povoleno na portech přepínače, použijte příkaz ***show running-config***, jak je znázorněno na obrázku 3. Ochrana BPDU a PortFast jsou ve výchozím nastavení vypnuty na všech rozhraních.

Pro konfiguraci a ověření přepínačů S1 a S2 použijte kontrolu syntaxe.

9.4.1.4 Vyrovnávání zátěže PVST+

Topologie na obrázku 1 ukazuje tři přepínače propojeny s 802.1Q trunk linkami. Existují dvě VLAN, 10 a 20, které jsou v těch linkách. Cílem je nakonfigurovat S3 jako kořenový můstek pro VLAN 20 a S1 jako kořenový můstek pro VLAN 10. Port F0/3 na S2 je port pro předávání do VLAN 20 a blokovací port pro VLAN 10. Port F0/2 na S2 je předávací port pro VLAN 10 a blokovací port pro VLAN 20.

Kromě vytvoření kořenového můstku je také možné vytvořit sekundární kořenový most. Sekundární kořenový most je přepínač, který se může stát kořenovým můstkem pro VLAN, pokud primární kořenový most selže. Pokud předpokládají, že si ostatní mosty ve VLAN zachovávají svou výchozí prioritu STP, tento přepínač se stane kořenovým můstkem, pokud selže primární kořenový most.

Postup konfigurace PVST + v této topologii:

Krok 1. Zvolte požadované přepínače jako primární a sekundární kořenové mosty pro každou VLAN. Například na obr. 1 je S3 primární můstek pro VLAN 20 a S1 je sekundární můstek pro VLAN 20.

Krok 2. Nakonfigurujte přepínač jako primární můstek pro VLAN pomocí příkazu ***spanning-tree vlan number root primary*****,** jak je znázorněno na obrázku 2.

Krok 3. Nakonfigurujte přepínač jako sekundární můstek pro VLAN pomocí příkazu ***spanning-tree vlan number root secondary***.

Jiným způsobem, jak zadat kořenový most, je nastavit prioritu STP na každém přepínači na nejnižší hodnotu tak, aby byl přepínač vybrán jako primární můstek pro jeho přidruženou VLAN.

Všimněte si, že na obr. 2 je S3 nakonfigurován jako primární kořenový most pro VLAN 20, S1 je nakonfigurován jako primární kořenový most pro VLAN 10. S2 si zachoval svou výchozí prioritu STP.

Obrázek také ukazuje, že S3 je nakonfigurován jako sekundární kořenový most pro VLAN 10 a S1 je nakonfigurován jako sekundární kořenový most pro VLAN 20. Tato konfigurace umožňuje vyrovnávání zatížení STP s provozem VLAN 10 procházející přes S1 a VLAN 20 procházejícím přes S3.

Dalším způsobem, jak zadat kořenový most, je nastavit prioritu přepínače na nejnižší hodnotu tak, aby byl přepínač vybrán jako primární můstek pro jeho přidruženou VLAN, jak je znázorněno na obrázku 3. Prioritu přepínače lze nastavit pro libovolnou instanci. Toto nastavení ovlivňuje pravděpodobnost, že je jako kořenový můstek vybrán přepínač. Nižší hodnota zvyšuje pravděpodobnost, že je přepínač vybrán. Rozsah je 0 až 61 440 v přírůstcích 4 096; Všechny ostatní hodnoty jsou odmítnuty. Například platná hodnota priority je 4 096 x 2 = 8 192.

Jak je znázorněno na obrázku 4, příkaz ***show spanning-tree active*** zobrazuje podrobnosti o konfiguraci pouze pro aktivní rozhraní. Uvedený výstup pro S1 je nakonfigurován s PVST +. Existuje řada příkazu spojených s příkazem ***show spanning-tree***.

Na obrázku 5, výstup ukazuje, že prioritou pro VLAN 10 je 4 096, což je nejnižší z tří příslušných priorit.

Použijte kontrolu syntaxe na Obr. 6 ke konfiguraci a ověření STP na S1 a S3.

9.4.2 Konfigurace Rapid PVST+

9.4.2.1 Mód STP – (Spanning Tree Mode)

Rapid PVST + je implementace Cisco produktu RSTP. Podporuje RSTP na bázi VLAN. Topologie na obrázku 1 má dvě VLAN: 10 a 20.

Poznámka: Výchozí konfigurace STP na přepínači řady Catalyst 2960 je PVST +. Tedy podporuje jednotky PVST +, Rapid PVST + a MST, avšak pouze jedna verze může být kdykoli aktivní pro všechny VLAN.

Příkazy Rapid PVST + řídí konfiguraci STP instancí VLAN. Instance rozhraní je vytvořeno při přiřazení rozhraní k VLAN a je odebráno, když je poslední rozhraní přesunuto do jiné VLAN. Stejně tak můžete nakonfigurovat STP přepínač a parametry portů, před vytvořením instance, použijí se při vytvoření instance.

Obrázek 2 zobrazuje syntaxi příkazu, potřebnou pro konfiguraci Rapid PVST + na přepínači Cisco. Je požadovaný příkaz pro konfiguraci Rapid PVST +, ***spanning-tree mode rapid-pvst***. Při specifikaci rozhraní pro konfiguraci, platná rozhraní obsahují fyzické porty, VLAN a kanály portů. Rozsah ID VLAN je od 1 do 4094 při instalaci rozšířeného obrazu softwaru (EI) a 1 až 1005 při instalaci standardního obrazu softwaru (SI). Rozsah kanálů portů je 1 až 6.

Obrázek 3 zobrazuje příkazy Rapid PVST +, nakonfigurované na S1.

Na obr. 4, příkaz ***show spanning-tree vlan 10***, zobrazí konfiguraci pro VLAN 10 na přepínači S1. Všimněte si, že priorita BID je nastavena na 4 096. Ve výstupu, příkaz "***Spanning tree enabled protocol rstp***" označuje, že na S1 běží Rapid PVST +. Vzhledem k tomu, že S1 je kořenový můstek pro VLAN 10, všechna jeho rozhraní jsou určené porty.

Na obr. 5 je ukázán příkaz, ***show running-config,*** pro ověření konfigurace Rapid PVST + na S1.

Poznámka: Obecně není nutné konfigurovat typ propojení na point-to-point, pro Rapid PVST +, protože je neobvyklé mít sdílený typ propojení. Ve většině případů je jediný rozdíl mezi konfigurací PVST + a Rapid PVST +, v příkazu ***spanning-tree mode rapid-pvst***.

9.4.3 Problémy z konfigurací STP

9.4.3.1 Analýza topologie STP

K analyzování topologie STP, postupujte takto:

Krok 1. Objevte topologii 2. vrstvy. Použijte síťovou dokumentaci, pokud existuje, nebo použijte příkaz ***show cdp neighbors*** k objevení topologie.

Krok 2. Po zjištění topologie 2. vrstvy použijte znalosti STP, k určení očekávané cesty. Je nutné vědět, který přepínač je kořenovým můstkem.

Krok 3. Pomocí příkazu ***show spanning-tree vlan*** zjistěte, který přepínač je kořenovým můstkem.

Krok 4. Pomocí příkazu ***show spanning-tree vlan*** na všech přepínačích zjistěte, které porty jsou ve stavu blokování nebo předávání a potvrďte svou očekávanou cestu 2. vrstvy.

9.4.3.2 Očekávaná topologie versus Aktuální topologie

V mnoha sítích je optimální topologie STP určena jako součást návrhu sítě a poté implementována prostřednictvím manipulace s prioritou a hodnotami cen cest. Mohou se naskytnout situace, když se nezohlední STP při návrhu a implementaci sítě, nebo nebyl zvažován dříve, než síť prošla významným růstem a změnami. V takových situacích je důležité vědět, jak analyzovat aktuální topologii STP v provozní síti.

Velká část řešení problémů spočívá ve srovnání skutečného stavu sítě se stavem očekávaným. Zjištěním rozdílů, by bylo možné získat informace o problémech při jejich řešení. Síťový profesionál by měl být schopen prozkoumat přepínače a určit jejich aktuální topologii a umět pochopit, jaká by měla být.

9.4.3.3 Přehled stavu STP

Použití příkazu *show spanning-tree* bez specifikování dalších možností poskytuje rychlý přehled stavu STP pro všechny VLAN konfigurovaných na přepínači. Pokud máte zájem pouze o určitou VLAN, omezíte rozsah tohoto příkazu specifikací její volby.

Pomocí příkazu *show spanning-tree vlan vlan_id* zobrazte informace o STP pro konkrétní VLAN. Pomocí tohoto příkazu získáte informace o roli a stavech každého portu na přepínači. Příklad výstupu na přepínači S1 zobrazuje všechny tři porty ve stavu předávání (FWD) a role tří portů jako portů určených nebo kořenových. Všechny zablokované porty zobrazují stav výstupu jako "BLK".

Výstup také poskytuje informace o BID lokálního přepínače a ID kořenu, což je BID kořenového můstku.

9.4.3.4 Důsledky selhání STP

U mnoha protokolů znamená porucha, ztrátu funkce, kterou protokol poskytuje. Pokud například OSPF nefunguje na směrovači, může dojít ke ztrátě připojení k sítím, které jsou k dispozici prostřednictvím tohoto směrovače. To by obecně neovlivnilo zbytek sítě. Je-li stále k dispozici připojení ke směrovači, je možné problém vyřešit a diagnostikovat.

U STP existují dva typy selhání. První je podobná problému OSPF. STP může chybně zablokovat porty, které měly přejít do stavu předávání. Připojení může být ztraceno pro provoz, který by běžně prošel tímto přepínačem, ale zbytek sítě zůstává nedotčena. Druhý typ selhání je mnohem rušivější, jak je ukázáno na obrázku 1. Stává se to, když STP chybně přepne jeden nebo více portů do předávacího stavu.

Nezapomeňte, že hlavička rámce Ethernet neobsahuje pole TTL, což znamená, že jakýkoli rámec, který vstupuje do smyčky, je nadále předáván přepínači po dobu neurčitou. Jedinými výjimkami jsou rámce, jejichž cílová adresa je zaznamenána v tabulce MAC adres. Tyto rámce jsou jednoduše předány do portu, který je spojen s MAC adresou, a nevstupují do smyčky. Nicméně, jakýkoli rámec, který je zaplavil přepínač, vstupuje do smyčky (obrázek 2). To může zahrnovat vysílání, více směrové vysílání a unicast s globálně neznámou cílovou MAC adresou.

Jaké jsou důsledky a odpovídající příznaky selhání STP (obrázek 3)?

Zatížení na všech linkách v přepínané síti LAN se rychle zvětší, jak více a více rámců vstupuje do smyčky. Tento problém není omezen na propojení, které tvoří smyčku, ale také ovlivňuje všechny další propojení v doméně, protože jsou všechny propojení zaplavena. Pokud selhání STP je omezeno na jediné propojení VLAN v jsou ovlivněny jen v téhle. Přepínače a trunk linky, které nenesou VLAN, pracují normálně.

Pokud selhání STP vytvořilo smyčku, provoz se zvyšuje exponenciálně. Přepínače potom zaplavují vysílání z více portů. Tímto způsobem vytvoříte kopie rámců pokaždé, když je předáváte.

Při spuštění řídícího provozu (například OSPF Hellos nebo EIGRP Hellos) se zařízení, která spouští tyto protokoly, začnou se rychle přetěžovat. Jejich procesory přistupují k 100% využití, zatímco se pokoušejí zpracovat neustále rostoucí zátěž řídicí úrovně provozu. V mnoha případech je to první známkou probíhající vysílací bouře, takže směrovače a přepínače 3. vrstvy vykazují poruchy řídící roviny a přitom běží s vysokým zatížením procesoru.

Přepínače mají časté změny tabulky MAC adres. Pokud existuje smyčka, přepínač může vidět rámec s určitou zdrojovou MAC adresou přicházející na jeden port a pak vidět jiný rámec se stejnou MAC adresou zdroje, přicházející na jiný port, o zlomek sekundy později. To způsobí, že přepínač aktualizuje tabulku MAC adres dvakrát pro stejnou adresu.

V důsledku kombinace velmi vysokého zatížení na všech linkách a procesorů přepínače, které běží při maximální zátěži, se tato zařízení obvykle stanou nedosažitelnými. Proto je velmi obtížné diagnostikovat problém, když se to děje.

9.4.3.5 Oprava problémů STP

Jedním ze způsobů, jak opravit selhání STP, je ručním odstraněním nadbytečných vazeb v přepojené síti, fyzicky nebo prostřednictvím konfigurace, dokud nejsou všechny smyčky z topologie odstraněny. Když jsou smyčky přerušeny, zatížení provozu a CPU, by měly rychle klesnout na normální úroveň a měla by být obnovena možnost připojení k zařízením.

Ačkoli tento zásah obnoví připojení k síti, není to konec procesu odstraňování problémů. Všechna redundance ze spínané sítě byla odstraněna a nyní musí být obnoveny redundantní propojení.

Pokud nedojde k zjištění základní příčiny selhání STP, je pravděpodobné, že obnovení redundantních vazeb vyvolá novou vysílací bouři. Před obnovením redundantních vazeb zjistěte a opravte příčinu selhání. Pečlivě sledujte síť, abyste zajistili opravu problémů.

9.5 Redundantní protokoly Prvního skoku

9.5.1 Koncepty Redundantních protokolů Prvního skoku

9.5.1.1 Limitace výchozí brány

STP protokoly umožňují fyzickou redundanci v přepínané síti. Hostitel v přístupové vrstvě hierarchické sítě však také využívá alternativní výchozí brány. Pokud rozhraní směrovače nebo směrovač (který slouží jako výchozí brána) selhalo, hostitelé s touto výchozí bránou jsou izolováni od vnějších sítí. Je zapotřebí mechanismu, který poskytuje alternativní výchozí brány v přepínaných sítích, kde jsou dva nebo více směrovačů připojených ke stejné VLAN.

Poznámka: Pro účely diskuse o redundanci směrovače neexistuje žádný funkční rozdíl mezi vícevrstvým přepínačem a směrovačem v distribuční vrstvě. V praxi je běžné, že vícevrstvý

přepínač funguje jako výchozí brána pro každou VLAN v přepínané síti. Tato diskuse se zaměřuje na funkčnost směrování bez ohledu na fyzické zařízení.

V přepínané síti má každý klient pouze jednu výchozí bránu. Neexistuje způsob, jak používat sekundární bránu, i když existuje druhá cesta k přenosu paketů z lokálního segmentu.

Na obrázku je R1 odpovědný za směrování paketů z PC1. Pokud se R1 stane nedostupným, směrovací protokoly mohou dynamicky konvergovat. R2 nyní směruje pakety z vnějších sítí, které by prošli R1. Avšak přenosy z vnitřní sítě spojené s R1, včetně provozu z pracovních stanic, serverů a tiskáren, které mají nakonfigurovanou jako výchozí bránu R1, jsou stále odesílány na R1 a vypuštěny.

Koncové zařízení je obvykle konfigurováno s jednou IP adresou pro výchozí bránu. Tato adresa se při změně topologie sítě nezmění. Není-li tato IP adresa výchozí brány dosažitelná, místní zařízení nemůže odesílat pakety z lokálního síťového segmentu a efektivně se odpojí od zbytku sítě. I když existuje redundantní směrovač, který by mohl sloužit jako výchozí brána pro daný segment, neexistuje žádná dynamická metoda, pomocí níž tato zařízení můžou určit adresu nové výchozí brány.

9.5.1.2 Redundance směrovače

Jeden způsob, jak zabránit i jedinému bodu selhání na výchozí bráně, je implementovat virtuální směrovač. K implementaci tohoto typu redundance směrovače, je potřeba nakonfigurovat více směrovačů, které společně pracují na zobrazování iluze jediného směrovače hostitelům v síti LAN, jak je znázorněno na obrázku. Sdílením IP a MAC adresy mohou dva nebo více směrovačů fungovat jako jeden virtuální.

IP adresa virtuálního směrovače je nakonfigurována jako výchozí brána pro pracovní stanice na určitém IP segmentu. Když jsou rámce odesílány z hostitelských zařízení na výchozí bránu, hostitelé používají ARP k vyřešení MAC adresy přidružené k adrese IP, výchozí brány. Rozlišení ARP vrátí MAC adresu virtuálního směrovače. Rámce, které jsou odesílány do MAC adresy virtuálního směrovače, pak mohou být fyzicky zpracovávány, aktuálně a aktivním směrovačem ve skupině virtuálních směrovačů. Protokol se používá k identifikaci dvou nebo více směrovačů jako zařízení, která jsou odpovědná za zpracování rámců, které jsou odesílány na adresu MAC nebo IP jednoho virtuálního směrovače. Hostitelská zařízení odesílají provoz na adresu virtuálního směrovače. Fyzický směrovač, který předává tento provoz, je pro hostitelská zařízení transparentní.

Protokol redundance poskytuje mechanismus, pro určení, který směrovač by měl mít aktivní roli při předávání provozu. Určuje také, kdy musí být role předávání převzata pohotovostním směrovačem. Přechod z jednoho předávajícího směrovače na druhý je pro koncové zařízení transparentní.

Schopnost sítě dynamicky se zotavit ze selhání zařízení, fungujícího jako výchozí brána, je známá jako redundance prvního skoku (first-hop).

9.5.1.3 Kroky k selhání směrovače

Když selže aktivní směrovač, redundantní protokol přepne pohotovostní směrovač na novou roli aktivního směrovače. Jedná se o kroky, ke kterým dojde při selhání aktivního směrovače:

- Pohotovostní směrovač přestane vidět zprávu Hello z předávacího směrovače.
- Pohotovostní směrovač přebírá roli předávání.
- Protože nový předávací směrovač přijímá jak adresu IP, tak MAC adresu virtuálního směrovače, hostitelská zařízení nevidí žádné narušení služby.

9.5.2 Odrůdy redundantních protokolů prvního skoku

9.5.2.1 Redundantní protokoly prvního skoku

Následující seznam definuje možnosti, které jsou k dispozici pro protokoly FHRP (First Hop Redundancy Protocols), jak je znázorněno na obrázku.

- **Hot Standby Router Protocol (HSRP)** - Cisco FHRP, který je navržen tak, aby umožňoval transparentní selhání služeb při zařízení IPv4 prvního skoku. Služba HSRP poskytuje vysokou dostupnost sítě tím, že poskytuje redundanci směrování prvního skoku pro hostitele protokolu IPv4 v sítích nakonfigurovaných s výchozí adresou brány IPv4. HSRP se používá ve skupině směrovačů pro výběr aktivního a pohotovostního zařízení. Ve skupině rozhraní zařízení, je aktivním zařízením to, které se používá pro směrování paketů. Pohotovostní zařízení je zařízení, které přebírá aktivitu, když selže aktivní zařízení nebo jsou splněny předem nastavené podmínky. Funkce pohotovostního směrovače HSRP je sledovat provozní stav skupiny HSRP a rychle přijmout odpovědnost za předávání paketů, pokud selže aktivní směrovač.
- **HSRP pro protokol IPv6** - Cisco FHRP, který poskytuje stejnou funkcionalitu HSRP, ale v prostředí IPv6. Skupina HSRP IPv6, má virtuální MAC adresu odvoze-

nou od čísla skupiny HSRP a virtuální adresu IPv6 lokální linky, odvozenou z virtuální MAC adresy HSRP. Pokud je skupina HSRP aktivní, směrovače odesílají periodické správy (RA), na adresu virtuální IPv6 lokální linky. Když se skupina stává neaktivní, tyto správy zastaví po odeslání konečné RA správy.

- **Virtual Router Redundancy Protocol verze 2 (VRRPv2)** - Nevlastní volební protokol, který dynamicky přiřazuje odpovědnost za jeden nebo více virtuálních směrovačů, VRRP směrovačům v IPv4 LAN síti. To umožňuje několika směrovačům na víceúčelovém propojení použít stejnou virtuální adresu IPv4. VRRP směrovač je nakonfigurován pro spuštění protokolu VRRP ve spojení s jedním nebo více dalšími směrovači připojenými k síti LAN. V konfiguraci je jeden směrovač zvolen jako virtuální mistr s ostatními směrovači, které fungují jako jeho zálohy, v případě jeho selhání.
- **VRRPv3** - Poskytuje schopnost podporovat adresy IPv4 a IPv6. VRRPv3 funguje v prostředích s více dodavateli a je škálovatelnější než VRRPv2.
- **Protokol vyvažování zátěže brány (GLBP)** - FHRP společnosti Cisco chrání přenos dat z chybného směrovače nebo obvodu, například HSRP a VRRP, a zároveň umožňuje vyvažování zátěže (nazývané také sdílení zatížení) mezi skupinou redundantních směrovačů.
- **GLBP pro IPv6** - Cisco FHRP, poskytující stejnou funkcionalitu GLBP, ale v prostředí IPv6. Služba GLBP pro protokol IPv6 poskytuje automatickou zálohu směrovače, pro hostitele protokolu IPv6, s nakonfigurovanou jednou výchozí bránou. Více směrovačů prvního skoku v síti LAN, kombinuje nabízení jediného virtuálního směrovače IPv6 prvního skoku, při sdílení zatížení předávání paketů IPv6.
- **ICMP Router Discovery Protocol (IRDP)** - specifikovaný v RFC 1256, je starším řešením FHRP. IRDP umožňuje hostitelům protokolu IPv4 lokalizovat směrovače, které poskytují připojení IPv4 k jiným (nelokálním) IP sítím.

9.5.3 Verifikace FHRP

9.5.3.1 Verifikace HSRP

Aktivní směrovač HSRP má následující vlastnosti:

- Reaguje na ARP požadavky výchozí brány s MAC adresou virtuálního směrovače.
- Předpokládá aktivní předávání paketů pro virtuální směrovač.
- Odesílá zprávy Hello.

- Zná IP adresu virtuálního směrovače.

Pohotovostní směrovač HSRP má následující vlastnosti:

- Poslouchá pravidelné zprávy Hello.
- Předpokládá aktivní předávání paketů, i pokud neslyší z aktivního směrovače.

Chcete-li ověřit stav HSRP, použijte příkaz ***show standby***. Na obrázku, výstup ukazuje, že směrovač je v aktivním stavu.

9.5.3.2 Verifikace GLBP

Ačkoli HSRP a VRRP poskytují odolnost brány, pro záložní členy skupiny redundance se šířka pásma proti směru dat nepoužívá, když je přístroj v pohotovostním režimu.

Pouze aktivní směrovač ve skupinách HSRP a VRRP předává přenos virtuální MAC adresy. Zdroje, které jsou přidruženy ke směrovači v pohotovostním režimu, nejsou plně využity. Pomocí těchto protokolů můžete provést vyvažování zátěže, vytvořením více skupin a přiřazením více výchozích bran, ale tato konfigurace vytváří administrativní zátěž.

GLBP je řešení společnosti Cisco, které umožňuje kromě automatického převzetí služeb a současného použití automatického výběru více dostupných bran, při selhání mezi těmito bránami. Více směrovačů sdílí zatížení rámců, které jsou z hlediska klienta odeslány na jednu adresu výchozí brány, jak je znázorněno na obrázku 1.

S GLBP můžete plně využít zdroje, bez administrativní zátěže pro konfiguraci více skupin a správu více konfigurací výchozí brány. GLBP má tyto vlastnosti:

- Umožňuje plné využití zdrojů na všech zařízeních bez administrativní zátěže při vytváření více skupin.
- Poskytuje jednu virtuální adresu IP a více virtuálních MAC adres.
- Směruje provoz na jednu bránu distribuovanou v rámci směrovačů.
- Poskytuje automatické přesměrování v případě selhání.

Pomocí příkazu ***show glbp*** ověřte stav GLBP. Obrázek 2 ukazuje, že GLBP skupina 1 je v aktivním stavu s virtuální adresou IP 192.168.2.100.

9.6 Shrnutí

9.6.1 Shrnutí

9.6.1.1 Aktivita třídy – Strom dokumentace

Strom dokumentace

Zaměstnanci ve vaší budově mají potíže s přístupem k webovému serveru v síti. Hledáte síťovou dokumentaci, kterou předchozí síťový inženýr použil předtím, než přešel na novou. Nicméně nemůžete najít žádnou síťovou dokumentaci.

Proto se rozhodnete vytvořit vlastní síťový systém pro vedení záznamů. Rozhodnete se začít v přístupové vrstvě hierarchie sítě. Zde se nacházejí redundantní přepínače, stejně jako firemní servery, tiskárny a místní počítače.

Vytvoříte matici pro záznam vaší dokumentace a zahrňte přepínače přístupové vrstvy do seznamu. Také se zadokumentujte názvy přepínačů, používané porty, propojení kabelů, kořenové porty, určené porty a alternativní porty.

9.6.1.2 Shrnutí

Problémy, které mohou vyplynout z redundantní sítě 2. vrstvy, zahrnují vysílací bouře, nestabilitu MAC databáze a duplicitní unicast rámce. STP je protokol 2. vrstvy, který zajišťuje, že existuje pouze jedna logická cesta mezi všemi cíli v síti, záměrným blokováním redundantních cest, které by mohly způsobit smyčku.

STP posílá rámce BPDU pro komunikaci mezi přepínači. Jeden přepínač je zvolen jako kořenový můstek pro každou instanci. Správce může tuto volbu ovládat změnou priority můstku. Kořenové můstky mohou být nakonfigurovány tak, aby umožňovaly překlenout vyvažování zatížení VLAN, nebo jejich skupinou v závislosti na použitém protokolu. STP pak přiřadí roli každému zúčastněnému portu za použití ceny cesty. Cena cesty se rovná součtu všech cen portů podél celé cesty ke kořenovému mostu. Každému portu je automaticky přiřazena cena portu. Lze jej však také ručně nakonfigurovat. Cesta s nejnižší cenou se stává preferovanou a všechny ostatní redundantní cesty jsou blokovány.

PVST + je výchozí konfigurace IEEE 802.1D na přepínačích Cisco. Spustí jednu instanci protokolu STP pro každou VLAN. Novější a rychlejší konvergující protokol RSTP, lze implementovat na přepínačích Cisco na bázi VLAN v podobě Rapid PVST +. MST je implementace protokolu Multiple Spanning Tree Protocol (MSTP), kde běží jedna instance stromu

pro definovanou skupinu VLAN. Funkce, jako je PortFast a ochrana BPDU, zajišťují, že hostitelé v přepínaném prostředí mají okamžitý přístup k síti bez zásahu do operací STP.

Redundantní protokoly prvního skoku, jako například HSRP, VRRP a GLBP, poskytují alternativní výchozí brány pro hostitele v redundantním směrovači nebo vícevrstvém přepínacím prostředí. Více směrovačů sdílí virtuální IP adresu a MAC adresu, kterou klient používá jako výchozí bránu. To zajišťuje, že hostitelé udržují připojení i v případě selhání jednoho zařízení sloužícího jako výchozí brána pro VLAN nebo soubor VLAN. Pokud používáte HSRP nebo VRRP, máte jeden směrovač aktivní nebo předává jen určité skupině, zatímco ostatní jsou v pohotovostním režimu.

10 KAPITOLA 3 – AGREGACE LINKY

10.1 Úvod

10.1.1 Úvod

10.1.1.1 Úvod

Agregace linky, je schopnost, vytvořit jedno logické spojení pomocí více fyzických vazeb mezi dvěma zařízeními. To umožňuje sdílení zátěže mezi fyzickými vazbami, spíše než mít STP, které blokuje jednu nebo více linek. EtherChannel je forma agregace linek používaná v přepínaných sítích.

Tato kapitola popisuje EtherChannel a metody použité k jeho vytvoření. Může být ručně nakonfigurován nebo může být vyjednán s protokolem Port Aggregation Protocol (PAgP) nebo s protokolem LACP (Link Aggregation Control Protocol) definovaným přes IEEE 802.3ad. Kontrolujeme konfiguraci, ověřování a odstraňování problémů s EtherChannel.

10.2 Koncepty agregace linky

10.2.1 Agregace linky

10.2.1.1 Agregace linky – Úvod

Na obrázku je přenos dat z několika propojení (obvykle 100 nebo 1000 Mb/s) agreguje na přístupovém přepínači a musí být odeslán do distribučních přepínačů. Z důvodu agregace provozu, musí být mezi přepínači přístupu a distribuce, k dispozici linka s větší šířkou pásma.

Je možné, že na agregované lince mezi přepínači přístupové a distribuční vrstvy, je možné použít rychlejší linky, například 10 Gb/s. Přidávání rychlejších linek je však nákladné. Navíc, jak se zvyšuje rychlost na přístupových linkách, ani nejrychlejší port na agregované lince již není dostatečně rychlý k agregaci provozu ze všech přístupových linek.

Je také možné vynásobit počet fyzických linek mezi přepínači, aby se zvýšila celková rychlost komunikace přepínače k přepínači. Ve výchozím nastavení je však STP na přepínačích aktivován. STP blokuje redundantní linky, aby se zabránilo smyčkám.

Z těchto důvodů je nejlepším řešením implementace konfigurace EtherChannelu.

10.2.1.2 Výhody EtherChannel

Technologie byla původně vyvinuta společností Cisco jako LAN přepínač-přepínač techniku, seskupit několik portů Fast Ethernet nebo Gigabit Ethernet do jednoho logického kanálu. Když je nakonfigurován, výsledné virtuální rozhraní se nazývá kanál portů. Fyzická rozhraní jsou spojena dohromady do rozhraní portového kanálu.

Technologie EtherChannel má mnoho výhod:

- Většina konfiguračních úloh může být provedena na rozhraní EtherChannel namísto každého jednotlivého portu, což zajišťuje konzistenci konfigurace v rámci všech linek.
- EtherChannel se spoléhá na existující porty přepínače. Není nutné upgradovat linku na rychlejší a dražší připojení, aby bylo dosaženo větší šířky pásma.
- Vyrovnávání zatížení probíhá mezi linkami, které jsou součástí stejného EtherChannelu. V závislosti na hardwarové platformě může být implementována jedna nebo více metod vyvažování zátěže. Tyto metody zahrnují vyvažování zatížení zdrojové a cílové MAC adresace nebo zdrojové a cílové IP adresace, přes fyzické linky.
- EtherChannel vytvoří agregaci, která je považována za jednu logickou linku. Pokud mezi dvěma přepínači existuje několik svazků EtherChannel, může STP zablokovat jeden ze svazků, aby se zabránilo smyčkám. Když STP blokuje jednu z redundantních linek, zablokuje celý EtherChannel. Tím se zablokují všechny porty patřící k této lince. Pokud je k dispozici pouze jedna linka, všechny fyzické propojení jsou aktivní, protože STP vidí pouze jednu (logickou) linku.
- EtherChannel poskytuje redundanci, protože celkové spojení je považováno za jedno logické spojení. Navíc ztráta jedné fyzické linky v kanálu nevytváří změnu topologie. Proto není nutný přepočet STP. Za předpokladu, že existuje alespoň jedno fyzické spojení, i když jeho celková propustnost klesá kvůli ztracenému propojení v EtherChannelu, zůstane funkční.

10.2.2 Operace EtherChannelu

10.2.2.1 Omezení Implementace

EtherChannel, lze implementovat seskupením více fyzických portů do jedné nebo více logických linek.

Poznámka: Typy rozhraní nelze smíchat. Například Fast Ethernet a Gigabit Ethernet nemohou být smíchány.

EtherChannel poskytuje plně duplexní šířku pásma až 800 Mb/s (Fast EtherChannel) nebo 8 Gb/s (Gigabit EtherChannel) mezi jedním přepínačem a hostitelem. V současné době každý EtherChannel může obsahovat až osm kompatibilně nakonfigurovaných portů. Přepínač Cisco IOS může v současné době podporovat šest EtherChannelů. Protože nové IOS jsou vyvinuty a platformy se mění, některé karty a platformy mohou podporovat větší počet portů, stejně jako podporovat větší počet linek. Koncept je stejný bez ohledu na rychlost nebo počet linek, o které se jedná. Při konfiguraci rozhraní na přepínačích si uvědomte hranice a specifikace hardwarové platformy.

Původním účelem bylo zvýšit rychlostní schopnosti agregovaných linek mezi přepínači. Tento koncept byl však rozšířen, protože technologie se stala populárnější a nyní mnoho serverů také podporuje agregaci linek. EtherChannel vytváří vztah jeden k jednomu. To znamená, že jedna linka spojuje pouze dvě zařízení. Linka může být vytvořena mezi dvěma přepínači nebo může být vytvořena mezi povoleným serverem a přepínačem. Provoz však nelze odeslat na dva různé přepínače prostřednictvím stejné linky EtherChannel.

Individuální konfigurace portu člena skupiny EtherChannel musí být v obou zařízeních konzistentní. Pokud jsou fyzické porty jedné strany konfigurovány jako trunk, musí být fyzické porty druhé strany také tak konfigurovány v rámci stejné nativní VLAN. Navíc musí být všechny porty v každé lince konfigurovány jako porty 2. vrstvy.

Poznámka: EtherChannel 3. vrstvy lze konfigurovat na vícevrstvých přepínačích Cisco Catalyst, jako je například Catalyst 3560, ale v tomto kurzu ne. Má jednu adresu IP spojenou s logickou agregací přepínačových portů.

10.2.2.2 Protokol Agregace portu

EtherChannel mohou být vytvořeny vyjednáváním pomocí jednoho ze dvou protokolů, PAgP nebo LACP. Tyto protokoly umožňují portům s podobnými vlastnostmi vytvořit kanál prostřednictvím dynamického vyjednávání se sousedními přepínači.

Poznámka: Je také možné nakonfigurovat statický nebo bezpodmínečný EtherChannel bez PAgP nebo LACP.

PAgP

PAgP je protokol společnosti Cisco, který pomáhá při automatické tvorbě linek EtherChannel. Když je linka nakonfigurována pomocí PAgP, PAgP pakety jsou posílány mezi porty s rozhraním EtherChannel a vyjednávají o vytvoření kanálu. Když PAgP identifikuje odpovídající linku, seskupí je do EtherChannelu. Pak je přidán k STP jako jediný port.

Pokud je povoleno, PAgP také spravuje EtherChannel. Pakety PAgP jsou odesílány každých 30 sekund. PAgP kontroluje konzistenci konfigurace a řídí přidání a selhání linek mezi dvěma přepínači. Zajišťuje, že při vytvoření EtherChannelu mají všechny porty stejný typ konfigurace.

Poznámka: V rozhraní EtherChannel je povinné, aby všechny porty měly stejnou rychlost, duplexní nastavení a informace o VLAN. Jakákoli změna portu po vytvoření kanálu také mění všechny ostatní porty kanálů.

PAgP pomáhá vytvářet spojení EtherChannel tak, že zjistí konfiguraci každé strany a zajistí, aby byly linky kompatibilní, a aby bylo možné v případě potřeby povolit spojení.

- **Zapnuto** - Tento režim přinutí rozhraní ke kanálu bez funkce PAgP. Rozhraní konfigurovaná v režimu zapnutí nevyměňují PAgP pakety.
- **PAgP je žádoucí** - tento režim PAgP umístí rozhraní v aktivním vyjednávacím stavu, ve kterém rozhraní iniciuje vyjednávání s jinými rozhraními posíláním PAgP paketů.
- **PAgP auto** - Tento režim PAgP umisťuje rozhraní v pasivním vyjednávacím stavu, ve kterém rozhraní reaguje na PAgP pakety, které přijímá, ale nezakládá vyjednávání.

Režimy musí být kompatibilní na každé straně. Pokud je jedna strana konfigurována tak, aby byla v automatickém režimu, je umístěna v pasivním stavu a čeká na druhou stranu, aby zahájila vyjednávání. Pokud je druhá strana také nastavena na režim automatický, jednání se nikdy nespustí a EtherChannel se nevytvoří. Pokud jsou všechny režimy deaktivovány pomocí příkazu *no*, nebo pokud není nakonfigurován žádný režim, kanál je vypnut.

Režim zapnutí umí ručně umístit rozhraní do EtherChannelu bez jakéhokoli vyjednávání. Funguje to pouze tehdy, když je zapnuta i druhá strana. Pokud je druhá strana nastavena pro vyjednávání parametrů prostřednictvím PAgP, nevytváří se žádný EtherChannel, protože strana, která je nastavena na režim zapnuto, nevyjednává.

10.2.2.3 LACP – Protokol kontroly agregační linky

LACP je součástí specifikace IEEE (802.3ad), která umožňuje připojit několik fyzických portů pro vytvoření jediného logického kanálu. LACP umožňuje přepnout k vyjednávání automatického balíčku, odesláním paketů LACP k partnerovi. Provádí podobnou funkci jako PAgP s EtherChannel. Vzhledem k tomu, že LACP je standardem IEEE, může být použit pro usnadnění EtherChannel v prostředí s více dodavateli. U zařízení Cisco jsou podporovány oba protokoly.

LACP poskytuje stejné vyjednávací výhody jako PAgP. Pomáhá vytvářet spojení EtherChannel tím, že zjistí konfiguraci každé strany a ujistí se, že jsou kompatibilní, takže v případě potřeby je možné zapnout linku EtherChannel. Obrázek ukazuje režimy pro LACP.

- **Zapnuto** - Tento režim nutí rozhraní na kanál bez LACP. Rozhraní konfigurovaná v režimu zapnutí nevyměňují LACP pakety.
- **LACP aktivní** - Tento režim umístí port v aktivním vyjednávacím stavu. V tomto stavu port iniciuje vyjednávání s jinými porty odesláním LACP paketů.
- **LACP pasivní** - Tento režim umístí port v pasivním vyjednávacím stavu. V tomto stavu port reaguje na LACP pakety, které přijímá, ale nezakládá vyjednávání.

Stejně jako u PAgP musí být režimy kompatibilní na obou stranách, aby se vytvořila linka EtherChannel. Režim zapnutí se opakuje, protože bezpodmínečně vytváří konfiguraci bez dynamického vyjednávání PAgP nebo LACP.

10.3 Konfigurace agregace linky

10.3.1 Konfigurace EtherChannel

10.3.1.1 Průvodce konfigurací

Následující pokyny a omezení jsou užitečné pro konfiguraci EtherChannelu:

- **Podpora EtherChannelu** - všechna ethernetová rozhraní na všech modulech musí podporovat EtherChannel bez požadavku, aby rozhraní byla fyzicky přilehlá nebo na stejném modulu.
- **Rychlost a duplex** - Nakonfigurujte všechna rozhraní v EtherChannel tak, aby fungovala stejnou rychlostí a stejným duplexním režimem, jak je znázorněno na obrázku.
- **VLAN shoda** - Všechna rozhraní v svazku EtherChannel musí být přiřazena ke stejné VLAN nebo musí být nakonfigurována jako trunk (také na obrázku).
- **Rozsah VLAN** - EtherChannel podporuje stejný povolený rozsah VLAN na všech rozhraních v kanálu. Pokud povolený rozsah VLAN, není stejný, rozhraní se nevytvoří, i když je nastaven na automatický nebo žádoucí režim.

Pokud je nutné toto nastavení změnit, nakonfigurujte je v režimu konfigurace rozhraní portového kanálu. Po nakonfigurování rozhraní kanálu portu ovlivňuje libovolná konfigurace aplikovaná na rozhraní portového kanálu také jednotlivé rozhraní.

10.3.1.2 Konfigurace rozhraní

Konfigurace EtherChannelu pomocí LACP je založeno na dvou krocích:

Krok 1. Určete rozhraní, které tvoří skupinu EtherChannel, pomocí příkazu ***interface range interface***. Klíčové slovo range, umožňuje vybrat několik rozhraní a nakonfigurovat je všechny dohromady. Dobrým postupem je začít tím, že vypnete tato rozhraní, takže žádná neúplná konfigurace nevytvoří aktivitu na lince.

Krok 2. Vytvořte rozhraní kanálu portů s příkazem ***channel-group identifier mode active***. Identifikátor určuje číslo skupiny kanálů. Klíčová slova *mode active*, toto označují jako konfiguraci LACP.

Poznámka: EtherChannel je standardně deaktivován.

Na obr. 1 jsou FastEthernet0/1 a FastEthernet0/2 připojeny do rozhraní kanálu portů EtherChannel 1.

Chcete-li změnit nastavení 2. vrstvy na rozhraní kanálu portů, zadejte příkaz ***interface port-channel*** a poté identifikátor rozhraní. V příkladu je EtherChannel konfigurován jako trunk rozhraní s povolenými VLAN. Na obr. 1 je také znázorněn kanál 1 portu rozhraní, který je konfigurován jako trunk s povolenými VLAN 1, 2 a 20.

10.3.2 Verifikace a řešení problémů s EtherChannel

10.3.2.1 Verifikace EtherChannel

Existuje několik příkazů k ověření konfigurace EtherChannelu. Nejprve příkaz *show interface port-channel*, zobrazuje obecný stav rozhraní kanálu portu. Na obr. 1 je rozhraní kanálu portu 1 nahoře.

Je-li na stejném zařízení nakonfigurováno více rozhraní kanálů portu, použijte příkaz *show etherchannel summary*, který jednoduše zobrazí jeden řádek informací na portovém kanálu. Na obr. 2 má přepínač nakonfigurovaný jeden EtherChannel. Skupina 1 používá LACP.

Rozhraní se skládá z rozhraní FastEthernet0/1 a FastEthernet0/2. Skupina je EtherChannel 2. vrstvy a používá se, jak je naznačeno písmeny SU vedle čísla kanálu portu.

Na libovolném fyzickém rozhraní člena balíku EtherChannel, může příkaz ***show interfaces etherchannel***, zobrazovat informace o roli rozhraní, jak je znázorněno na obrázku 4. Rozhraní FastEthernet 0/1 je součástí balíčku EtherChannel 1. Protokol pro tento kanál je LACP.

10.3.2.2 Řešení problémů z EtherChannel

Všechna rozhraní v EtherChannelu musí mít stejně nakonfigurovanou rychlost a duplex, nativní a povolenou VLAN na trunk linkách a přístup k VLAN na přístupových portech:

- Přiřaďte všechny porty v EtherChannelu k téže VLAN nebo je nakonfigurujte jako trunk. Porty s různými nativními sítěmi VLAN nemohou vytvořit EtherChannel.
- Při konfiguraci EtherChannel z trunk portů ověřte, zda je režim kanálu stejný pro všechny. Nekonzistentní trunk režimy na portech EtherChannel mohou způsobit, že EtherChannel nebude fungovat a porty budou vypnuty (errdisable state).
- EtherChannel podporuje stejný povolený rozsah VLAN na všech portech. Pokud povolený rozsah VLAN není stejný, porty netvoří EtherChannel, ani když je PAgP nastaven na automatický nebo požadovaný režim.
- Dynamické možnosti vyjednávání pro PAgP a LACP musí být kompatibilně konfigurovány na obou koncích etherChannel.

Poznámka: Je snadné zaměnit PAgP nebo LACP pomocí protokolu DTP, protože oba jsou protokoly, které se používají k automatizaci chování na trunk linkách. PAgP a LACP se používají pro agregaci linek. Služba DTP se používá k automatizaci vytváření linek. Když je nakonfigurován ethernetový kanál, obvykle je nakonfigurován EtherChannel (PAgP nebo LACP) a pak DTP.

Na obr. 1 jsou rozhraní F0/1 a F0/2 na přepínači S1 a S2 propojena s EtherChannelem. Výstup indikuje, že je EtherChannel vypnutý.

Na obrázku 2, podrobnější výstup naznačuje, že existují nekompatibilní režimy PAgP nakonfigurované na S1 a S2.

Poznámka: EtherChannel a STP musí spolupracovat. Z tohoto důvodu je důležité, aby byly zadány příkazy týkající se EtherChannelu, což je důvod, proč vidíte (na obrázku 3), že rozhraní Port-Channel 1 bylo odstraněno a znovu přidáno s příkazem *channel group*.

10.4 Shrnutí

10.4.1 Shrnutí

10.4.1.1 Shrnutí

EtherChannel shromažďuje více propojených linek dohromady, čímž vyvažuje zátěž nad nadbytečnými cestami mezi dvěma zařízeními. Všechny porty v jednom EtherChannelu

musí mít stejnou rychlost, duplexní nastavení a informace o VLAN na všech rozhraních zařízení, na obou koncích. Nastavení nakonfigurovaná v konfiguračním režimu rozhraní kanálu portu budou rovněž aplikována na jednotlivé rozhraní v tomto EtherChannel. Nastavení nakonfigurovaná na jednotlivých rozhraních se nepoužijí na EtherChannel nebo na další rozhraní v něm.

PAgP je protokol společností Cisco, který pomáhá při automatické tvorbě linek EtherChannel. Režimy PAgP jsou Zapnutý, PAgP žádoucí a PAgP auto. LACP je součástí specifikace IEEE, která také umožňuje připojit více fyzických portů do jednoho logického kanálu. Režimy LACP jsou Zapnutý, LACP aktivní a LACP pasivní. PAgP a LACP nekomunikují. Režim zapnutí se opakuje jak v PAgP, tak v LACP, neboť vytváří EtherChannel bezpodmínečně bez použití PAgP nebo LACP.

11 KAPITOLA 4 – BEZDRÁTOVÉ LOKÁLNÍ SÍTĚ

11.1 Úvod

11.1.1 Úvod

11.1.1.1 Úvod

Bezdrátové sítě mohou poskytnout mobilitu klientů, možnost připojení z libovolného místa a kdykoliv a možnost roamingu během připojení. Bezdrátová síť LAN (WLAN) je klasifikace bezdrátové sítě, která se běžně používá v prostředí domů, kanceláří a školního areálu. Přestože využívá radiové frekvence namísto kabelů, je běžně implementován v prostředí komutované sítě a jeho formát rámce je podobný jako u ethernetu.

Tato kapitola popisuje technologii WLAN, komponenty, zabezpečení, plánování, implementaci a odstraňování problémů. Jsou diskutovány taky, typy síťových útoků, na které jsou bezdrátové sítě obzvláště náchylné.

11.2 Bezdrátové koncepty

11.2.1 Úvod k bezdrátovým technologiím

11.2.1.1 Podpora mobility

Dnešní obchodní sítě se vyvíjejí, aby podporovaly lidi, kteří jsou v pohybu. Lidé jsou připojeni pomocí více zařízení, včetně počítačů, notebooků a chytrých telefonů. Jedná se o vizi mobility, kde si lidé mohou mezi sebou spojit své zařízení na cestě.

Existuje mnoho různých infrastruktur (kabelové sítě LAN, sítě poskytovatelů služeb), které umožňují tento typ mobility, avšak v podnikovém prostředí je nejdůležitější bezdrátová síť LAN (WLAN).

Produktivita již není omezena na pevné pracovní místo nebo definované časové období. Lidé nyní očekávají, že budou kdekoli a kdykoli propojeni, od kanceláře až po letiště nebo doma. Cestující zaměstnanci byli omezováni na placení telefonů pro kontrolu zpráv a návrat několika telefonních hovorů mezi lety. Zaměstnanci nyní mohou kontrolovat e-maily, hlasovou poštu a stav projektů na chytrých telefonech, pořád.

Uživatelé nyní očekávají, že budou moci rolovat bezdrátově. Roaming umožňuje bezdrátovému zařízení udržovat přístup k internetu bez ztráty spojení.

Prohlédněte si video na obrázku a vysvětlete, jak bezdrátové sítě umožňují mobilitu.

11.2.1.2 Bezdrátové výhody

Existuje mnoho výhod pro podporu bezdrátových sítí jak v podnikovém prostředí, tak doma. Mezi výhody patří zvýšená flexibilita, zvýšená produktivita, snížené náklady, schopnost růstu a přizpůsobení měnícím se požadavkům.

Obrázek 1 poskytuje příklady bezdrátové flexibility pro mobilního zaměstnance.

Většina firem se spoléhá na LAN založené na přepínačích pro každodenní provoz v kanceláři. Zaměstnanci se však stávají mobilnějšími a chtějí udržovat přístup ke svým podnikovým prostředkům LAN z jiných míst, než jsou jejich kanceláře. Pracovníci si chtějí vzít bezdrátová zařízení na schůzky, do kanceláře spolupracovníků, do konferenční místnosti a dokonce i zákaznické weby, a to při zachování přístupu ke všem kancelářským prostředkům. Bezdrátová síť poskytuje tento typ flexibility. Namísto toho, aby vynaložili značné množství času na přepravu potřebného firemního materiálu nebo na lokalizaci kabelových připojení pro přístup k síťovým zdrojům pomocí bezdrátové sítě, mohou být zdroje LAN snadno dostupné pro různé druhy bezdrátových zařízení.

Ačkoli je to těžké měřit, bezdrátový přístup může mít za následek vyšší produktivitu a uvolněnější zaměstnance. Díky bezdrátové síti mají zaměstnanci možnost pracovat, pokud chtějí, kde chtějí. Mohou reagovat na dotazy zákazníků, ať už v kanceláři, nebo na večeři. Mohou rychle a jednoduše přistupovat k e-mailům a jiným pracovním zdrojům, poskytovat lepší správu, lepší a rychlejší výsledky pro zákazníky a zvyšovat zisky.

Bezdrátové sítě mohou také snížit náklady. V podnicích s bezdrátovou infrastrukturou, která je již zavedena, se uskutečňuje úspora, kdykoli jsou požadovány změny zařízení nebo pohyby, jako například při přemístění zaměstnance v rámci budovy nebo při reorganizaci zařízení nebo laboratoře nebo při přechodu na dočasná místa nebo místa projektu.

Dalším důležitým přínosem bezdrátové sítě je schopnost přizpůsobit se měnícím se potřebám a technologiím. Přidání nového zařízení do sítě je bezproblémové díky bezdrátové síti. Zvažte bezdrátové připojení doma. Uživatelé mohou surfovat po internetu z kuchyňského stolu, obývacích pokojů nebo dokonce venku. Domácí uživatelé připojují nová zařízení, například chytré telefony a inteligentní podložky, notebooky a inteligentní televizory.

Jak je znázorněno na obrázku 2, bezdrátový domácí směrovač umožňuje uživateli připojit se k němu bez dodatečných nákladů nebo nepříjemností při spouštění kabelů na různá místa v domě.

11.2.1.3 Bezdrátové technologie

Bezdrátová komunikace se používá v řadě profesí.

Ačkoli se mix bezdrátových technologií neustále rozšiřuje, zaměřuje se tato diskuse na bezdrátové sítě, které uživatelům umožňují být mobilní. Bezdrátové sítě lze klasifikovat jako:

- Bezdrátové osobní sítě (WPAN) - pracují v rozsahu několika stop. Ve WPAN se používají zařízení Bluetooth nebo Wi-Fi s přímým připojením.
- Bezdrátové sítě LAN (WLAN) - fungují v rozmezí několika set metrů, například v místnosti, v domě, v kanceláři a dokonce i v prostředí kampusu.
- Bezdrátová širokopásmová síť (WWAN) - funguje v rozsahu km, jako je metropolitní oblast, buněčná hierarchie nebo dokonce na meziměstských linkách přes mikrovlnná relé.

Klepněte na každou součást na obrázku a zobrazte další informace o různých bezdrátových technologiích, které jsou k dispozici pro připojení zařízení k těmto bezdrátovým sítím:

- **Bluetooth** - původně WPAN standard IEEE 802.15, který používá proces párování zařízení pro komunikaci na vzdálenost až do 100 metrů. Novější verze jsou standardizovány speciálním zájmovým sdružením (https://www.bluetooth.org/).
- **Wi-Fi (bezdrátová věrnost)** – WLAN standard IEEE 802.11, běžně nasazený, aby poskytl přístup k síti, domácím a firemním uživatelům a aby zahrnoval přenos dat, hlasu a videa na vzdálenost až 300 metrů.
- **WiMAX (celosvětová interoperabilita pro mikrovlnný přístup)** – WWAN standard IEEE 802.16, který poskytuje bezdrátový širokopásmový přístup až do vzdálenosti 30 mil. Je alternativou kabelového a DSL širokopásmového připojení. Mobilita byla přidána do sítě WiMAX v roce 2005 a nyní ji mohou využít poskytovatelé služeb k poskytování celulárního širokopásmového připojení.
- **Mobilní širokopásmové připojení** - skládá se z různých firemních, vnitrostátních a mezinárodních organizací, které využívají mobilní přístup k poskytovatelům mobilních širokopásmových sítí. Nejprve k dispozici v mobilních telefonech druhé generace v roce 1991 (2G) s vyššími rychlostmi dostupnými v letech 2001 a 2006 jako součást třetí (3G) a čtvrté (4G) generace mobilní komunikační technologie.

- **Satelitní širokopásmové připojení** - poskytuje přístup k síti na vzdálená místa pomocí směrovací satelitní paraboly, která je propojena se specifickým geostacionárním oběžným satelitem GEO. Obvykle je dražší a vyžaduje jasný výhled.

Existuje mnoho typů bezdrátových technologií. Zaměření této kapitoly je však na sítě WLAN 802.11.

11.2.1.4 Rádiové frekvence

Všechna bezdrátová zařízení pracují v oblasti rádiových vln elektromagnetického spektra. Odpovídají se Mezinárodní telekomunikační unii - Radiokomunikačnímu sektoru (ITU-R) k regulaci přidělování spektra rádiových frekvencí (RF). Rozsahy frekvencí, nazývané pásma, jsou přidělovány pro různé účely. Některé pásma v elektromagnetickém spektru jsou silně regulovány a používají se pro aplikace, jako jsou řídicí systémy řízení letového provozu a komunikace v nouzových situacích. Jiné pásma jsou bez licence, jako jsou průmyslové, vědecké, lékařské (ISM) a nelicencovaná národní informační infrastruktura (UNII).

Poznámka: Sítě WLAN pracují ve frekvenčním pásmu ISM 2,4 GHz a v pásmu UNII 5 GHz.

Bezdrátová komunikace se vyskytuje v rozmezí radiových vln (tj. 3 Hz až 300 GHz) elektromagnetického spektra, jak je znázorněno na obrázku. Rozsah radiových vln je rozdělen na sekci rádiových frekvencí a sekci mikrovlnných frekvencí. Všimněte si, že WLAN, Bluetooth, celulární a satelitní komunikace fungují v rozsahu mikrovlnných jednotek UHF, SHF a EHF.

Bezdrátová zařízení LAN mají vysílače a přijímače naladěné na specifické frekvence rozsahu rádiových vln. Konkrétně jsou bezdrátové sítě 802.11 přiděleny následující frekvenční pásma:

- 2,4 GHz (UHF) - 802.11b/g/n/ad
- 5 GHz (SHF) - 802.11a/n/ac/ad
- 60 GHz (EHF) - 802.11ad

11.2.1.5 Standardy 802.11

WLAN norma IEEE 802.11 definuje, jak se RF, v nevyužitých frekvenčních pásmech ISM používá pro fyzickou vrstvu a MAC podvrstvu bezdrátových spojení.

V průběhu let byly vytvořeny různé implementace standardu IEEE 802.11. Následující body zdůrazňují tyto standardy:

- **802.11** - Vydáno v roce 1997 a nyní zastaralé, jde o originální specifikaci WLAN, která pracuje v pásmu 2,4 GHz a nabízela rychlost až 2 Mb/s. Když byla vydána, bezdrátové sítě LAN pracovaly na rychlosti 10 Mb/s, takže nová bezdrátová technologie nebyla přijata z nadšením. Bezdrátová zařízení mají jednu anténu pro přenos a příjem bezdrátových signálů.
- **IEEE 802.11a** - Vydán v roce 1999, pracuje v méně přeplněném frekvenčním pásmu 5 GHz a nabízí rychlosti až 54 Mb/s. Vzhledem k tomu, že tento standard pracuje na vyšších frekvencích, má menší oblast pokrytí a je méně účinný při pronikání stavebními konstrukcemi. Bezdrátová zařízení mají jednu anténu pro přenos a příjem bezdrátových signálů. Zařízení pracující v rámci této normy, nejsou interoperabilní s normami 802.11b a 802.11g.
- **IEEE 802.11b** - Vydáno v roce 1999, pracuje ve frekvenčním pásmu 2,4 GHz a nabízí rychlosti až 11 Mb/s. Zařízení implementující tuto normu mají delší dosah a jsou schopnější pronikat do struktur budovy než zařízení založená na technologii 802.11a. Bezdrátová zařízení mají jednu anténu pro přenos a příjem bezdrátových signálů.
- **IEEE 802.11g** - Vydáno v roce 2003, pracuje ve frekvenčním pásmu 2,4 GHz a nabízí rychlosti až 54 Mb/s. Zařízení používající tuto normu, musí proto pracovat na stejné rádiové frekvenci a rozsahu 802.11b, ale s šířkou pásma 802.11a. Bezdrátová zařízení mají jednu anténu pro přenos a příjem bezdrátových signálů. Je zpětně kompatibilní s operačním systémem 802.11b. Při podpoře klienta 802.11b je však celková šířka pásma snížena.
- **IEEE 802.11n** - vydaný v roce 2009, pracuje ve frekvenčních pásmech 2,4 GHz a 5 GHz a je označován jako dvoupásmové zařízení. Typické rychlosti přenosu dat se pohybují od 150 Mb/s do 600 Mb/s, se vzdáleností dosahu do 70 m. K dosažení vyšších rychlostí však AP a bezdrátové klienty vyžadují více antén využívajících technologii MIMO (Multi-Input and Multi-Output). MIMO používá více antén jako vysílač i přijímač ke zlepšení komunikačního výkonu. Můžou být podporovány až čtyři antény. Standard 802.11n je zpětně kompatibilní ze zařízeními 802.11a/b/g. Podpora smíšeného prostředí však omezuje očekávané datové rychlosti.
- **IEEE 802.11ac** - vydáno v roce 2013, pracuje ve frekvenčním pásmu 5 GHz a poskytuje datové rychlosti v rozsahu od 450 Mb/s do 1,3 Gb/s. Používá technologii MIMO ke zlepšení komunikačního výkonu. Může být podporováno až osm antén.

Standard 802.11ac je zpětně kompatibilní ze zařízeními 802.11a/n. Podpora smíšeného prostředí však omezuje očekávané datové rychlosti.

- **IEEE 802.11ad** - je naplánován na vydání v roce 2014 a také známý jako WiGig, využívá třípásmové Wi-Fi řešení s výkonem 2,4 GHz, 5 GHz a 60 GHz, a nabízí teoretické rychlosti až 7 Gb/s. Pásmo 60 GHz však představuje technologii line-of-site. A proto nemůže pronikat stěnami. Při roamingu se zařízení přepne na nižší pásma 2,4 GHz a 5 GHz. Je zpětně kompatibilní se stávajícími zařízeními Wi-Fi. Podpora smíšeného prostředí však omezuje očekávané datové rychlosti.

Tento obrázek shrnuje každý standard 802.11.

11.2.1.6 Certifikace Wi-Fi

Normy zajišťují interoperabilitu zařízení vyráběných různými výrobci. Mezinárodně jsou, tři organizace, které ovlivňující standardy WLAN jsou:

- **ITU-R** - upravuje přidělování RF spektra a satelitních drah.
- **IEEE** - Určuje, jak je RF modulováno pro přenos informací. Udržuje standardy pro lokální a metropolitní sítě s normou IEEE 802 LAN / MAN. Dominantními standardy v řadě IEEE 802 jsou Ethernet 802.3 a WLAN 802.11. Ačkoli IEEE má specifikované standardy pro RF modulační zařízení, nestanovuje výrobní standardy. Proto interpretace standardů 802.11 různými dodavateli může způsobit problémy s interoperabilitou mezi jejich zařízeními.
- **Wi-Fi Alliance** - Wi-Fi Alliance® je globální, neziskové, průmyslové sdružení zabývající se podporou růstu a akceptace WLAN. Jedná se o sdružení dodavatelů, jehož cílem je zlepšit interoperabilitu produktů, které jsou založeny na standardu 802.11, tím, že osvědčí dodavatele za dodržování průmyslových norem a dodržování norem.

Wi-Fi Alliance certifikuje Wi-Fi a následující kompatibilitu produktů:

- Kompatibilní s IEEE 802.11a/b/g/n/ac/ad
- IEEE 802.11i je zabezpečené pomocí WPA2 ™ a protokolem EAP
- Wi-Fi Protected Setup (WPS) pro zjednodušení připojení zařízení
- Wi-Fi Direct umožňuje sdílení médií mezi zařízeními
- Wi-Fi Passpoint pro zjednodušení bezpečného připojení k síti Wi-Fi
- Wi-Fi Miracast umožňuje bezproblémové zobrazení videa mezi zařízeními

Poznámka: K dispozici jsou i další produkty z Wi-Fi certifikací, jako je WMM® (Wi-Fi Multimedia ™), Tunnel Direct Link Setup (TDLS) a WMM-Power Save.

Obrázek 1 zobrazuje loga Wi-Fi Alliance, která určují kompatibilitu specifických funkcí. Zařízení, která zobrazují konkrétní loga, podporují identifikovanou funkci. Zařízení může zobrazovat kombinaci těchto log.

Klepnutím na tlačítko Přehrát na obrázcích 2 až 4 zobrazíte videa funkcí Wi-Fi Direct, Wi-Fi Passpoint a Wi-Fi Miracast.

11.2.1.7 Porovnání WLAN s LAN

WLAN sdílejí podobný původ se sítěmi LAN. IEEE přijala 802 LAN/MAN portfolio standardů architektury počítačových sítí. Dvě dominantní pracovní skupiny jsou Ethernet 802.3 a WLAN 802.11. Existují však mezi nimi důležité rozdíly.

WLAN používají RF místo kabelů na fyzické vrstvě a podsložku MAC vrstvy datového spojení. Ve srovnání s kabelem má RF následující vlastnosti:

- RF nemá hranice, jako jsou hranice drátu v plášti. To umožňuje datovým rámcům, které cestují přes RF médium, být k dispozici každému, kdo může přijímat signál.
- RF není chráněno před vnějšími signály, zatímco kabel je v izolačním plášti. Vysílače, které pracují nezávisle ve stejné zeměpisné oblasti, ale používají stejný nebo podobný RF, se mohou navzájem rušit.
- Rádiový přenos podléhá stejným výzvám, které jsou součástí jakékoliv vlnové technologie, jako je například spotřební rádio. Například pokud rádio cestuje dále od zdroje, rozhlasové stanice mohou začít hrát nad sebou a zvyšuje se statický šum. Signál je nakonec zcela ztracen. Kabelové sítě LAN mají kabely vhodné délky pro zachování síly signálu.
- RF pásma jsou v různých zemích regulovány různě. Používání WLAN sítí, podléhá dodatečným standardním předpisům a souborům, které se nepoužívají pro kabelové sítě LAN.

WLAN se také liší od kabelových sítí LAN takto:

- WLAN připojují klienty k síti prostřednictvím bezdrátového přístupového bodu (AP) nebo bezdrátového směrovače namísto přepínače.
- WLAN připojují mobilní zařízení, která jsou často napájena z baterie, na rozdíl od zařízení s připojením LAN. Bezdrátové NIC mají tendenci snižovat životnost baterie mobilního zařízení.

- WLAN podporují hostitele, kteří požadují přístup na RF médium. 802.11 předepisuje předcházení kolizím (CSMA/CA) namísto detekce kolize (CSMA/CD) pro přístup k médiím, aby se aktivně zabránilo kolizím v médiích.
- WLAN používají jiný formát rámce než kabelové sítě LAN. WLAN vyžadují další informace v hlavičce rámce 2. vrstvy.
- WLAN vyvolávají další problémy s ochranou soukromí, protože rádiové frekvence se mohou dostat mimo zařízení.

11.2.2 WLAN komponenty

11.2.2.1 Bezdrátové NIC (síťové karty)

Nejjednodušší bezdrátová síť vyžaduje minimálně dvě zařízení. Každé zařízení musí mít rádiový vysílač a rádiový přijímač naladěný na stejné frekvence.

Nicméně většina bezdrátových aplikací vyžaduje:

- Koncové zařízení s bezdrátovými síťovými kartami
- Infrastrukturní zařízení, například bezdrátový směrovač nebo bezdrátový AP

Pro bezdrátovou komunikaci vyžadují koncové zařízení bezdrátovou NIC, která obsahuje rádiový vysílač/přijímač a požadovaný ovladač softwaru, aby byl funkční. Notebooky, tablety a chytré telefony nyní obsahují integrované bezdrátové síťové karty. Pokud však zařízení nemá integrovanou bezdrátovou síťovou kartu, lze použít bezdrátový adaptér USB.

Obrázek zobrazuje dva typy bezdrátových adaptérů. Ten vlevo je nainstalován v rozšiřujícím slotu počítače. Jeden vpravo je připojen k portu zařízení přes USB.

11.2.2.2 Bezdrátový domácí směrovač

Typ zařízení infrastruktury, ke kterému se koncová zařízení přidružují a ověřují, jsou založeny na velikosti a požadavcích sítě WLAN.

Například domácí uživatel typicky propojuje bezdrátová zařízení pomocí malého bezdrátového směrovače. Bezdrátový směrovač slouží jako:

- **Přístupový bod** - poskytuje bezdrátový přístup 802.11a/b/g/n/ac
- **Přepínač** - poskytuje čtyřportový, plně duplexní 10/100/1000 Ethernetový přepínač pro připojení kabelových zařízení
- **Směrovač** - poskytuje výchozí bránu pro připojení k jiným síťovým infrastrukturám

Jak je znázorněno na obrázku, bezdrátový směrovač je běžně implementován jako bezdrátové zařízení pro malé podniky nebo obytné budovy. Bezdrátový směrovač se připojí k modemu ISP DLS a inzeruje jeho služby odesláním signálů, obsahujících identifikátor SSID. Vnitřní zařízení bezdrátově objeví SSID identifikátor směrovače a pokusí se k němu připojit a ověřit přístup k Internetu.

Očekávané zatížení bezdrátového směrovače v tomto prostředí je natolik nízké, že by mělo být schopno spravovat poskytování WLAN, Ethernetu 802.3 a připojit se k poskytovateli internetových služeb. Většina bezdrátových směrovačů poskytuje také pokročilé funkce, jako je vysokorychlostní přístup, podpora živého vysíláni videa, adresování IPv6, QoS, konfigurační nástroje a porty USB pro připojení tiskáren nebo přenosných jednotek.

Navíc pro domácí uživatele, kteří chtějí rozšířit své síťové služby, mohou být implementovány bezdrátové i kabelové adaptéry Powerline. Díky těmto zařízením se zařízení může připojit přímo k síti prostřednictvím elektrických zásuvek, což je ideální pro živé vysílání HD videa a hraní online. Jsou snadno nastavitelné: jednoduše zapojte do zásuvky nebo napájení a zařízení připojte stisknutím tlačítka.

11.2.2.3 Bezdrátová řešení v podniku

Organizace poskytující bezdrátové připojení k jejich uživatelům vyžadují infrastrukturu WLAN, která poskytuje další možnosti připojení.

Poznámka: IEEE 802.11 označuje bezdrátový klient jako stanici. V této kapitole se pojem bezdrátový klient používá k popisu libovolného bezdrátového zařízení.

Síť malých firem zobrazená na obrázku 1 je Ethernetová LAN 802.3. Každý klient se připojí k přepínači pomocí síťového kabelu. Přepínač je místem, kde klienti získají přístup k síti. Všimněte si, že bezdrátový AP se také připojí k přepínači. V tomto příkladu lze použít bezdrátové síťové připojení Cisco WAP4410N nebo WAP131 AP.

Bezdrátoví klienti používají svou bezdrátovou síťovou kartu, aby objevili nedaleké AP, které inzerovaly svoje SSID. Klienti se pak pokusí přidružit a autentizovat s AP, jak je znázorněno na obrázku 2. Po ověření mají uživatelé bezdrátových sítí přístup k síťovým prostředkům.

Poznámka: Bezdrátové potřeby malé organizace se liší od potřeby velké organizace. Velká bezdrátová nasazení vyžadují další hardware, který zjednoduší instalaci a správu sítě.

11.2.2.4 Bezdrátový Přístupový Bod (AP)

Rozhraní AP lze kategorizovat buď jako autonomní přístupové body nebo jako přístupové body založené na řadičích.

Autonomní AP

Autonomní AP, jsou samostatná zařízení, konfigurovaná pomocí Cisco CLI nebo GUI. Jsou užitečné v situacích, kdy je v síti vyžadováno pouze několik AP. Volitelně lze více AP kontrolovat pomocí bezdrátových doménových služeb (WDS) a spravovat pomocí Wireless LAN Solution Engine (WLSE).

Poznámka: Domácí směrovač je příklad autonomního AP, protože na zařízení je umístěna celá konfigurace AP.

Obrázek 1 zobrazuje autonomní AP v malé síti. Pokud se požadavky na bezdrátové připojení zvýší, bude vyžadováno více AP. Každá AP by fungoval nezávisle na ostatních a vyžadoval by ruční konfiguraci a správu.

AP založeny na řídicích jednotkách

Zařízení založená na řadičích jsou závislá na serveru a nevyžadují počáteční konfiguraci. Cisco nabízí dvě řešení. Rozhraní AP založené na řadičích jsou užitečné v situacích, kdy je v síti vyžadováno mnoho AP. Protože jsou přidány další, každý AP je automaticky konfigurován a spravován řídícím zařízením WLAN.

Obrázek 2 zobrazuje řídící AP v malé síti. Všimněte si, jak je nyní vyžadován řadič WLAN pro správu přístupových bodů. Výhodou správce je, že může být použit pro správu mnoha AP.

Poznámka: Některé modely AP mohou pracovat buď v autonomním režimu, nebo v režimu založeném na řadičích.

11.2.2.5 Řešení malých bezdrátových nasazení

Pro řešení malých požadavků na bezdrátové nasazení, společnost Cisco nabízí tato bezdrátová autonomní AP:

- **Cisco WAP4410N** - Tento AP je ideální pro malé organizace, které vyžadují dva přístupové body a podporují malou skupinu uživatelů.

- **Cisco WAP121 a WAP321** - Tyto AP jsou ideální pro malé organizace, které chtějí zjednodušit bezdrátové rozvinutí pomocí několika přístupových bodů.
- **Cisco AP541N** - Tento AP je ideální pro malé a střední organizace, které chtějí robustní a snadno ovladatelný shluk přístupových bodů.

Poznámka: Většina přístupových bodů na podnikové úrovni podporuje dokumenty o oprávnění PoE (Proof of Entitlement).

Obrázek 1 zobrazuje a shrnuje přístupové AP společnosti Cisco pro malé podniky

Obrázek 2 zobrazuje vzorovou topologii pro síť malých firem pomocí přístupových bodů WAP4410N. Každý AP je nakonfigurován a spravován individuálně. To může být problém, když je vyžadováno několik AP.

Z tohoto důvodu podporují WAP121, WAP321 a AP541N sdružování AP bez použití řadiče. Shluk poskytuje jediný administrační bod a umožňuje administrátorovi zobrazovat nasazení AP jako jednu bezdrátovou síť, spíše než řadu samostatných zařízení. Funkce shlukování usnadňuje nastavení, konfiguraci a správu rostoucí bezdrátové sítě. Může být nasazeno více přístupových bodů a posunout jednotnou konfiguraci ke všem zařízením v rámci clusteru a spravovat bezdrátovou síť jako jediný systém, aniž byste se obávali rušení mezi AP, bez nakonfigurování každého AP, jako samostatného zařízení.

Konkrétně WAP121 a WAP321 podporují jednoúčelové nastavení (SPS), což usnadňuje a zrychluje nasazení AP, jak je znázorněno na obrázku 3. SPS pomáhá umožnit bezdrátové síti LAN škálovat až na čtyři WAP121 a až osm zařízení WAP321, které poskytují širší pokrytí a podporu dalších uživatelů. Protože obchodní potřeby se mění a rostou. Rozhraní Cisco AP541N může spojit dohromady až 10 AP a může podporovat několik clusterů.

Cluster může být vytvořen mezi dvěma AP, pokud jsou splněny následující podmínky:

- Režim shlukování je povolen.
- AP, které se připojují ke clusteru, mají stejné jméno clusteru.
- AP jsou připojeny na stejném segmentu sítě.
- AP používají stejný režim rádia (to znamená, že obě radiostanice používají 802.11n).

11.2.2.6 Řešení pro velká bezdrátová nasazení

Organizace, které vyžadují sdružování více AP, vyžadují robustnější a škálovatelnější řešení. V případě větších organizací s řadou přístupových bodů poskytuje Cisco, řídící řešení založená na řídících jednotkách, včetně architektury Cisco Meraki Cloud Managed Architecture a architektury Cisco Unified Wireless Network Architecture.

Poznámka: Existují i další řešení založená na řadičích, jako jsou řídící jednotky používající režim Flex. Další informace naleznete na adrese http://www.cisco.com.

Cisco Meraki Cloud Managed Architecture

Je architektura řešení pro správu, která slouží k zjednodušení bezdrátového nasazení. Pomocí této architektury jsou AP spravovány centrálně z řadiče v cloudu, jak je znázorněno na obrázku 1. Cloudová síť a správa poskytují centralizovanou správu, viditelnost a ovládání bez nákladů a složitosti řídicích zařízení nebo softwaru pro správu překrývání.

Tento proces snižuje náklady a složitost. Ovladač nastavuje nastavení správy, jako jsou aktualizace firmwaru, nastavení zabezpečení, bezdrátová síť a nastavení SSID.

Poznámka: Pouze data správy procházejí infrastrukturou Meraki. Žádný provoz od uživatele nepřechází datová centra Meraki. Pokud tedy společnost Cisco Meraki nemůže přistupovat ke cloudu, síť bude nadále fungovat normálně. To znamená, že uživatelé se mohou stále ověřovat, pravidla brány firewall zůstávají na místě a dopravní toky jsou plné. Jsou přerušeny pouze funkce správy, například reporty a konfigurační nástroje.

Cisco Meraki Cloudová architektura vyžaduje následující:

- **Cisco MR Cloud správa bezdrátového AP**- k řešení široké škály bezdrátového nasazení existují různé modely.
- **Meraki Cloud Controller (MCC)** - MCC poskytuje centralizovanou správu, optimalizaci a monitorování systému WLAN. MCC není zařízení, které je nutné zakoupit a nainstalovat pro správu bezdrátových přístupových bodů. Služba MCC je spíše služba založená na cloudových sítích, která neustále sleduje, optimalizuje a hlásí chování sítě.
- **Panel založený na webu** - webový panel provádí konfiguraci a diagnostiku na dálku.

11.2.2.7 Řešení pro velká bezdrátová nasazení

Architektura Cisco Unified Wireless Network

Řešení architektury bezdrátové sítě Cisco Unified, které používá návrh rozdělených MAC, řídí AP pomocí řadiče WLAN (WLC) a lze jej volitelně spravovat pomocí bezdrátových řídicích systémů (WCS) společnosti Cisco. Lehké přístupové body komunikují s řadičem WLAN pomocí protokolu Lightworth Control Point Protocol (LWAPP). Řadič má veškerou inteligenci pro komunikaci a AP je "hloupý terminál", který jednoduše zpracovává pakety.

Architektura bezdrátové sítě Cisco Unified vyžaduje následující zařízení:

- **Lehké přístupové body** - modely bezdrátových přístupových bodů, Cisco Aironet 1600, 2600 nebo 3600 poskytují robustní a spolehlivý přístup k bezdrátové síti pro hostitele.
- **Řadiče pro malé a střední podniky** - bezdrátové ovladače řady Cisco 2500, virtuální bezdrátový řadič společnosti Cisco nebo modul Cisco Wireless Controller pro Cisco ISR G2 poskytují malou pobočkovou nebo jednopodlažní podnikovou implementaci WLAN se vstupní bezdrátovou datovou sítí.

K dispozici jsou také další ovladače WLAN s větší kapacitou. Například bezdrátový řadič Cisco 5760 a Cisco 8500 jsou navrženy tak, aby nákladově efektivně spravovaly, zabezpečovaly a optimalizovaly výkonnost značných bezdrátových sítí, jako je poskytovatel služeb a rozsáhlé nasazení v areálu.

Obrázek 1 shrnuje lehké AP.

Klepněte na každou součást na obrázku 2 a zobrazte další informace o ovladačích pro malé a střední podniky.

11.2.2.8 Bezdrátové antény

Většina přístupových bodů v podnikové třídě vyžaduje použití externích antén, aby se staly plně funkčními jednotkami. Společnost Cisco vyvinula antény, které jsou speciálně navrženy pro použití s 802.11, a zároveň vyhovují konkrétním podmínkám nasazení, včetně fyzického uspořádání, vzdálenosti a estetiky.

Cisco Aironet AP mohou používat:

- **Všesměrové Wi-Fi antény** - tovární Wi-Fi zařízení často používají základní dipólové antény, označované také jako "gumové kachny", které jsou podobné těm, které jsou používány na vysílačkách. Všesměrové antény poskytují pokrytí 360 stupňů a jsou ideální v otevřených kancelářských prostorách, chodbách, konferenčních místnostech a vnějších prostorech.

- **Směrové antény Wi-Fi** - směrové antény zaměřují rádiový signál v daném směru. To zvyšuje signál k a od AP ve směru, kterým směřuje anténa, poskytující silnější signál v jednom směru a menší intenzitu signálu ve všech ostatních.
- **Antény Yagi** - Typ směrové antény pro rozhlasové vysílání, která může být použita pro dálkové Wi-Fi sítě. Tyto antény se typicky používají k rozšíření rozsahu venkovních hotspotů v určitém směru nebo k dosažení venku budovy.

Na obrázku jsou zobrazeny různé vnitřní a venkovní antény Cisco.

Technologie MIMO IEEE v 802.11n/ac/ad, se používá ke zvýšení dostupné šířky pásma. Konkrétně MIMO používá více antén k výměně více dat, než by bylo možné udělat pomocí jedné antény. Až čtyři antény mohou být použity pro zvýšení výkonu.

Poznámka: Ne všechny bezdrátové směrovače jsou stejné. Například smřovače vstupní úrovně 802.11n podporují šířku pásma 150 Mb/s pomocí jednoho Wi-Fi rádia a jednou anténou připojenou k jednotce. Podpora vyšších přenosových rychlostí vyžaduje směrovač 802.11n, který vyžaduje více radiostanic a antén pro paralelní správu více kanálů dat. Například dvě radiostanice a dvě antény na směrovači 802.11n podporují až 300 Mb/s, zatímco 450 a 600 Mb/s se vyžadují tři až čtyři rádia a antény.

11.2.3 Topologie WLAN 802.11

11.2.3.1 Režimy bezdrátové 802.11 topologie

Bezdrátové sítě LAN mohou využívat různé síťové topologie. Standard 802.11 identifikuje dva hlavní režimy bezdrátové topologie:

- **Režim ad hoc** - Pokud se dvě zařízení bezdrátově připojují bez pomoci zařízení infrastruktury, například bezdrátového směrovače nebo AP. Mezi příklady patří Bluetooth a Wi-Fi Direct.
- **Režim infrastruktury** - Pokud se bezdrátově klienti propojí přes bezdrátový směrovač nebo AP, například v sítích WLAN. AP se připojují k síťové infrastruktuře pomocí kabelového distribučního systému (DS), jako je Ethernet.

Obrázek 1 zobrazuje příklad režimu ad hoc a na obr. 2 je uveden příklad režimu infrastruktury.

11.2.3.2 Režim Ad Hoc

Bezdrátová síť, je ad hoc, když dvě bezdrátová zařízení komunikují peer-to-peer bez použití AP nebo bezdrátových směrovačů. Klientská pracovní stanice s možností bezdrátového připojení může být například nakonfigurována tak, aby fungovala v režimu ad hoc, umožňující připojení jiného zařízení. Bluetooth a Wi-Fi Direct jsou příklady tohoto režimu.

Poznámka: Standard IEEE 802.11 označuje síť ad hoc jako nezávislou základní službu (IBSS).

Na obrázku je uveden souhrn režimu ad hoc.

Variantou topologie ad hoc je situace, kdy je pro vytvoření osobního hotspotu povolen, chytrý telefon nebo tablet s mobilním datovým přístupem. Tato funkce je někdy označována jako Tethering. Hotspot je obvykle dočasné rychlé řešení, které umožňuje inteligentnímu telefonu poskytovat bezdrátové služby. Jiná zařízení se mohou přidružit a ověřit pomocí inteligentního telefonu s připojením k Internetu. Apple iPhone odkazuje na to, jako na funkci Osobní Hotspot, zatímco zařízení Android to označuje buď jako Tethering nebo Přenosní Hotspot.

11.2.3.3 Režim infrastruktury

Architektura IEEE 802.11 se skládá z několika komponentů, které spolupracují a poskytují WLAN, která podporuje klienty. Definuje dvě stavební bloky topologie režimu infrastruktury: Základní servisní sada (BSS) a Rozšířená servisní sada (ESS).

Základní servisní sada - BSS

BSS se skládá z jediného AP, který propojuje všechny přidružené bezdrátové klienty. Na obrázku 1 jsou zobrazeny dvě BSS. Kruhy zobrazují oblast pokrytí, v níž mohou bezdrátoví klienti zůstat v komunikaci. Tato oblast se nazývá oblast základní služby (Basic Service Area - BSA). Pokud se bezdrátový klient přesune z BSA, již nemůže přímo komunikovat s jinými bezdrátovými klienty v rámci BSA. BSS je stavební blok topologie, zatímco BSA je skutečná oblast pokrytí.

MAC adresa 2. vrstvy se používá k jednoznačné identifikaci každé BSS, která se nazývá Identifikátor sady základních služeb (BSSID). Proto je BSSID formálním názvem BSS a vždy bude spojen pouze s jedním AP.

Rozšířená servisní sada

Když jediný BSS poskytuje nedostatečné pokrytí RF, dvě nebo více BSS můžou být spojeny, prostřednictvím společného distribučního systému (DS) do ESS. Jak je znázorněno na obrázku 2, ESS je spojení dvou nebo více BSS propojených kabelem DS. Bezdrátoví klienti v jednom BSA mohou nyní komunikovat s bezdrátovými klienty v jiném BSA, v rámci stejného systému ESS. Roamingové mobilní bezdrátoví klienti se mohou přesunout z jednoho BSA do jiného (v rámci stejného ESS) a bezproblémově se připojit.

Obdélníková oblast zobrazuje oblast pokrytí, ve které mohou členové ESS komunikovat. Tato oblast se nazývá rozšířená oblast služeb (ESA). ESA typicky zahrnuje několik BSS v překrývajících se nebo oddělených konfiguracích.

Každý systém ESS je identifikován identifikátorem SSID a v systému ESS je každý BSS identifikován jeho BSSID. Z bezpečnostních důvodů lze prostřednictvím ESS rozšířit další SSID a oddělit úroveň přístupu k síti.

11.3 Operace bezdrátové LAN

11.3.1 Struktura rámce 802.11

11.3.1.1 Bezdrátový rámec 802.11

Všechny rámce 2. vrstvy se skládají z části záhlaví, užitečného zatížení a FCS sekce, jak je znázorněno na obrázku 1. Formát rámce 802.11 je podobný formátu rámce Ethernet, s výjimkou, že obsahuje více polí.

Jak je znázorněno na obrázku 2, všechny bezdrátové rámce 802.11 obsahují následující pole:

- **Kontrola rámce** - Určuje typ bezdrátového rámce s obsahem podpolí, pro verzi protokolu, typ rámce, typ adresy, správu napájení a nastavení zabezpečení.
- **Doba trvání** - Obvykle se používá k označení zbývající doby potřebné k příjmu přenosu dalšího rámce.
- **Adresa1** - Obvykle obsahuje MAC adresu přijímajícího bezdrátového zařízení nebo AP.
- **Address2** - Obvykle obsahuje MAC adresu vysílajícího bezdrátového zařízení nebo AP.
- **Adresa3** - Někdy obsahuje MAC adresu cíle, například rozhraní směrovače (výchozí brána), ke které je připojen AP.

- **Kontrola sekvencí** - obsahuje podřízené číslo sekvence a podpoložky fragmentu. Sekvenční číslo udává pořadové číslo každého rámce. Číslo fragmentu udává číslo každého rámce odeslaného fragmentovaným rámcem.
- **Adresa4** - Obvykle chybí, protože se používá pouze v režimu ad hoc.
- **Užitné zatížení** - Obsahuje data pro přenos.
- **FCS** - sekvence kontroly rámce. Použita pro řízení chyb 2. vrstvy.

Obrázek 3 zobrazuje snímání Wireshark rámce signálu WLAN. Všimněte si, jak bylo pole Kontrola rámce také rozbaleno, pro zobrazení jeho podpolí.

Poznámka: Obsah polí Adresa se liší podle nastavení v poli Kontrola rámce.

11.3.1.2 Pole Kontroly Rámce

Pole Kontrola rámce, obsahuje několik podpolí, jak je znázorněno na obrázku 1.

Konkrétně obsahuje následující:

- **Verze protokolu** - poskytuje aktuální verzi použitého protokolu 802.11. Přijímací zařízení používají tuto hodnotu k určení, zda je podporována verze protokolu přijatého rámce.
- **Typ a podtyp rámce** - Určují funkci rámce. Bezdrátový rámec může být buď řídicí, datový nebo správce. Pro každý typ rámce existuje několik polí podtypů. Každý podtyp určuje konkrétní funkci, která se má provést pro příslušný typ rámce.
- **ToDS a FromDS** - Označují, zda se rámec objeví nebo vystupuje z DS a používá se pouze v datových rámcích bezdrátových klientů přidružených k AP.
- **Další fragmenty** - Určuje, zda mají následovat další fragmenty rámce, ať již data nebo typ správy.
- **Opakovat** - Označuje, zda je rámec pro datové nebo řídicí typy rámců opakovaně vysílán.
- **Správa napájení** - Označuje, zda je odesílající zařízení v aktivním režimu nebo režimu úspory energie.
- **Další data** - Ukazuje zařízení, které je v úsporném režimu, že AP má více rámců k odeslání. Používá se také pro přístupové body, které označují, že je třeba sledovat další vysílací rámce.
- **Zabezpečení** - Označuje, zda se v rámci používá šifrování a ověřování. Může být nastaveno pro všechny datové a řídicí rámce, které mají podtyp nastavený na ověření.

- **Rezervováno** - Může indikovat, že všechny přijaté datové rámce musí být zpracovány v pořadí.

Obrázek 2 zobrazuje snímání Wireshark rámce signálu WLAN. Všimněte si, že pole Typ rámce a pole Podtyp rámce určují, zda je rámec řídicí, správce nebo datový. V příkladu je Typ rámce '0x0', který se identifikuje jako rámec správy. Hodnota podtypu '8' označuje toto jako rámec signálu. Je speciálně označen jako "0x08".

11.3.1.3 Typ bezdrátového rámce

Poznámka: Pole Typ rámce a Podtyp rámce se používají k identifikaci typu bezdrátového přenosu. Jak je znázorněno na obrázku, bezdrátový rámec může být jeden ze tří typů:

- Rámec správy - slouží k udržování komunikace, jako je vyhledávání, ověřování a přidružení k AP.
- Kontrolní rámec - slouží k usnadnění výměny datových rámců mezi bezdrátovými klienty.
- Datový rámec - slouží k přenosu informací o užitečném zatížení, jako jsou webové stránky a soubory.

11.3.1.4 Rámce Správy

Rámce správy se používají výlučně k vyhledávání, ověřování a přiřazení k AP.

Obrázek 1 zobrazuje hodnotu polí běžných rámců správy, včetně:

- **Rámec žádosti o přidružení** - (0x00) Odeslaný z bezdrátového klienta umožňuje AP přidělit prostředky a synchronizovat se. Rámec obsahuje informace o bezdrátovém připojení, včetně podporovaných datových rychlostí a SSID sítě, na bezdrátový klient, na který se chce přidružit. Pokud je požadavek přijat, AP rezervuje paměť a vytvoří ID sdružení pro toto zařízení.
- **Rámec odezvy asociace** - (0x01) Odeslaný z AP do bezdrátového klienta obsahujícího přijetí nebo odmítnutí žádosti o přidružení. Je-li to přijatelné, rámec obsahuje informace, jako je ID asociace a podporované přenosové rychlosti.
- **Rámec žádosti o opětovné přidružení** - (0x02) Zařízení odešle požadavek na opětovné přidružení, když klesne z rozsahu aktuálně přidruženého AP a najde další AP se silnějším signálem. Nový AP koordinuje předávání informací, které mohou být stále obsaženy ve vyrovnávací paměti předchozího AP.

- **Rámec odezvy na opětovné přidružení** - (0x03) Odeslaný z AP obsahující přijetí nebo odmítnutí do zařízení s rámci o žádost. Rámec obsahuje informace potřebné pro přidružení, jako je ID asociace a podporované přenosové rychlosti.
- **Rámec žádosti sondy** - (0x04) Odeslaný z bezdrátového klienta, když vyžaduje informace od jiného bezdrátového klienta.
- **Rámec odezvy sondy** - (0x05) Odeslané z informací o kapacitě obsahujících AP, jako jsou podporované přenosové rychlosti, po obdržení rámce požadavku sondy.
- **Signální rámec** - (0x08) Odeslán pravidelně od AP, aby oznámil svou přítomnost a poskytl SSID a další předem nastavené parametry.
- **Oddělovací rámec** - (0x0A) Odeslán ze zařízení, které chce ukončit připojení. Umožňuje AP vynechat přidělení paměti a odebrat zařízení z tabulky přidružení.
- **Autentifikační rámec** - (0x0B) Odesílající zařízení pošle ověřovací rámec AP obsahující jeho identitu.
- **Ne-autentifikační rámec** - (0x0C) Odeslán od bezdrátového klienta, který chce ukončit připojení z jiným bezdrátovým klientem.

Signály jsou jediným rámcem správy, který může AP pravidelně vysílat. Všechny ostatní snímací, ověřovací a přidružené rámce se používají pouze během procesu asociace.

Obrázek 2 zobrazuje ukázku snímání Wireshark rámce správy. Hodnoty v poli se mění, aby odrážely účel rámce.

Poznámka: Ukázaný příklad byl zachycen pomocí služby Wireshark. Wireshark však musí být speciálně konfigurován tak, aby zachytil přenos WLAN. Schopnost zaznamenávat provoz se liší mezi operačními systémy a může vyžadovat speciální bezdrátovou síťovou kartu.

11.3.1.5 Kontrolní rámce

Kontrolní rámce slouží ke správě výměny informací mezi bezdrátovým klientem a AP. Pomáhají předcházet kolizím na bezdrátovém médiu.

Na obrázku je zobrazena hodnota polí společných kontrolních rámců, včetně:

- **Rámec požadavku na zaslání (RTS)** - RTS a CTS rámce poskytují volitelné schéma snižování kolizí pro AP se skrytými bezdrátovými klienty. Bezdrátový klient odešle rámec RTS jako první krok ve dvoucestném podání ruky, který je požadován před odesláním datových rámců.
- **Rámec připraveno k odeslání (CTS)** - bezdrátový přístupový bod odpovídá na rámec RTS s rámcem CTS. Poskytuje oprávnění požadujícímu bezdrátovému klientovi

odeslat datový rámec. CTS přispívá ke správě řízení kolize tím, že obsahuje časovou hodnotu. Toto časové zpoždění minimalizuje šanci, že ostatní bezdrátoví klienti budou vysílat, když žádající klient předá zprávu.

- **Potvrzovací rámec (ACK)** - Po přijetí datového rámce pošle přijímající bezdrátový klient poštu ACK rámce odesílajícímu klientovi, pokud nejsou nalezeny žádné chyby. Pokud odesílající klient neobdrží rámce ACK během předem stanoveného časového období, odesílající klient obnoví rámec.

Kontrolní rámce jsou integrální součástí bezdrátového přenosu a hrají významnou roli v metodě tvrzení médií, používané bezdrátovým systémem, nazývaným "Carrier Sense Multiple Access with Collision Avoidance" (CSMA / CA).

11.3.2 Bezdrátové Operace

11.3.2.1 CSMA/CA

Připomeňme si, že metoda zpochybnění media je metoda, při které zařízení určují, jak a kdy přistupovat k médiu, když má být komunikace přesunuta přes síť. WLAN IEEE 802.11 používají MAC protokol CSMA/CA. Zatímco název je podobný rozhraní CSMA/CD, provozní koncept je zcela jiný.

Systémy Wi-Fi jsou polovodičové, sdílené mediální konfigurace. Proto mohou bezdrátoví klienti vysílat a přijímat na stejném rádiovém kanálu. To způsobuje problém, protože bezdrátový klient během posílání neslyší, což znemožňuje detekci kolize. K řešení tohoto problému vyvinula IEEE další mechanismus vyhýbání se kolizím nazvaný Distribuovaná koordinační funkce (DCF). Pomocí služby DCF bezdrátový klient vysílá pouze v případě, že je kanál jasný. Všechny přenosy jsou potvrzeny, proto pokud bezdrátový klient neobdrží potvrzení, předpokládá vznik kolize a opakuje přenos po náhodném čekacím intervalu.

Bezdrátoví klienti a přístupové body používají rámce RTS a CTS k usnadnění skutečného přenosu dat.

Jak je znázorněno na obrázku 1, když bezdrátový klient odešle data, nejprve donutí méduim zjistit, zda vysílají jiná zařízení. V opačném případě pošle RTS rámec do AP. Tento rámec se používá pro vyžádání vyhrazeného přístupu k RF, po určitou dobu. AP přijímá rámec, pokud je k dispozici, uděluje bezdrátovému klientovi přístup k RF, odesláním rámce CTS se stejnou dobou trvání. Všechna ostatní bezdrátová zařízení, která sledují rámec CTS, přenášejí médium na vysílací uzel pro přenos.

Rámec řízení CTS zahrnuje časové období, ve kterém může vysílací uzel vysílat. Jiní bezdrátoví klienti zadržují přenosy alespoň po stanovenou dobu trvání.

Obrázek 2 zobrazuje vývojový diagram popisující proces CSMA/CA.

11.3.2.2 Bezdrátoví klienti a Asociace Přístupového bodu

Aby bezdrátová zařízení mohla komunikovat po síti, musí se nejprve přiřadit k AP nebo bezdrátovému směrovači. Důležitou součástí procesu 802.11 je objevování sítě WLAN a následné připojení k ní.

Rámce správy používají bezdrátová zařízení k dokončení následujícího třífázového procesu:

- Objevit nový bezdrátový AP.
- Autentizovat se s AP.
- Spolupracovat s AP.

11.3.2.3 Asociační Parametry

Chcete-li se vzájemně přiřadit, musí se bezdrátový klient a AP dohodnout na konkrétních parametrech. Parametry musí být konfigurovány na AP a následně na klientovi, aby bylo možné tyto procesy vyjednávat. Mezi běžné konfigurační parametry bezdrátového připojení patří:

- **Režim sítě** - vztahuje se na standardy WLAN 802.11. AP a bezdrátové směrovače mohou pracovat ve smíšeném režimu, jak je znázorněno na obrázku 1, což znamená, že mohou současně používat více standardů.
- **SSID** - SSID je jedinečný identifikátor, který bezdrátové klienty používají k rozlišení mezi více bezdrátovými sítěmi ve stejném okolí. Je-li povoleno vysílání SSID, název SSID se klientovi zobrazí v seznamu dostupných bezdrátových sítí. V závislosti na konfiguraci sítě mohou některé AP v síti sdílet identifikátor SSID. Jména jsou obvykle dlouhá 2 až 32 znaků. Na obrázku 1 je SSID nakonfigurován jako Home-Net a je povoleno vysílání SSID.
- **Nastavení kanálů** - odkazuje na frekvenční pásma, které se používají k přenosu bezdrátových dat. Bezdrátové směrovače a přístupové body mohou zvolit nastavení kanálu nebo jej lze nastavit ručně, pokud dojde k rušení s jiným AP nebo bezdrátovým zařízením. Na obrázku 1 je kanál manuálně nastaven na 6, což je frekvence 2,437 GHz.

- **Bezpečnostní režim** - odkazuje na nastavení parametrů zabezpečení, například WEP, WPA nebo WPA2. Vždy povolte nejvyšší podporovanou úroveň zabezpečení. Pro domácí nebo malou kancelář byste použili službu Osobní WPA2, jak je znázorněno na obrázku 2.
- **Šifrování** - služba WPA2 vyžaduje, abyste zvolili šifrování. Použijte AES vždy, když je to možné.
- **Heslo** - vyžaduje se od bezdrátového klienta, aby se autentizoval do AP. Heslo se někdy nazývá bezpečnostním klíčem. Zabraňuje narušitelům a dalším nechtěným uživatelům přístup k bezdrátové síti.

11.3.2.4 Objevování přístupových bodů

Bezdrátová zařízení musí zjistit a připojit se k AP nebo bezdrátovému směrovači. Bezdrátoví klienti se připojují k AP pomocí procesu skenování (snímání). Tento proces může být:

- **Pasivní režim** - AP otevřeně inzeruje svou službu pravidelným odesíláním vysílacích signálních rámců obsahujících SSID, podporované standardy a nastavení zabezpečení. Primárním účelem signálu je umožnit bezdrátovým klientům zjistit, které sítě a přístupové body jsou k dispozici v dané oblasti, a tak jim umožňují zvolit, kterou síť a AP použít.
- **Aktivní režim** - klienti bezdrátové sítě musí znát název identifikátoru SSID. Bezdrátový klient zahájí proces vysíláním rámce požadavku sondy na více kanálů. Žádost sondy obsahuje název SSID a podporované standardy. Aktivní režim může být vyžadován, pokud je AP nebo bezdrátový směrovač nakonfigurován tak, aby nevyžadoval vysílací rámy.

Obrázek 1 ukazuje, jak pasivní režim pracuje s vysíláním AP rámce velmi tak často.

Obrázek 2 ukazuje, jak aktivní režim pracuje s bezdrátovým klientem vysílajícím požadavek sondy pro konkrétní SSID. AP s tímto identifikátorem SSID, reaguje na snímaný snímač.

Bezdrátový klient mohl také odeslat požadavek sondy bez názvu SSID, aby zjistil nedaleké sítě WLAN. AP, nakonfigurované pro vysílání rámců signálu, reagují na bezdrátový klient s odpovědí sondy a poskytují název SSID. Rozhraní AP s vypnutou funkcí SSID na vysílání nereagují.

11.3.2.5 Autentifikace

Standard 802.11 byl původně vyvinut se dvěma autentizačními mechanismy:

- **Otevřená autentizace** - zásadně NULL autentizace, kde bezdrátový klient říká "ověřte mě" a AP reaguje "ano". Otevřená autentizace poskytuje bezdrátové připojení k libovolnému bezdrátovému zařízení a měla by být použita pouze v situacích, kdy bezpečnost není důležitou záležitostí.
- **Autentizace sdíleného klíče** - Technika je založena na klíči, který je předem sdílen mezi klientem a AP.

Obrázek 1 poskytuje jednoduchý přehled procesu autentizace. Ve většině instalací ověřování sdíleného klíče je však tato výměna následující:

1. Bezdrátový klient vyšle do AP autentizační rámec.

2. AP reaguje na textovou výzvu klienta.

3. Klient šifruje zprávu pomocí sdíleného klíče a vrátí šifrovaný text zpět do AP.

4. AP pak dešifruje šifrovaný text pomocí sdíleného klíče.

5. Pokud se dešifrovaný text shoduje s výzvou, AP autentizuje klienta. Pokud zprávy neodpovídají, bezdrátový klient není ověřen a bezdrátový přístup je odepřen.

Po ověření bezdrátového klienta, AP přejde do fáze přidružení. Jak je znázorněno na obrázku 2, fáze přidružení dokončí nastavení a vytvoří datové spojení mezi bezdrátovým klientem a AP.

Jako součást této fáze:

- Bezdrátový klient předává rámec žádosti o přidružení, který obsahuje jeho MAC adresu.
- AP reaguje na přidruženou odpověď, která obsahuje BSSID přístupového bodu, což je MAC adresa.
- AP mapuje logický port známý jako identifikátor sdružení (AID) bezdrátovému klientovi. Podpora AID je ekvivalentní portu přepínače a umožňuje přepnutí infrastruktury sledovat rámce určené pro bezdrátové klienty, které mají být předány.

Po připojení bezdrátového klienta k AP je nyní možné provoz mezi klientem a AP.

11.3.3 Správa kanálů

11.3.3.1 Saturace frekvenčního kanálu

Jak bylo vysvětleno dříve, bezdrátové zařízení sítě LAN, mají vysílače a přijímače naladěné na specifické frekvence rádiových vln pro komunikaci. V obvyklé praxi, se frekvence přidělují jako rozsahy. Takové rozsahy jsou pak rozděleny na menší rozsahy nazývané kanály.

Je-li poptávka po konkrétním kanálu příliš vysoká, pravděpodobně se tento kanál přemění. Nasycení bezdrátového média zhoršuje kvalitu komunikace. V průběhu let byla vytvořena řada technik pro zlepšení bezdrátové komunikace a zmírnění saturace. Níže uvedené techniky zmírňují saturaci kanálů efektivnějším způsobem, pomocí kanálů:

- **Rozprostřené spektrum s přímou sekvencí (DSSS)** - DSSS je modulační technika s rozšířeným spektrem. Spektrum je navrženo tak, aby šířilo signál přes větší frekvenční pásmo, čímž je odolnější vůči rušení. Se službou DSSS se signál vynásobí "vytvořeným šumem" známým jako rozšiřující kód. Protože přijímač ví, o rozšiřujícím kódu a kdy byl přidán, může ho matematicky odstranit a znovu vytvořit původní signál. Ve skutečnosti to vytváří redundanci vysílaného signálu ve snaze zabránit ztrátě kvality bezdrátového média. Služba DSSS používá server 802.11b. Používají se také bezdrátové telefony pracující v pásmech 900 MHz, 2,4 GHz, 5,8 GHz, mobilních sítích CDMA a sítích GPS. (Obrázek 1)
- **Rozprostřené Spektrum Frekvenčních skoků (FHSS)** - FHSS také spoléhá na metody šíření spektra v komunikaci. Je to podobné jako DSSS, ale vysílá rádiové signály rychlým přepnutím nosného signálu, mezi mnoho frekvenčních kanálů. S FHSS musí být odesílatele a přijímače synchronizovány tak, aby "věděli", který kanál bude skákat. Tento proces přeskakování kanálů umožňuje efektivnější využití kanálů a snižuje jejich kongesci. Vysílače a 900 MHz bezdrátové telefony také používají FHSS a taky Bluetooth používá variantu FHSS. Používá se také v původním standardu 802.11. (Obrázek 2)
- **Ortogonální multiplex dělení frekvencí (OFDM)** - OFDM je podmnožina multiplex frekvenčního dělení, ve které jeden kanál využívá více sub-kanálů na sousedních frekvencích. Sub-kanály v systému OFDM jsou přesně vzájemně ortogonální a umožňují překrytí sub-kanálů bez interferencí. V důsledku toho systémy OFDM dokáží maximalizovat spektrální účinnost, aniž by způsobily rušení v sousedních kanálech. Ve skutečnosti to usnadňuje přijímací stanici "slyšet" signál. Vzhledem k

tomu, že OFDM používá sub-kanály, je využití kanálu velmi účinné. OFDM se používá řadou komunikačních systémů včetně 802.11a/g/n/ac. (Obrázek 3)

11.3.3.2 Výběr kanálů

Moduly IEEE 802.11b/g/n fungují na mikrovlnných frekvencích rádiového spektra. Normy IEEE 802.11b/g/n pracují v rozmezí 2,4 GHz až 2,5 GHz, zatímco standardy 802.11a/n/ac pracují v pásmu více než 5 GHz. Obrázek 1 ukazuje, který standard 802.11 pracuje v pásmech 2,4 GHz, 5 GHz a 60 GHz. Každé spektrum je rozděleno na kanály se středovou frekvencí a šířkou pásma, které jsou analogické způsobu rozdělení rozhlasových pásem.

Pásmo 2,4 GHz je rozděleno na více kanálů. Celková šířka pásma kombinovaného kanálu je 22 MHz, přičemž každý kanál je rozdělen po 5 MHz. Norma 802.11b identifikuje 11 kanálů pro Severní Ameriku. Šířka pásma 22 MHz, kombinovaná se 5 MHz rozdělením mezi frekvencemi, vede k překrývání mezi po sobě následujícími kanály, jak je znázorněno na obrázku 2.

Poznámka: V Evropě existuje 13 kanálů 802.11b.

Dochází k rušení, když nežádoucí signál překrývá kanál vyhrazený pro požadovaný signál, což způsobuje případné zkreslení. Řešením rušení je použití nepřekrývajících se kanálů. Konkrétně kanály 1, 6 a 11 nejsou kanály 802.11b, které se překrývají, jak je znázorněno na obrázku 3.

Nejlepším postupem pro sítě WLAN vyžadující více přístupových bodů je použití nepřekrývajících se kanálů. Pokud existují tři sousedící AP, použijte kanály 1, 6 a 11. Pokud jsou pouze dva, vyberte libovolné dva, které jsou od sebe vzdáleny pět kanálů, např. kanály 5 a 10. Většina přístupových bodů může automaticky vybrat kanál založený na použitých sousedních kanálech. Některé produkty nepřetržitě monitorují rádiový prostor a dynamicky upravují nastavení kanálu v reakcích na změny prostředí.

Protože podniková síť WLAN migruje do sítě 802.11n, mohou se využívat kanály ve větším, méně přeplněném pásmu 5 GHz, což snižuje "náhodné odmítnutí služby (DoS)". Například standard 802.11n používá OFDM a může podporovat tři nepřekrývající se kanály, jak je znázorněno na obrázku 4.

802.11n může také využívat propojení kanálu, které kombinuje dva kanály 20 MHz do jednoho kanálu 40 MHz, jak je znázorněno na obrázku 5. Spojení kanálů zvyšuje propustnost doručování dat, pomocí dvou kanálů najednou.

Většina moderních přístupových bodů může automaticky upravovat kanály tak, aby obcházely rušení.

Poznámka: IEEE 802.11ac používá OFDM s šířkami kanálů 80, 160 a 80 + 80.

11.3.3.3 Plánování zavádění WLAN

Zavedení sítě WLAN, která co nejlépe využívá zdroje a poskytuje nejlepší služby, může vyžadovat pečlivé plánování. WLAN se mohou pohybovat od poměrně jednoduchých instalací až po velmi komplexní a složité návrhy. Před zavedením bezdrátové sítě by měl být dobře zdokumentovaný plán.

Počet uživatelů, které WLAN může podporovat, není přímočarý výpočet. Počet uživatelů závisí na geografickém uspořádání zařízení, včetně počtu těles a zařízení, které se mohou vejít do prostoru, uživatelských datových rychlostí, použitím nepřekrývajících se kanálů více AP v ESS a nastavením výkonu přenosu.

Viz plán půdorysu na obrázku 1. Při plánování umístění AP, správce nemůže jednoduše kreslit kruhy oblasti pokrytí a dát je přes plán. Přibližná oblast kruhového pokrytí je důležitá, ale existují další doporučení:

- Pokud mají AP používat stávající kabeláže nebo pokud existují místa, kde nelze umístit AP, poznačte si tato místa na mapě.
- Umístěte AP nad překážky.
- Umístěte AP vertikálně v blízkosti stropu ve středu každé oblasti pokrytí, pokud je to možné.
- Umístěte AP do míst, kde se očekává, že uživatelé budou. Například konferenční místnosti jsou typicky lepší umístění pro AP než chodba.

Když byly tyto body vyřešeny, odhadněte očekávanou oblast pokrytí AP. Tato hodnota se liší v závislosti na standardu WLAN nebo mixu používaných norem, povaze zařízení, vysílacím výkonu, na který je AP nakonfigurován a podobně. Při plánování oblastí pokrytí vždy konzultujte specifikace použitých AP.

BSA představují oblast pokrytí poskytovanou jedním kanálem. ESS by měl mít 10 až 15 procentní překrytí mezi BSA. Při překrytí 15 procent mezi BSA, SSID s nepřekrývajícími se kanály (tj. Jedna buňka na kanálu 1 a druhá na kanálu 6) můžou vytvořit roamingové schopnosti.

Obrázek 2 uvádí ukázku toho, jak se BSA mohou překrývat.

Mezi další faktory patří průzkumy na místě, což je podrobná analýza umístění různých AP.

11.4 Bezpečnost bezdrátové LAN

11.4.1 Ohrožení WLAN

11.4.1.1 Bezdrátové zabezpečení

Potíže s udržováním bezpečné kabelové sítě, vzrůstají s bezdrátovou sítí. Bezpečnost by měla být prioritou pro každého, kdo používá nebo spravuje sítě.

WLAN je otevřena pro každého, kdo je v dosahu AP a má příslušné pověření, aby se k němu přidružil. Díky bezdrátovému rozhraní NIC a znalostem průlomových technik nemusí útočník fyzicky vstoupit na pracoviště, aby získal přístup k síti WLAN.

Obavy o bezpečnost jsou ještě významnější při řešení obchodních sítí, neboť živobytí podniku se opírá o ochranu svých informací. Přerušení zabezpečení může mít pro podnik významné dopady, zvláště pokud podnik udržuje finanční informace spojené se svými zákazníky. Bezdrátové sítě jsou stále více nasazovány v podnicích a v mnoha případech se vyvinuly z pohodlné, do kritické části sítě. Přestože sítě WLAN byly vždy cílem útoků, nyní jsou hlavním cílem.

Útoky mohou být generovány cizinci, nespokojenými zaměstnanci a dokonce i neúmyslně. Bezdrátové sítě jsou specificky náchylné k několika hrozbám, včetně:

- Bezdrátových útočníků
- Nepřátelských AP
- Zachycení dat
- DoS útoků

Na obrázku klikněte na každou hrozbu a získáte další informace.

Poznámka: Další hrozby, jako například MAC spoofing bezdrátového klienta, cracking a útoky na infrastrukturu sítě, jsou mimo rozsah této kapitoly.

11.4.1.2 Útoky DoS

Bezdrátové útoky DoS mohou být výsledkem:

- **Nesprávně nakonfigurované zařízení** - Chyby konfigurace mohou zakázat síť WLAN. Správce by například mohl neúmyslně změnit konfiguraci a zakázat síť, nebo by mohl útočník s oprávněními správce úmyslně zakázat síť WLAN.

- **Záškodný uživatel, který záměrně zasahuje do bezdrátové komunikace** - Jejich cílem je zcela zakázat bezdrátovou síť nebo až do místa, kde nebude přístup k žádnému legitimnímu zařízení.
- **Náhodné rušení** - WLAN pracují v nelicencovaném frekvenčním pásmu. Proto jsou všechny bezdrátové sítě, bez ohledu na bezpečnostní prvky, náchylné k rušení od jiných bezdrátových zařízení. Náhodná rušení mohou nastat například z mikrovlnné trouby, bezdrátových telefonů, dětských monitorů a dalších. Pásmo 2,4 GHz je náchylnější k rušení než pásmo 5 GHz.

Chcete-li minimalizovat riziko útoku DoS kvůli nesprávně nakonfigurovaným zařízením proti škodlivému útoku, zatvrďte všechna zařízení, nechte hesla bezpečná, vytvořte zálohy a zajistěte, aby byly všechny konfigurační změny zpracovány mimo provoz.

Náhodné rušení se vyskytuje pouze při zavádění jiného bezdrátového zařízení. Nejlepším řešením je monitorování sítě WLAN pro případné rušení a jejich řešení. Vzhledem k tomu, že pásmo 2,4 GHz je náchylnější k rušení, může být oblast 5 GHz použita v oblastech náchylných k rušení. Některá řešení umožňují přístupovým bodům automaticky upravit kanály a použít pásmo 5 GHz k vyrovnání rušení. Například některé řešení 802.11n/ac/ad se automaticky přizpůsobí proti rušení.

Obrázek ukazuje, jak může bezdrátový telefon nebo dokonce mikrovlnná trouba zasahovat do komunikace WLAN.

Technologie Cisco CleanAir, umožňuje zařízením identifikovat a lokalizovat zdroje rušení jiné než 802.11. Vytváří síť, která má schopnost automaticky přizpůsobit se změnám ve svém prostředí.

11.4.1.3 Rámce správy DoS Útoků

I když je nepravděpodobné, že zákeřný uživatel může úmyslně iniciovat útok DoS pomocí zařízení na rušení RF, které způsobují náhodné rušení. Je pravděpodobné, že se pokusí manipulovat s řídícími rámci, aby spotřebovali zdroje AP a udržovali kanály příliš zaneprázdněny, aby obsluhovali legitimní uživatelský provoz.

Rámce správy mohou být manipulovány za účelem vytvoření různých typů útoků DoS. Dva společné rámce správy útoku zahrnují:

- **Rozpoznávací útok** - ten nastane, když útočník pošle řadu "ne-asociovaných" příkazů všem bezdrátovým klientům v BSS. Tyto příkazy způsobují odpojení všech klientů. Po odpojení se bezdrátoví klienti okamžitě pokusí o opětovné přidružení, což

vytváří značný provoz. Útočník pokračuje v odesílání nesouvislých rámců a cyklus se opakuje.

- **CTS zaplavení** - k tomu dochází, když útočník využívá metody CSMA/CA, aby monopolizoval šířku pásma a odepřel všem ostatním bezdrátovým klientům přístup do AP. Aby to bylo možné, útočník opakovaně zaplavuje BSS s rámci Clear to Send (CTS) do falešného STA. Všichni ostatní klienti, kteří sdílejí RF médium, obdrží CTS a zadržují své přenosy, dokud útočník nepřestane vysílat rámce CTS.

Obrázek 1 zobrazuje, jak bezdrátový klient a AP obvykle používají protokol CSMA/CA pro přístup k médiu.

Obrázek 2 ukazuje, jak je zaplavení CTS vytvořeno útočníkem, který odesílá rámce CTS falešnému bezdrátovému klientovi. Všichni ostatní klienti musí nyní čekat zadaný čas v rámci CTS. Útočník však stále posílá CTS rámce, čímž ostatní klienti čekají po dobu neurčitou. Útočník nyní ovládá médium.

Poznámka: Jedná se pouze o jeden příklad útoku rámce správy. Existuje mnoho dalších.

Pro zmírnění těchto útoků společnost Cisco vyvinula řadu řešení, včetně funkce Cisco Management Frame Protection (MFP), která také poskytuje úplnou proaktivní ochranu proti spoofingu rámců a zařízení. Modul Cisco Adaptive Wireless IPS, přispívá k tomuto řešení, systémem včasného zjišťování, kde jsou shodné podpisy útoku.

Výbor IEEE 802.11 vydal také dvě normy, týkající se bezdrátové bezpečnosti. Standard 802.11i, který je založen na zařízení Cisco MFP, specifikuje bezpečnostní mechanismy pro bezdrátové sítě, zatímco standard ochrany 802.11w, řídí problém s manipulací s rámci správy.

11.4.1.4 Nepřátelské Přístupové Body

Nepřátelský AP je AP nebo bezdrátový směrovač, který byl buď:

- Připojen k podnikové síti bez výslovné autorizace a proti firemní politice. Každý, kdo má přístup do areálu, může instalovat (škodný nebo neškodný) levný bezdrátový směrovač, který může potenciálně povolit přístup k zabezpečeným síťovým zdrojům.
- Připojen nebo povolen útočníkem pro zachycení dat klientů, jako jsou MAC adresy klientů (bezdrátových i kabelových), nebo pro zachycení a maskování datových paketů, pro získání přístupu k síťovým zdrojům nebo pro spuštění útoku typu man-in-the-middle.

Další úvahou je, jak snadné je vytvořit hotspot osobní sítě. Například uživatel se zabezpečeným síťovým přístupem umožňuje autorizovanému hostiteli systému Windows stát se AP. Tímto způsobem může obejít bezpečnostní opatření a další neautorizovaná zařízení nyní mohou přistupovat k síťovým prostředkům, jako sdílené zařízení.

Aby se zabránilo instalaci nepřátelských přístupových bodů, organizace musí používat monitorovací software pro aktivní sledování rádiového spektra pro neoprávněné AP. Příklad vzorku Cisco Prime Infrastructure pro správu síťového softwaru, zobrazuje mapu RF určující umístění vetřelce s detekovanou MAC adresou.

Poznámka: Cisco Prime je software pro správu sítě, který pracuje s jiným softwarem pro správu, aby poskytovaly společný vzhled a centrální polohu všech informací o síti. To je obvykle nasazeno ve velkých organizacích.

11.4.1.5 Útok Man-in-the-Middle(MITM)

Jeden ze sofistikovanějších útoků, které může uživatel se zlými úmysly použít, se nazývá útok MITM. Existuje mnoho způsobů, jak ho vytvořit.

Populární bezdrátový útok MITM se nazývá útok "zlého dvojče AP", kde útočník zavádí nepřátelský AP a konfiguruje ho se stejným SSID jako legitimní AP. Umístění s bezplatným Wi-Fi, jako jsou letiště, kavárny a restaurace, jsou rozšířena pro tento typ útoku kvůli otevřené autentizaci.

Připojením bezdrátových klientů se zobrazí dva AP, které nabízejí bezdrátový přístup. Ti, kteří se nacházejí blízko AP, najdou silnější signál a s největší pravděpodobností se spojují se špatným dvojčem AP. Uživatelský provoz je nyní odeslán do AP, který zase zachycuje data a předává je do legitimního AP. Návrat návštěvnosti z legitimní AP je odeslán do AP, zachycen a potom postoupen nepřipravenému STA. Útočník může ukrást uživatelské heslo, osobní informace, získat přístup k síti a ohrozit uživatelský systém.

Například na obrázku 1 je škodlivý uživatel v kavárně Bob's Latte a chce zachytit provoz od nic nečekajících bezdrátových klientů. Útočník spouští software, který umožňuje, aby se jeho notebook stal zlým dvojčem AP se stejným SSID a kanálem jako legitimní bezdrátový směrovač.

Na obrázku 2 uživatel vidí dvě dostupná bezdrátová připojení, ale vybírá a přidružuje se k zlému dvojči AP. Útočník zachycuje uživatelská data a předává legitimní přístupový bod, který zase směruje provoz zpět na špatný AP. Zlé dvojče AP zachycuje zpáteční provoz a předává informace nic netušícímu uživateli.

Porážka útoku, jako je útok MITM, závisí na propracovanosti infrastruktury WLAN a ostražitosti při monitorování činnosti v síti. Proces začíná identifikací legálních zařízení v síti WLAN. K tomu musí být uživatelé ověřeni. Poté, co jsou známa všechna legitimní zařízení, může být síť monitorována pro abnormální zařízení nebo provoz.

Podnikové sítě WLAN, které používají nejmodernější zařízení WLAN, poskytují správcům nástroje, které společně fungují jako systém prevence narušení bezdrátového připojení (IPS). Mezi tyto nástroje patří skenery, které identifikují nepřátelské AP a sítě ad hoc. A řízení rádiových zdrojů (RRM), které monitorují RF pásmo kvůli aktivitě a zatížení AP. AP, který je obsazenější než obvykle, upozorňuje administrátora na možný neoprávněný provoz.

11.4.2 Zabezpečení WLAN

11.4.2.1 Přehled Bezdrátového zabezpečení

Zabezpečení se vždy týkalo Wi-Fi, protože hranice sítě se přesunula. Bezdrátové signály mohou procházet pevnými předměty, jako jsou stropy, podlahy, stěny, mimo domov nebo kancelářské prostory. Bez přísných bezpečnostních opatření by instalace WLAN mohla být ekvivalentní tomu, že by byly Ethernetové porty všude, i venku.

Aby se řešily hrozby, udržením bezdrátových vetřelců venku a ochranou dat, byly použity dva prvky včasného zabezpečení:

- **Maskování SSID** - AP a některé bezdrátové směrovače umožňují deaktivaci rámců signálu SSID. Bezdrátovým klientům musí ručně identifikovat SSID, pro připojení k síti.
- **Filtrování MAC adres** - Správce může ručně povolit nebo zakázat bezdrátový přístup klientům, na základě jejich hardwarové MAC adresy.

Ačkoli tyto dvě funkce by odradily většinu uživatelů, skutečnost spočívá v tom, že ani maskování SSID, ani filtrování MAC adres by odradilo odhodlaného vetřelce. SSID se snadno objevují, i když je AP nevydává a MAC adresy mohou být obelhány. Nejlepším způsobem, jak zabezpečit bezdrátovou síť, je použití ověřovacích a šifrovacích systémů, jak je znázorněno na obrázku 1.

Byly zavedeny dva typy autentizace s původním standardem 802.11:

- **Autentizace Otevřeného systému** - Kterýkoli bezdrátový klient by se měl snadno připojit a měl by být používán pouze v situacích, kdy bezpečnost není znepokojivá,

například v místech poskytujících volný přístup k internetu, jako jsou kavárny, hotely a ve vzdálených oblastech.

- **Autentizace Sdíleného klíče** - Poskytuje mechanismy jako WEP, WPA nebo WPA2 k ověřování a šifrování dat mezi bezdrátovým klientem a AP. Heslo však musí být předem sdíleno mezi oběma stranami, které se mají připojit.

Graf na obrázku 2 shrnuje různé typy ověřování.

11.4.2.2 Ověřování metodou Sdíleného klíče

Jak je znázorněno na obrázku 1, jsou k dispozici tři techniky sdílení klíčů:

- **WEP (Wired Equivalent Privacy)** - původní specifikace 802.11 navržená tak, aby poskytovala ochranu soukromí podobnou připojení k síti pomocí kabelového připojení. Data jsou zajištěna metodou šifrování RC4 se statickým klíčem. Klíč se však nikdy nezmění při výměně paketů, což usnadňuje nabouráni do sítě.
- **WPA (Wi-Fi Protected Access)** - standard Wi-Fi Alliance, který používá WEP, ale zajišťuje data s mnohem silnějším šifrovacím algoritmem TKIP (Temporal Key Integrity Protocol). TKIP mění klíč pro každý paket, čímž je mnohem obtížnější nabourání do sítě.
- **IEEE 802.11i/WPA2** - IEEE 802.11i je průmyslovým standardem pro zabezpečení bezdrátových sítí. Verze Wi-Fi Aliance se nazývá WPA2. 802.11i a WPA2, používají AES pro šifrování. AES je v současnosti považován za nejsilnější šifrovací protokol.

WEP již není doporučován. Jeho sdílené klíče se ukázaly jako chybné a proto by se nikdy neměl používat. Abychom čelili sdílené slabosti klíčů WEP, bylo prvním přístupem společností zkusit techniky, jako je maskování SSID a filtrování MAC adres. Tyto techniky se ukázaly jako příliš slabé.

V důsledku slabosti zabezpečení založeného na WEP došlo k dočasnému bezpečnostnímu opatření. Prodejci jako Cisco, kteří chtějí uspokojit požadavky na lepší bezpečnost, vyvinuli vlastní systémy a současně pomohli vyvíjet standard 802.11i. Na cestě k síti 802.11i byl vytvořen algoritmus šifrování TKIP, který byl propojen s bezpečnostní metodou WPA.

Moderní bezdrátové sítě by měly vždy používat standard 802.11i/WPA2. Je verze 802.11i a proto se výrazy WPA2 a 802.11i často používají zaměnitelně.

Od roku 2006 je každé zařízení, které nese logo certifikované Wi-Fi, certifikováno protokolem WPA2.

11.4.2.3 Metody šifrování

Šifrování se používá k ochraně dat. Pokud útočník zachytil zašifrované údaje, nebude schopen jej v libovolné rozumné době rozluštit.

IEEE normy 802.11i, WPA a WPA2 používají následující protokoly šifrování:

- **Protokol časové integrity klíčů (TKIP)** - TKIP je šifrovací metoda používaná službou WPA. Poskytuje podporu starším zařízením WLAN tím, že řeší původní nedostatky spojené se šifrováním WEP 802.11. Využívá WEP, ale šifruje užitečné zatížení 2. vrstvy pomocí TKIP a provádí kontrolu šifrování zpráv (MIC) v zašifrovaném paketu, aby nedošlo k poškození zprávy.
- **Advanced Encryption Standard (AES)** - metoda AES je šifrovací metoda používaná WPA2. Jedná se o preferovanou metodu, protože je v souladu s průmyslovým standardem IEEE 802.11i. AES provádí stejné funkce jako TKIP, ale je to mnohem silnější metoda šifrování. Používá režim Počítání znaků s protokolem CCMP, který umožňuje cílovým hostitelům rozpoznat, zda byly zablokovány šifrované a nešifrované bity.

Poznámka: Vždy zvolte WPA2 s AES, pokud je to možné.

11.4.2.4 Ověřování Domácího Uživatele

Obrázek zobrazuje volby režimu zabezpečení dostupné pro bezdrátový směrovač. Uvádí od nejslabšího (tj. Zakázáno) po nejsilnějšího (tj. WPA2 Personal nebo Enterprise).

WPA a WPA2 podporují dva typy ověřování:

- **Osobní (Personal)** - určené pro domácí nebo malé kancelářské sítě, uživatelé ověřují pomocí před-sdíleného klíče (PSK). Bezdrátoví klienti se autentizují pomocí AP pomocí předem sdíleného hesla. Není vyžadován žádný speciální server ověřování.
- **Podnikové (Enterprise)** - Určeno pro podnikové sítě, ale vyžaduje autentizační server RADIUS. Ačkoli je složitější ho nastavit, poskytuje další zabezpečení. Zařízení musí být ověřeno serverem RADIUS a uživatelé se musí ověřit pomocí standardu 802.1X, který používá ověřovací protokol EAP.

Přihlašovací proces 802.1X používá EAP pro komunikaci s AP a serverem RADIUS. EAP je rámec pro ověřování přístupu k síti. Může poskytnout bezpečný mechanismus autentizace a vyjednat bezpečný soukromý klíč, který pak může být použit pro bezdrátovou šifrovací relaci, využívající šifrování TKIP nebo AES.

11.4.2.5 Ověřování v Podniku

V sítích, které mají přísnější požadavky na zabezpečení, je vyžadováno další ověření nebo přihlášení k tomu, aby poskytli bezdrátovým klientům přístup. Volbou podnikového režimu zabezpečení, se vyžaduje ověřování, autorizace a účtování (AAA) serveru RADIUS.

Obrázek zobrazuje pole, která se zobrazují při výběru podnikové verze WPA nebo WPA2. Tato pole jsou potřebná k tomu, aby AP poskytla potřebné informace pro kontakt s AAA serverem:

- **IP Adresa serveru RADIUS** - to je dosažitelná adresa serveru RADIUS.
- **Čísla portů RADIUS** - oficiálně přiřazené porty UDP 1812 pro ověřování RADIUS a 1813 pro RADIUS účetnictví, ale mohly by fungovat i pomocí portů UDP 1645 a 1646, jak je znázorněno na obrázku
- **Sdílený klíč** - slouží k ověření AP pomocí serveru RADIUS.

Sdílený klíč není parametrem, který musí být nakonfigurován u bezdrátového klienta. Požaduje se pouze na AP, aby se ověřil pomocí serveru RADIUS.

Poznámka: Neexistuje žádné uvedené pole Heslo, protože skutečná autentizace a autorizace uživatele, je zpracována standardem 802.1X, který poskytuje centralizované ověřování koncových uživatelů založených na serveru.

11.5 Konfigurace Bezdrátové LAN

11.5.1 Konfigurace Bezdrátového Směrovače

11.5.1.1 Plánováni Implementace Bezdrátového Směrovače

Většina domácích bezdrátových směrovačů je připravena k obsluze z krabice. Nepotřebují žádnou další konfiguraci. Výchozí adresy IP, uživatelské jména a hesla bezdrátového směrovače však lze snadno najít na internetu. Jednoduše zadejte vyhledávací frázi "výchozí adresa IP bezdrátového směrovače" nebo "výchozí hesla bezdrátového směrovače" a podívejte se na seznam mnoha webů, které tyto informace poskytují. Proto by měla být vaší první prioritou, změna těchto výchozích hodnot z bezpečnostních důvodů.

Před instalací bezdrátového směrovače zvažte změnu následujících výchozích nastavení:

- **Připojení k Internetu** - Přiřazení IP adresy pro připojení k Internetu zpravidla nastavuje ISP prostřednictvím protokolu DHCP, jak je znázorněno na obrázku. V této kapitole staticky nastavíte tuto adresu v aktivitách.
- **Nastavení DHCP** - Bezdrátové směrovače jsou dodávány s protokolem DHCP, který je již konfigurován pro připojení WLAN a LAN. Je ovšem nejlepší praxí zabezpečení pro změnu výchozího nastavení DHCP. Tato nastavení jsou součástí nastavení sítě zobrazené na obrázku.
- **Název SSID** - Název sítě WLAN bude nastaven na výchozí název, který by měl být změněn.
- **Zabezpečení WLAN** - bezdrátové směrovače doma nebudou mít žádné šifrování ani bezpečnostní heslo. WLAN bude otevřena a dostupná pro připojení všech bezdrátových zařízení. WPA2 s šifrováním AES a silné heslo by mělo být nakonfigurováno.
- **Přístup ke správě** - Výchozí hesla pro přístup ke všem značkám bezdrátového směrovače jsou snadno dostupná na internetu. Proto by mělo být heslo změněno, aby se zabránilo neoprávněnému přístupu ke konfiguračnímu rozhraní bezdrátového směrovače.

11.5.1.2 Připojení Bezdrátového Směrovače k Internetu

Bezdrátový směrovač má několik portů pro připojení kabelových zařízení. Například bezdrátový směrovač na obrázku má port USB, internetový port a čtyři LAN porty. Port Internet je ethernetový port, který slouží k připojení směrovače k zařízením poskytovatele služeb, jako je například DSL nebo kabelový modem.

Topologie pro připojení zařízení je znázorněna na obrázku 2. Postupy pro připojení bezdrátového směrovače k portu širokopásmového modemu jsou následující:

Krok 1. Na směrovači připojte přímý ethernetový kabel k portu označenému jako **Internet**. Tento port může být také označen jako **WAN**. Přepínací logika zařízení předává všechny pakety přes tento port, pokud je komunikace do a z Internetu a dalších připojených počítačů.

Krok 2. V širokopásmovém modemu poskytovatele služeb připojte druhý konec kabelu k příslušnému portu. Typické štítky pro tento port jsou **Ethernet**, **Internet** nebo **WAN**.

Krok 3. Zapněte širokopásmový modem a zapojte napájecí kabel do směrovače. Poté, co modem vytvoří připojení k ISP, začne komunikovat se směrovačem. Indikátory směrovače na internetu se rozsvítí a signalizují komunikaci. Modem poskytne směrovači informace o

síti potřebné pro přístup k Internetu, včetně veřejné adresy IP adresy, masky podsítě a adresy serveru DNS.

11.5.1.3 Přihlášení do směrovače

Chcete-li získat přístup ke grafickému rozhraní konfigurace bezdrátového směrovače, otevřete webový prohlížeč. Do pole Adresa zadejte výchozí privátní IP adresu bezdrátového směrovače. Výchozí IP adresu naleznete v dokumentaci, která byla dodána s bezdrátovým směrovačem, nebo můžete vyhledávat na Internetu. Na obrázku je uvedena IP adresa 192.168.0.1, což je běžná výchozí hodnota pro některé výrobce. Bezpečnostní okno vyzve k povolení o přístup ke grafickému rozhraní směrovače. Slovo **admin** se běžně používá jako výchozí uživatelské jméno a heslo. Znovu zkontrolujte dokumentaci bezdrátového směrovače nebo vyhledávejte na Internetu.

11.5.1.4 Konfigurace IP adresace

V domácí nebo malé kancelářské síti byste normálně ponechali připojení k internetu nastaveno na automatické. V případě laboratoří a aktivit v této kapitole pak propojíte bezdrátový směrovač, buď do laboratorní sítě, nebo do simulované sítě. Internetová služba nebude povolena.

Na obrázku 1 je typ připojení nastaven na statickou IP. Adresovací parametry byly ručně nakonfigurovány. Na obrázku 2 bylo výchozí adresování DHCP změněno, aby se použila podsíť 10.10.10.0/24. Adresa DNS je nastavena na stejný server DNS, jak je znázorněno na obrázku 1.

Po uložení této konfigurace ztratíte připojení k bezdrátovému směrovači. Chcete-li obnovit přístup, obnovte nastavení IP. Potom do pole adresy webového prohlížeče zadejte IP adresu nového směrovače, 10.10.10.1.

11.5.1.5 Konfigurace Bezdrátového Nastavení

Po vytvoření připojení k směrovači, je dobré postupovat při konfiguraci některých základních nastavení pro zabezpečení bezdrátové sítě:

- **Režim sítě** - Některé bezdrátové směrovače umožňují vybrat, který standard 802.11 je třeba implementovat. Na obrázku 1 je zobrazena možnost "Mix". To znamená, že bezdrátová zařízení, která se připojují ke směrovači, mohou mít řadu bezdrátových NIC nainstalovaných včetně 802.11a, b, g a n.

- **Název sítě (SSID)** - Přiřaďte SSID k bezdrátové síti. Home-Net se používá na obrázku 1. Pokud je vysílání SSID zakázáno, musíte ručně zadat SSID na bezdrátových zařízeních.
- **Standardní kanál** - Standardy 802.11b a 802.11g běžně používají kanály 1, 6 a 11, aby se zabránilo rušení. Na obrázku 1 je kanál manuálně nastaven na 6.
- **Zabezpečení bezdrátového připojení** - konfigurujte nejsilnější režim zabezpečení, což je WPA2 se šifrováním AES, jak je znázorněno na obrázku 2.

11.5.1.6 Konfigurace Správy Přístupu

Přestože jsme změnili adresu správy, abychom přistupovali k směrovači na 10.10.10.1, je heslo stále nastaveno na výchozí. Pro bezdrátové směrovače Packet Tracer, změníte heslo správce na kartě Administration, jak je znázorněno na obrázku 1.

11.5.2 Konfigurace Bezdrátových Klientů

11.5.2.1 Připojování Bezdrátových Klientů

Je-li nakonfigurován AP nebo bezdrátový směrovač, vyzkoušejte bezdrátové připojení pomocí konfigurace bezdrátového klienta pro přístup k síti WLAN, jak je znázorněno na obrázku. Ověřte, zda je klient úspěšně připojen k správné bezdrátové síti, zejména proto, že je k dispozici mnoho sítí WLAN, se kterými se můžete připojit.

11.5.3 Řešení problémů WLAN

11.5.3.1 Přístupy k odstraňování problémů

Odstraňování jakéhokoli problému v síti by se mělo řídit systematickým přístupem. Logické síťové modely, jako jsou modely OSI a TCP/IP, rozdělují síťové funkce do modulárních vrstev.

Při odstraňování problémů mohou být tyto vrstvené modely aplikovány na fyzickou síť, aby se izolovaly problémy se sítí. Například pokud příznaky naznačují problém s fyzickým připojením, může se síťový technik zaměřit na řešení problémů s obvodem, který pracuje na fyzické vrstvě. Pokud tento okruh funguje správně, technik se podívá na oblasti v jiné vrstvě, které by mohly způsobit problém.

Pro vyřešení problémů se sítí se používají tři hlavní přístupy k řešení problémů:

- Zdola-nahoru - Začněte ve vrstvě 1 a pokračujte v práci. (Obrázek 1)
- Shora-dolů - Začněte v horní vrstvě a pracujte dolů. (Obrázek 2)
- Rozděl a panuj - Ping cílové destinace. Pokud pingy selhávají, ověřte spodní vrstvy. Pokud jsou pingy úspěšné, ověřte horní vrstvy. (Obrázek 3)

11.5.3.2 Bezdrátový Klient se Nepřipojí

Při odstraňování problémů se sítí WLAN je doporučen postup odstraňování.

Na obrázku není bezdrátový klient připojen k síti WLAN. Pokud není připojení, zkontrolujte následující:

- Potvrďte konfiguraci sítě v počítači pomocí příkazu ***ipconfig***. Ověřte, zda počítač obdržel adresu IP prostřednictvím protokolu DHCP nebo zda je nakonfigurován se statickou adresou IP.
- Zkontrolujte, zda se zařízení může připojit k drátové síti. Připojte zařízení k pevné síti LAN a odešlete ***ping*** na známou adresu IP.
- V případě potřeby znovu načtěte příslušné ovladače pro klienta. Možná bude nutné vyzkoušet jinou bezdrátovou síťovou kartu.
- Pokud pracuje bezdrátová síťová karta klienta, zkontrolujte nastavení zabezpečení a nastavení šifrování v klientovi. Pokud nastavení zabezpečení neodpovídají, klient nemůže získat přístup k síti WLAN.

Pokud je počítač v provozu, ale bezdrátové připojení funguje špatně, zkontrolujte následující:

- Jak daleko je PC od AP? Je počítač mimo plánovanou oblast pokrytí (BSA)?
- Zkontrolujte nastavení kanálu na bezdrátovém klientovi. Klientský software by měl detekovat příslušný kanál, pokud je SSID správný.
- Zkontrolujte přítomnost dalších zařízení v oblasti, která mohou zasahovat do pásma 2,4 GHz. Příklady jiných zařízení jsou bezdrátové telefony, dětské monitory, mikrovlnné trouby, bezdrátové bezpečnostní systémy a potenciálně nepřátelské AP. Data z těchto zařízení mohou způsobit narušení v síti WLAN a problémy s přerušovaným připojením mezi bezdrátovým klientem a AP.

Dále zkontrolujte, zda jsou všechna zařízení skutečně na svém místě. Zvažte možný problém s fyzickou bezpečností. Je napájení všech zařízení zapnuto?

Nakonec zkontrolujte propojení mezi kabelovými zařízeními, které hledají špatné konektory nebo poškozené nebo chybějící kabely. Pokud jsou fyzická zařízení na svém místě, ověřte kabelovou LAN pingem zařízeních, včetně AP. Pokud připojení stále selhává, možná se něco děje s AP nebo jeho konfigurací.

11.5.3.3 Řešení Problémů Když je Síť Pomalá

K optimalizaci a zvýšení šířky pásma směrovačů dvou pásem 802.11n/ac, je potřeba buď:

- **Upgrade bezdrátových klientů** - starší zařízení 802.11b a dokonce i zařízení 802.11g mohou zpomalit celou síť WLAN. Pro dosažení nejlepšího výkonu by všechna bezdrátová zařízení měla podporovat stejnou nejvyšší přijatelnou úroveň.
- **Rozdělení provozu** - Nejjednodušší způsob, jak zvýšit výkon bezdrátového připojení, je rozdělení bezdrátové komunikace mezi pásma 2,4 GHz a 5 GHz. Proto může 802.11n (nebo lepší) používat tyto dvě pásma jako dvě samostatné bezdrátové sítě, které vám pomohou spravovat provoz. Existuje několik důvodů pro použití přístupu založeného na rozdělení provozu:
- Pásmo 2,4 GHz může být vhodné pro základní internetovou komunikaci, která není časově citlivá.
- Šířka pásma může být stále sdílena s ostatními pobočkami sítě WLAN.
- Pásmo 5 GHz je mnohem méně přeplněné než pásmo 2,4 GHz. Ideální pro stream multimédií.
- Pásmo 5 GHz má více kanálů. Proto je zvolený kanál pravděpodobně bez rušení.

Ve výchozím nastavení používají směrovače s dvojím pásmem stejný název sítě jak v pásmu 2,4 GHz, tak v pásmu 5 GHz. Nejjednodušší způsob, jak segmentovat provoz, je přejmenování jedné z bezdrátových sítí. Se samostatným popisným názvem je snadnější se připojit ke správné síti.

Chcete-li zlepšit dosah bezdrátové sítě, zajistěte, aby fyzické umístění bezdrátového směrovače neobsahovalo žádné překážky, například nábytek, příslušenství a vysoké spotřebiče. Blokují signál, který zkracuje rozsah sítě WLAN. Pokud se problém stále nevyřeší, může být použito zařízení Wi-Fi Range Extender nebo nasazení bezdrátové technologie Powerline.

11.5.3.4 Update firmwaru

Většina bezdrátových směrovačů nabízí aktualizovatelný firmware. Verze mohou obsahovat opravy běžných problémů hlášených zákazníky, stejně jako bezpečnostní chyby zabez-

pečení. Pravidelně byste měli zkontrolovat webové stránky výrobce pro aktualizovaný firmware. Po stažení je možné pomocí grafického uživatelského rozhraní nahrát firmware do bezdrátového směrovače, jak je znázorněno na obrázku. Uživatelé budou odpojeni od sítě WLAN a Internetu až do dokončení inovace. Bezdrátový směrovač pravděpodobně bude muset několikrát restartovat, než se obnoví normální síťové operace.

11.6 Shrnutí

11.6.1 Shrnutí

11.6.1.1 Shrnutí

WLAN se často provádějí v prostředí domů, kanceláří a školního areálu. Pro 802.11 sítě WLAN se používají pouze frekvence 2,4 GHz, 5,0 GHz a 60 GHz. ITU-R upravuje přidělování RF spektra, zatímco IEEE poskytuje standardy 802.11, které určují, jak se tyto frekvence používají pro fyzickou a MAC podvrstvu bezdrátových sítí. Wi-Fi Aliance potvrzuje, že dodavatelské produkty odpovídají normám a normám v oboru.

Bezdrátový klient používá bezdrátovou síťovou kartu pro připojení k infrastrukturnímu zařízení, například bezdrátovému směrovači nebo bezdrátovému AP. Bezdrátoví klienti se připojují pomocí SSID. AP je možné implementovat jako samostatná zařízení, v malých clusterech nebo v rozsáhlejších řídicích sítích.

Cisco Aironet AP může používat všesměrové antény, směrovou anténu nebo anténu Yagi pro přímé signály. Technologie MIMO IEEE 802.11n/ac/ad, využívá ke zlepšení propustnosti a podporuje až čtyři antény současně.

V režimu infrastruktury se AP propojují se síťovou infrastrukturou pomocí kabelového DS. Každý AP definuje BSS a je jednoznačně identifikován jeho BSSID. K systému ESS lze připojit více BSS. Použití konkrétního SSID v systému ESS poskytuje bezproblémové možnosti roamingu mezi systémy BSS v systému ESS. Další identifikátory SSID mohou být použity k oddělení úrovně přístupu k síti definované tím, že je používán SSID.

Bezdrátový klient se nejdříve autentizuje pomocí AP a poté se přidružuje k tomuto AP. Měla by být použita autentizační norma 802.11i/WPA2. AES je metoda šifrování, která by měla být použita u WPA2.

Při plánování bezdrátové sítě by neměly být kanály, které se překrývají, použity při nasazování více přístupových bodů, aby pokrývaly určitou oblast. Mezi BSA by mělo dojít v případě ESS k překrytí 10-15%. Aplikace Cisco AP podporují PoE pro zjednodušení instalace.

12 KAPITOLA 5 – ÚPRAVA A ODSTRAŇOVÁNÍ PROBLÉMŮ JEDNO-OBLASTNÍ OSPF

12.1 Úprava a Odstraňování Problémů Jedno-oblastní OSPF

12.1.1 Úvod

12.1.1.1 Úvod

OSPF je populární protokol pro směrování stavu linky, který lze vyladit mnoha způsoby. Mezi nejběžnější metody jemného ladění patří manipulace s volebním procesem určeného/záložního směrovače (DR/BDR), propagace výchozích tras, jemné doladění rozhraní OSPFv2 a OSPFv3 a povolení autentizace.

Tato kapitola OSPF popisuje tyto laděné funkce, příkazy konfiguračního režimu k implementaci těchto funkcí pro IPv4 i IPv6 a komponenty a příkazy používané k řešení OSPFv2 a OSPFv3.

12.2 Vylepšené Konfigurace Jedno-oblastní OSPF

12.2.1 Směrování v Distribuční a Jádrové vrstvě

12.2.1.1 Směrování versus Přepínání

Škálovatelná síť vyžaduje hierarchický návrh sítě. Zaměření předchozích kapitol bylo na přístupové a distribuční vrstvy. Jak je znázorněno na obrázku 1, přepínače 2. vrstvy, agregace linek, redundance LAN a bezdrátové sítě LAN jsou všechny technologie, které poskytují nebo zlepšují přístup uživatelů k síťovým prostředkům.

Škálovatelné sítě také vyžadují optimální dosažitelnost mezi místy. Vzdálenou síťovou dostupnost zajišťují směrovače a přepínače 3. vrstvy, které fungují v distribučních a jádrových vrstvách, jak je znázorněno na obrázku 2. Směrovače a přepínače 3. vrstvy se dozvědí o vzdálených sítích jedním ze dvou způsobů:

- **Ručně** - vzdálené sítě jsou manuálně zadávány do tabulky tras pomocí statických cest.
- **Dynamicky** - Vzdálené trasy se automaticky naučují pomocí dynamického směrovacího protokolu, jako je například protokol EIGRP nebo OSPF.

12.2.1.2 Statické Směrování

Příklad na obrázku poskytuje vzorový scénář statického směrování. Správce sítě může ručně nakonfigurovat statickou cestu k dosažení určité sítě. Na rozdíl od dynamického směrovacího protokolu, se statické trasy neaktualizují automaticky a musí být ručně přepracovány, kdykoli se změní topologie sítě. Statická trasa se nezmění, dokud ji správce znovu neprovede.

Statické směrování má tři hlavní použití:

- Zajištění snadné údržby tabulky směrování v menších sítích, u nichž se neočekává významný růst.
- Směrování do a ze stub sítí. Stub síť, je síť přístupná jednou cestou a směrovač má pouze jednoho souseda.
- Použití jedné výchozí cesty, která představuje cestu k jakékoli síti, která nemá přesnější shodu s jinou cestou ve směrovací tabulce. Výchozí trasy se používají k odesílání provozu do libovolného místa určení, mimo další směrový směrovač.

12.2.1.3 Dynamické Směrovací Protokoly

Dynamické Směrování

Směrovací protokoly umožňují směrovačům dynamicky sdílet informace o vzdálených sítích, jak je znázorněno na obrázku. Směrovače přijímající aktualizaci, automaticky přidávají tyto informace do svých směrovacích tabulek. Směrovací protokoly potom určují nejlepší cestu nebo cestu ke každé síti. Primární přínos dynamických směrovacích protokolů spočívá v tom, že směrovače vyměňují informace o směrování, když dochází ke změně topologie. Tato výměna umožňuje směrovačům automaticky se dozvědět o nových sítích a také najít alternativní cesty, pokud dojde k selhání propojení s aktuální sítí.

Ve srovnání se statickým směrováním, vyžadují dynamické směrovací protokoly nižší administrativní režii. Náklady na použití dynamických směrovacích protokolů však vyčleňují část zdrojů směrovače pro provoz protokolů, včetně času procesoru a šířky pásma sítě. Navzdory výhodám dynamického směrování má statické směrování stále své místo. Existují chvíle, kdy statické směrování je vhodnější a jindy, kdy je lepší volbou dynamické směrování. Je však důležité pochopit, že statické a dynamické směrování se vzájemně nevylučují. Spíše většina sítí používá kombinaci dynamických směrovacích protokolů a statických cest.

Dva nejběžnější dynamické směrovací protokoly jsou EIGRP a OSPF. Zaměření této kapitoly je na OSPF.

Poznámka: Všechny dynamické směrovací protokoly jsou schopny reklamy a propagace statických cest v aktualizacích směrování.

12.2.1.4 OSPF – Open Shortest Path First

OSPF je běžně implementovaný protokol směrování stavu spojení. Byla vyvinuta jako náhrada protokolu vzdáleného směrování vektorů, RIP. Ovšem OSPF má významné výhody oproti RIP, neboť nabízí rychlejší konvergenci a měřítka pro mnohem větší síťové implementace.

Funkce OSPF, jak je znázorněno na obrázku, zahrnují:

- **Bez tříd** - je bez tříd podle návrhu. Proto podporuje VLSM a CIDR.
- **Efektivní** - Změny směrování spouštějí aktualizace směrování (žádné periodické aktualizace). Pomocí algoritmu SPF zvolí nejlepší cestu.
- **Rychlá konvergence** - Rychle šíří změny v síti.
- **Škálovatelná** - funguje dobře v malých a velkých sítích. Směrovače mohou být seskupeny do oblastí podporujících hierarchický systém.
- **Bezpečná** - Podporuje ověřování zpráv Digest 5 (MD5). Pokud je povoleno, směrovače OSPF akceptují šifrované směrování aktualizací od vrstevníků pouze se stejným před-sdíleným heslem.

12.2.1.5 Konfigurace Jedno-oblastního OSPF

Tato kapitola je zaměřena na úpravu a odstraňování problémů s OSPF. Nicméně je dobré přezkoumat základní implementaci směrovacího protokolu OSPF.

Příklad na obrázku 1 zobrazuje topologii použitou pro konfiguraci OSPFv2. Směrovače v topologii mají počáteční konfiguraci včetně povolených adres rozhraní. V současné době neexistuje žádné statické směrování nebo dynamické směrování nakonfigurované na žádném směrovači. Všechna rozhraní na směrovačích R1, R2 a R3 (s výjimkou zpětné vazby na R2) se nacházejí v oblasti páteře OSPF. ISP směrovač se používá jako brána směrovací domény k Internetu.

Na obr. 2, je rozhraní Gigabit Ethernet 0/0 na R1 konfigurované tak, aby odráželo jeho skutečnou šířku pásma 1 000 000 kilobitů. Dále z konfiguračního režimu směrovače OSPF je přidělen identifikátor směrovače. Referenční šířka pásma je upravena tak, aby odpovídala rychlým rozhraním, a inzerují se tři sítě připojené k R1. Všimněte si, jak se maska zástupných znaků používá k identifikaci konkrétních sítí.

Na obr. 3, je rozhraní Gigabit Ethernet 0/0 na R2, také nakonfigurováno tak, aby odráželo jeho skutečnou šířku pásma. Je přidělen identifikátor směrovače, referenční šířka pásma je upravena tak, aby odpovídala rychlým rozhraním, a jsou uváděny tři sítě připojené k R2. Všimněte si, jak lze zabránit použití masky zástupných znaků tím, že identifikujete rozhraní směrovače se čtyř-jádrovou maskou. Tím může OSPF efektivně používat masku podsítě přiřazenou rozhraní, jako inzerovanou síťovou masku.

Použijte kontrolu syntaxe na obr. 4, abyste nastavili šířku pásma na rozhraní R3 G0/0, zadejte konfigurační režim OSPF směrovače, přiřaďte správné ID směrovače, upravte referenční šířku pásma a inzerujte tři přímo připojené sítě pomocí rozhraní směrovače a Zástupné masky s čtyřnásobnou nulou.

Všimněte si informačních zpráv, které ukazují, že R3 vytvořil plnou sousedskou blízkost s R1 s ID směrovače 1.1.1.1 a R2 s ID směrovače 2.2.2.2. Síť OSPF se konvergovala.

12.2.1.6 Verifikace Jedno-oblastního OSPF

Užitečné příkazy k ověření OSPF obsahují následující:

- ***Show ip ospf neighbor*** - Příkaz na ověření, že směrovač vytvořil spojení ze sousedními směrovači. Není-li identifikátor směrovače sousedního směrovače zobrazen, nebo pokud se nezobrazí jako stav FULL, oba směrovače nevytvořily sousední OSPF.
- ***Show ip protocols*** - Příkaz poskytuje rychlou cestu k ověření zásadních informací o konfiguraci OSPF. To zahrnuje identifikátor procesu OSPF, ID směrovače, sítě směrující inzerci, sousedy, ze kterých směrovač přijímá aktualizace a výchozí administrativní vzdálenost, což je hodnota 110 pro OSPF.
- ***Show ip ospf*** - Příkaz se používá k zobrazení ID procesního protokolu OSPF a identifikátoru směrovače, jakož i informace o OSPF SPF a oblasti OSPF.
- ***Show ip ospf interface*** - Příkaz poskytuje podrobný seznam pro každé rozhraní podporující protokol OSPF a je velmi užitečný pro určení, zda byly řádně sestaveny příkazy sítě.
- ***Show ip ospf interface brief*** - Příkaz je užitečný pro zobrazení souhrnu a stavu rozhraní OSPF.

Obrázky 1 až 5 zobrazují odpovídající výstup každého ověřovacího příkazu zadaného na R1.

Pomocí příkazu kontroly syntaxe na obrázku 6 ověřte sousední spojení, důležité informace o konfiguraci OSPF a zobrazte souhrn rozhraní OSPF na R2.

Pomocí příkazu kontroly syntaxe na obrázku 7 ověřte sousední spojení, důležité informace o konfiguraci OSPF a zobrazte souhrn rozhraní OSPF na R3.

12.2.1.7 Konfigurace Jedno-oblastního OSPFv3

Následuje přehled základní implementace směrovacího protokolu OSPFv3 pro protokol IPv6.

Příklad na obrázku 1 zobrazuje topologii použitou pro konfiguraci OSPFv3. Směrovače v topologii mají počáteční konfiguraci včetně povolených rozhraní IPv6. V současné době neexistuje žádné statické směrování nebo dynamické směrování nakonfigurované na žádném směrovači. Všechna rozhraní na směrovačích R1, R2 a R3 (s výjimkou zpětné vazby na R2) se nacházejí v oblasti páteře OSPF.

Na obr. 2 je z konfiguračního režimu směrovače OSPFv3 na R1 identifikátor směrovače ručně přiřazen a referenční šířka pásma je upravena tak, aby odpovídala rychlým rozhraním. Dále jsou nakonfigurována rozhraní účastnící se OSPFv3. Gigabitový ethernet 0/0 je také konfigurován tak, aby odrážel jeho skutečnou šířku pásma. Všimněte si, jak se při konfiguraci OSPFv3 nevyžaduje žádná maska zástupných znaků.

Na obr. 3 je z konfiguračního režimu směrovače OSPFv3 na R2, identifikátor směrovače ručně přiřazen a referenční šířka pásma je upravena tak, aby odpovídala rychlým rozhraním. Dále jsou nakonfigurována rozhraní účastnící se OSPFv3. Opět je Gigabit Ethernet 0/0 také konfigurován tak, aby odrážel jeho skutečnou šířku pásma.

Použijte nástroj kontroly syntaxe na obrázku 4, abyste ručně přiřadili identifikátor směrovače a upravili referenční šířku pásma. Dále postupně nakonfigurujte příslušná rozhraní od rozhraní Gigabit Ethernet 0/0. Také přiřadit skutečné šířce pásma k tomuto rozhraní.

Všimněte si informačních zpráv, které ukazují, že R3 vytvořil plnou sousedskou blízkost s R1 s ID směrovače 1.1.1.1 a R2 s ID směrovače 2.2.2.2. Síť OSPFv3 konvergovala.

12.2.1.8 Verifikace Jedno-oblastního OSPFv3

Užitečné příkazy k ověření OSPFv3 zahrnují následující:

- ***Show ipv6 ospf neighbor*** - Příkaz ověřuje, zda směrovač vytvořil sousední směrovače. Není-li identifikátor směrovače sousedního směrovače zobrazen, nebo pokud se nezobrazí jako stav FULL, oba směrovače nevytvořily sousední OSPF.

- ***show ipv6 protocols*** - Příkaz poskytuje rychlou cestu k ověření zásadních informací o konfiguraci OSPFv3, včetně ID procesu protokolu OSPF, ID směrovače a rozhraní povolených pro OSPFv3.
- ***Show ipv6 route ospf*** - Příkaz poskytuje specifické informace o trasách OSPFv3 ve směrovací tabulce.
- ***show ipv6 ospf interface brief*** - Příkaz je užitečný pro zobrazení souhrnu a stavu rozhraní podporujících OSPFv3.

Obrázky 1 až 4 zobrazují odpovídající výstup každého ověřovacího příkazu zadaného na R1.

12.2.2 Více přístupové sítě OSPF

12.2.2.1 Typy sítí OSPF

Chcete-li konfigurovat úpravy OSPF, začněte základní implementací směrovacího protokolu OSPF.

OSPF definuje pět typů sítí, jak je znázorněno na obrázcích 1 až 5:

- **Point-to-Point** - dva směrovače propojené přes společné propojení. Na lince nejsou žádné další směrovače. Toto je často konfigurace v sítích WAN. (Obrázek 1)
- **Broadcast multiaccess (BMA)**- Více směrovačů propojených přes ethernetovou síť. (Obrázek 2)
- **Non-Broadcast Multiaccess (NBMA)** - Více směrovačů propojených v síti, která neumožňuje vysílání, jako je např. Frame Relay. (Obrázek 3)
- **Point-to-multipoint** - více směrovačů propojených v topologii rozbočovače-a-paprsků, přes síť NBMA. Často se používá k připojení poboček (paprsků) na centrální místo (rozbočovač). (Obr. 4)
- **Virtuální propojení** - Speciální síť OSPF používaná k propojení vzdálených oblastí OSPF do oblasti páteře. (Obrázek 5)

Více přístupová (Multiaccess) síť je síť s více zařízeními na stejném sdíleném médiu, které sdílí komunikaci. Ethernetové sítě LAN, jsou nejběžnějším příkladem vysílaných více přístupových sítí. Ve vysílacích sítích jsou všechna zařízení v síti vidět a taky všechny vysílací a multicastové rámce. Jsou to sítě s více přístupovými právy, protože mohou existovat četné hostitelské počítače, tiskárny, směrovače a další zařízení, které jsou všechny členy stejné sítě.

12.2.2.2 Výzvy ve Více přístupových sítích

Více přístupové sítě mohou pro OSPF vytvořit dvě výzvy týkající se zaplavení LSA rámci:

- **Vytvoření více přidružení** - ethernetové sítě by mohly potenciálně propojit mnoho směrovačů OSPF přes běžné propojení. Vytvoření přidružení s každým směrovačem je zbytečné a nežádoucí. To by vedlo k nadměrnému počtu LSA vyměňovaných mezi směrovači ve stejné síti.
- **Rozsáhlé zaplavení LSA** - Link-state směrovače zaplavují jejich link-state pakety při inicializování OSPF, nebo když tam je změna v topologii. Tato povodeň může být nadměrná.

Následující vzorec může být použit pro výpočet počtu požadovaných přidružení. Počet požadovaných přidružení pro libovolný počet směrovačů (označených jako n) v síti, s více přístupy je:

N (n - 1) / 2

Obrázek 1 znázorňuje jednoduchou topologii čtyř směrovačů, které jsou všechny připojeny k téže síti s více přístupovými sítěmi. Bez nějakého druhu mechanismu, který by snížil počet sousedů, by společně tyto směrovače měly tvořit šest vedlejších částí: 4 (4 - 1)/2 = 6, jak je znázorněno na obrázku 2. Obrázek 3 ukazuje, že když jsou směrovače přidávány do sítě, počet sousedů se dramaticky zvyšuje.

12.2.2.3 Určený Směrovač OSPF

Řešení pro řízení počtu sousedních přidružení a zaplavení LSA v síti s více přístupy je DR. V systémech OSPF pro více přístupů, volí DR jako sběrný a distribuční bod pro odeslané a přijaté LSA. BDR je zvolen v případě selhání DR. BDR pasivně naslouchá této výměně a udržuje vztah se všemi směrovači. Pokud DR přestane vyrábět Hello pakety, BDR se sama propaguje a převezme roli DR.

Všechny ostatní směrovače, které nejsou DR nebo BDR, se stanou DROTHER (směrovač, který není ani DR ani BDR).

Na obr. 1 byl zvolen R1 jako určený směrovač pro Ethernet LAN propojující R2, R3 a R4. Všimněte si, jak byl počet přidružení snížen na 3.

Směrovače v síti s více přístupy zvolí DR a BDR. DROTHER tvoří v síti pouze plné sousedství s DR a BDR. Namísto zaplavení LSA do všech směrovačů v síti vysílá DROTHER pouze LSA do DR a BDR pomocí adresy 224.0.0.6 (všechny DR směrovače).

Klepnutím na tlačítko Přehrát na obrázku 2 zobrazíte animaci role DR. V animaci R1 posílá LSA do DR. BDR poslouchá. DR je odpovědný za předávání LSA z R1 do všech ostatních směrovačů. DR používá multicast adresu 224.0.0.5 (všechny směrovače OSPF). Konečným výsledkem je, že v síti s více přístupovými body, se dělá veškeré zaplavení LSA pouze jedním směrovačem.

Poznámka: Volby DR/BDR se vyskytují pouze v sítích s více účastníky a nevyskytují se v sítích typu point-to-point.

12.2.2.4 Verifikace rolí DR/BDR

V topologii více přístupů zobrazené na obrázku 1, jsou tři směrovače vzájemně propojeny prostřednictvím společné sítě s více přístupy, 192.168.1.0/28. Každý směrovač je konfigurován s uvedenou IP adresou na rozhraní Gigabit Ethernet 0/0.

Vzhledem k tomu, že směrovače jsou připojeny přes běžnou vysílací síť více přístupů, OSPF automaticky zvolil DR a BDR. V tomto příkladu byl R3 zvolen jako DR, protože jeho ID je 3.3.3.3, což je nejvyšší v této síti. R2 je BDR, protože má druhé nejvyšší ID v síti.

Pro ověření rolí směrovače použijte příkaz ***show ip ospf interface*** (Obrázek 2). Výstup generovaný na R1 potvrzuje, že:

- R1 není DR nebo BDR, ale je DROTHER s výchozí prioritou 1. (1)
- DR je směrovač R3 s ID 3.3.3.3 s IP adresou 192.168.1.3, zatímco BDR je R2 s ID 2.2.2.2 na IP adrese 192.168.1.2. (2)
- R1 má dvě přidružení: jeden s BDR a jeden s DR. (3)

Výstup generovaný na R2, obr. 3 potvrzuje, že:

- R2 je BDR s výchozí prioritou 1. (1)
- DR je směrovač R3 s ID 3.3.3.3 s IP adresou 192.168.1.3, zatímco BDR je R2 s ID 2.2.2.2 na IP adrese 192.168.1.2. (2)
- R2 má dvě přidružení: Jedno se sousedem s ID směrovače 1.1.1.1 (R1) a druhé s DR. (3)

Výstup generovaný na R3, obr. 4 potvrzuje, že:

- R3 je DR s výchozí prioritou 1. (1)
- DR je směrovač R3 s ID 3.3.3.3 a s IP adresou 192.168.1.3, zatímco BDR je R2 s ID 2.2.2.2 na IP adrese192.168.1.2. (2)
- R3 má dvě přidružení: jedno se sousedem s ID 1.1.1.1 (R1) a druhé s BDR. (3)

12.2.2.5 Verifikace přidružení DR/BDR

Ověření OSPF přidružení pomocí příkazu ***show ip ospf neighbor***, jak je znázorněno na obrázku 1.

Na rozdíl od sériových linek, které zobrazují pouze stav FULL/-, stav sousedů v sítích s více přístupy může být:

- FULL/DROTHER - Jedná se o DR nebo BDR směrovač, který je plně sousedící se směrovačem, který není DR nebo BDR. Tito dva sousedé si mohou vyměnit balíčky Hello, aktualizace, dotazy, odpovědi a potvrzení.
- FULL/DR – Směrovač, plně sousedí s uvedeným sousedem DR. Tito dva sousedé, si mohou vyměnit balíčky Hello, aktualizace, dotazy, odpovědi a potvrzení.
- FULL/BDR - Směrovač plně sousedí s označeným BDR sousedem. Tito dva sousedé si mohou vyměnit balíčky Hello, aktualizace, dotazy, odpovědi a potvrzení.
- 2-WAY/DROTHER - Směrovač, který není DR nebo BDR, má sousední vztah s jiným směrovačem, který není DR nebo BDR. Tito dva sousedé si vymění jen Hello pakety.

Normální stav pro OSPF směrovač, je obvykle FULL. Pokud je směrovač uvíznutý v jiném stavu, je to známka toho, že se vyskytují problémy při vytváření přidružení. Jediná výjimka je 2-WAY stav, který je normální ve více přístupové vysílací síti.

V systémech s více přístupovými sítěmi tvoří DROTHER pouze FULL přidružení s DR a BDR. Nicméně, DROTHER budou stále tvořit 2-WAY sousedství s jinými DROTHER směrovači, které se připojují k síti. To znamená, že všechny DROTHER směrovače v síti s více přístupy stále přijímají balíčky Hello ze všech ostatních DROTHER směrovačů. Tímto způsobem jsou si vědomi všech směrovačů v síti. Když dva směrovače DROTHER tvoří sousedství, sousední stav se zobrazí jako 2-WAY/DROTHER.

Výstup generovaný R1 potvrzuje, že R1 má vedle sebe směrovač:

- R2 s ID směrovače 2.2.2.2 je v plném stavu a role R2 je BDR. (1)
- R3 s ID směrovače 3.3.3.3 je v plném stavu a role R3 je DR. (2)

Výstup generovaný R2 na obr. 2 potvrzuje, že R2 má vedle sebe směrovač:

- R1 s ID směrovače 1.1.1.1 je v plném stavu a R1 není DR ani BDR. (1)
- R3 s ID směrovače 3.3.3.3 je v plném stavu a role R3 je DR. (2)

Výstup vygenerovaný R3 na obr. 3 potvrzuje, že R3 má vedle sebe směrovač:

- R1 s ID směrovače 1.1.1.1 je v plném stavu a R1 není DR ani BDR. (1)
- R2 s ID směrovače 2.2.2.2 je v plném stavu a role R2 je BDR. (2)

12.2.2.6 Původní Výběrový Proces DR/BDR

Jak se volí DR a BDR? Rozhodnutí voleb OSPF vychází z následujících kritérií v pořadí:

1. Směrovače v síti, zvolí směrovač s nejvyšší prioritou rozhraní, jako DR. Ten s druhou nejvyšší prioritou rozhraní je zvolen jako BDR. Prioritu lze nakonfigurovat tak, aby se jednalo o libovolné číslo v rozmezí 0 - 255. Čím vyšší je priorita, tím spíš bude směrovač vybrán jako DR. Pokud je priorita nastavena na hodnotu 0, směrovač se nemůže stát DR. Výchozí priorita více přístupových vysílacích rozhraní je 1. Protože není-li nastaveno jinak, všechny směrovače mají stejnou hodnotu priority a musí se při volbách DR/BDR spoléhat na jinou metodu přerušení.

2. Pokud jsou priority rozhraní stejné, pak je směrovač s nejvyšším ID zvolen DR. Ten s druhým nejvyšším ID je BDR.

Připomeňme si, že ID směrovače je určeno jedním ze tří způsobů:

- ID lze ručně konfigurovat.
- Není-li nakonfigurováno žádné ID směrovače, je určeno nejvyšší IP adresou zpětné vazby.
- Pokud nejsou nakonfigurována žádná rozhraní zpětné vazby, ID směrovače je určeno nejvyšší aktivní adresou IPv4.

Poznámka: V síti IPv6, pokud nejsou nakonfigurovány žádné adresy IPv4, musí být identifikátor směrovače ručně konfigurován pomocí příkazu ***router-id rid***. Jinak se OSPFv3 nespustí.

Na obrázku jsou všechny ethernetová rozhraní s výchozí prioritou 1. V důsledku toho se na základě výše uvedených kritérií výběru používá identifikátor OSPF směrovače pro volbu DR a BDR. R3 s nejvyšším ID se stává DR. A R2, s druhým nejvyšším ID, se stává BDR.

Poznámka: Sériová rozhraní mají výchozí priority nastavené na hodnotu 0. Proto nevybírají DR a BDR.

Proces voleb DR a BDR se uskuteční, jakmile je v síti s více přístupy aktivní první směrovač s rozhraním umožňujícím OSPF. K tomu může dojít při zapnutí směrovačů nebo při konfiguraci příkazu sítě OSPF pro toto rozhraní. Proces volby trvá jen několik vteřin. Pokud

všechny směrovače v síti s více přístupovými právy nedokončily zavádění, je možné, že směrovač s nižším identifikátorem směrovače se stává DR. (Může to být směrovač nižší třídy, který používá méně času k zavedení.)

12.2.2.7 Výběrový proces DR/BDR

Volby DR a BDR nejsou preventivní. Pokud po volbách DR a BDR do sítě přidá nový směrovač s vyšší prioritou nebo vyšším ID směrovače, nově přidaný směrovač nepřebírá roli DR nebo BDR. Je tomu tak proto, že tyto role již byly přiřazeny. Přidáním nového směrovače se nezahájí nový volební proces.

Po zvolení DR zůstane DR, dokud nenastane jedna z následujících událostí:

- DR selže
- Proces OSPF na DR selhává nebo je zastaven
- Rozhraní pro více přístupů na DR selhává nebo je vypnuto

Pokud DR selže, BDR je automaticky povýšen na DR. Tak je tomu i v případě, že po inicializaci volby DR/BDR do sítě se přidá další síť s vyšší prioritou nebo identifikátorem směrovače. Avšak poté, co je BDR povýšen na DR, dojde k novým volbám BDR a DROTHER směrovač s vyšší prioritou nebo identifikátorem je zvolen jako nový BDR.

Obrázky 1 až 4 ilustrují různé scénáře týkající se volebního procesu DR a BDR.

Na obr. 1 selže aktuální DR (R3). Proto předem zvolený BDR (R2), přebírá roli DR. Následně, se uskuteční zvolení nového BDR. Protože R1 je jediný DROTHER, je zvolen jako BDR.

Na obr. 2 se R3 po několika minutách znovu připojil k síti. Vzhledem k tomu, že DR a BDR již existují, R3 nepřebírá žádnou roli, místo toho se stane DROTHER.

Na obr. 3 je do sítě přidán nový směrovač R4 s vyšším ID směrovače. DR (R2) a BDR (R1) si zachovávají svou roli. R4 se automaticky stane DROTHER.

Na obr. 4 selhal R2. BDR (R1) se automaticky stává DR a volební proces vybírá R4 jako BDR, protože má vyšší ID.

12.2.2.8 Priorita OSPF

DR se stává ústředním bodem pro shromažďování a distribuci LSA. Proto musí mít tento směrovač dostatečnou kapacitu procesoru a paměti pro zvládnutí pracovní zátěže. Je možné ovlivnit volební proces DR/BDR prostřednictvím konfigurace.

Pokud jsou priority rozhraní stejné pro všechny, směrovač s nejvyšším identifikátorem je zvolen DR. Je možné konfigurovat ID směrovače pro manipulaci s volbami DR/BDR. Tento proces však funguje pouze v případě, že existuje přísný plán pro nastavení ID na všech směrovačích. Ve velkých sítích to může být těžkopádné.

Namísto spoléhání se na ID směrovače je lepší kontrolovat volby nastavením priorit rozhraní. Priority jsou hodnota specifická pro rozhraní, což znamená, že poskytuje lepší kontrolu nad víceúrovňovou sítí. To také směrovači umožňuje být DR v jedné síti a DROTHER v jiné.

Chcete-li nastavit prioritu rozhraní, použijte následující příkazy:

- *Ip ospf priority hodnota* - příkaz rozhraní OSPFv2
- *Ipv6 ospf priority hodnota* - příkaz rozhraní OSPFv3

Hodnota může být:

- 0 - nestává se DR nebo BDR.
- 1 - 255 - Čím vyšší je priorita, tím pravděpodobněji se směrovač stává DR nebo BDR.

Na obrázku mají všechny směrovače stejnou prioritu OSPF, protože hodnota priority je výchozí 1, pro všechna rozhraní. Proto ID směrovače slouží k určení DR (R3) a BDR (R2). Změna hodnoty priority na rozhraní, od 1 na vyšší hodnotu by umožnila, aby se stal směrovač během příštích voleb DR nebo BDR.

Pokud je priorita rozhraní nakonfigurována po zapnutí funkce OSPF, musí správce vypnout proces OSPF na všech směrovačích a znovu povolit proces OSPF, aby vynutil nové volby DR/BDR.

12.2.2.9 Změna Priority OSPF

V topologii na obr. 1 je R3 DR a R2 je BDR. Bylo rozhodnuto, že:

- R1 by měl být DR a bude konfigurován s prioritou 255.
- R2 by měl být BDR a bude mít výchozí prioritu 1.
- R3 by nikdy neměl být DR nebo BDR a bude konfigurován s prioritou 0.

Obrázek 2 změní na rozhraní R1 Gigabit 0/0 prioritu z 1 na 255.

Obrázek 3 změní na rozhraní R3 Gigabit 0/0 prioritu z 1 na 0.

Změny se automaticky nezmění, protože DR a BDR jsou již zvoleny. Proto musí být volby OSPF vyjednány pomocí jedné z následujících metod:

- Vypněte rozhraní směrovače a znovu jej povolte počínaje DR, pak BDR a pak všechny ostatní směrovače.
- Resetujte proces OSPF pomocí příkazu ***clear ip ospf process*** na privilegovaném režimu EXEC na všech směrovačích.

Obrázek 4 zobrazuje, jak vymazat proces OSPF na R1. Předpokládejme, že je v konfiguraci R2 a R3 konfigurován také příkaz ***clear ip ospf process***. Všimněte si, že byly generovány informace o stavu OSPF.

Výstup zobrazený na obrázku 5 potvrzuje, že R1 je nyní DR s prioritou 255 a identifikuje nové sousední vztahy s R1.

12.2.3 Propagace Výchozího Směrování

12.2.3.1 Propagace výchozí statické trasy v OSPFv2

S protokolem OSPF, je směrovač připojený k Internetu a používá k šíření výchozí trasy k jiným směrovačům v směrovací doméně OSPF. Tento směrovač se někdy nazývá hraničním, vstupem nebo směrovačem brány. V terminologii OSPF je však umístěný mezi směrovací doménou OSPF a sítí, která není OSPF, ale také se nazývá autonomním systémovým hraničním směrovačem (ASBR).

Na obr. 1, R2 je jeden domácí směrovač k poskytovateli služeb. Proto je vše, co je pro R2 nezbytné k dosažení Internetu, výchozí statickou cestou k poskytovateli služeb.

Poznámka: V tomto příkladu, je jako rozhraní simulující připojení k poskytovateli služeb, použito rozhraní zpětné vazby s adresou IP 209.165.200.225.

Chcete-li propagovat výchozí trasu, musí být okrajový směrovač (R2) konfigurován pomocí:

- Výchozí statické trasy, použitím ***ip route 0.0.0.0 0.0.0.0 {ip-address|exit-intf}***.
- Příkaz ***default-information originate***, vyvolá konfiguraci směrovače. Toto instruuje R2 jako zdroj výchozí informace o trase a propaguje výchozí statickou cestu v aktualizacích OSPF.

Obrázek 2 ukazuje, jak nakonfigurovat plně specifikovanou výchozí statickou trasu k poskytovateli služeb.

12.2.3.2 Verifikace Propagované Původní Trasy

Ověřte výchozí nastavení trasy na R2 pomocí příkazu ***show ip route***, jak je znázorněno na obrázku 1.

Pomocí kontroly syntaxe na Obr. 2 ověřte, zda byla výchozí trasa rozšířena do R1 a R3. Všimněte si, že zdroj trasy je O * E2, což znamená, že byl naučen pomocí OSPF. Hvězdička označuje tuto trasu, jako dobrého kandidáta na výchozí trasu. Označení E2 označuje, že jde o externí trasu.

Externí trasy jsou buď externí typ 1, nebo externí typ 2. Rozdíl mezi těmito dvěma způsoby je způsob, jakým je vypočtena metrika trasy. Metrika trasy typu 2, je vždy externí, bez ohledu na vnitřní metriku dosažení této trasy. Metrika typu 1 představuje přidání externích a interních cen použitých k dosažení této trasy. Trasa typu 1 má vždy přednost, před cestou typu 2 pro tentýž cíl.

12.2.3.3 Propagace Výchozí Statické Trasy v OSPFv3

Proces šíření výchozí statické cesty v OSPFv3 je téměř totožný s OSPFv2.

Na obr. 1 je R2 jeden domácí směrovač k poskytovateli služeb. Proto je vše, co je pro R2 nezbytné k dosažení Internetu, výchozí statickou cestou k poskytovateli služeb.

Poznámka: V tomto příkladu je pro simulaci připojení k poskytovateli služeb použito rozhraní zpětné vazby s adresou IP 2001:DB8:FEED:1::1/64.

Obrázek 2 zobrazuje aktuální směrovací tabulku IPv6 na R1. Všimněte si, že nezná cestu k internetu.

Chcete-li propagovat výchozí trasu, musí být hraniční směrovač (R2) konfigurován pomocí:

- Výchozí statická trasa pomocí příkazu ***ipv6 route ::/0 {ipv6-address | Exit-intf}***.
- Příkaz ***default-information originate***, konfiguračního módu směrovače. Toto instruuje R2, být jako zdroj výchozí informace o trase a propaguje výchozí statickou cestu v aktualizacích OSPF.

Příklad na obrázku 3 konfiguruje plně přednastavenou výchozí statickou cestu k poskytovateli služeb.

12.2.3.4 Verifikace Propagované Původní Trasy IPv6

Ověřte výchozí nastavení statické trasy na R2 pomocí příkazu ***show ipv6 route***, jak je znázorněno na obrázku 1.

Pomocí kontroly syntaxe na Obr. 2 ověřte, zda byla výchozí trasa rozšířena na hodnotu R1. Všimněte si, že zdroj trasy je OE2, což znamená, že byl naučen pomocí OSPFv3. Označení E2 označuje, že jde o externí trasu.

Na rozdíl od směrovací tabulky IPv4, IPv6 nepoužívá hvězdičku k signalizaci, že trasa je vhodným kandidátem pro výchozí trasu.

12.2.4 Zabezpečení OSPF

12.2.4.1 Směrovače jsou Cíle

Úloha směrovačů v síti je tak zásadní, že jsou často cílem útoků v síti. Správci sítí si musí být vědomi toho, že směrovače jsou ohroženi útokem stejně jako systémy koncových uživatelů.

Obecně platí, že směrovací systémy mohou být napadány narušením směrovačů nebo falšováním informací obsažených v protokolu směrování. Falšované informace o směrování mohou být obecně používány k tomu, aby způsobily, že se systémy mohou chybně informovat, že způsobí útok typu DoS (DoS) nebo způsobí, že se provoz bude řídit cestou, která by za normálních okolností nenastala. Důsledky padělání informací o směrování jsou:

- Přesměrování provozu pro vytvoření směrovacích smyček
- Přesměrování provozu, aby mohlo být monitorováno na nejistém spojení
- Přesměrování provozu, aby se zlikvidoval

Klepnutím na tlačítko Přehrát v animaci zobrazíte příklad útoku, který vytvoří směrovací smyčku. Útočník se mohl připojit přímo k propojení mezi směrovači R1 a R2. Injektuje informace o falešných směrováních určených pouze směrovači R1, což znamená, že R2 je preferovaným místem určení hostitelské trasy 192.168.10.10/32. Přestože R1 má vstupní směrovací tabulku do přímo připojené sítě 192.168.10.0/24, přidá injektovanou trasu do své směrovací tabulky kvůli delší masce podsítě. Trasa s delší shodou masky podsítě se považuje za lepší, než trasa s kratší maskou. V důsledku toho, když směrovač přijme paket, vybírá delší masku podsítě, protože jde o přesnější cestu k cíli.

Když PC3 odešle paket na PC1 (192.168.10.10/24), pak R1 nepředá paket hostiteli PC1. Namísto toho směruje paket směrovači R2, protože zdánlivě nejlepší cesta k 192.168.10.10/32 je přes R2. Když R2 obdrží paket, podívá se na něj ve své směrovací tabulce a předá jej zpět do R1, který vytvoří smyčku.

Chcete-li zmírnit útoky protokolu směrování, nakonfigurujte ověření OSPF.

12.2.4.2 Zabezpečení Směrovacích Updatů

Když bylo na směrovači nakonfigurováno sousední ověřování, směrovač ověřil zdroj každého balíčku aktualizace směrování, který obdržel. Toho bylo dosaženo výměnou ověřovacího klíče (někdy označovaného jako heslo), který je znám jak odesílajícímu, tak přijímajícímu směrovači.

Chcete-li informace o aktualizaci směrování bezpečně vyměnit, povolte ověřování OSPF. Autentizace OSPF může být buď žádná (Null), jednoduchá nebo Message Digest 5 (MD5).

OSPF podporuje 3 typy ověřování:

- **Null** - Toto je výchozí metoda a znamená, že pro OSPF není použito ověřování.
- **Ověřování pomocí jednoduchého hesla** - Toto je také označováno jako ověřování prostým polem, protože heslo v aktualizaci je odesláno v textovém formátu po síti. Toto je považováno za starší metodu ověřování OSPF.
- **Autentifikace MD5** - Jedná se o nejbezpečnější a nejvhodnější metodu autentizace. Autentizace MD5 poskytuje vyšší zabezpečení, protože heslo se nikdy nevyměňuje mezi sousedy. Místo toho se vypočítá pomocí algoritmu MD5. Výsledky shody ověřují odesílatelé.

Klepnutím na tlačítko Přehrát v animaci zjistíte, jak se ověřování MD5 používá k ověření sousedních zpráv.

Poznámka: RIPv2, EIGRP, OSPF, IS-IS a BGP podporují různé formy autentifikace MD5.

12.2.4.3 Autentifikace MD5

Následující příklad ukazuje, jak se autentizace MD5 používá k ověření dvou sousedních směrovačů OSPF.

Na obr. 1, kombinuje R1 směrovací zprávu s předběžně sdíleným tajným klíčem a vypočítá podpis pomocí algoritmu MD5. Podpis je také znám jako hodnota hash.

Na obrázku 2, R1 přidá podpis ke směrovací zprávě a odešle ji R2.

MD5 nešifruje zprávu, proto je obsah snadno čitelný.

Na obr. 3, R2 otevře paket, spojuje směrovací zprávu s předem sdíleným tajným klíčem a vypočítá podpis pomocí algoritmu MD5.

- Pokud se podpisy shodují, pak R2 akceptuje aktualizaci směrování.

- Pokud se podpisy neshodují, pak R2 tuto aktualizaci odmítne.

OSPFv3 neobsahuje vlastní autentizační schopnosti. Místo toho se zcela spoléhá na protokol IPSec, který zajišťuje komunikaci mezi sousedy pomocí příkazu ***ipv6 ospf authentication ipsec spi***. To je přínosné pro zjednodušení protokolu OSPFv3 a standardizaci jeho autentifikačního mechanismu.

12.2.4.4 Konfigurace OSPF Autentifikace MD5

OSPF podporuje autentifikaci protokolu směrování pomocí MD5. Ověřování MD5 lze globálně povolit pro všechna rozhraní nebo na základě rozhraní.

Chcete-li aktivovat autentizaci OSPF MD5 globálně, nakonfigurujte:

- Příkaz ***ip ospf message-digest-key klíč md5 heslo,*** do rozhraní konfiguračního módu.
- Příkaz ***area area-id authentication message-digest,*** do konfiguračního módu směrovače.

Tato metoda vynucuje ověřování na všech rozhraních podporujících protokol OSPF. Pokud rozhraní není nakonfigurováno příkazem ***ip ospf message-digest-key***, nebude schopen vytvořit přidružení s ostatními sousedy v OSPF.

Aby byla zajištěna větší flexibilita, ověřování je nyní podporováno na základě rozhraní. Chcete-li povolit autentizaci MD5 na základě rozhraní, nakonfigurujte:

- Příkaz ***ip ospf message-digest-key klíč md5 heslo***
- Příkaz ***ip ospf authentication message-digest***

Globální ověřování a autentizace MD5 na rozhraní OSPF, mohou být použity na stejném směrovači. Nastavení rozhraní však přepíše globální nastavení. Hesla ověřování MD5 nemusí být v celé oblasti stejná. Musí však být stejná mezi sousedy.

Předpokládejme například, že všechny směrovače na obrázku konvergovaly pomocí OSPF a směrování funguje správně. Ověření OSPF bude implementováno na všech směrovačích.

12.2.4.5 Příklad OSPF Autentifikace MD5

Příklad na obrázku 1, konfiguruje R1, aby povolil ověřování MD5 na všech rozhraních OSPF. Všimněte si informačních zpráv, které uvádějí, že sousední přidružení OSPF s R2 a R3 se změnily na stav dolů, protože R2 a R3 dosud nebyly nakonfigurovány pro podporu ověřování MD5.

Jako alternativu ke globální autentizaci MD5, příklad na obrázku 2 ukazuje, jak nakonfigurovat R1, aby povolil ověřování MD5 na základě rozhraní OSPF. Znovu zjistěte, jak se sousední přidružení OSPF změnily na stav dolů.

Použijte kontrolu syntaxe na obrázku 3, pro kontrolu globálního ověřování MD5 na R2 a rozhraních OSPF na R3.

Znovu se objevují informační zprávy. První zpráva, protože sousední přidružení s R1 bylo obnoveno. Sousednost s R3 však přešla do stavu dolů, protože R3 stále není nakonfigurován.

Poté, co je R3 nakonfigurován, byly obnoveny všechny sousední přidružení.

12.2.4.6 Verifikace OSPF Autentifikace MD5

Chcete-li ověřit, zda je zapnuto ověřování MD5, použijte příkaz ***show ip ospf interface***. Ověřením toho, zda je směrová tabulka dokončena, to lze úspěšné ověřit.

Obrázek 1 verifikuje MD5 ověření na sériovém OSPF rozhraní 0/0/0 na R1.

Obrázek 2 potvrzuje, že ověřování bylo úspěšné.

Pomocí kontroly syntaxe na Obr. 3 ověřte MD5 ověření na R2 a R3.

12.3 Řešení problémů v Implementacích Jedno-Oblastních OSPF

12.3.1 Komponenty pro Řešení Problémů v Jedno-oblastní OSPF

12.3.1.1 Přehled

OSPF je populárně implementovaný směrovací protokol, používaný ve velkých podnikových sítích. Řešení problémů souvisejících s výměnou informací o směrování je jednou z nejdůležitějších dovedností pro profesionály v síti, kteří se podílejí na zavádění a údržbě rozsáhlých podnikových sítí, které používají OSPF jako IGP.

Problémy s tvorbou sousedství OSPF jsou uvedeny na obrázku.

12.3.1.2 Stavy OSPF

K řešení OSPF je důležité pochopit, jak OSPF směrovače, procházejí různými stavy OSPF při vytváření přidružení.

Tato část uvádí stav OSPF a poskytuje souhrn funkcí jednotlivých stavů.

Při odstraňování problémů se sousedy OSPF si uvědomte, že stavy FULL nebo 2WAY jsou normální. Všechny ostatní stavy jsou přechodné. To znamená, že směrovač by neměl zůstat v těchto stavech na delší dobu.

12.3.1.3 Příkazy Řešení Problémů OSPF

Existuje mnoho různých příkazů OSPF, které lze použít k řešení problémů. Níže jsou shrnuty nejběžnější z těchto příkazů:

- ***show ip protocols*** (obrázek 1) - slouží k ověření důležitých informací o konfiguraci OSPF, včetně ID procesu protokolu OSPF, ID směrovače, ID sítí, které směrovač inzeruje, ID sousedů, ze kterých směrovač přijímá aktualizace, a standardní administrativní vzdálenost, to je 110 pro OSPF.
- ***show ip ospf neighbor*** (Obrázek 2) - Používá se k ověření, že směrovač má přidružení ze sousední směrovači. Zobrazuje ID sousedního směrovače, sousední prioritu, stav OSPF, Dead Časovač, IP adresu sousedního rozhraní a rozhraní, na kterém je soused přístupný. Není-li ID sousedního směrovače zobrazeno, nebo pokud se nezobrazuje jako stav FULL nebo 2WAY, tak oba směrovače nevytvořily přidružení. Pokud dva směrovače nedosahují sousednosti, informace o stavu spojení se nezmění. Neúplné databáze odkazových stavů mohou způsobit nepřesné stromy SPF a směrovací tabulky. Trasy do cílové sítě nemusí existovat nebo nemusí být nejoptimálnější.
- ***show ip ospf interface*** (Obrázek 3) - Používá se k zobrazení OSPF parametrů nakonfigurovaných na rozhraní, jako je ID procesu protokolu, jemuž je rozhraní přiřazeno. Oblast, ve které jsou součásti rozhraní, metrika rozhraní, Hello a Dead intervaly. Přidání názvu a čísla rozhraní k příkazu zobrazuje výstup pro určité rozhraní.
- ***show ip ospf*** (Obrázek 4) - Používá se k prozkoumání ID procesu protokolu OSPF a ID směrovače. Tento příkaz navíc zobrazuje informace o oblasti OSPF, stejně jako poslední výpočet algoritmu SPF.
- ***show ip route ospf*** (Obrázek 5) - Používá se k zobrazení pouze naučených cest OSPF ve směrovací tabulce. Výstup ukazuje, že R1 se prostřednictvím OSPF dozvěděl o čtyřech vzdálených sítích.
- ***clear ip ospf [process-id] process*** - slouží k resetování sousedních přidružení OSPFv2.

12.3.1.4 Komponenty Řešení Problémů OSPF

Jak je znázorněno na obrázku, problémy OSPF se obvykle týkají:

- Sousedních přidružení
- Chybících tras
- Výběrů cest

Při odstraňování problémů sousedů ověřte, zda směrovač vytvořil přidružení se sousedními směrovači pomocí příkazu ***show ip ospf neighbor***. Pokud není sousedství, směrovače nemohou vyměňovat trasy. Ověřte, zda jsou rozhraní funkční a povolená pro OSPF pomocí příkazů ***show ip interface brief*** a ***show ip ospf interface***. Pokud rozhraní fungují a jsou povolena pro OSPF, ujistěte se, že rozhraní obou směrovačů jsou konfigurována pro stejnou oblast OSPF a nejsou konfigurována jako pasivní.

Pokud je sousednost mezi dvěma směrovači zavedena, ověřte, zda jsou ve směrovací tabulce cesty OSPF, pomocí příkazu ***show ip route ospf***. Pokud neexistují žádné trasy protokolu OSPF, ověřte, zda v síti nejsou žádné jiné směrovací protokoly s nižší administrativní vzdáleností. Ověřte, zda jsou všechny požadované sítě inzerovány do OSPF. Také ověřte, zda je na směrovači nakonfigurován přístupový seznam, který by filtroval buď příchozí nebo odchozí směrování aktualizací.

Pokud jsou všechny požadované trasy v směrovací tabulce, ale cesta, která je provozována, není správná, ověřte metriku OSPF na rozhraní. Také buďte opatrní v případech, kdy jsou rozhraní vyšší než 100 Mb/s, protože všechna rozhraní nad touto šířkou pásma mají ve výchozím nastavení stejnou metriku OSPF.

12.3.2 Řešení Problémů Směrování Jedno-Oblastního OSPF

12.3.2.1 Řešení Problémů ze Sousedy

Tento příklad zvýrazní, jak řešit problémy sousedů. V topologii na obrázku 1 jsou všechny směrovače nakonfigurovány tak, aby podporovaly směrování OSPF.

Rychlý pohled na směrovací tabulku R1, jak je ukázáno na obrázku 2, ukazuje, že nepřidává žádné cesty OSPF. Existuje několik důvodů, proč by to mohlo být. Předpokladem pro vytvoření sousedního vztahu mezi dvěma směrovači je však připojení 3. vrstvy OSI.

Výstup na obrázku 3 potvrzuje, že rozhraní S0/0/0 je zapojeno a aktivní. Úspěšný ping také potvrzuje, že je aktivní sériové rozhraní R2. Úspěšný ping neznamená, že se vytvoří soused-

ství, protože je možné mít překrývající se podsítě. Ještě musíte ověřit, zda rozhraní připojených zařízení sdílí stejnou podsíť. Pokud ping nebyl úspěšný, zkontrolujte kabeláž a zkontrolujte, zda jsou rozhraní připojených zařízení správně nakonfigurována a funkční.

Pro rozhraní, které má být povoleno pro OSPF, musí být v rámci procesu směrování OSPF, nakonfigurován odpovídající příkaz sítě. Aktivní rozhraní OSPF lze ověřit pomocí příkazu ***show ip ospf interface***. Výstup na obrázku 4 ověřuje, že rozhraní S0/0/0 je povoleno pro OSPF. Pokud nejsou povolena propojená rozhraní na dvou směrovačích, nebudou tvořit sousedství.

Ověřte nastavení OSPF pomocí příkazu ***show ip protocols***. Výstup zobrazený na obrázku 5 ověřuje, že OSPF je povolen a také uvádí seznam sítí, které jsou inzerovány jako povolené. Pokud adresa IP v rozhraní spadá do sítě, která byla povolena pro OSPF, rozhraní bude povoleno pro OSPF.

Všimněte si však, že rozhraní S0/0/0 je uvedeno jako pasivní. Připomeňme, že příkaz pasivního rozhraní zastaví jak odchozí, tak i příchozí směrování aktualizací, protože účinek příkazu způsobí, že směrovač přestane odesílat a přijímat Hello pakety. Z tohoto důvodu se směrovače nestanou sousedy.

Chcete-li rozhraní zakázat jako pasivní, použijte příkaz ***no passive-interface***, konfigurace směrovače, jak je znázorněno na obrázku 6. Po vypnutí pasivního rozhraní se směrovače přidruží, jak ukazuje automaticky generovaná informační zpráva.

Rychlé ověření směrovací tabulky, jak je znázorněno na obrázku 7, potvrzuje, že OSPF nyní vyměňuje informace o směrování.

Dalším problémem, který může nastat, je situace, kdy dva sousední směrovače mají na svých propojovacích rozhraních nesprávné rozměry MTU. Velikost MTU je největší paket síťové vrstvy, který směrovač předá každé rozhraní. Směrovače mají výchozí velikost MTU 1500 bajtů. Tuto hodnotu však lze změnit pro pakety IPv4 pomocí příkazu konfigurace ***ip mtu sizeinterface*** nebo příkazu ***ipv6 mtu sizeinterface*** pro pakety IPv6. Pokud by dva propojovací směrovače neměli hodnoty MTU a pokoušeli by se vytvořit přilehlost, ale neměly by si vyměnit své LSDB a sousední vztah by selhal.

12.3.2.2 Řešení Problémů se Směrovacími Tabulkami OSPF

V topologii na obrázku 1, jsou všechny směrovače nakonfigurovány tak, aby podporovaly směrování OSPF.

Stručný pohled na směrovací tabulku R1 (Obrázek 2) ukazuje, že přijímá výchozí informace o trase, R2 (172.16.2.0/24) a spojení mezi R2 a R3 (192.168.10.8/30). Však neobdrží trasu R3.

Výstup na obrázku 3 ověří nastavení OSPF na R3. Všimněte si, že R3 inzeruje pouze spojení mezi R3 a R2. Neinformuje síť R3 (192.168.1.0/24).

Pro rozhraní, které má být povoleno pro OSPF, musí být v rámci procesu směrování OSPF nakonfigurován odpovídající příkaz sítě. Výstup na obrázku 4 potvrzuje, že R3 není inzerována v OSPF.

12.3.3 Řešení Problémů Směrovaní v Jedno-Oblastní OSPFv3

12.3.3.1 Příkazy Řešení Problémů OSPFv3

Viz referenční topologie OSPFv3.

Odstraňování problémů OSPFv3 je téměř totožné s OSPFv2. Proto mnoho příkazů OSPFv2 a kritéria odstraňování problémů platí také pro OSPFv3.

Například, toto jsou následující ekvivalentní příkazy používané s OSPFv3:

- ***show ipv6 protocols*** (Obrázek 2) - Tento příkaz se používá k ověření zásadních informací o konfiguraci OSPFv3, včetně ID procesu OSPFv3, ID směrovače a rozhraní, ze kterých směrovač přijímá aktualizace.
- ***show ipv6 ospf neighbor*** (Obrázek 3) - Používá se k ověření, že směrovač vytvořil přidružení se sousedním směrovačem. Tento výstup zobrazuje ID sousedního směrovače, sousedskou prioritu, stav OSPFv3, Dead časovač, ID sousedního rozhraní a rozhraní, kterému je soused přístupný. Pokud není identifikátor směrovače sousedního směrovače zobrazen nebo pokud se nezobrazuje jako stav FULL nebo 2WAY, oba směrovače nevytvořily sousední OSPFv3. Pokud dva směrovače nedosahují sousednosti, informace o stavu spojení se nezmění. Neúplné databáze odkazových stavů mohou způsobit nepřesné stromy SPF a směrovací tabulky. Trasy do cílových sítí nemusí existovat, nebo nemusí být nejoptimálnějšími cestami.
- ***Show ipv6 ospf interface*** (Obrázek 4) - Používá se k zobrazení OSPFv3 parametrů nakonfigurovaných na rozhraní, jako je ID procesního protokolu OSPFv3, jemuž je rozhraní přiřazeno. Oblast, ve které se rozhraní nachází, metriku rozhraní a Hello a Dead intervaly. Přidání názvu a čísla rozhraní k příkazu zobrazuje výstup pro určité rozhraní.

- ***show ipv6 ospf*** (Obrázek 5) - Používá se k prozkoumání ID procesu protokolu OSPF a ID směrovače, stejně jako informace o přenosu LSA.
- ***show ipv6 route ospf*** (Obrázek 6) - Používá se k zobrazení pouze naučených cest OSPFv3 ve směrovací tabulce. Výstup ukazuje, že R1 se prostřednictvím OSPFv3 dozvěděl o čtyřech vzdálených sítích.
- ***clear ipv6 ospf [process-id] process*** - slouží k resetování sousedních přidružení OSPFv3.

12.3.3.2 Řešení Problémů s OSPFv3

V topologii na obrázku 1 jsou všechny směrovače nakonfigurovány tak, aby podporovaly směrování OSPFv3.

Rychlý pohled na směrovací tabulku R1 IPv6 (Obrázek 2) ukazuje, že obdrží výchozí trasu, R2 (2001:DB8:CAFE:2::/64) a spojení mezi R2 a R3 (2001:DB8:CAFE:A002::/64). Ovšem neobdrží trasu R3 OSPFv3 (2001:DB8:CAFE:3::/64).

Výstup na obrázku 3 ověřuje nastavení OSPFv3 na R3. Všimněte si, že OSPF je povoleno pouze na rozhraní S0/0/1. Zdá se, že na rozhraní R3 G0/0 není povoleno.

Na rozdíl od OSPFv2, OSPFV3 nepoužívá síťový příkaz. Místo toho je OSPFv3 povolen přímo na rozhraní. Výstup na obrázku 4 potvrzuje, že rozhraní R3 není povoleno pro OSPFv3.

Příklady na obrázku 5 umožňují OSPFv3 rozhraní R3 Gigabit Ethernet 0/0. R3 by nyní měl inzerovat R3 na své sousedy OSPFv3.

12.4 Shrnutí

12.4.1 Shrnutí

12.4.1.1 Shrnutí

OSPF definuje pět typů sítí: point-to-point, více přístupové vysílání, více přístupové ne-vysílání, point-to-multipoint a virtuální linky.

Více přístupové sítě, mohou pro OSPF vyvolat dvě výzvy týkající se zaplavení LSA: vytvoření více přílivů a rozsáhlé zaplavení LSA. Řešením řízení počtu sousedních objektů a zaplavení LSA ve více přístupové síti je DR a BDR. Pokud DR zastaví výrobu Hello paketů, BDR se propaguje a převezme roli DR.

Směrovače v síti, zvolí směrovač s nejvyšší prioritou rozhraní, jako DR. Ten s druhou nejvyšší prioritou rozhraní je zvolen BDR. Čím vyšší je priorita, tím pravděpodobněji bude zvolen, jako DR. Je-li nastavena na hodnotu 0, směrovač se nemůže stát DR. Výchozí priorita více přístupových vysílacích rozhraní je 1. Protože není-li nastaveno jinak, všechny směrovače mají stejnou hodnotu priority a musí se při volbách DR/BDR spoléhat na jinou metodu přerušení. Pokud jsou priority rozhraní stejné, pak je směrovač s nejvyšším ID zvolen DR. Ten s druhým nejvyšším ID je BDR. Přidání nového směrovače nezahájí nový volební proces.

Chcete-li propagovat výchozí trasu v OSPF, musí být směrovač nakonfigurován s výchozí statickou trasou a příkaz ***default-information originate*** musí být přidán do konfigurace. Ověřte trasy pomocí příkazu ***show ip route*** nebo ***show ipv6 route***.

Aby byl OSPF nápomocný při správném určování cesty, musí být referenční šířka pásma změněna na vyšší hodnotu, aby vyhovovala sítím s linkami rychlejší než 100 Mb/s. Chcete-li upravit referenční šířku pásma, použijte příkaz ***autocost reference-bandwidth Mbps***. Chcete-li upravit šířku pásma rozhraní, použijte příkaz ***bandwidth kilobits***. Metriku lze ručně nakonfigurovat na rozhraní pomocí příkazu režimu konfigurace rozhraní ***ip ospf cost hodnota***.

Intervaly Hello a Dead, musí odpovídat nebo se sousední přidružení nevyskytuje. Chcete-li tyto intervaly upravit, použijte následující příkazy rozhraní:

- ***ip ospf hello-interval*** sekundy
- ***ip ospf dead-interval*** sekundy
- ***ipv6 ospf hello-interval*** sekundy
- ***ipv6 ospf dead-interval*** sekund

OSPF podporuje 3 typy ověřování: Null, jednoduché ověřování pomocí hesla a ověřování MD5. Ověření MD5 lze konfigurovat globálně nebo na rozhraní. Chcete-li ověřit, zda je implementace MD5 povolena, použijte příkaz ***show ip ospf interface***.

Při odstraňování problémů se sousedy OSPF si uvědomte, že stavy FULL nebo 2WAY jsou normální. Následující příkazy shrnují odstraňování problémů OSPF protokolu IPv4:

- ***show ip protocols***
- ***show ip ospf neighbor***
- ***show ip ospf interface***
- ***show ip ospf***

- ***show ip route ospf***
- ***clear ip ospf [process-id] process***

Odstraňování problémů v OSPFv3 je podobné OSPFv2. Následující příkazy jsou ekvivalentní příkazy používané s protokolem OSPFv3: ***show ipv6 protocols, show ipv6 ospf neighbor, show ipv6 ospf interface, show ipv6 ospf, show ipv6 route ospf a clear ipv6 ospf [process-id] process***.

13 KAPITOLA 6 – VÍCE-OBLASTNÍ OSPF

13.1 Více-Oblastní OSPF

13.1.1 Úvod

13.1.1.1 Úvod

Více přístupové OSPF, se používá k rozdělení velké sítě OSPF. Příliš mnoho směrovačů v jedné oblasti zvyšuje zatížení procesoru a vytváří velkou databázi linek. V této kapitole jsou uvedeny pokyny pro efektivní rozdělení velké jednotlivé oblasti do více oblastí. Prostor 0, který se používá v jedno-oblastním OSPF, je znám jako oblast páteře.

Diskuse je zaměřena na výměnu LSA mezi oblastmi. Kromě toho jsou k dispozici funkce pro konfiguraci OSPFv2 a OSPFv3. Tato kapitola se zakončuje zobrazovacími příkazy použitými k ověření konfigurace OSPF.

13.2 Operace Více-Oblastního OSPF

13.2.1 Proč Více-Oblastní OSPF?

13.2.1.1 Jedno-Oblastní OSPF

Jedno-oblastní OSPF je užitečný v menších sítích, kde není spojení směrovače složité a cesty k jednotlivým cílům lze snadno odvodit.

Pokud je však oblast příliš velká, musí být vyřešeny následující problémy (viz obrázek pro ilustraci):

- **Velká směrovací tabulka** - OSPF ve výchozím nastavení nevykonává shrnutí trasy. Pokud trasy nejsou shrnuty, směrovací tabulka může být velmi velká, v závislosti na velikosti sítě.
- **Velká databáze stavů linek (LSDB)** - Vzhledem k tomu, že LSDB pokrývá topologii celé sítě, musí každý směrovač udržovat záznam pro každou síť v oblasti, i když není pro každou směrovou tabulku vybrána žádná trasa.
- **Časté výpočty algoritmu SPF** - Ve velké síti jsou změny nevyhnutelné, takže směrovače stráví mnoho cyklů procesoru, které přepočítávají algoritmus SPF a aktualizují směrovací tabulku.

Aby OSPF bylo efektivnější a škálovatelnější, podporuje hierarchické směrování pomocí oblastí. Oblast OSPF je skupina směrovačů, které sdílejí stejné informace o stavu propojení v databázích stavů linek.

13.2.1.2 Více Oblastní OSPF

Pokud je velká oblast OSPF rozdělena na menší, nazývá se více oblastní OSPF. Je užitečný pro rozsáhlejší nasazení v síti, čímž se sníží režie zpracování a paměti.

Například kdykoli směrovač obdrží nové informace o topologii, stejně jako s přidáním, odstraněním nebo úpravami linky, musí směrovač znovu spustit algoritmus SPF, vytvořit nový strom SPF a aktualizovat směrovací tabulku. Algoritmus SPF je náročný na procesor a čas potřebný k výpočtu závisí na velikosti oblasti. Příliš mnoho směrovačů v jedné oblasti zvětšuje LSDB a tím, zvyšuje zatížení procesoru. Proto uspořádání směrovačů do oblastí efektivně rozděluje jednu potenciálně rozsáhlou databázi do menších a spravovatelnějších databází.

Více oblastní OSPF, vyžaduje hierarchický návrh sítě. Hlavní oblast se nazývá oblast páteře (oblast 0) a všechny ostatní oblasti se musí připojit k ní. Při hierarchickém směrování se stále rozkládá mezi oblastmi (inter area). Zatímco mnoho z nudných směrovacích operací, jako je přepočet databáze, se udržuje v oblasti.

Jak je znázorněno na obrázku 1, hierarchicko-topologické možnosti více oblastních OSPF mají tyto výhody:

- **Menší směrovací tabulky** - Existuje méně položek směrovací tabulky, protože síťové adresy mohou být shrnuty mezi jednotlivými oblastmi. Například R1 shrnuje trasy z oblasti 1 do oblasti 0 a R2 shrnuje trasy z oblasti 51 do oblasti 0. R1 a R2 také propagují výchozí statickou cestu k oblasti 1 a 51.
- **Snížená režie aktualizací odkazových stavů** - Minimalizuje požadavky na zpracování a paměť, protože existuje méně směrovačů, které si LSA vyměňují.
- **Snížená frekvence výpočtů SPF** - lokalizuje dopad změny topologie v oblasti. Například minimalizuje dopad aktualizace směrování, protože zatopení LSA se zastaví na hranici oblasti.

Na obr. 2 předpokládejme, že propojení mezi dvěma interními směrovači v oblasti 51 selže. Pouze směrovače v oblasti 51 vyměňují LSA a znovu spouští algoritmus SPF pro tuto událost. R1 neobdrží LSA z oblasti 51 a nepřepočítává algoritmus SPF.

13.2.1.3 Dvouvrstvá Hierarchie Oblastí OSPF

Více oblastní OSPF je implementováno ve dvouvrstvé hierarchii oblastí:

- **Páteřní (Transit) oblast** - oblast OSPF, jejíž primární funkcí je rychlý a efektivní pohyb IP paketů. Páteřní oblasti jsou propojené s jinými typy oblastí OSPF. Obecně se koncoví uživatelé nenacházejí v oblasti páteře. Páteřní oblast se nazývá také oblast OSPF 0. Hierarchické vytváření sítí definuje oblast 0 jako jádro, na které se přímo připojují všechny ostatní oblasti. (Obrázek 1)
- **Pravidelná oblast (bez páteře)** - spojuje uživatele a zdroje. Pravidelné oblasti jsou obvykle zřízeny podél funkčních nebo geografických skupin. Ve výchozím nastavení pravidelná oblast neumožňuje provoz z jiné oblasti, aby použila své linky k oslovení jiných oblastí. Veškerá doprava z jiných oblastí musí překročit tranzitní oblast. (Obrázek 2)

Poznámka: Pravidelná oblast může mít řadu podtypů, včetně standardní plochy, oblasti stub, totální stub oblasti a oblasti, která není tak zchátralá (NSSA). Stub, totální stub a NSSA jsou mimo rozsah této kapitoly.

OSPF prosazuje tuto rigidní dvouvrstvou hierarchii oblastí. Podkladová fyzická konektivita sítě musí mapovat strukturu dvouvrstvého prostoru se všemi nepatřičnými oblastmi, které se přímo připojují k oblasti 0. Veškerá doprava, která se pohybuje z jedné oblasti do druhé oblasti, musí procházet oblastí páteře. Tento provoz je označován jako interakční provoz.

Optimální počet směrovačů na oblast se liší podle faktorů, jako je stabilita sítě, ale společnost Cisco doporučuje následující pokyny:

- Oblast by neměla mít více než 50 směrovačů.
- Směrovač by neměl být, ve více než třech oblastech.
- Každý směrovač by neměl mít více než 60 sousedů.

13.2.1.4 Typy OSPF Směrovačů

OSPF směrovače různých typů řídí provoz, který vstupuje do a ven z oblastí. Jsou kategorizovány na základě funkce, kterou vykonávají ve směrovací doméně.

Existují čtyři různé typy směrovačů OSPF:

- **Interní směrovač** - Jedná se o směrovač, který má všechny své rozhraní ve stejné oblasti. Všechny interní směrovače v oblasti mají identické LSDB. (Obrázek 1)

- **Páteřní směrovač** - Jedná se o směrovač v oblasti páteře. Páteřní oblast je obecně nastavena na oblast 0. (obrázek 2)
- **Oblastní hraniční směrovač (ABR)** - Jedná se o směrovač, který má rozhraní připojené k více oblastem. Musí udržovat oddělené LSDB pro každou oblast, do které je připojen, a může se pohybovat mezi oblastmi. ABR jsou výstupní body pro oblast, což znamená, že směrovací informace určené pro jinou oblast se tam mohou dostat pouze přes ABR místní oblasti. ABR mohou být konfigurovány tak, aby shrnovaly informace o směrování z LSDB jejich připojených oblastí. Distribuují informace o směrování do páteře. Páteřní směrovače pak předávají informace dalším ABR. Ve více oblastní síti, může oblast mít jeden nebo více ABR. (Obrázek 3)
- **Autonomní systémový hraniční směrovač (ASBR)** - Jedná se o směrovač, který má alespoň jedno rozhraní připojené k externí interní síti (jiný autonomní systém), například k síti OSPF. ASBR může importovat informace o síti OSPF do sítě OSPF a naopak pomocí procesu nazvaného, redistribuce tras. (Obr. 4)

Redistribuce se objevuje, když ASBR spojuje různé směrovací domény (např. EIGRP a OSPF) a konfiguruje je pro výměnu a inzerování směrovacích informací mezi těmito směrovacími doménami.

Směrovač lze klasifikovat jako více než jeden typ. Pokud se například směrovač připojí k oblasti 0 a oblasti 1 a navíc udržuje informace o směrování pro jinou síť než OSPF, spadá pod tři různé klasifikace: páteřní směrovač, ABR a ASBR.

13.2.2 Operace LSA ve Více Oblastním OSPF

13.2.2.1 OSPF Typy LSA

LSA jsou stavebními kameny OSPF LSDB. Individuálně pracují jako záznamy databáze a poskytují specifické informace o síti. V kombinaci popisují celou topologii sítě nebo oblasti OSPF.

RFC pro OSPF aktuálně určují až 11 různých typů LSA (obrázek 1). Každá implementace více oblastního OSPF, však musí podporovat prvních pět LSA: LSA 1 až 5 (obrázek 2). Zaměření tohoto tématu je na těchto prvních pět typů LSA.

Každý směrovač je definován jako typ LSA. LSA obsahuje pole ID linky, které identifikuje podle čísla sítě a masky objekt, ke kterému se připojuje. V závislosti na typu má ID linky

jiný význam. LSA se liší podle toho, jak jsou generovány a propagovány v doméně směrování.

13.2.2.2 OSPF LSA Typ 1

Jak je znázorněno na obrázku, všechny směrovače propagují své přímo propojené propojení OSPF v LSA typu 1 a předávají informace o jejich síti sousedům OSPF. LSA obsahuje seznam přímo připojených rozhraní, typů linek a jejich stavů.

LSA typu 1 jsou také označovány jako položky linek směrovače.

LSA typu 1 jsou zaplaveny pouze v oblasti, ze které pocházejí. ABR následně propagují sítě naučené z LSA typu 1 do jiných oblastí jako LSA typu 3.

ID odkazu LSA typu 1 je identifikován identifikátorem směrovače původního směrovače.

13.2.2.3 OSPF LSA Typ 2

Typ LSA typu 2 existuje pouze u sítí s více přístupovými vysíláními a ne-vysílacími (NBMA), kde je vybrán DR a alespoň dva směrovače v segmentu více přístupů. LSA typu 2 obsahuje identifikátor směrovače a IP adresu DR, spolu s identifikátorem směrovače všech ostatních směrovačů v segmentu více přístupů. Typ 2 LSA je vytvořen pro každou síť více přístupů v oblasti.

Účelem LSA typu 2 je poskytnout jiným směrovačům informace o více přístupových sítích v rámci stejné oblasti.

DR povodně, typu 2 LSA, se nacházejí pouze v oblasti, ze které pocházejí. LSA typu 2 nejsou přesměrovány mimo oblast.

LSA typu 2 jsou také označovány jako položky síťových odkazů.

Jak je znázorněno na obrázku, ABR1 je DR pro síť Ethernet v oblasti 1. Vygeneruje LSA typu 2 a přesune ji do oblasti 1. ABR2 je DR pro síť s více přístupovými kanály v oblasti 0. V oblasti 2 nejsou žádné sítě, a proto se v této oblasti nikdy nepropagují LSA typu 2.

ID stavu linky sítě LSA je IP adresa DR, která jej inzeruje.

13.2.2.4 OSPF LSA Typ 3

LSA typu 3, používají ABR pro inzerci sítí z jiných oblastí. ABR sbírají LSA typu 1 v LSDB. Poté, co oblast OSPF konvergovala, ABR vytvoří LSA typu 3 pro každou ze svých naučených sítí. Proto musí ABR s mnoha cestami, vytvářet LSA typu 3 pro každou síť.

Jak je znázorněno na obrázku, ABR1 a ABR2 zaplavují LSA typu 3 z jedné oblasti do jiných oblastí. ABR propagují LSA typu 3 do jiných oblastí. Při rozsáhlém nasazení OSPF s mnoha sítěmi mohou propagace LSA typu 3 způsobit významné problémy s povodněmi. Z tohoto důvodu se důrazně doporučuje nakonfigurovat manuální shrnutí trasy na ABR.

ID stavu linky je nastaveno na číslo sítě a inzeruje se také maska.

Přijímání LSA typu 3 do jeho oblasti nezpůsobuje směrovači spuštění algoritmu SPF. Trasy inzerované v LSA typu 3 jsou vhodně přidány nebo smazány ze směrovací tabulky směrovače, ale úplný výpočet SPF není nutný.

13.2.2.5 OSPF LSA Typ 4

LSA typu 4 a typu 5 se používají společně k identifikaci ASBR a inzerování externích sítí do směrovací domény OSPF.

Souhrnný typ LSA typu 4, je generován systémem ABR pouze tehdy, pokud existuje ASBR v oblasti. LSA typu 4 identifikuje ASBR a poskytuje k němu cestu. Celý provoz určený pro externí autonomní systém vyžaduje znalost směrovací tabulky ASBR, která vznikla z vnějších tras.

Jak je znázorněno na obrázku, ASBR pošle LSA typu 1, identifikující se jako ASBR. LSA obsahuje speciální bit známý jako externí bit (e bit), který se používá k identifikaci směrovače jako ASBR. Když ABR1 obdrží LSA typu 1, zaznamená e bit, vytvoří typ LSA typu 4 a zatopí páteř (oblast 0) LSA typu 4. Následné ABR zaplavují jiné oblasti LSA typu 4.

ID stavu propojení je nastaveno na ID směrovače ASBR.

13.2.2.6 OSPF LSA Typ 5

Externí LSA typu 5, popisují cesty do sítí mimo autonomní systém OSPF. LSA typu 5 pochází z ASBR a zaplavují celý autonomní systém.

LSA typu 5 jsou také označovány jako autonomní systémové externí položky LSA.

Na obrázku, ASBR generuje LSA typu 5, pro každou ze svých vnějších cest a zaplavuje její oblast. Následné ABR také zaplavují jiné oblasti LSA typu 5. Směrovače v ostatních oblastech používají informace z modelu LSA typu 4 k dosažení vnějších tras.

V rozsáhlém nasazení OSPF s mnoha sítěmi může propagace více LSA typu 5 způsobit významné problémy se zaplavením. Z tohoto důvodu se důrazně doporučuje nakonfigurovat ruční shrnutí trasy na ASBR.

13.2.3 Směrovací Tabulka a Typy Cest OSPF

13.2.3.1 Vstupy Směrovací Tabulky OSPF

Obrázek 1 poskytuje ukázkovou směrovací tabulku pro více oblastní topologii OSPF s odkazem na externí síť, která není OSPF. Trasy v směrovací tabulce IPv4, jsou identifikovány pomocí následujících deskriptorů:

- **O-** LSA směrovače (typ 1) a sítě (typ 2) LSA popisují podrobnosti v rámci oblasti. Směrovací tabulka odráží tuto informaci o stavu spojení s označením O, což znamená, že trasa je uvnitř oblasti.
- **O IA** - Když ABR obdrží souhrnné LSA, přidá je do LSDB a generuje je do místní oblasti. Když ABR přijímá externí LSA, přidá je do LSDB a zaplavuje s nimi oblast. Interní směrovače pak asimilují informace do svých databází. Shrnutí LSA se ve směrovací tabulce objevují jako IA (trasy interakce).
- **O E1** nebo **O E2** - Externí LSA se objeví ve směrovací tabulce označené jako vnější cesty typu 1 (E1) nebo externí trasy typu 2 (E2).

Obrázek 2, zobrazuje směrovací tabulku protokolu IPv6 se záznamy směrovače OSPF, interní oblasti a externí směrovací tabulky.

13.2.3.2 Výpočet Cest OSPF

Každý směrovač používá k vytvoření stromu SPF, algoritmus SPF, proti LSDB. Strom slouží k určení nejlepších cest.

Jak je znázorněno na obrázku, pořadí, ve kterém jsou vypočteny nejlepší cesty, je následující:

1. Všechny směrovače vypočítají nejlepší cesty k cílům v rámci své oblasti (uvnitř oblasti) a přidávají tyto položky do směrovací tabulky. Jedná se o LSA typu 1 a 2, které jsou ve směrovací tabulce uvedeny se směrovacím označením O. (1)

2. Všechny směrovače vypočítají nejlepší cesty k ostatním oblastem sítě. Tyto nejlepší cesty jsou záznamy o trase interní oblasti, nebo LSA typu 3 a 4 a jsou označeny směrovacím označením OIA. (2)

3. Všechny směrovače (s výjimkou těch, které jsou ve formě vyčnívající oblasti) vypočítávají nejlepší cesty k cíli externího autonomního systému (typ 5). Ty jsou označeny buď označením trasy O E1 nebo O E2, v závislosti na konfiguraci. (3)

13.3 Konfigurace Více Oblastních OPSF

13.3.1 Konfigurace Více Oblastních OSPF

13.3.1.1 Implementace Více Oblastních OSPF

OSPF může být implementován jako jedno-oblastní nebo více oblastní. Typ zvolené implementace OSPF závisí na konkrétních požadavcích a stávající topologii.

Existují 4 kroky k implementaci více oblastního OSPF, jak je zobrazeno na obrázku.

Kroky 1 a 2 jsou součástí procesu plánování.

Krok 1. Získejte síťové požadavky a parametry - To zahrnuje určení počtu hostitelských a síťových zařízení, schématu IP adresování, velikost směrovací domény, velikost směrovacích tabulek, riziko změn topologie a další charakteristiky sítě.

Krok 2. Definujte parametry OSPF - Na základě informací shromážděných během Kroku 1 musí správce sítě určit, zda je upřednostňovanou implementací OSPF s jednou nebo více oblastmi. Je-li vybráno více, je třeba při určování parametrů OSPF zohlednit správce sítě, který zahrnuje:

- **Plán IP adresování** - To řídí, jak může být OSPF nasazeno a jak může být rozmístění měněno. Musí být vytvořen podrobný plán IP adresace spolu s informacemi o IP podsíti. Dobrý plán IP adresace by měl umožnit využití návrhu a sumarizace více oblastí. Tento plán snadněji měří síť, optimalizuje chování OSPF a šíření LSA.
- **Oblasti OSPF** - Rozdělení sítě OSPF do oblastí, snižuje velikost LSDB a omezuje šíření aktualizací stavů linek, při změně topologie. Musí být identifikovány směrovače, které mají být ABR a ASBR, stejně jako ty, které mají provést jakákoli shrnutí nebo redistribuci.
- **Topologie sítě** - sestává z linek, které propojují síťové zařízení a patří do různých oblastí OSPF v návrhu více oblastní sítě. Topologie je důležitá pro určení primárních a záložních linek. Primární a záložní linky, jsou definovány změnami metrik OSPF na rozhraních. Podrobný plán topologie sítě by měl být také použit, k určení různých oblastí OSPF, ABR a ASBR, stejně jako ke shrnutí a redistribuci bodů, pokud se používá.

Krok 3. Nakonfigurujte implementaci více oblastního OSPF, na základě parametrů.

Krok 4. Ověřte implementaci OSPF na základě parametrů.

13.3.1.2 Konfigurace Více Oblastních OSPF

Obr. 1 zobrazuje referenční topologie OSPF s více oblastmi. V tomto příkladu:

- R1 je ABR, protože má rozhraní v oblasti 1 a rozhraní v oblasti 0.
- R2 je interní páteřní směrovač, protože všechna jeho rozhraní jsou v oblasti 0.
- R3 je ABR, protože má rozhraní v oblasti 2 a rozhraní v oblasti 0.

Neexistují žádné speciální příkazy potřebné pro implementaci této síti. Směrovač se jednoduše stává ABR, pokud má v různých oblastech dvě síťová hlášení.

Jak je znázorněno na obrázku 2, R1 je přiřazeno ID směrovače 1.1.1.1. Tento příklad umožňuje fungování, ve dvou LAN rozhraních v oblasti 1. Sériové rozhraní je nakonfigurováno jako součást oblasti OSPF 0. Protože R1, má rozhraní připojená ke dvěma různým oblastem a je to ABR.

Použijte kontrolu syntaxe na Obr. 3, pro konfiguraci více oblastního OSPF na R2 a R3. V této kontrole syntaxe, na R2, použijte zástupnou masku adresy síťové adresy. Na R3 použijte zástupnou masku 0.0.0.0 pro všechny sítě.

Po dokončení konfigurace R2 si všimněte informativních zpráv informujících o sousedství s R1 (1.1.1.1).

Po dokončení konfigurace R3 si všimněte informačních zpráv, které informují o sousedství s R2 (2.2.2.2). Také si všimněte, jak schéma IP adresace použité pro identifikátor směrovače usnadňuje identifikaci souseda.

Poznámka: Inverzní masky zástupných znaků používané pro konfiguraci R2 a R3 se úmyslně liší, aby prokázaly dvě alternativy, k zadávání příkazů sítě. Metoda použitá pro R3 je jednodušší, protože zástupná maska je vždy 0.0.0.0 a nemusí být vypočtena.

13.3.1.3 Konfigurace Více Oblastních OSPFv3

Stejně jako OSPFv2 je implementace více oblastní topologie OSPFv3 na obr. 1 jednoduchá. Neexistují žádné speciální příkazy. Směrovač se jednoduše stává ABR, pokud má dvě rozhraní v různých oblastech.

Například na obrázku 2, je R1 přiřazen směrovači ID 1.1.1.1. Příklad také umožňuje OSPF na rozhraní LAN v oblasti 1 a sériové rozhraní v oblasti 0. Vzhledem k tomu, že R1 má rozhraní propojená se dvěma různými oblastmi, stává se to ABR.

Použijte kontrolu syntaxe na Obr. 3, pro konfiguraci více oblastní OSPFv3 na R2 a R3.

Po dokončení konfigurace R2 si všimněte zprávy, že existuje sousedství s R1 (1.1.1.1).

Po dokončení konfigurace R3 si všimněte zprávy, že existuje sousedství s R2 (2.2.2.2).

13.3.2 Shrnutí OSPF Cesty

13.3.2.1 Sumarizace OSPF Cesty

Sumarizace pomáhá udržovat směrovací tabulky malé. Jedná se o konsolidaci několika cest do jedné reklamy, která pak může být propagována do oblasti páteře.

Obvykle jsou LSA typu 1 a typu 2 generovány uvnitř každé oblasti, přeloženy do LSA typu 3 a odeslány do jiných oblastí. Pokud by oblast 1 měla 30 reklamních sítí, pak by bylo do páteře předáno 30 LSA typu 3. Se shrnutím trasy ABR konsoliduje 30 sítí do jedné ze dvou reklam.

Na obr. 1, R1 konsoliduje všechny síťové reklamy do jednoho souhrnného LSA. Namísto předávání jednotlivých LSA pro každou trasu v oblasti 1, R1 předá souhrnnou LSA do jádrového směrovače C1. C1 postupně předává souhrnné LSA z R2 a R3. R2 a R3, je pak předá do svých vnitřních směrovačů.

Sumarizace také pomáhá zvýšit stabilitu sítě, protože snižuje zbytečné zaplavení LSA. To přímo ovlivňuje množství kapacity šířky pásma, CPU a paměti spotřebované procesem směrování OSPF. Bez sumarizace tras, je každý LSA specifického spojení, propagován do OSPF páteře a dále, což způsobuje zbytečnou síťovou komunikaci.

Na obr. 2 selže síťové spojení na R1a. R1a pošle LSA na R1. Avšak, R1 nešíří aktualizace, protože má nakonfigurovanou souhrnnou cestu. Specifické zaplavení propojení LSA mimo oblast se neobjevuje.

13.3.2.2 Sumarizace Interní a Externí Cesty

V OSPF, lze shrnutí konfigurovat pouze na ABR nebo ASBR. Namísto šíření mnoha specifických sítí, směrovače ABR a ASBR propagují souhrnnou trasu. Směrovače ABR shrnují typy LSA a směrovače ASBR shrnující LSA typu 5.

Ve výchozím nastavení souhrnné LSA (typu 3) a externí LSA (typu 5) neobsahují shrnuté (agregované) trasy. Ve výchozím nastavení souhrnné LSA nejsou shrnuty.

Jak je znázorněno na obrázcích 1 a 2, shrnutí trasy lze nakonfigurovat takto:

- **Sumarizace trasy vnitřní oblasti** – Sumarizace vnitřní trasy se vyskytuje na ABR a vztahuje se na trasy z každé oblasti. Nevztahuje se na externí trasy, které jsou do

systému OSPF vkládány prostřednictvím redistribuce. Chcete-li provést účinnou sumarizaci interaktivních tras, síťové adresy v rámci oblastí by měly být přiděleny souvisle, aby mohly být tyto adresy shrnuty do minimálního počtu souhrnných adres.

- **Sumarizace Externí trasy** - Sumarizace externích tras je specifická pro externí trasy, které jsou zasílány do OSPF, prostřednictvím redistribuce tras. Opět je důležité zajistit souvislost externích rozsahů adres, které jsou sumarizovány. Obecně pouze ASBR, shrnují vnější trasy. Jak je ukázáno na obrázku 2, externí cesty EIGRP jsou shrnuty ASBR R2 v jediném LSA a odeslány do R1 a R3.

Poznámka: Souhrnná externí trasa je na ASBR, konfigurována pomocí příkazu ***summary-address adresa maska***.

13.3.2.3 Sumarizace Cesty Interní Oblasti

OSPF neprovádí automatické shrnutí. Shrnutí interní cesty musí být ručně nakonfigurováno na ABR.

Shrnutí vnitřních cest pro distribuci interní oblasti, může být provedeno pouze na ABR. Když je shrnutí nakonfigurováno na ABR, do oblasti páteře je vstřikován jediný LSA typu 3, který popisuje souhrnnou cestu. Více cest uvnitř oblasti je shrnuto jedním LSA.

Souhrnná trasa je generována, pokud nejméně jedna podsíť v oblasti spadá do rozsahu souhrnných adres. Shrnutá metrika trasy se rovná nejnižší ceně všech podsítí v rámci rozsahu souhrnných adres.

Poznámka: ABR může pouze shrnout trasy, které jsou v oblastech k němu připojených.

Obrázek 1 znázorňuje víceúrovňovou topologii OSPF. Směrovací tabulky R1 a R3 se zkoumají, aby se zjistila účinnost shrnutí.

Obrázek 2 zobrazuje směrovací tabulku R1 před načtením shrnutí, zatímco obrázek 3 zobrazuje směrovací tabulku R3. Všimněte si, jak má R3 v současné době dvě sítě interakcí se sítí R1 a oblastí 1.

13.3.2.4 Výpočet Celkové Cesty

Obrázek ukazuje, že shrnutí sítí do jedné adresy a masky lze provést ve třech krocích:

Krok 1. Seznam sítí v binárním formátu. V příkladu jsou dvě oblasti sítě, s adresami 10.1.1.0/24 a 10.1.2.0/24, uvedeny v binárním formátu.

Krok 2. Počítá se počet dalekých odpovídajících bitů pro určení masky souhrnné trasy. Jak bylo zdůrazněno, prvních 22 bitů zleva odpovídá shodě. Výsledkem je prefix **/22** nebo maska podsítě **255.255.252.0**.

Krok 3. Zkopírujte shodné bity a potom přidejte nulové bity pro určení sumarizace síťové adresy. V tomto příkladu mají odpovídající bity s nulami na konci síťovou adresu 10.1.0.0/22. Tato souhrnná adresa shrnuje čtyři sítě: 10.1.0.0/24, 10.1.1.0/24, 10.1.2.0/24 a 10.1.3.0/24.

V příkladu, souhrnná adresa odpovídá čtyřem sítím, i když existují pouze dvě sítě.

13.3.2.5 Shrnutí Konfigurace Cesty Interní Oblasti

Na obr. 1, aby byl demonstrován efekt shrnutí trasy, je R1 konfigurován tak, aby sumarizoval cesty vnitřní oblasti 1.

Chcete-li manuálně nakonfigurovat souhrn interakcí na trase ABR, použijte ***příkaz area id-oblasti range adresa maska***. To instruuje ABR, aby shrnul cesty pro konkrétní oblast, před tím, než je vstříkne do jiné oblasti, prostřednictvím páteře jako souhrnné LSA typu 3.

Poznámka: V OSPFv3 je příkaz identický kromě síťové adresy IPv6. Syntaxe příkazu pro OSPFv3 je ***area id-oblasti range prefix***.

Obrázek 2 shrnuje dvě trasy interní oblasti 1, do jedné souhrnné trasy interakcí OSPF na R1. Souhrnná cesta 10.1.0.0/22 ve skutečnosti shrnuje čtyři síťové adresy, 10.1.0.0/24 až 10.1.3.0/24.

Obrázek 3 zobrazuje trasy OSPF ze směrovací tabulky IPv4 na R1. Všimněte si, jak se objevila nová položka s ukončovacím rozhraním Null0. Aplikace Cisco IOS automaticky vytvoří souhrnnou cestu k rozhraní Null0, pokud je nakonfigurováno manuální shrnutí, aby se zabránilo smyčkám směrování. Paket odeslaný do nulového rozhraní je vynechán.

Předpokládejme například, že R1 obdržel balíček určený pro 10.1.0.10. I když by odpovídala R1 souhrnné trase, nemá další platnou trasu v oblasti 1. Proto by se odkazoval na směrovací tabulku pro další nejdelší shodu, co by byla položka Null0. Paket by byl předán do rozhraní Null0 a byl by vypuštěn. Zabraňuje tomu, aby směrovač předával paket na výchozí trasu a případně vytvořil směrovací smyčku.

Obrázek 4 zobrazuje aktualizovanou směrovací tabulku R3. Všimněte si, jak nyní do souhrnné trasy 10.1.0.0/22, jde pouze jedna interakce. Přestože tento příklad pouze snížil směrovací tabulku o jeden záznam, mohlo by být provedeno shrnutí pro shrnutí mnoha sítí. To by snížilo velikost směrovacích tabulek.

Pomocí kontroly syntaxe na obrázku 5, shrňte trasy oblasti 2 na R3.

13.3.3 Verifikace Více Oblastního OSPF

13.3.3.1 Verifikace Více Oblastního OSPF

Stejné ověřovací příkazy, které se používají k ověření OSPF pro jednu oblast, lze také použít pro ověření více oblastní topologie OSPF na obrázku:

- ***show ip ospf neighbor***
- ***show ip ospf***
- ***show ip ospf interface***

Příkazy, které ověřují specifické informace více oblastí, zahrnují:

- ***show ip protocols***
- ***show ip ospf interface brief***
- ***show ip route ospf***
- ***show ip ospf database***

Poznámka: Pro ekvivalentní příkaz v OSPFv3 jednoduše nahraďte ip, ipv6.

13.3.3.2 Verifikace Hlavních Nastavení Více Oblastního OSPF

Pomocí příkazu, ***show ip protocols,*** ověřte stav OSPF. Výstup příkazu odhaluje, které směrovací protokoly jsou konfigurovány na směrovači. Zahrnuje také specifikace směrovacího protokolu, jako je ID směrovače, počet oblastí ve směrovači a sítě zahrnuté v konfiguraci směrovacího protokolu.

Obrázek 1 zobrazuje nastavení OSPF na R1. Všimněte si, že příkaz ukazuje, že existují dvě oblasti. Sekce Směrování pro Sítě, označuje sítě a jejich příslušné oblasti.

Použijte krátký příkaz ***show ip ospf interface brief***, pro zobrazení stručných informací, týkajících se rozhraní OSPF. Tento příkaz odhaluje užitečné informace, jako je ID procesního protokolu OSPF, jemuž je rozhraní přiřazeno. A oblast, které jsou rozhraní součástí, a metriku rozhraní.

Obr. 2, ověřuje rozhraní podporující protokol OSPF a oblasti, ke kterým patří.

Pomocí kontroly syntaxe na obr. 3, ověřte obecná nastavení R2 a R3.

13.3.3.3 Verifikace Cest OSPF

Nejběžnějším příkazem, který se používá k ověření konfigurace OSPF pro více oblastí, je příkaz ***show ip route***. Přidání parametru ***ospf*** zobrazuje pouze informace týkající se OSPF.

Obrázek 1 zobrazuje směrovací tabulku R1. Všimněte si, jak záznamy **O IA** v směrovací tabulce určují sítě naučené z jiných oblastí. Konkrétně **O** představuje trasy OSPF a **IA** představuje interní oblasti, což znamená, že cesta pochází z jiné oblasti. Připomeňme se, že R1 je v oblasti 0 a podsítě 192.168.1.0 a 192.168.2.0 jsou připojeny k R3 v oblasti 2. Položka [110/1295] ve směrovací tabulce představuje administrativní vzdálenost, která je přiřazena OSPF (110) a Celkovou metriku trasy (metrika 1295).

Pomocí kontroly syntaxe na Obr. 2, ověřte směrovací tabulku R2 a R3, příkazem ***show ip route ospf***.

13.3.3.4 Verifikace LSDB Více Oblastního OSPF

Pomocí příkazu ***show ip ospf database*** ověřte obsah LSDB.

V příkazu ***show ip ospf database*** je k dispozici mnoho možností.

Například obrázek 1 zobrazuje obsah LSDB na R1. Oznámení R1, má vstupy pro oblast 0 a oblast 1, protože ABR musí udržovat samostatnou LSDB pro každou oblast, do které patří. Ve výstupu identifikuje tři směrovače, v sekci Stavů Linek Směrování. Sekce Shrnutí Stavu Síťových Linek, identifikuje sítě naučené z jiných oblastí a který soused inzerovala síť.

Pomocí kontroly syntaxe na obrázku 2, ověřte LSDB na R2 a R3 pomocí příkazu ***show ip ospf database***. R2 má pouze rozhraní v oblasti 0. Proto je zapotřebí pouze jedna LSDB. Stejně jako R1 a R3 obsahuje dvě LSDB.

13.3.3.5 Verifikace Více Oblastního OSPFv3

Podobně jako OSPFv2 poskytuje OSPFv3 podobné ověřovací příkazy. Viz referenční topologie OSPFv3 na obrázku 1.

Obrázek 2, zobrazuje nastavení OSPFv3 pro R1. Všimněte si, že příkaz potvrzuje, že existují dvě oblasti. Rovněž identifikuje každé rozhraní povolené pro danou oblast.

Obrázek 3, ověřuje rozhraní podporující OSPFv3 a oblast, do které patří.

Obrázek 4, zobrazuje směrovací tabulku R1. Všimněte si, jak směrovací tabulka IPv6 zobrazuje položky **OI** ve směrovací tabulce pro identifikaci sítí naučených z jiných oblastí. Konkrétně **O** představuje trasy OSPF a **I** představuje interní oblasti, což znamená, že cesta pochází z jiné oblasti. Připomeňme si, že R1 je v oblasti 0 a podsíť 2001: DB8: CAFE3 ::/64 je připojena k R3 v oblasti 2. Položka [110/1295] ve směrovací tabulce představuje administrativní vzdálenost, která je přiřazena OSPF (110). A celkovou metrika trasy (1295).

Obrázek 5, zobrazuje obsah LSDB na R1. Příkaz nabízí podobné informace jako protějšek OSPFv2. Ovšem v OSPFv3, LSDB obsahuje další typy LSA, které nejsou k dispozici v OSPFv2.

13.4 Shrnutí

13.4.1 Shrnutí

13.4.1.1 Shrnutí

Jednoduchá OSPF je užitečná v menších sítích, ale ve větších sítích je více oblastní OSPF lepší volbou. Protože, řeší problémy s velkou směrovací tabulkou, velkou databází linek a častými výpočty SPF algoritmu, jak je znázorněno na obrázcích 1 a 2.

Hlavní oblast se nazývá oblast páteře (oblast 0) a všechny ostatní oblasti se musí připojit k páteřní oblasti. Směrování se stále vyskytuje mezi oblastmi, zatímco mnoho směrovacích operací, jako je přepočet databáze, se udržuje v oblasti.

Existují čtyři různé typy směrovačů OSPF: Interní směrovač, Páteřní směrovač, Oblastní hraniční směrovač (ABR) a Autonomní systémový hraniční směrovač (ASBR). Směrovač lze klasifikovat, jako více než jeden směrovač.

Šíření stavů linek (LSA), je základním prvkem OSPF. Tato kapitola se soustředila na typy LSA 1 a 5. LSA typu 1 jsou označovány jako položky linek směrovače. LSA typu 2 jsou označovány jako položky síťových linek a jsou zatopeny DR. LSA typu 3, jsou označovány jako souhrnné položky linek a jsou vytvářeny a propagovány pomocí ABR. Souhrnný typ LSA typu 4 je generován systémem ABR pouze tehdy, když existuje ASBR v oblasti. Externí LSA typu 5, popisují cesty do sítí, mimo autonomní systém OSPF. LSA typu 5 pochází z ASBR a zaplavují celý autonomní systém.

Trasy OSPF ve směrovací tabulce IPv4, jsou identifikovány pomocí následujících deskriptorů: O, O IA, O E1 nebo O E2. Každý směrovač používá k vytvoření stromu SPF, algoritmus SPF proti LSDB. Strom SPF slouží k určení nejlepších cest.

Příklad konfigurace více oblastního OSPF:

R1 (config) # router ospf 10

R1 (config-router) # router-id 1.1.1.1

R1 (config-router) # network 10.1.1.1 0.0.0.0 area 1

R1 (config-router) # network 10.1.2.1 0.0.0.0 area 1

R1 (config-router) # network 192.168.10.1 0.0.0.0 area 0

OSPF neprovádí automatické shrnutí. V OSPF lze shrnutí nakonfigurovat pouze na ABR nebo ASBR. Shrnutí trasy interní oblasti, musí být ručně nakonfigurováno, vyskytuje se na ABR a vztahuje se na trasy z každé oblasti. Chcete-li manuálně nakonfigurovat souhrn interakcí na trase ABR, použijte příkaz ***area id-oblasti range adresa maska***.

Sumarizace externí trasy je specifická pro trasy, které jsou vkládány do OSPF prostřednictvím redistribuce tras. Obecně, pouze ASBR shrnuje vnější trasy. Souhrnná externí trasa je na ASBR nakonfigurována pomocí příkazu ***summary-address adresa maska***.

Příkazy, které se používají k ověření konfigurace OSPF, jsou následující:

- ***show ip ospf neighbor***
- ***show ip ospf***
- ***show ip ospf interface***
- ***show ip protocols***
- ***show ip ospf interface brief***
- ***show ip route ospf***
- ***show ip ospf database***

14 KAPITOLA 7 – EIGRP

14.1 EIGRP – Enhanced Interior Gateway Routing Protocol

14.1.1 Úvod

14.1.1.1 Úvod

Rozšířený vnitřní protokol směrování brány (EIGRP), je pokročilý protokol vzdáleného vektorového směrování, vyvinutý společností Cisco. Jak název napovídá, EIGRP je vylepšením dalšího směrovacího protokolu IGRP (Internal Gateway Routing Protocol). IGRP je starší třídní protokol vzdáleného vektorového směrování, zastaralý od verze IOS 12.3.

EIGRP je vzdálený směrovací protokol, který obsahuje funkce nalezené v protokolech stavu linky. EIGRP je vhodný pro mnoho různých topologií a médií. V dobře navržené síti může systém EIGRP zahrnovat více topologií a může poskytnout extrémně rychlý čas konvergence s minimálním síťovým provozem.

Tato kapitola uvádí EIGRP a poskytuje základní konfigurační příkazy, které ji nakonfigurují na Cisco IOS směrovači. Také zkoumá provoz směrovacího protokolu a poskytuje podrobnější informace o tom, jak EIGRP určuje nejlepší cestu.

14.2 Vlastnosti EIGRP

14.2.1 Základní Funkce EIGRP

14.2.1.1 Funkce EIGRP

EIGRP byl zpočátku vydán v roce 1992, jako proprietární protokol dostupný pouze u zařízení Cisco. V roce 2013, vydala společnost Cisco základní funkcionalitu EIGRP jako otevřený standardu pro IETF, jako informační RFC. To znamená, že další síťoví dodavatelé nyní mohou implementovat EIGRP na svém zařízení, aby spolupracovali se směrovači Cisco i jinými, se systémem EIGRP. Nicméně rozšířené funkce EIGRP, jako je EIGRP stub, potřebné pro dynamické vícenásobné virtuální privátní sítě (DMVPN), nebudou uvolněny do IETF. Jako informativní RFC bude společnost Cisco i nadále udržovat kontrolu nad systémem EIGRP.

EIGRP zahrnuje vlastnosti protokolů směrování a vektorové vzdálenosti. Je však stále založen na principu klíče vzdáleného vektoru směrovacího protokolu, ve kterém se informace o zbytku sítě dozví od přímých sousedů.

EIGRP je pokročilý distanční vektorový směrovací protokol, který obsahuje funkce, které nejsou nalezeny v jiných protokolech směrování vektorů vzdálenosti, jako jsou RIP a IGRP.

Rozptylující Aktualizační Algoritmus

Jako výpočetní motor, který řídí EIGRP, se rozptylující aktualizační algoritmus (DUAL) nachází ve středu směrovacího protokolu. DUAL zaručuje bezproblémové a záložní cesty v celé doméně směrování. S využitím systému DUAL uchovává EIGRP, všechny dostupné trasy zálohování pro cíle, aby se v případě potřeby rychle přizpůsobily alternativním trasám.

Vytvoření sousedních přidružení

EIGRP vytváří vztahy s přímo propojenými směrovači, které jsou také povoleny pro EIGRP. Sousední přidružení se používají ke sledování stavu těchto sousedů.

Spolehlivý přenosový protokol (RTP)

Spolehlivý přenosový protokol (RTP) je jedinečný pro EIGRP a poskytuje dodávku EIGRP paketů sousedům. RTP a sledování sousedních přidružení, nastaví stupeň pro DUAL.

Částečné a ohraničené aktualizace

EIGRP používá termíny, částečné a ohraničené, když se odkazuje na jeho aktualizace. Na rozdíl od RIP, neposílá periodické aktualizace a položky tras nezestárnou. Částečný termín znamená, že aktualizace obsahuje pouze informace o změnách trasy, jako například novou linku nebo linku, která se stává nedostupnou. Termínem ohraničený, odkazujeme na šíření částečných aktualizací, které jsou zasílány pouze směrovačům, které ovlivňují změny. Tím se minimalizuje šířka pásma, která je požadována pro odesílání EIGRP aktualizací.

Rovnoměrné a nerovnoměrné vyrovnávání zatížení cen

EIGRP podporuje rovnoměrné vyrovnávání cen a nerovnoměrné vyvažování zátěže cen, což umožňuje správcům lépe distribuovat tok dopravy ve svých sítích.

Poznámka: Termín hybridní směrovací protokol je používán v některé starší dokumentaci k definování EIGRP. Tento pojem je však zavádějící, protože EIGRP není hybrid mezi protokolem vzdáleného vektoru a směrovacím protokolem. Je pouze vzdálený směrovací protokol. Proto společnost Cisco už tento termín nepoužívá.

14.2.1.2 Moduly Závislé od Protokolu

EIGRP má schopnost směrování několika různých protokolů včetně protokolu IPv4 a protokolu IPv6, pomocí protokolově závislých modulů (PDM). I když je nyní zastaralý, EIGRP také použil PDM protokol, pro směrování síťových vrstev, Novell IPX.

PDM odpovídají za úkoly specifické pro protokol sítě. Příkladem je modul EIGRP, který je zodpovědný za odesílání a přijímání paketů, které jsou zapouzdřené v protokolu IPv4. Tento modul je také zodpovědný za analýzu paketů EIGRP a informování DUAL o nových přijatých informacích. EIGRP požádá DUAL o rozhodnutí o směrování, ale výsledky jsou uloženy v směrovací tabulce IPv4.

PDM odpovídají za specifické směrovací úkoly pro každý protokol síťové vrstvy, včetně:

- Udržování sousedních a topologických tabulek směrovačů EIGRP, které patří do této sady protokolů
- Vytváření a překládání protokolových paketů pro DUAL
- Propojení DUAL se směrovací tabulkou
- Výpočet metriky a předání této informace DUAL
- Implementace filtrů a přístupových seznamů
- Provádění funkcí redistribuce do a z jiných směrovacích protokolů
- Redistribuce tras, které jsou naučeny od jiných směrovacích protokolů

Když směrovač objeví nového souseda, zaznamená adresa a rozhraní souseda, slouží jako záznam v tabulce sousedů. Existuje jedna tabulka sousedů pro každý modul závislá na protokolu, jako je IPv4. EIGRP také udržuje tabulku topologie. Tabulka topologie obsahuje všechny cíle, které inzerují sousední směrovače. Pro každou PDM je také samostatná tabulka topologie.

14.2.1.3 RTP – Reliable Transport Protocol

EIGRP používá protokol RTP, pro doručování a příjem paketů EIGRP. EIGRP byl navržen jako směrovací protokol nezávislý na síti. Protože tento návrh nemůže používat služby UDP nebo TCP. To umožňuje použít protokol EIGRP pro protokoly jiné než protokoly TCP/IP, jako například IPX a AppleTalk. Tento obrázek koncepčně ukazuje, jak funguje RTP.

Ačkoli "spolehlivá" část jména protokolu RTP, zahrnuje jak spolehlivé dodávky, tak nespolehlivé doručení paketů EIGRP, podobně jako TCP a UDP. Spolehlivý protokol RTP vyžaduje potvrzení, které příjemce vrátí odesílateli. Nespolehlivý paket RTP nevyžaduje potvr-

zení. Aktualizační paket EIGRP je například odeslán spolehlivě přes RTP a vyžaduje potvrzení. Balík Hello je také odeslán přes RTP, ale nespolehlivě. To znamená, že Hello pakety nevyžadují potvrzení.

RTP může posílat pakety EIGRP, jako unicast nebo multicast.

- EIGRP multicast pakety protokolu IPv4, používají vyhrazenou adresu IPv4 pro více směrové vysílání 224.0.0.10.
- EIGRP multicast pakety protokolu IPv6, jsou odesílány na vyhrazenou adresu IPv6 více směrového vysílání FF02 :: A.

14.2.1.4 Autentifikace

Stejně jako ostatní směrovací protokoly lze EIGRP nakonfigurovat pro ověřování. RIPv2, EIGRP, OSPF, IS-IS a BGP mohou být nakonfigurovány tak, aby ověřovaly své směrovací informace.

Je správnou praxí autentizace přenášených směrovacích informací. Tímto způsobem zajistí, že směrovače budou přijímat informace o směrování z jiných směrovačů, které byly nakonfigurovány se stejným heslem nebo informacemi o ověření.

Poznámka: Ověřování nešifruje aktualizace směrování EIGRP.

14.2.2 Typy EIGRP Paketů

14.2.2.1 Typy EIGRP Paketů

EIGRP používá pět různých typů paketů, některé v párech. Pakety EIGRP jsou odesílány buď spolehlivým nebo nespolehlivým přenosem, pomocí protokolu RTP a mohou být odesílány jako unicast, multicast nebo i obojí. Typy paketů EIGRP se také nazývají formáty paketů EIGRP nebo zprávy EIGRP.

Jak je ukázáno na obrázku 1, pět typů paketů EIGRP zahrnuje:

Hello pakety - Používá se pro objevování sousedů a pro udržení sousedních přidružení.

- Odesílány s nespolehlivým doručením
- Multicast (na většině typů sítí)

Aktualizační pakety - Propagují informace směrování k sousedům EIGRP.

- Odesílány se spolehlivým doručením
- Unicast nebo multicast

Potvrzovací pakety - slouží k potvrzení přijetí zprávy EIGRP, která byla odeslána pomocí spolehlivého doručení.

- Odesílány s nespolehlivým doručením
- Unicast

Dotazové pakety - slouží k dotazování tras od sousedů.

- Odesílány se spolehlivým dodáním
- Unicast nebo multicast

Pakety odpovědí - Odeslané jako odpověď na dotaz EIGRP.

- Odeslané se spolehlivým dodáním
- Unicast

Obrázek 2 ukazuje, že zprávy EIGRP jsou obvykle zapouzdřené do paketů, IPv4 nebo IPv6. EIGRP pro zprávy IPv4 používají jako protokol síťové vrstvy protokol IPv4. Pole protokolu IPv4 používá 88, pro označení datové části paketu zprávy IPv4. Zprávy protokolu EIGRP pro protokoly IPv6 jsou zapouzdřeny, do paketů IPv6, pomocí dalšího pole záhlaví 88.

14.2.2.2 Hello Pakety EIGRP

EIGRP používá malé balíčky Hello, aby objevil další směrovače podporující protokol EIGRP, na přímo propojených linkách. Hello pakety, používají směrovače k vytvoření sousedních přidružení EIGRP, známých také jako sousední vztahy.

Hello pakety EIGRP, jsou odesílány jako multicast, IPv4 nebo IPv6 a používají nespolehlivé doručení služby RTP. To znamená, že přijímač neodpovídá potvrzovacím paketům.

- Vyhrazená multicast adresa EIGRP pro IPv4, je 224.0.0.10.
- Vyhrazená multicast adresa EIGRP pro IPv6, je FF02::A.

EIGRP směrovače, objeví sousedy a vytvoří sousední směrovače pomocí Hello paketů. Ve většině sítí jsou Hello pakety odesílány, jako multicast pakety, každých pět sekund. EIGRP také používá Hello pakety k udržení stanovených přidružení. EIGRP směrovač předpokládá, že pokud obdrží Hello pakety od souseda, soused a jeho trasy zůstávají životaschopnými.

EIGRP používá Zadržující časovač pro stanovení maximální doby, po kterou má směrovač počkat, než obdrží příští paket předtím, než prohlásí, že soused je nedosažitelný. Ve výcho-

zím nastavení je doba zadržení, trojnásobek intervalu Hello paketů, nebo 15 sekund na většině sítí a 180 sekund na nízkonákladových sítích NBMA. Pokud vyprší čas čekání, EIGRP deklaruje trasu jako vypnutou a DUAL vyhledá novou cestu odesláním dotazů.

14.2.2.3 Aktualizační Pakety a Pakety Potvrzení EIGRP

Aktualizační pakety EIGRP

EIGRP odešle aktualizační pakety pro šíření informací o směrování. Aktualizační pakety jsou odesílány pouze v případě potřeby. Pakety obsahují pouze potřebné informace o směrování a jsou odesílány pouze směrovačům, které je vyžadují.

Na rozdíl od RIP, EIGRP neposílá periodické aktualizace a záznamy tras nezestárnou. Namísto toho EIGRP odesílá přírůstkové aktualizace pouze tehdy, když se změní stav cíle. To může zahrnovat, že když bude k dispozici nová síť, stávající síť nebude dostupná nebo se změní metrika směrování pro existující síť.

EIGRP používá termíny částečné a ohraničené při odkazu na jeho aktualizace. Částečný termín znamená, že aktualizace obsahuje pouze informace o změnách trasy. Termínem "ohraničený" se rozumí šíření částečných aktualizací, které jsou zasílány pouze těm směrovačům, které ovlivňují změny.

Odesíláním informací o směrování, které jsou potřebné, pouze pro ty směrovače, které je potřebují, EIGRP minimalizuje šířku pásma, která je potřebná k odesílání aktualizací.

Pakety aktualizace EIGRP používají spolehlivé doručení, což znamená, že odesílající směrovač vyžaduje potvrzení. Aktualizované pakety jsou odesílány jako multicast, pokud jsou vyžadovány více směrovači, nebo jako unicast, pokud to vyžaduje pouze jeden směrovač. Na obrázku, protože jsou linky point-to-point, aktualizace se odesílají jako unicast.

Potvrzovací pakety EIGRP

EIGRP pošle pakety potvrzení (ACK), pokud je použito spolehlivé doručení. Potvrzení EIGRP je Hello paket bez jakýchkoli dat. RTP používá spolehlivé doručování paketů aktualizace, dotazů a odpovědí EIGRP. Potvrzovací pakety jsou vždy odesílány jako nespolehlivé unicast pakety. Nespolehlivé doručení dává smysl, jinak by byla vznikla nekonečná potvrzovací smyčka.

Na obrázku, R2 ztratila připojení k síti LAN, připojené k rozhraní Gigabit Ethernet. R2 okamžitě pošle aktualizaci na R1 a R3 a zaznamená tuto sestupnou trasu. R1 a R3 reagují potvrzením, aby R2 věděl, že obdržel aktualizace.

14.2.2.4 Dotazovací a Odpovídající Pakety EIGRP

Dotazovací Pakety EIGRP

DUAL používá dotazovací a odpovídající pakety, při hledání sítí a dalších úloh. Dotazy a odpovědi, používají spolehlivé doručení. Dotazy mohou používat multicast nebo unicast, zatímco odpovědi jsou vždy odesílány jako unicast.

Na obrázku R2 ztratila konektivitu k síti LAN a vysílá dotazy všem sousedům EIGRP, kteří hledají jakékoliv cesty do sítě LAN. Protože dotazy používají spolehlivé doručení, musí přijímající směrovač vrátit potvrzení EIGRP. Potvrzení informuje odesílatele, že obdržel dotazovou zprávu. Aby tento příklad byl jednoduchý, byla v grafice vynechána potvrzení.

Odpovídající pakety EIGRP

Všichni sousedé musí poslat odpověď bez ohledu na to, zda mají nebo nemají cestu k vypnuté síti. Protože odpovědi také využívají spolehlivé doručení, směrovače jako R2 musí odesílat potvrzení.

Možná není zřejmé, proč by R2 poslal dotaz na síť, o které ví, že je nefunkční. Ve skutečnosti je k dispozici pouze rozhraní R2, které je připojeno k síti. Další směrovač může být připojen ke stejné síti LAN a má alternativní cestu k ní. Proto se R2, dotazuje na takový směrovač, před úplným odstraněním sítě z tabulky topologie.

14.2.3 Zprávy EIGRP

14.2.3.1 Zprávy Zapouzdření EIGRP

Datová část zprávy EIGRP je zapouzdřena v paketu. Toto datové pole se nazývá typ, délka, hodnota (TLV). Typy TLV, relevantní pro tento kurz jsou parametry EIGRP, interní IP cesty a externí IP cesty.

Záhlaví paketu EIGRP je součástí každého paketu EIGRP, bez ohledu na jeho typ. Záhlaví paketu EIGRP a TLV, jsou pak zapouzdřeny v paketu IPv4. V hlavičce paketů IPv4, je pole protokolu nastaveno na hodnotu 88, čímž se indikuje EIGRP a cílová adresa IPv4 je nastavena na multicast 224.0.0.10. Pokud je EIGRP paket zapouzdřen do rámce Ethernet, cílovou adresou MAC je také adresa multicast, 01-00-5E-00-00-0A.

Na obrázcích 1 až 4, je uveden datový rámec Ethernet. EIGRP pro protokol IPv4 je zapouzdřen v paketu IPv4. Pro IPv6 by se použil podobný typ zapouzdření. Pro IPv6, je zapouzdřen pomocí hlavičky protokolu IPv6. Cílová adresa IPv6 by byla multicast adresa FF02::A, pak další pole záhlaví, by bylo nastaveno na 88.

14.2.3.2 Hlavička Paketu EIGRP a TLV

Každá zpráva EIGRP obsahuje hlavičku, jak je znázorněno na obrázku 1. Důležité pole obsahuje pole Opcode a pole Čísla Autonomního Systému. Opcode určuje typ paketu EIGRP následujícím způsobem:

- Aktualizace
- Dotaz
- Odpověď
- Hello

Autonomní číslo systému určuje proces směrování EIGRP. Na rozdíl od RIP, více instancí EIGRP může běžet v síti. Autonomní systémové číslo se používá pro sledování každého běžícího procesu.

Obrázek 2 ukazuje TLV parametry EIGRP. Zpráva parametrů EIGRP obsahuje váhy, které používá pro kompozici své metriky. Ve výchozím nastavení jsou váženy, pouze šířky pásma a zpoždění. Oba jsou rovnocenné. Proto je pole K1 pro šířku pásma a pole K3 pro zpoždění, nastaveny na 1. Ostatní hodnoty K jsou nastaveny na 0.

Doba zadržení je doba, po kterou má soused EIGRP, který obdrží tuto zprávu, počkat, než bude uvažovat o rozšíření, že směrovač nebude fungovat.

Obrázek 3 ukazuje interní IP trasy TLV. Interní IP zpráva, se používá k inzerci tras EIGRP v autonomním systému. Mezi důležité pole patří pole metrických údajů (zpoždění a šířka pásma), pole masky podsítě (délka prefixu) a cílové pole.

Zpoždění se vypočítá jako součet zpoždění, od zdroje k cíli, v desítkách mikrosekund. Šířka pásma je nejnižší nakonfigurovaná šířka pásma, libovolného rozhraní podél trasy.

Maska podsítě je určena jako délka prefixu, nebo počet síťových bitů v masce podsítě. Například délka prefixu pro masku podsítě 255.255.255.0 je 24, protože 24 je počet síťových bitů.

Cílové pole ukládá adresu cílové sítě. Přestože se na tomto obrázku zobrazí pouze 24 bitů, toto pole se mění podle hodnoty, síťové části 32bitové síťové adresy. Například síťová část 10.1.0.0/16, je 10.1. Z toho důvodu, cílové pole ukládá prvních 16 bitů. Protože minimální délka tohoto pole je 24 bitů, zbytek pole je vyplněn nulami. Pokud je síťová adresa delší než 24 bitů (např. 192.168.1.32/27), pole cílení je rozšířeno o dalších 32 bitů (celkem 56 bitů) a nepoužité bitové kódy jsou naloženy nulami.

Obrázek 4 zobrazuje protokoly TLV pro externí trasy IP. Externí zpráva IP se používá, když jsou importovány externí trasy do směrovacího procesu EIGRP. V této kapitole budeme importovat nebo přerozdělovat výchozí statickou cestu do EIGRP. Všimněte si, že dolní polovina externích tras TLV, zahrnuje všechna pole používaná interním IP TLV.

Poznámka: Maximální přenosová jednotka (MTU), není metrika použitá společností EIGRP. MTU je součástí aktualizací směrování, ale není určena pro určení směrovací metriky.

14.3 Konfigurace EIGRP pro IPv4

14.3.1 Konfigurace EIGRP pro IPv4

14.3.1.1 Síťová Topologie EIGRP

Obrázek 1, zobrazuje topologii použitou v tomto kurzu, na konfiguraci protokolu EIGRP pro protokol IPv4. Typy sériových rozhraní a jejich přidružené šířky pásma nemusí nutně odrážet běžné typy připojení nalezené v dnešních sítích. Šířky pásma sériových linek použité v této topologii byly vybrány tak, aby pomohly vysvětlit výpočet metriky směrovacího protokolu a proces optimálního výběru cesty.

Směrovače v topologii mají počáteční konfiguraci včetně adres na rozhraní. V současné době neexistuje žádné statické směrování nebo dynamické směrování nakonfigurované na žádném směrovači.

Obrázky 2, 3 a 4 zobrazují konfigurace rozhraní pro tři směrovače EIGRP v topologii. Pouze směrovače R1, R2 a R3 jsou součástí směrovací domény EIGRP. ISP směrovač se používá jako brána směrovací domény k Internetu.

14.3.1.2 Čísla Autonomních Systémů

EIGRP používá příkaz ***router eigrp autonomní-systém,*** pro povolení procesu EIGRP. Autonomní systémové číslo uvedené v konfiguraci EIGRP nesouvisí s celosvětově přidělenými autonomními systémovými čísly používanými externími směrovacími protokoly, které jsou přiděleny úřadem Internet Assigned Numbers Authority (IANA).

Takže jaký je rozdíl mezi globálně přiřazeným autonomním systémovým číslem IANA a autonomním systémovým číslem EIGRP?

Globálně přidělený autonomní systém IANA, je sbírka sítí pod správní kontrolou jediného subjektu, který představuje společnou směrovací politiku na internetu. Na obrázku jsou společnosti A, B, C a D všechny pod správní kontrolou ISP1. ISP1 představuje společnou směrovací politiku pro všechny tyto společnosti při propagaci tras k ISP2.

Pokyny pro vytváření, výběr a registraci autonomního systému jsou popsány v dokumentu RFC 1930. Globální autonomní systémová čísla jsou přidělena IANA, stejnou autoritou, která přiřazuje prostor IP adres. Místní regionální internetový registr (RIR) odpovídá za přiřazení autonomního systémového čísla subjektu z jeho bloku přiřazených autonomních systémových čísel. Před rokem 2007 bylo autonomní systémové číslo, 16bitové číslo v rozmezí 0 až 65 535. Dnes je přiřazeno, 32bitové autonomní systémové číslo, které zvyšuje počet dostupných autonomních systémových čísel na více než 4 miliardy.

Obvykle poskytovatelé internetových služeb (ISP), poskytovatelé internetového páteřního systému a velké instituce připojující sek jiným subjektům, vyžadují autonomní systémové číslo. Tito poskytovatelé internetových služeb a velké instituce používají protokol směrování externí brány BGP, pro šíření informací o směrování. BGP je jediný směrovací protokol, který ve své konfiguraci používá skutečné autonomní číslo systému.

Převážná většina společností a institucí s IP sítěmi nepotřebují autonomní systémové číslo, protože jsou řízeny větší entitou, jako je ISP. Tyto společnosti používají protokoly vnitřní brány, jako jsou RIP, EIGRP, OSPF a IS-IS, pro směrování paketů v rámci svých vlastních sítí. Jedná se o jednu z mnoha nezávislých a oddělených sítí v rámci autonomního systému ISP. Ten odpovídá za směrování paketů v rámci jeho autonomního systému a mezi jinými autonomními systémy.

Autonomní systémové číslo použité pro konfiguraci EIGRP, je významné pouze pro směrovací doménu. Funguje jako identifikátor procesu, který pomáhá směrovačům sledovat více spuštěných instancí. Je to nutné, protože je možné mít v síti více než jednu instanci EIGRP. Každá instance může být konfigurována pro podporu a výměnu aktualizací směrování různých sítí.

14.3.1.3 Příkazy EIGRP Směrovače

Aplikace Cisco IOS zahrnuje spouštějící procesy a konfigurace, několika různých typů dynamických směrovacích protokolů. Příkaz globálního konfiguračního režimu směrovače se používá k zahájení konfigurace jakéhokoli dynamického směrovacího protokolu. Topologie uvedená na obrázku 1, se slouží k demonstraci tohoto příkazu.

Jak je znázorněno na obrázku 2, za nímž následuje otazník (?), Příkaz globálního konfiguračního režimu směrovače, obsahuje seznam všech dostupných směrovacích protokolů podporovaných touto specifickou verzí IOS, která běží na směrovači.

Následující příkaz globálního konfiguračního režimu se používá k zadání konfiguračního režimu směrovače EIGRP a zahájení konfigurace jeho procesu:

Router (config) # router eigrp autonomní systém

Argumentu autonomního systému lze přiřadit jakékoli 16bitové číslo, v hodnotě mezi číslem 1 a 65 535. Všechny směrovače v směrovací doméně EIGRP musí používat stejné autonomní číslo systému.

Obrázek 3 ukazuje konfiguraci procesu EIGRP na směrovačích R1, R2 a R3. Všimněte si, že výzva se změní z příkazu globálního konfiguračního režimu do režimu konfigurace směrovače.

V příkladu 1, se identifikuje tento konkrétní proces EIGRP, který běží na tomto směrovači. Aby bylo možné vytvořit sousední přidružení, vyžaduje EIGRP, aby všechny směrovače ve stejné doméně směrování byly nakonfigurovány se stejným autonomním systémovým číslem. Na obr. 3 je stejný EIGRP povolen ve všech třech směrovačích se stejným autonomním systémovým číslem 1.

Příkaz ***router eigrp autonomní-systém,*** nespustí samotný proces EIGRP. Směrovač nezačne odesílat aktualizace. Spíše tento příkaz poskytuje pouze přístup ke konfiguraci nastavení.

Chcete-li zcela odstranit proces směrování EIGRP ze zařízení, použijte příkaz globálního konfiguračního režimu ***no router eigrp autonomní-systém***, který zastaví proces EIGRP a odstraní všechny existující konfigurace směrovače.

14.3.1.4 ID Směrovače EIGRP

Určení ID směrovače

ID směrovače EIGRP, se používá k jedinečné identifikaci každého směrovače v směrovací doméně. ID směrovače se používá v protokolech směrování protokolů EIGRP a OSPF, ačkoli role identifikátoru je v OSPF významnější.

V implementacích EIGRP IPv4 není použití ID směrovače tak zřejmé. EIGRP pro protokol IPv4 používá 32bitový ID směrovače, k identifikaci původního směrovače pro redistribuci externích tras. Potřeba identifikátoru směrovače se stává zřetelnější v diskusi o protokolu EIGRP pro protokol IPv6. Zatímco identifikační číslo směrovače je nezbytné k přerozdělení,

detaily redistribuce EIGRP jsou mimo rámec tohoto učebního plánu. Pro účely tohoto učebního plánu je třeba pouze pochopit, co je ID směrovače a jak je odvozen.

Směrovače Cisco odvozují identifikační číslo směrovače založené na třech kritériích s následující prioritou:

1. Použijte adresu IPv4 nakonfigurovanou pomocí příkazu režimu konfigurace ***eigrp router-id***.

2. Není-li identifikátor směrovače nakonfigurován, směrovač zvolí nejvyšší adresu IPv4 libovolného z jeho rozhraní zpětné vazby.

3. Není-li nakonfigurováno žádné rozhraní zpětné vazby, směrovač zvolí nejvyšší aktivní IPv4 adresu kteréhokoli z jeho fyzických rozhraní.

Správce sítě explicitně nenakonfiguroval identifikátor směrovače pomocí příkazu ***eigrp router-id***, tím pádem si EIGRP generuje vlastní identifikační číslo směrovače pomocí buď adresy zpětné vazby nebo fyzické adresy IPv4. Adresa zpětné vazby je virtuální rozhraní a je automaticky konfigurováno v režimu Spuštěno. Rozhraní nemusí být povoleno pro EIGRP, což znamená, že nemusí být zahrnuto do jednoho z příkazů sítě. Rozhraní však musí být ve stavu Spuštěno/Spuštěno.

Pomocí výše popsaných kritérií zobrazuje obrázek výchozí ID směrovače EIGRP, které jsou určeny nejvyšší aktivní adresou IPv4.

Poznámka: Příkaz ***eigrp router-id,*** slouží ke konfiguraci ID směrovače pro EIGRP. Některé verze systému IOS budou přijímat příkaz ***router-id***, aniž byste nejprve zadali ***eigrp***. Běžící konfigurace však zobrazí ***eigrp router-id,*** bez ohledu na to, který příkaz je použit.

14.3.1.5 Konfigurace ID Směrovače EIGRP

Příkaz *eigrp router-id*

Příkaz ***eigrp router-id***, se používá ke konfiguraci ID směrovače EIGRP a má přednost před libovolnými adresami IPv4, fyzickým rozhraním nebo rozhraním ze zpětnou vazbou. Syntaxe příkazu je:

Router (config) # router eigrp autonomní-systém

Router (config-router) # eigrp router-id ipv4-adresa

Poznámka: Adresa IPv4, která slouží k označení ID směrovače, je ve skutečnosti 32bitové číslo zobrazené v desítkovém zápisu.

ID směrovače lze nakonfigurovat libovolnou adresou IPv4 se dvěma výjimkami: 0.0.0.0 a 255.255.255.255. ID směrovače by mělo být jedinečné 32bitové číslo v směrovací doméně EIGRP. Jinak se mohou vyskytnout nesrovnalosti směrování.

Obrázek 1 ukazuje konfiguraci ID směrovače EIGRP pro směrovače R1 a R2 pomocí příkazu ***router eigrp autonomní-systém***.

Adresa zpětné vazby použitá jako ID směrovače

Další možností zadání ID směrovače EIGRP, je použít IPv4 adresu zpětné vazby. Výhodou použití rozhraní zpětné vazby místo adresy fyzického rozhraní je to, že na rozdíl od fyzických rozhraní nemůže selhat. Neexistují žádné skutečné kabely nebo sousední zařízení, na kterých závisí rozhraní zpětné vazby, protože jsou ve stavu Spuštěno. Proto pomocí adresy zpětné vazby, pro identifikátor směrovače, může poskytnout konzistentnější ID směrovače než pomocí adresy rozhraní.

Není-li použit příkaz ***eigrp router-id*** a jsou nakonfigurována rozhraní zpětné vazby, EIGRP zvolí nejvyšší IPv4 adresu libovolného rozhraní se zpětnou vazbou. Následující příkazy slouží k povolení a konfiguraci rozhraní zpětné vazby:

Router (config) # interface loopback číslo

Router (config-if) # ip address ipv4-adresa maska-podsítě

Poznámka: ID směrovače EIGRP se nezmění, pokud není proces EIGRP odstraněn příkazem ***no router eigrp***, nebo pokud je ID směrovače ručně nakonfigurováno příkazem ***eigrp router-id***.

Ověření procesu EIGRP

Obrázek 2 ukazuje výstup pro R1, včetně ID. Příkaz ***show ip protocols***, zobrazuje parametry a aktuální stav všech procesů protokolu aktivního směrování, včetně EIGRP a OSPF. Příkaz ***show ip protocols***, zobrazuje různé typy výstupů specifické pro každý směrovací protokol.

Pomocí kontroly syntaxe na Obr. 3, nakonfigurujte a ověřte ID směrovače pro R3.

14.3.1.6 Příkaz Network (Síť)

Režim konfigurace směrovače EIGRP umožňuje konfiguraci směrovacího protokolu EIGRP. Obrázek 1 ukazuje, že R1, R2 a R3 mají všechny sítě, které by měly být zahrnuty do jedné směrovací domény EIGRP. Chcete-li povolit směrování protokolu EIGRP na rozhraní, použijte příkaz ***network*** a zadejte klasickou síťovou adresu pro každou přímo připojenou síť.

Příkaz ***network,*** má stejnou funkci jako u všech směrovacích protokolů IGP. Příkaz ***network*** v EIGRP:

- Umožňuje jakémukoli rozhraní tohoto směrovače, které odpovídá síťové adrese příkazu ***network***, režimu konfigurace síťového směrovače pro odesílání a přijímání aktualizací EIGRP.
- Síť rozhraní je součástí aktualizací směrování EIGRP.

Router (config-router) # network ipv4-síťová-adresa

Argument *ipv4-síťová-adresa*, je třídní síťová adresa IPv4 pro toto rozhraní. Obrázek 2 ukazuje síťové příkazy konfigurované pro R1. Na obrázku je použito jediné třídní síťové prohlášení, síť 172.16.0.0, která zahrnuje obě rozhraní v podsítích 172.16.1.0/24 a 172.16.3.0/30. Všimněte si, že se používá pouze klasická síťová adresa.

Obrázek 3 ukazuje síťový příkaz používaný k povolení EIGRP na rozhraní R2, pro podsítě 172.16.1.0/24 a 172.16.2.0/24. Když je EIGRP nakonfigurován na rozhraní R2 S0/0/0, DUAL odešle na konzolu zprávu oznamující, že bylo na tomto rozhraní vytvořeno sousední přidružení s jiným směrovačem EIGRP. Toto nové sousedství se děje automaticky, protože oba, R1 a R2, používají stejné autonomní číslo systému **eigrp 1** a oba směrovače nyní posílají aktualizace na svých rozhraních v síti 172.16.0.0.

Ve výchozím nastavení je povolen příkaz ***eigrp log-neighbor-changes***. Tento příkaz slouží:

- Zobrazení změn v sousedních přidruženích EIGRP.
- Pomáhá ověřit sousední přidružení, během konfigurace EIGRP.
- Informování administrátora sítě, jakmile byly odstraněny všechny přidružení EIGRP.

14.3.1.7 Příkaz Network a Zástupní Maska

Ve výchozím nastavení, příkazem ***network*** a IPv4 adresou, jako 172.16.0.0. Všechny rozhraní na směrovači, které mají třídní síťovou adresu, jsou povoleny pro EIGRP. Mohou však existovat časy, kdy správce sítě nechce zahrnout všechna rozhraní v síti povolením EIGRP. Například na obrázku 1 předpokládejme, že správce chce povolit EIGRP na R2, ale pouze pro podsíť 192.168.10.8 255.255.255.252 na rozhraní S0/0/1.

Chcete-li nakonfigurovat protokol EIGRP pouze pro inzerování specifických podsítí, použijte volbu zástupné masky příkazem sítě:

Router (config-router) # network adresa-sítě adresa [zástupná maska]

Přemýšlejte o zástupné masce jako o inverzní masce podsítě. Inverzní maska podsítě 255.255.255.252, je 0.0.0.3. Chcete-li vypočítat inverzní masku podsítě, odečtěte masku podsítě z 255.255.255.255 následujícím způsobem:

255.255.255.255

- 255.255.255.252

---

0. 0. 0. 3 - Zástupní maska

Obrázek 2 pokračuje v konfiguraci sítě EIGRP na R2. Příkaz 192.168.10.8 0.0.0.3 sítě specificky povoluje EIGRP na rozhraní S0/0/1, které je členem podsítě 192.168.10.8 255.255.255.252.

Některé verze IOS také umožňují zadat masku podsítě místo masky zástupní. Obrázek 3 ukazuje příklad konfigurace stejného rozhraní S0/0/1 na R2, ale tentokrát pomocí masky podsítě v síťovém příkazu. Pokud je však použita maska podsítě, IOS převede příkaz do formátu zástupné masky v rámci konfigurace. To je ověřeno na výstupu příkazem, ***show running-config*** na obrázku 3.

Pomocí kontroly syntaxe na obr. 4, nakonfigurujte síťové příkazy EIGRP pro směrovač R3.

14.3.1.8 Pasivní Rozhraní

Jakmile je v síti EIGRP povoleno nové rozhraní, pokusí se vytvořit sousední přidružení se směrovačem, pro odesílání a přijímání aktualizací EIGRP.

Někdy může být nezbytné nebo výhodné zahrnout do aktualizace EIGRP směrování přímo připojenou síť, ale neumožnit vytváření žádných sousedních přidružení. Příkaz ***passive-interface,*** lze použít k zabránění sousedních přidružení. Existují dva hlavní důvody pro povolení příkazu ***passive-interface***:

- Chcete-li potlačit zbytečnou aktualizaci provozu, například když je rozhraním LAN, bez připojení dalších směrovačů
- Chcete-li zvýšit bezpečnostní prvky, jako je zabránění neznámým směrovačům při přijímání aktualizací EIGRP

Obrázek 1 ukazuje, že R1, R2 a R3 nemají sousedy na rozhraních Gigabit Ethernet 0/0.

Příkaz režimu konfigurace směrovače, ***passive-interface***, zakáže přenos a příjem Hello paketů na těchto rozhraních.

Router (config) # router eigrp as-číslo

Router (config-router) # passive-interface typ-rozhraní číslo-rozhraní

Obrázek 2 ukazuje příkaz ***passive-interface***, konfigurovaný tak, aby potlačoval Hello pakety v LAN pro R1 a R3. R2 je konfigurován pomocí kontroly syntaxe.

Bez sousedního přidružení, si EIGRP nemůže vyměnit trasy se sousedem. Příkaz ***passive-interface*** proto zabraňuje výměně tras na rozhraní. Ačkoli EIGRP neodesílá nebo neobdrží aktualizace o směrování na rozhraní nakonfigurovaném příkazem ***passive-interface***, stále obsahuje adresu rozhraní v směrování aktualizací odeslaných z aktivních rozhraní.

Poznámka: Chcete-li konfigurovat všechna rozhraní jako pasivní, použijte příkaz ***passive-interface default***. Chcete-li rozhraní zakázat jako pasivní, použijte příkaz ***no passive-interface typ-rozhraní číslo-rozhraní***.

Příkladem použití pasivního rozhraní pro zvýšení zabezpečení je to, když se síť musí připojit k organizaci jiného výrobce, pro kterou místní správce nemá žádnou kontrolu, například při připojení k síti ISP. V takovém případě by správce místní sítě musel propagovat propojení prostřednictvím vlastní sítě, ale nechtěl, aby organizace třetí strany přijímala nebo posílala směrovací aktualizace do místního směrovacího zařízení, protože to představuje bezpečnostní riziko.

Ověření pasivního rozhraní

Chcete-li ověřit, zda je jakékoliv rozhraní směrovače nakonfigurováno jako pasivní, použijte příkaz ***show ip protocols***, jak je znázorněno na obrázku 3. Všimněte si, že ačkoli GigabitEthernet 0/0, rozhraní R3, je pasivní rozhraní, EIGRP stále obsahuje síťovou adresu rozhraní ze sítě 192.168.1.0 v aktualizacích směrování.

Pomocí kontroly syntaxe na obr. 4, nakonfigurujte R2, aby potlačil Hello pakety EIGRP na rozhraní Gigabit Ethernet 0/0.

14.3.2 Verifikace EIGRP pro IPv4

14.3.2.1 Verifikace EIGRP: Zkoumání Sousedů

Než může EIGRP odesílat nebo přijímat nějaké aktualizace, směrovače musí zřídit sousední přidružení. Směrovače EIGRP vytvářejí sousední směrovače tím, že si vyměňují Hello pakety.

Pomocí příkazu ***show ip eigrp neighbors***, zobrazte tabulku sousedů a ověřte, že EIGRP vytvořil sousední přidružení. Pro každý směrovač byste měli vidět IPv4 adresu přilehlého směrovače a rozhraní, které tento směrovač používá k dosažení tohoto souseda. Pomocí této topologie má každý směrovač dva sousedy uvedené v tabulce sousedů.

Výstup příkazu ***show ip eigrp neighbors*** zahrnuje:

- **H sloupec** - seznamy sousedů, v pořadí, v jakém byly naučeni.
- **Adresa** - IPv4 adresa souseda.
- **Rozhraní** - Místní rozhraní, na kterém byl přijat tento Hello paket.
- **Zdržení** - aktuální čas zdržení. Když je přijat Hello paket, tato hodnota se resetuje na maximální dobu zadržení pro toto rozhraní a počítá se na nulu. Pokud je dosaženo nuly, soused je považován za Vypnut.
- **Uptime** - Doba, od které byl tento soused přidán do tabulky sousedů.
- **Hladký časový spínač (SRTT) a re-transmisní časový limit (RTO)** - používané službou RTP pro správu spolehlivých paketů EIGRP.
- **Počítání fronty** - Mělo by být vždy nula. Pokud je více než nula, potom pakety EIGRP čekají na odeslání.
- **Číslo sekvence** - slouží k sledování aktualizací, dotazů a odpovědí paketů.

Příkaz ***show ip eigrp neighbors***, je velmi užitečný pro ověřování a odstraňování problémů s EIGRP. Pokud soused není uveden poté, co byly sousední směrovače vybudovány, ověřte si místní rozhraní, abyste se ujistili, že jsou aktivovány, pomocí příkazu ***show ip interface brief***. Pokud je rozhraní aktivní, vyzkoušejte ping IPv4 adresy souseda. Pokud ping selže, znamená to, že sousední rozhraní je Vypnuto a musí být aktivováno. Pokud je ping úspěšný a EIGRP stále nevidí směrovač jako souseda, zkontrolujte následující konfigurace:

- Jsou oba směrovače nakonfigurovány se stejným autonomním číslem systému EIGRP?
- Je přímo připojená síť součástí výkazů sítě EIGRP?

14.3.2.2 Verifikace EIGRP: příkaz show ip protocols

Příkaz ***show ip protocols***, zobrazí parametry a další informace o aktuálním stavu jakýchkoli aktivních směrovacích protokolech IPv4, nakonfigurovaných na směrovači. Příkaz ***show ip protocols***, zobrazuje různé typy výstupů, specifické pro každý směrovací protokol.

Výstup na obrázku 1, ukazuje několik parametrů EIGRP, včetně:

1. EIGRP je aktivní dynamický směrovací protokol na R1, konfigurovaném s autonomním systémovým číslem 1.

2. ID směrovače EIGRP R1, je 1.1.1.1.

3. Administrativní vzdálenosti EIGRP na R1, jsou vnitřní AD 90 a externí 170 (výchozí hodnoty).

4. Ve výchozím nastavení, síť EIGRP, automaticky neuvádí sítě. V aktualizacích směrování jsou zahrnuty podsítě.

5. Sousední přidružení na R1, používají s jinými směrovači k přijímání aktualizací směrování EIGRP.

Poznámka: Před IOS 15, bylo automatické shrnutí EIGRP ve výchozím nastavení povoleno.

Výstup z příkazu ***show ip protokols***, je užitečný při ladění operací směrování. Informace v poli, Zdroje informací o směrování, mohou pomoci identifikovat směrovač podezřelý z poskytování špatných směrovacích informací. Pole, Směrovací informační zdroje, uvádí všechny směrovací zdroje EIGRP, které software Cisco IOS používá k sestavení směrovací tabulky IPv4. Pro každý zdroj si všimněte následující:

- Adresa IPv4
- Administrativní vzdálenost
- Čas, kdy byla od tohoto zdroje přijata poslední aktualizace

Jak je znázorněno na obrázku 2, EIGRP má výchozí AD 90 pro vnitřní cesty a 170 pro trasy z externího zdroje, například výchozí trasy. Ve srovnání s jinými IGP, je EIGRP nejvhodnějším nástrojem Cisco IOS, protože má nejnižší administrativní vzdálenost. EIGRP má třetí AD hodnotu 5, pro souhrnné trasy.

14.3.2.3 Verifikace EIGRP: Zkoumání Směrovací Tabulky IPv4

Dalším způsobem, jak ověřit, zda jsou funkce EIGRP a další funkce směrovače správně nakonfigurovány, je zkontrolovat směrovací tabulky protokolu IPv4, příkazem ***show ip route***. Stejně jako u všech dynamických směrovacích protokolů musí správce sítě ověřit informace ve směrovací tabulce, aby bylo zajištěno, že jsou naplněny podle očekávání na základě zadaných konfigurací. Z tohoto důvodu je důležité mít dobré znalosti konfiguračních příkazů směrovacího protokolu, stejně jako operace směrovacího protokolu a procesy používané směrovacím protokolem pro sestavení směrovací tabulky IP.

Všimněte si, že výstupy používané v průběhu tohoto kurzu pocházejí z Cisco IOS 15. Před IOS 15, bylo automatické shrnutí EIGRP ve výchozím nastavení povoleno. Stav automatického shrnutí může mít vliv na informace zobrazené ve směrovací tabulce IPv4. Pokud je použita předchozí verze IOS, automatické shrnutí může být deaktivováno pomocí příkazu pro konfiguraci směrovače ***no auto-summary***:

Router (config-router) # no auto-summary

Obrázek 1 ukazuje topologii pro R1, R2 a R3.

Na obr. 2 je směrovací tabulka IPv4 zkoumána, pomocí příkazu ***show ip route***. Trasy EIGRP, jsou označeny ve směrovací tabulce s písmenem D. Písmeno D, bylo použito k reprezentaci EIGRP, protože protokol je založen na algoritmu DUAL.

Příkaz ***show ip route*** ověří, že trasy přijaté sousedy EIGRP jsou nainstalovány do směrovací tabulky IPv4. Příkaz ***show ip route***, zobrazuje celou směrovací tabulku, včetně dynamických, přímo připojených vzdálených sítí a statických cest. Z tohoto důvodu je obvykle prvním příkazem ke kontrole konvergence. Po směrování je správně nakonfigurován na všech směrovačích, příkaz ***show ip route*** odráží, že každý směrovač má úplnou směrovací tabulku s cestou do každé sítě v topologii.

Všimněte si, že R1 ve své směrovací tabulce IPv4, nainstaloval trasy do tří vzdálených sítí IPv4:

- 172.16.2.0/24, přijatá od směrovače R2 na rozhraní Serial0/0/0
- 192.168.1.0/24, přijatá od směrovače R2 na rozhraní Serial0/0/1
- 192.168.10.8/30, obdržená od obou rozhraní R2 na rozhraní Serial0/0/0 a od R3 na rozhraní Serial0/0/1

R1 má dvě cesty k síti 192.168.10.8/30, protože její náklady nebo metrika pro dosažení této sítě jsou stejné nebo rovné, přes oba směrovače. Známé to jako rovnocenné ceny cest. R1 využívá obě cesty k dosažení této sítě, což je známo jako vyvažování zátěže. Metrika EIGRP je popsána později v této kapitole.

Obrázek 3 zobrazuje směrovací tabulku R2. Všimněte si, že jsou zobrazeny podobné výsledky, včetně rovnocenné ceny tras pro síť 192.168.10.4/30.

Obrázek 4 zobrazuje směrovací tabulku pro R3. Podobně jako u výsledků pro R1 a R2 se vzdálené sítě naučí pomocí EIGRP, včetně rovnocenných cen cest, pro síť 172.16.3.0/30.

14.3.3 Objevování Počáteční Cesty EIGRP

14.3.3.1 Sousední Přidružení EIGRP

Cílem jakéhokoli dynamického směrovacího protokolu je dozvědět se o vzdálených sítích z jiných směrovačů a dosažení konvergence v doméně směrování. Předtím, než lze vyměnit pakety EIGRP mezi směrovači, musí EIGRP, nejprve objevit své sousedy. Sousedé jsou další směrovače, které používají EIGRP na přímo připojených sítích.

EIGRP používá Hello pakety k vytvoření a udržování sousedních přidružení. Pro dva směrovače EIGRP, které se stanou sousedy, se musí shodovat několik parametrů mezi oběma směrovači. Například, dva směrovače EIGRP musí používat stejné metrické parametry a oba musí být konfigurovány se stejným autonomním systémovým číslem.

Každý směrovač EIGRP, udržuje sousední tabulku, která obsahuje seznam směrovačů na sdílených linkách, které mají tento směrovač s EIGRP. Sousední tabulka se používá ke sledování stavu těchto sousedů.

Na obrázku jsou dva směrovače EIGRP, které vyměňují počáteční Hello pakety. Když aktivní směrovač obdrží Hello paket na rozhraní, přidá tento směrovač do své tabulky sousedů.

1. Na lince se objeví nový směrovač R1 a odešle Hello paket přes všechna jeho rozhraní, nakonfigurovaná pomocí EIGRP.

2. R2 přijímá Hello paket na rozhraní s podporou EIGRP. Odpovídá aktualizačním paketem, který obsahuje všechny cesty, které má ve své směrovací tabulce, s výjimkou těch, které byly načteny prostřednictvím tohoto rozhraní. Sousední přidružení však není zřízeno, dokud R2 také nepošle Hello paket na R1.

3. Poté, co se oba směrovače vyměnily Hello pakety, vznikne sousední přidružení. R1 a R2 aktualizují své tabulky sousedů, přidáním sousedního směrovače jako souseda.

14.3.3.2 Tabulka Topologie EIGRP

Aktualizace EIGRP obsahují sítě, které jsou přístupné ze směrovače, který odesílá aktualizaci. Při výměně aktualizací EIGRP mezi sousedy, směrovač který přijímá tyto položky, přidává je do tabulky topologie EIGRP.

Každý směrovač EIGRP udržuje tabulku topologie pro každý nakonfigurovaný protokol, jako například IPv4 a IPv6. Tabulka topologie obsahuje záznamy tras pro každou destinaci, kterou se směrovač dozví z jejích přímo propojených sousedů.

Obrázek ukazuje pokračování procesu počátečního zjišťování trasy z předchozí stránky. Nyní ukazuje aktualizaci tabulky topologie.

Když směrovač obdrží aktualizaci směrování EIGRP, přidá směrovací informace do své tabulky topologie EIGRP a odpoví s potvrzením.

1. R1 obdrží aktualizaci EIGRP od souseda R2 a ta obsahuje informace o trasách, které soused inzeruje, včetně metriky pro každý cíl. R1 přidá všechny položky aktualizace do své tabulky topologie. Tabulka zahrnuje všechny destinace inzerované sousedními směrovači a ceny (metriku) pro dosažení každé sítě.

2. aktualizační pakety EIGRP, používají spolehlivé doručení. Proto R1 reaguje s potvrzovacím paktem, který informuje R2, že obdržel aktualizaci.

3. R1 pošle aktualizaci EIGRP na R2, který inzeruje trasy, o kterých si uvědomuje, s výjimkou těch, které se naučil z R2.

4. R2 obdrží aktualizaci EIGRP od souseda R1 a přidá tyto informace do vlastní tabulky topologie.

5. R2 reaguje na aktualizační paket EIGRP z R1, potvrzením.

14.3.3.3 Konvergence EIGRP

Obrázek znázorňuje poslední kroky procesu počátečního zjišťování trasy.

1. Po obdržení aktualizačních paketů EIGRP z R2, pomocí informace v tabulce topologie aktualizuje R1 svoji směrovací tabulku IP, s nejlepším způsobem cesty ke každému cíli včetně metriky a dalšího směrovače.

2. Podobně jako R1, taky R2 aktualizuje svou směrovací tabulku IP s nejlepšími cenami cest do každé sítě.

V tomto okamžiku je EIGRP na obou směrovačích považován za konvergovaný.

14.3.4 Metrika

14.3.4.1 Kompozitní Metrika EIGRP

Ve výchozím nastavení používá EIGRP v kompozitní metrice následující hodnoty pro výpočet preferované cesty k síti:

- **Šířka pásma** - nejpomalejší šířka pásma mezi všemi odchozími rozhraními, po cestě od zdroje k cíli.
- **Zpoždění** - Kumulativní (součet) všech zpoždění rozhraní po cestě (v desítkách mikrosekund).

Mohou být použity následující hodnoty, ale nedoporučují se, protože obvykle vedou k častému přepočtu tabulky topologie:

- **Spolehlivost** - představuje nejhorší spolehlivost mezi zdrojem a cílovým serverem, který je založen na, udržováni naživu.
- **Zatížení** - představuje nejhorší zatížení na propojení mezi zdrojem a cílovým serverem, které se vypočítá na základě rychlosti paketů a nakonfigurované šířky pásma rozhraní.

Poznámka: Přestože je MTU součástí aktualizací směrovací tabulky, není to metrika směrování používaná nástrojem EIGRP.

Kompozitní metrika

Obrázek 1 ukazuje kompozitní metrický vzorec, používaný EIGRP. Vzorec se skládá z hodnot K1 až K5, známých jako metrická váha EIGRP. K1 a K3 představují šířku pásma a zpoždění. K2 představuje zatížení a K4 a K5 představují spolehlivost. Ve výchozím nastavení jsou hodnoty K1 a K3 nastaveny na hodnotu 1 a hodnoty K2, K4 a K5 jsou nastaveny na 0. Výsledkem je, že při výpočtu výchozí kompozitní metriky, se používají pouze hodnoty šířky pásma a zpoždění. EIGRP pro protokoly IPv4 a IPv6 používají stejný vzorec pro kompozitní metriku.

Metoda výpočtu metriky (hodnoty k) a autonomní systémové číslo EIGRP, musí souhlasit mezi sousedy EIGRP. Pokud neodpovídají, směrovače nejsou sousední.

Výchozí hodnoty k, lze měnit pomocí příkazu ***metric weights***:

Router (config-router) # metric weights tos k1 k2 k3 k4 k5

Poznámka: Úprava hodnoty metrických vah, se obecně nedoporučuje a je mimo rozsah tohoto kurzu. Jejich význam je však důležitý, při vytváření sousedů. Pokud jeden směrovač změnil metrickou váhu a jiný směrovač ne, nedochází k vytváření sousedství.

Ověření hodnot k

Příkaz ***show ip protokols***, se používá k ověření hodnot k. Výstup příkazu pro R1, je znázorněn na obrázku 2. Všimněte si, že hodnoty k na R1, jsou nastaveny na výchozí hodnotu.

14.3.4.2 Zkoumání Hodnot Rozhraní

Zkoumání metrických hodnot

Příkaz ***show interfaces***, zobrazuje informace o rozhraní, včetně parametrů použitých pro výpočet metriky EIGRP. Na obrázku je uveden příkaz pro rozhraní Serial 0/0/0 na R1.

- **BW** - šířka pásma rozhraní (v kilobitech za sekundu).
- **DLY** - Zpoždění rozhraní (v mikrosekundách).
- **Spolehlivost** - Spolehlivost rozhraní jako zlomek 255 (255/255 je 100% spolehlivost), počítáno jako exponenciální průměr za pět minut. Ve výchozím nastavení hodnota EIGRP, nezahrnuje jeho hodnotu při výpočtu metriky.
- **Txload, Rxload** - Vysílání a příjem zatížení na rozhraní, jako zlomek 255 (255/255 je zcela nasycený), počítané jako exponenciální průměr za pět minut. Ve výchozím nastavení hodnota EIGRP, nezahrnuje jeho hodnotu při výpočtu metriky.

Poznámka: Během tohoto kurzu je šířka pásma určena v kb/s. Výstup směrovače, však zobrazuje šířku pásma pomocí zkratky Kbit/sec. Výstup směrovače, také zobrazuje zpoždění, jako usec. V tomto kurzu se zpoždění určuje v mikrosekundách.

14.3.4.3 Metrika Šířky Pásma

Metrika šířky pásma je statická hodnota používaná některými směrovacími protokoly, jako jsou EIGRP a OSPF, pro výpočet jejich směrovací metriky. Šířka pásma se zobrazuje v kilobitech za sekundu (kb/s). Většina sériových rozhraní používá výchozí hodnotu šířky pásma 1544 kb/s nebo 1 544 000 b/s (1,544 Mb/s). Jedná se o šířku pásma připojení T1. Některé sériové rozhraní, však používají jinou výchozí hodnotu šířky pásma. Obrázek 1, ukazuje topologii použitou v této části. Typy sériových rozhraní a jejich přidružené šířky pásma nemusí nutně odrážet běžné typy připojení, které se dnes nacházejí v sítích.

Vždy ověřte šířku pásma příkazem ***show interfaces***.

Výchozí hodnota šířky pásma, může nebo nemusí, odrážet skutečnou fyzickou šířku pásma rozhraní. Pokud se skutečná šířka pásma linky liší od výchozí hodnoty šířky pásma, měla by být hodnota upravena.

Konfigurace parametru šířky pásma

Na většině sériových linek, je metrika šířky pásma výchozí, 1544 kb/s. Protože EIGRP i OSPF využívají šířku pásma ve výchozích metrických výpočtech, správná hodnota pro šířku pásma je velmi důležitá pro přesnost směrovacích informací.

Pro změnu metriky šířky pásma použijte následující příkaz režimu konfigurace rozhraní:

Router (config-if) # bandwidth kilobits-šířka pásma-hodnota

Chcete-li obnovit výchozí hodnotu, použijte příkaz ***no bandwidth***.

Na obr. 2, má vazba mezi R1 a R2 šířku pásma 64 kb/s a spojení mezi R2 a R3 má šířku pásma 1,024 kb/s. Obrázek ukazuje konfigurace používané ve všech třech směrovačích, pro změnu šířky pásma na příslušných sériových rozhraních.

Ověření parametru šířky pásma

Pomocí příkazu ***show interfaces***, ověřte nové parametry šířky pásma, jak je znázorněno na obrázku 3. Je důležité upravit metriku šířky pásma na obou stranách propojení, abyste zajistili správné směrování v obou směrech.

Změna hodnoty šířky pásma nemění aktuální šířku pásma na lince. Příkaz šířky pásma upravuje pouze metriku používanou směrovacími protokoly, jako jsou například EIGRP a OSPF.

14.3.4.4 Metrika Zpoždění

Zpoždění je měřítko doby, po kterou paket přechází po trase. Metrika zpoždění (DLY) je statická hodnota založená na typu propojení, ke kterému je rozhraní připojeno, a je vyjádřeno v mikrosekundách. Zpoždění není dynamicky měřeno. Jinými slovy, směrovač ve skutečnosti nezaznamenává, jak dlouho trvá paketům, aby dosáhly cíle. Hodnota zpoždění, podobně jako hodnota šířky pásma, je výchozí hodnota, kterou může správce sítě změnit.

Při určování metriky EIGRP je zpoždění kumulativní (součet) všech zpoždění rozhraní na cestě (měřeno v desítkách mikrosekund).

Tabulka na obrázku 1, zobrazuje výchozí hodnoty zpoždění pro různé rozhraní. Všimněte si, že výchozí hodnota je 20 000 mikrosekund pro sériová rozhraní a 10 mikrosekund pro rozhraní Gigabit Ethernet.

Pomocí příkazu ***show interfaces***, ověřte hodnotu zpoždění na rozhraní, jak je znázorněno na obrázku 2. Přestože rozhraní s různými šířkami pásma může mít stejnou hodnotu zpoždění, implicitně společnost Cisco doporučuje změnit tento parametr, pokud správce sítě nemá specifický důvod tak neudělat.

14.3.4.5 Jak Vypočítat Metriku EIGRP

Přestože EIGRP automaticky vypočítá metriku směrovací tabulky používanou k výběru nejlepší cesty, je důležité, aby správce sítě chápal, jak byly tyto metriky určeny.

Na obrázku je znázorněna složená metrika EIGRP. Pomocí výchozích hodnot pro K1 a K3, lze výpočet zjednodušit na nejpomalejší šířku pásma (nebo minimální šířku pásma) plus součet všech zpoždění.

Jinými slovy, zjišťováním hodnot šířky pásma a zpoždění pro všechny odchozí rozhraní cest, můžeme určit metriku EIGRP takto:

Krok 1. Určete linku s nejpomalejší šířkou pásma. Tuto hodnotu použijte pro výpočet šířky pásma (10 000 000/šířka pásma).

Krok 2. Určete hodnotu zpoždění pro každé odchozí rozhraní na cestě k cíli. Přidejte hodnoty zpoždění a vydělte 10 (součet zpoždění/10).

Krok 3. Tato kompozitní metrika vytváří hodnotu 24 bitů. EIGRP však používá 32 bitovou hodnotu. Vynásobením hodnoty 24 bitů s 256, se kompozitní metrika rozšiřuje na 32 bitů. Proto přidejte vypočtené hodnoty pro šířku pásma a zpoždění a násobte součet 256, abyste získali metriku EIGRP.

Výstup směrovací tabulky pro R2 ukazuje, že cesta k 192.168.1.0/24 má EIGRP metrickou hodnotu 3.012.096.

14.3.4.6 Výpočet Metriky EIGRP

Obrázek 1 zobrazuje topologii tří směrovačů. Tento příklad ukazuje, jak EIGRP určuje metriku zobrazenou ve směrovací tabulce R2, pro síť 192.168.1.0/24.

Šířka pásma

EIGRP používá ve svém metrickém výpočtu nejpomalejší šířku pásma. Nejpomalejší šířka pásma, může být určena zkoumáním každého rozhraní mezi R2 a cílovou sítí 192.168.1.0. Rozhraní Serial 0/0/1, na R2, má šířku pásma 1,024 kb/s. Rozhraní GigabitEthernet 0/0 na R3 má šířku pásma 1 000 000 kb/s. Proto má nejpomalejší šířku pásma 1,024 kb/s a používá se při výpočtu metriky.

EIGRP rozděluje referenční hodnotu šířky pásma 10 000 000 o hodnotu šířky pásma rozhraní v kb/s. Výsledkem toho jsou vyšší hodnoty šířky pásma, které dostávají nižší metriky a nižší hodnoty šířky pásma, které dostávají vyšší metriku. 10 000 000 je vyděleno z 1 024. Pokud výsledek není celé číslo, pak je hodnota zaokrouhlena dolů. V tomto případě 10 000 000, dělených 1 024, se rovná 9,765.625. Hodnota 0.625 je vypuštěna, aby se získala hodnota 9,765 pro část šířky pásma složené metriky, jak je znázorněno na obrázku 2.

Zpoždění

Stejná odchozí rozhraní se používají, k určení hodnoty zpoždění, jak je znázorněno na obrázku 3.

EIGRP používá součet všech zpoždění do cíle. Rozhraní Serial 0/0/1, na R2, má zpoždění 20 000 mikrosekund. Gigabitové rozhraní 0/0 na R3 má zpoždění 10 mikrosekund. Součet těchto zpoždění je děleno 10. V příkladu (20 000 + 10)/10, výsledkem je hodnota 2 001 pro zpožďovací část kompozitní metriky.

Výpočet metriky

Použijte vypočtené hodnoty pro šířku pásma a zpoždění v metrickém vzorci. Výsledkem je metrická hodnota 3,012,096, jak je znázorněno na obrázku 4. Tato hodnota odpovídá hodnotě uvedené ve směrovací tabulce R2.

14.3.5 Tabulka Topologie a DUAL

14.3.5.1 Koncepty DUAL

EIGRP používá Algoritmus Difuzní Aktualizace (DUAL), který poskytuje nejlepší cestu bez smyček a cesty bez zpětných vazeb.

DUAL používá několik termínů, které jsou podrobněji popsány v této části:

- Successor (Nástupce)
- Dosažitelná vzdálenost (FD)
- Dosažitelný nástupce (FS)
- Ohlášená vzdálenost (RD) nebo reklamní vzdálenost (AD)
- Realizovatelná podmínka nebo podmínka proveditelnosti (FC)

Tyto termíny a pojmy jsou v centru mechanismu vyhýbání se smyčkám.

14.3.5.2 Úvod do DUAL

EIGRP používá konvergentní algoritmus DUAL. Konvergence je kritická pro síť, aby se zabránilo smyčkám směrování.

Směrovací smyčky, dokonce i dočasné, mohou být škodlivé pro výkon sítě. Protokoly pro směrování vektorů vzdálenosti, jako je RIP, zabraňují smyčkám směrování s časovači přerušení a horizontem rozdělení. Ačkoli EIGRP používá obě tyto techniky, používá je trochu jinak. Primárním způsobem, jakým EIGRP zabraňuje smyčkám směrování, je algoritmus DUAL.

Kliknutím na tlačítko Přehrát na obrázku zobrazíte základní operace DUAL.

DUAL algoritmus se používá pro získání volné smyčky ve všech případech během výpočtu trasy. To umožňuje synchronizovat všechny směrovače, zapojené do změny topologie současně. Směrovače, které nejsou ovlivněny změnami topologie, nejsou zapojeny do překomponování. Tato metoda poskytuje EIGRP, rychlejší konvergenční časy než jiným protokolům směrování vektorových vzdáleností.

Proces rozhodování pro všechny výpočty tras, provádí DUAL přes Finite State Machine (FSM). FSM je model, podobný vývojovému diagramu, který se skládá z následujících položek:

- Konečný počet etap (stavů)
- Přechody mezi těmito etapami
- Operace

DUAL FSM, sleduje všechny trasy, využívá metriky EIGRP k výběru efektivních cest bez smyček a určuje trasy s nejlevnější cenou cesty, která má být vložena do směrovací tabulky.

Překomponování algoritmu DUAL, může být náročné na procesor. EIGRP se vyhne překomponování, kdykoli je to možné, tím, že udrží seznam zálohovacích cest, které již DUAL považoval za bez smyčkové. Pokud selže hlavní cesta ve směrovací tabulce, nejlepší trasa zálohy se okamžitě přidá do směrovací tabulky.

14.3.5.3 Nástupce a Dosažitelná Vzdálenost

Obrázek 1 ukazuje topologii tohoto tématu. Nástupcem je sousední směrovač, který se používá pro přesměrování paketů a je nejméně nákladnou cestou do cílové sítě. IP adresa nástupce je zobrazena ve sloupci směrovací tabulky hned za slovem via.

FD je nejnižší vypočítaná metrika pro dosažení cílové sítě. FD je metrika uvedená v položce směrovací tabulky jako druhé číslo uvnitř závorek. Stejně jako u jiných směrovacích protokolů je toto také známé, jako metrika pro trasu.

Prozkoumáním směrovací tabulky pro R2 na obr. 2, si všimněte, že nejlepší cesta EIGRP pro síť 192.168.1.0/24, je přes R3 a že dosažitelná vzdálenost je 3,012,096. Toto je metrika, která byla vypočtena v předchozím tématu.

14.3.5.4 Dosažitelní Nástupci, Dosažitelné Podmínky a Ohlášená Vzdálenost

DUAL může rychle konvergovat po změně topologie, protože může použít zálohovací cesty do jiných sítí, bez re-kompozice. Tyto záložní cesty jsou známé, jako dosažitelní nástupci (FS).

FS je soused, který má záložní cestu bez smyček, do stejné sítě, jako nástupce a splňuje podmínku proveditelnosti (FC). Nástupcem R2 pro síť 192.168.1.0/24, je R3, který poskytuje nejlepší cestu, nebo nejnižší metriku cílové síti. Všimněte si na obr. 1, že R1 poskytuje alternativní cestu, ale je to FS? Předtím než R1 může být FS pro R2, musí nejprve splňovat standard FC.

Hodnota FC je splněna, pokud je sousedova ohlášená vzdálenost (RD) k síti menší než vzdálenost, kterou má místní směrovač ke stejné cílové síti. Je-li ohlášená vzdálenost menší, představuje trasu bez smyček. Uvedená vzdálenost, je prostě vzdálenost EIGRP souseda ke stejné cílové síti. Uvedená vzdálenost je metrika, kterou směrovač hlásí sousedovi, o svých vlastních nákladech do této sítě.

Na obr. 2, je dosažitelná vzdálenost R1 k 192.168.1.0/24, rovna 2,170,112.

- R1 hlásí R2, že jeho FD na 192.168.1.0/24 je 2 170 112.
- Z hlediska R2 je 2,170,112 RD na R1.

R2 používá tyto informace k určení, zda R1 splňuje FC, a zda může být FS.

Jak je znázorněno na obr. 3, protože RD na R1 je menší než vlastní FD na R2, tím R1 splňuje FC.

R1 je nyní FS pro R2 do sítě 192.168.1.0/24.

V případě selhání v cestě R2 na 192.168.1.0/24, přes R3, pak R2 okamžitě nainstaluje cestu přes R1 (FS) ve své směrovací tabulce. R1 se stává novým nástupcem cesty R2 k této síti, jak je znázorněno na obrázku 4.

14.3.5.5 Tabulka Topologie: Příkaz show ip eigrp topology

Obrázek 1 ukazuje topologii.

Tabulka topologie EIGRP, obsahuje všechny cesty, které jsou známé každému sousedovi. Protože směrovač zjistí trasy od sousedů, jsou tyto trasy instalovány v tabulce topologie EIGRP.

Jak je znázorněno na obrázku 2, použijte příkaz pro zobrazení tabulky topologie, ***show ip eigrp topology***. V tabulce topologie jsou uvedeni všichni nástupci a FS, které DUAL vypočítá pro cílové sítě. Pouze nástupce je nainstalován do směrovací tabulky IP.

14.3.5.6 Tabulka Topologie: Příkaz show ip eigrp topology

Jak je znázorněno na obrázku 1, první řádek v tabulce topologie zobrazuje:

- **P** - trasa v pasivním stavu. Pokud DUAL neprovádí výpočty rozptýlení pro určení cesty pro síť, trasa je ve stabilním režimu, známém jako pasivní stav. Pokud DUAL přepočítá nebo hledá novou cestu, trasa je v aktivním stavu a zobrazí A. Všechny cesty v tabulce topologie by měly být v pasivním stavu pro stabilní směrovací doménu.
- **192.168.1.0/24** - Cílová síť, která se také nachází ve směrovací tabulce.
- **1 nástupce** - Zobrazí počet nástupců pro tuto síť. Pokud do této sítě existuje několik stejných cen cest, existuje několik nástupců.
- **FD je 3012096** - FD, metrika EIGRP pro dosažení cílové sítě. Toto je metrika zobrazená ve směrovací tabulce IP.

Jak je znázorněno na obrázku 2, první pod-vstup na výstupu zobrazuje nástupce:

- **via 192.168.10.10** - adresa dalšího skoku nástupce, R3. Tato adresa je zobrazena ve směrovací tabulce.
- **3012096** - FD na 192.168.1.0/24. Je to metrika zobrazená ve směrovací tabulce.
- **2816** - RD nástupce a je to cena cesty R3, na dosažení této sítě.
- **Serial 0/0/1** - výstupní rozhraní použité k dosažení této sítě, které se také zobrazuje ve směrovací tabulce.

Jak je znázorněno na obrázku 3, druhá podkapitola zobrazuje FS, R1 (pokud neexistuje druhý záznam, pak neexistují žádné FS):

- **via 172.16.3.1** - adresa dalšího skoku FS, R1.
- **41024256** - Nové FD na R2 do 192.168.1.0/24, pokud se R1 stane novým nástupcem, tak bude i s novou metrikou zobrazenou ve směrovací tabulce IP.
- **2170112** – RD na FS nebo metrika R1 pro dosažení této sítě. RD musí být nižší, než je aktuální FD, aby splňoval standard FC.
- **Serial 0/0/0** - Toto je výstupní rozhraní použité pro dosažení FS, pokud se tento směrovač stane nástupcem.

14.3.5.7 Tabulka Topologie: Žádný Dosažitelný Nástupce

Chcete-li zjistit, jak DUAL používá nástupce a FS, prohlédněte směrovací tabulku R1, za předpokladu, že je síť konvergována, jak je znázorněno na obrázku 1.

Obrázek 2 zobrazuje částečný výstup z příkazu ***show ip route*** na R1. Cesta k 192.168.1.0/24 ukazuje, že nástupcem je R3 přes 192.168.10.6, s FD 2,170,112.

Směrovací tabulka IP, obsahuje pouze nejlepší cestu nástupce. Chcete-li zjistit, zda existují nějaké FS, musíme prozkoumat tabulku topologie EIGRP. Tabulka topologie na obrázku 3, ukazuje pouze nástupce 192.168.10.6, což je R3. Neexistují žádné FS. Při pohledu na aktuální fyzickou topologii nebo síťový diagram je zřejmé, že existuje cesta zálohování 192.168.1.0/24 přes R2. R2 není FS, protože nesplňuje FC. Ačkoli při pohledu na topologii je zřejmé, že R2 je záložní cesta, EIGRP nemá mapu síťové topologie. Je to vzdálený směrovací protokol a ví pouze o vzdálených síťových informacích, od svých sousedů.

DUAL neuloží trasu přes R2, do tabulky topologie. Všechny odkazy mohou být zobrazeny pomocí příkazu ***show ip eigrp all-links***. Tento příkaz zobrazí linky, zda vyhovují FC nebo nikoli.

Jak je znázorněno na obrázku 4, příkaz ***show ip eigrp topology all-links***, ukazuje všechny možné cesty k síti, včetně nástupců, FS a dokonce i těch tras, které nejsou FS. FD na R1 do 192.168.1.0/24 je 2,170,112 prostřednictvím nástupce R3. Aby R2 byl považován za FS, musí splňovat FC. RD na R2, do R1, k dosažení 192.168.1.0/24 musí být menší než aktuální R1. Podle čísla R2 je RD 3,012,096, což je vyšší než současný FD na R1.

I když R2 vypadá jako životaschopná záložní cesta k 192.168.1.0/24, R1 nemá tušení, že cesta není potenciální smyčkou zpětné vazby. EIGRP je protokol směrování vektorů vzdáleností, aniž by byl schopen vidět kompletní topologickou mapu sítě bez smyček. Metoda DUAL, která zaručuje, že soused má cestu bez smyček, je, že metrika souseda musí uspokojit FC. Tím, že zajistí, že RD souseda je menší než jeho vlastní FD, směrovač může předpokládat, že tento sousední směrovač není součástí vlastní inzerované trasy. Čímž se vždy vyhýbá potenciální smyčce.

R2 může být použit jako nástupce, pokud R3 selže. Je však delší prodleva před přidáním do směrovací tabulky. Předtím, než může být R2 použit jako nástupce, musí DUAL provádět další zpracování.

14.3.6 Konvergence a DUAL

14.3.6.1 DUAL Stroj Konečného Stavu (FSM)

Hlavním bodem systému EIGRP, je DUAL a jeho motor pro výpočet tras. Vlastním názvem této technologie je DUAL Finite State Machine (FSM). Obsahuje veškerou logiku použitou pro výpočet a porovnání tras, v síti EIGRP. Na obrázku je zjednodušená verze DUAL FSM.

FSM je abstraktní stroj, nikoliv mechanický přístroj s pohyblivými částmi. FSM definuje množinu možných stavů, které mohou projít určitou sadou událostí, jaké způsobují tyto stavy a jaké události jsou výsledkem těchto stavů. Návrháři používají nástroje FSM k popisu toho, jak algoritmus zařízení, počítačového programu nebo směrování reaguje na sadu vstupních událostí.

FSM jsou mimo rozsah tohoto kurzu. Koncept se však používá ke zkoumání některých výstupů, pomocí příkazu ***debug eigrp fsm***. Pomocí tohoto příkazu můžete zkontrolovat, co DUAL dělá při odstranění trasy ze směrovací tabulky.

14.3.6.2 DUAL: Dosažitelný Nástupce

R2 v současnosti používá R3, jako nástupce k 192.168.1.0/24. Kromě toho R2 aktuálně uvádí R1 jako FS, jak je znázorněno na obrázku 1.

Výstup R2, z příkazu ***show ip eigrp topology*** na obr. 2 ověřuje, že R3 je nástupcem a R1 je FS pro síť 192.168.1.0/24. Chcete-li porozumět tomu, jak DUAL může používat FS, když cesta s nástupcem již není k dispozici, tím je selhání spojení, simulováno mezi R2 a R3.

Před simulací selhání, musí být ladění DUAL povoleno, pomocí příkazu ***debug eigrp fsm*** na R2, jak je znázorněno na obrázku 3. Selhání spojení je simulováno pomocí příkazu ***shutdown*** na rozhraní Serial 0/0/1.

Výstup ladění, zobrazuje aktivitu generovanou DUAL při propojení linek. R2 musí informovat všechny sousedy EIGRP o ztraceném propojení a také aktualizovat vlastní tabulky směrování a topologie. Tento příklad zobrazuje pouze vybraný výstup ladění. Zejména zjistíte, že FSM vyhledá a najde FS pro trasu v tabulce topologie EIGRP.

FS na R1 se stává nástupcem a je instalován ve směrovací tabulce jako nová nejlepší cesta k 192.168.1.0/24, jak je znázorněno na obrázku 4. U FS se tato změna směrovací tabulky stane téměř okamžitě.

Jak je vidět na obrázku 5, tabulka topologie pro R2 nyní ukazuje, že R1 je nástupce a neexistují žádné nové FS. Pokud je spojení mezi R2 a R3 aktivováno znovu, R3 se vrátí jako nástupce a R1 se opět stává FS.

14.3.6.3 DUAL: Žádný Dosažitelný Nástupce

Příležitostně, cesta k nástupci selže a neexistují žádné FS. V tomto případě DUAL nemá zaručenou cestu zálohování bez síťové smyčky, takže cesta není v tabulce topologie jako FS. Pokud v tabulce topologie neexistují žádné FS, DUAL uvede síť do aktivního stavu. Pak se aktivně dotáže svých sousedů o nového nástupce.

R1 v současné době používá R3 jako nástupce k 192.168.1.0/24, jak je znázorněno na obrázku 1. Nicméně R1 nemá R2 uveden jako FS, protože R2 nesplňuje FC. Chcete-li pochopit, jak DUAL hledá nového nástupce, pokud neexistuje FS, je selhání spojení simulováno mezi R1 a R3.

Předtím, než je simulováno selhání propojení, je povoleno ladění DUAL pomocí příkazu ***debug eigrp fsm*** na R1, jak je znázorněno na obrázku 2. Selhání spojení je simulováno pomocí příkazu ***shutdown*** na rozhraní Serial 0/0/1.

Když nástupce již není k dispozici a neexistuje žádný možný nástupce, DUAL uvede cestu do aktivního stavu. Pak pošle dotazy EIGRP, které požadují od ostatních směrovačů cestu k síti. Jiné směrovače vracejí odpovědi a umožňují odesílateli dotazu zjistit, zda mají nebo nemají cestu k požadované síti. Pokud žádná z odpovědí nemá cestu k této síti, odesílatel dotazu nemá k této síti žádnou cestu.

Vybraný výstup ladění na obr. 2, ukazuje síť 192.168.1.0/24, vloženou do aktivního stavu a dotazy EIGRP zaslané jiným sousedům. R2 odpoví s cestou k této síti, která se stává novým nástupcem a je nainstalována do směrovací tabulky.

Pokud odesílatel dotazů, obdrží odpovědi, které obsahují cestu k požadované síti, přidá se preferovaná cesta, jako nový nástupce a přidá se do směrovací tabulky. Tento proces trvá déle, než kdyby DUAL měl ve své tabulce topologie FS a byl by schopen rychle přidat novou trasu do směrovací tabulky. Na obr. 3 si všimněte, že R1 má novou trasu k síti 192.168.1.0/24. Novým nástupcem je směrovač R2.

Obrázek 4 ukazuje, že tabulka topologie pro R1, má nyní R2 jako nástupce bez nových FS. Pokud je spojení mezi R1 a R3 opět aktivní, R3 se vrátí jako nástupce. Avšak R2 stále není FS, protože nesplňuje FC.

14.4 Konfigurace EIGRP pro IPv6

14.4.1 EIGRP pro IPv4 versus IPv6

14.4.1.1 EIGRP pro IPv6

Podobně jako jeho protějšek IPv4, IPv6 vyměňuje informace směrování, aby naplnil směrovací tabulku IPv6 se vzdálenými prefixy. EIGRP pro IPv6, byl k dispozici v Cisco IOS 12.4 (6)T.

Poznámka: V protokolu IPv6 se adresa sítě označuje jako prefix a maska podsítě se nazývá délka prefixu.

EIGRP pro IPv4 běží přes síťovou vrstvu, komunikuje s ostatními kolegy a inzeruje pouze trasy IPv4. EIGRP pro IPv6 má stejné funkce jako pro IPv4, ale používá protokol IPv6 jako síťovou vrstvu, komunikuje s EIGRP pro kolegy IPv6 a reklamní cesty.

EIGRP pro IPv6, také používá jako výpočetní modul DUAL, aby zajistil cestu bez smyčky a cestu bez zálohování v celé doméně směrování.

Stejně jako u všech směrovacích protokolů IPv6, EIGRP má oddělený proces od jeho protokolu IPv4. Procesy a operace jsou v podstatě stejné jako v protokolu IPv4. Nicméně, běží nezávisle. EIGRP pro IPv4 a IPv6, mají samostatné tabulky svazků, tabulky topologie a tabulky směrování IP, jak je znázorněno na obrázku. Jeto samostatný modul, závislý na protokolu (PDM).

Konfigurační a ověřovací příkazy EIGRP, pro konfiguraci a ověřování IPv6, jsou velmi podobné těm, které se používají pro IPv4. Tyto příkazy jsou popsány později v této části.

14.4.1.2 Porovnání EIGRP pro IPv4 a IPv6

Následuje srovnání hlavních rysů EIGRP pro IPv4 a IPv6:

- **Reklamní trasy** - EIGRP pro IPv4 inzeruje sítě IPv4. Zatímco EIGRP pro IPv6 inzeruje prefixy IPv6.
- **Distanční vektor** - EIGRP pro IPv4 a IPv6 jsou pokročilé protokoly směrování vektorových vzdáleností. Oba protokoly používají stejné administrativní vzdálenosti.
- **Konvergenční technologie** - využívají algoritmus DUAL. Oba protokoly používají stejné DUAL techniky a procesy, včetně nástupce, FS, FD a RD.

- **Metrika** - oba využívají šířku pásma, zpoždění, spolehlivost a zatížení pro jejich kompozitní metriku. Oba směrovací protokoly používají stejnou kompozitní metriku a ve výchozím nastavení používají pouze šířku pásma a zpoždění.
- **Transportní protokol** - RTP je zodpovědný, za zaručení dodávky paketů EIGRP všem sousedům pro oba protokoly.
- **Aktualizační zprávy** - posílají se přírůstkové aktualizace, při změně stavu cíle. Termíny, částečné a ohraničené, se používají při odkazu na aktualizace pro oba protokoly.
- **Mechanismus zjišťování sousedů** – využívá se jednoduchý mechanismus Hello, který se dozví o sousedních směrovačích a vytváří přidružení.
- **Adresy zdrojů a cílů** – odesílají se zprávy na adresu 224.0.0.10. Tyto zprávy používají zdrojovou adresu IPv4 výstupního rozhraní. EIGRP pro protokol IPv6 pošle své zprávy na multicast adresu, FF02 :: A. EIGRP zprávy IPv6, pochází z lokální adresy IPv6 výstupního rozhraní.
- **Autentizace** – využívá se autentizace službou MD5.
- **ID směrovače** – používá se 32bitové číslo pro ID směrovače. Je reprezentováno v desetinné notaci a je obvykle označováno jako adresa IPv4. Pokud směrovač EIGRP pro IPv6 nebyl nakonfigurován s adresou IPv4, musí se ke konfiguraci 32bitového identifikátoru směrovače, použít příkaz ***eigrp router-id***. Proces určení ID je pro oba stejný.

14.4.1.3 IPv6 Adresy Lokální Linky

Směrovače, které používají dynamický směrovací protokol, například EIGRP, si mohou vyměňovat zprávy mezi sousedy ve stejné podsíti nebo propojení. Směrovače potřebují odesílat a přijímat zprávy směrovacího protokolu, pouze s jejich přímo propojenými sousedy. Tyto zprávy jsou vždy odeslány ze zdrojové IP adresy směrovače, který provádí přesměrování.

Pro tento účel jsou ideální lokální adresy IPv6. Místní IPv6 adresa linky, umožňuje zařízením komunikovat s jinými zařízeními podporujícími protokol IPv6, na stejné lince a pouze v této podsíti. Pakety se zdrojovou nebo cílovou adresou lokální linky, nemohou být směrovány za linku, odkud vznikl paket.

EIGRP pro zprávy IPv6, jsou odesílány pomocí:

- **Zdrojová adresa IPv6** - Toto je adresa IPv6, která je lokální adresou výstupního rozhraní.

- **Cílová adresa IPv6** - Když paket musí být odeslán do multicast adresy, je odeslán na adresu IPv6 FF02 :: A, ze všech směrovačů s místní vazbou. Pokud paket může být odeslán, jako unicast adresa, je odeslán na místní adresu sousedního směrovače.

Poznámka: Místní adresy linek IPv6 jsou v rozsahu FE80 ::/10. Hodnota /10 udává, že prvních 10 bitů je 1111 1110 10xx xxxx, což vede k tomu, že první hextet, má rozsah 1111 1110 1000 0000 (FE80) až 1111 1110 1011 1111 (FEBF).

14.4.2 Konfigurace EIGRP pro IPv6

14.4.2.1 Síťová Topologie EIGRP pro IPv6

Obrázek 1 ukazuje topologii sítě, která se používá pro konfiguraci protokolu EIGRP pro IPv6. Pokud je síť spuštěna duálně, a to jak na IPv4, tak na IPv6 ve všech zařízeních, lze na všech směrovačích nakonfigurovat EIGRP pro IPv4 i IPv6. V této části se však zaměřujeme pouze na EIGRP pro IPv6.

Pro každý směrovač byly nakonfigurovány pouze globální unicast adresy IPv6.

Obrázky 2, 3 a 4 zobrazují konfigurace počátečního rozhraní na každém směrovači. Všimněte si hodnoty šířky pásma rozhraní z předchozích EIGRP, pro konfiguraci protokolu IPv4. Vzhledem k tomu, že protokol EIGRP pro IPv4 a IPv6 používá stejné metriky, ovlivňuje parametr šířky pásma, oba směrovací protokoly.

14.4.2.2 Konfigurace IPv6 Adresy Lokální Linky

Adresy lokálních linek, se automaticky vytvoří při přiřazení globální unicast adresy IPv6 na rozhraní. Globální adresy typu unicast, nejsou na rozhraní vyžadovány, avšak adresy lokální linky IPv6 jsou.

Pokud nejsou nakonfigurovány ručně, směrovače Cisco, vytvoří místní adresu spojení pomocí předpony FE80::/10 a procesu EUI-64, jak je znázorněno na obrázku 1. EUI-64 zahrnuje použití 48bitové MAC adresy, vložení FFFE uprostřed a převrácení sedmého bitu. Pro sériová rozhraní používá Cisco, MAC adresu rozhraní Ethernet. Směrovač s několika sériovými rozhraními může přiřadit stejnou adresu lokální linky, každému rozhraní IPv6, protože adresy lokálních linek, musí být na daném místě lokální.

Adresy lokálních linek, vytvořené pomocí formátu EUI-64, nebo v některých případech ID náhodných rozhraní, ztěžují rozpoznávání a zapamatování těchto adres. Vzhledem k tomu, že protokoly IPv6, pro směrování používají lokální unicast adresy IPv6 a další informace o adresách skoků ve směrovací tabulce, je běžnou praxí, že je to snadno rozpoznatelná adresa.

Konfigurace adresy ručně, poskytuje možnost vytvořit adresu, která je rozpoznatelná a snadněji zapamatovatelná.

Adresu lokální linky, lze nakonfigurovat ručně pomocí, stejného příkazu konfigurace rozhraní, který se používá k vytvoření globálních unicast adres IPv6, ale s různými parametry:

Router (config-if) # ipv6 address link-local-adresa link-local

Adresa lokální linky, má předponu v rozsahu FE80 až FEBF. Pokud začíná adresa tímto hextetem (segment 16 bitů), klíčové slovo **link-local** (lokální linka) musí odpovídat adrese.

Obrázek 2 zobrazuje konfiguraci adresy, pomocí ***ipv6 address***. Adresa lokální linky FE80 :: 1 se používá k tomu, aby byla snadno rozpoznatelná jako součást směrovače R1. Stejná lokální adresa spojení IPv6, je nakonfigurována na všech rozhraních R1. FE80 :: 1 a může být nakonfigurována na každé lince, protože musí být jedinečná.

Podobně jako R1, na obrázku 3 je směrovač R2 konfigurován s FE80 :: 2 jako lokální adresou IPv6 na všech jeho rozhraních.

14.4.2.3 Konfigurace Procesu Směrování EIGRP pro IPv6

Příkaz ***ipv6 unicast-routing***, umožňuje směrování protokolu IPv6 na směrovači. Tento příkaz je vyžadován před konfigurováním protokolu IPv6. Tento příkaz není nutný ke konfiguraci adresy IPv6 na rozhraní, ale je nutný, aby byl směrovač povolen pro IPv6.

EIGRP pro IPv6

Následující příkaz globálního konfiguračního režimu slouží k zadání režimu konfigurace směrovače EIGRP pro IPv6:

Router (config) # ipv6 router eigrp autonomní systém

Podobně jako EIGRP pro IPv4 musí být hodnota autonomního systému stejná ve všech směrovačích v doméně. Na obr. 1, nebylo možné nakonfigurovat proces směrování EIGRP pro protokol IPv6, dokud nebylo povoleno směrování IPv6 příkazem ***ipv6 unicast-routing***.

ID směrovače

Jak je znázorněno na obrázku 2, příkaz ***eigrp router-id***, se používá ke konfiguraci ID směrovače. EIGRP pro IPv6, používá hodnotu identifikátoru směrovače, 32 bitů. Chcete-li získat tuto hodnotu, použijete stejný proces jako při protokolu IPv4. Příkaz ***eigrp router-id***, má

přednost před libovolnými adresami IPv4, se zpětnou vazbou nebo fyzickým rozhraním. Pokud EIGRP pro IPv6 nemá žádné aktivní rozhraní s adresou IPv4, pak je vyžadován příkaz ***eigrp router-id***.

ID směrovače by mělo být jedinečné 32bitové číslo v doméně směrování. Jinak se mohou vyskytnout nesrovnalosti ve směrování.

Poznámka: Příkaz ***eigrp router-id***, slouží ke konfiguraci ID směrovače. Některé verze systému IOS budou přijímat příkaz ***router-id***, aniž byste nejprve zadali ***eigrp***.

Ve výchozím nastavení je proces EIGRP pro IPv6, ve stavu vypnutí. Pro aktivaci procesu není vyžadován příkaz vypnutí, jak je znázorněno na obrázku 3. Tento příkaz není vyžadován ani pro IPv4. Ačkoli pro IPv6 je povoleno, sousední přidružení a směrovací aktualizace nelze odeslat a přijímat, dokud EIGRP není aktivován na příslušných rozhraních.

Příkaz ***no shutdown*** a identifikátor směrovače jsou vyžadovány pro směrovač, který tvoří sousední přidružení.

Obrázek 4 ukazuje kompletní konfiguraci protokolu EIGRP IPv6, pro směrovač R2.

Použijte kontrolu syntaxe na obr. 5, pro konfiguraci procesu EIGRP IPv6 na směrovači R3.

14.4.2.4 Příkaz ipv6 eigrp interface

EIGRP pro IPv6, používá jinou metodu pro povolení rozhraní. Namísto použití příkazu ***network***, režimu konfigurace síťového směrovače pro zadání odpovídajících adres rozhraní, tak si je nakonfigurují přímo na rozhraní.

Pro povolení EIGRP IPv6 na rozhraní, použijte následující příkaz konfigurace rozhraní:

Router (config-if) # ipv6 eigrp autonomní systém

Hodnota autonomního systému, musí být stejná jako autonomní systémové číslo použité pro povolení směrovacího procesu EIGRP. Podobně jako příkaz network, použitý v protokolu IPv4, příkaz ***ipv6 eigrp interface***:

- Umožňuje rozhraní vytvářet přidružení a odesílat nebo přijímat aktualizace
- Obsahuje prefix tohoto rozhraní pro aktualizace směrování IPv6

Obrázek 1 ukazuje konfiguraci umožňující EIGRP na směrovačích R1 a R2. Všimněte si zprávy na sériovém rozhraní 0/0/0 v R2:

% DUAL-5-NBRCHANGE: EIGRP-IPv6 2: Neighbor FE80::1 (Serial0/0/0) is up: new adjacency

Tato zpráva naznačuje, že R2 nyní vytvořil sousední přidružení se sousedem na adrese místní linky FE80::1. Vzhledem k tomu, že na všech třech směrovačích, byly nakonfigurovány statické adresy místních linek, je snadné zjistit, že tato sousednost je se směrovačem R1 (FE80::1).

Pomocí kontroly syntaxe na obrázku 2, povolíte na rozhraní EIGRP IPv6 na R3.

Pasivní rozhraní s protokolem EIGRP pro protokol IPv6

Stejný příkaz ***passive-interface***, který se používá pro protokol IPv4, slouží ke konfiguraci rozhraní jako pasivní, s protokolem EIGRP IPv6. Jak je ukázáno na obrázku 3, příkaz ***show ipv6 protocols***, se používá k ověření konfigurace.

14.4.3 Verifikace EIGRP pro IPv6

14.4.3.1 Verifikace EIGRP pro IPv6: Zkoumání Sousedů

Podobně jako u protokolu EIGRP pro protokol IPv4, než mohou být odesílány nebo přijímány aktualizace, směrovače musí stanovit sousední přidružení, jak je znázorněno na obrázku 1.

Pomocí příkazu ***show ipv6 eigrp neighbors***, vidíte tabulku sousedů a ověříte, zda EIGRP pro IPv6, vytvořil sousední přidružení. Výstup zobrazený na obrázku 2, zobrazuje adresu IPv6 propojení souseda a rozhraní, které tento směrovač používá k dosažení tohoto souseda EIGRP. Použití smysluplných adres lokálních linek, usnadňuje rozpoznání sousedů u R2 FE80::2 a u R3 FE80::3.

Výstup z příkazu ***show ipv6 eigrp neighbors***, zahrnuje:

- **H sloupec** - Seznamy sousedů v pořadí, ve kterém se naučili.
- **Adresa** - adresa IPv6 - místní adresa souseda.
- **Rozhraní** - Místní rozhraní, na kterém byl přijat Hello paket.
- **Zadržení** - aktuální čas zadržení. Když je přijat Hello paket, tato hodnota je resetována na maximální dobu zadržení, pro toto rozhraní a poté se počítá na nulu. Pokud je dosaženo nuly, soused je považován za deaktivovaný.
- **Uptime** - Doba, od které byl tento soused přidán do tabulky sousedů.
- **SRTT a RTO** - používané RTP, pro správu spolehlivých paketů EIGRP.
- **Počítání fronty** - Mělo by být vždy nula. Je-li hodnota větší než nula, EIGRP pakety čekají na odeslání.

- **Číslo sekvence** - slouží k sledování aktualizací, dotazů a odpovědí paketů.

Příkaz ***show ipv6 eigrp neighbors***, je užitečný pro ověření a odstraňování problémů s protokolem EIGRP. Pokud očekávaný soused není uveden, ujistěte se, že oba konce propojení jsou Aktivní/Aktivní, pomocí příkazu ***show ipv6 interface brief***. Stejné požadavky existují pro vytvoření sousedních přidružení, jako u IPv4. Pokud mají obě strany spojení aktivní rozhraní, zkontrolujte zda:

- Jsou oba směrovače konfigurovány se stejným autonomním číslem systému EIGRP?
- Je na rozhraní povoleno EIGRP pro IPv6 se správným autonomním systémovým číslem?

14.4.3.2 Verifikace EIGRP pro IPv6: Příkaz show ip protocols

Příkaz ***show ipv6 protocols***, zobrazuje parametry a další informace o stavu jakýchkoli aktivních směrovacích protokolech IPv6, které jsou na směrovači aktuálně nakonfigurovány. Příkaz zobrazuje různé typy výstupů specifické pro každý směrovací protokol IPv6.

Výstup na obrázku označuje několik parametrů protokolu EIGRP, pro dříve popsané parametry IPv6, včetně:

1. EIGRP pro IPv6 je aktivní dynamický směrovací protokol na R1 konfigurovaném s autonomním systémovým číslem 2.

2. Jedná se o hodnoty k, použité pro výpočet kompozitních metrik EIGRP. K1 a K3 jsou standardně 1 a K2, K4 a K5 jsou ve výchozím nastavení 0.

3. Identifikátor směrovače EIGRP pro IPv6 R1, je 1.0.0.0.

4. Stejné jako EIGRP pro IPv4, pro IPv6 mají administrativní vzdálenosti vnitřní AD 90 a externí 170 (výchozí hodnoty).

5. Rozhraní povolená pro protokol EIGRP pro protokol IPv6.

Výstup z příkazu ***show ipv6 protocols***, je užitečný při ladění operací směrování. V sekci Rozhraní je uvedeno, která rozhraní jsou povolena. To je užitečné pro ověření, zda je EIGRP povolen na všech vhodných rozhraních se správným autonomním systémovým číslem.

14.4.3.3 Verifikace EIGRP pro IPv6: Zkoumání Směrovací Tabulky

Stejně jako u všech směrovacích protokolů je cílem naplnit směrovací tabulku IP s trasami do vzdálených sítí a najít nejlepší cesty k dosažení těchto sítí. Stejně jako u protokolu IPv4 je důležité zkontrolovat směrovací tabulku IPv6 a určit, zda je naplněna správnými cestami.

Směrovací tabulka IPv6, se zkoumá pomocí příkazu ***show ipv6 route***. EIGRP pro trasy protokolu IPv6 jsou označeny ve směrovací tabulce jako D, podobně jako u IPv4.

Obrázek 1 ukazuje, že R1 ve své směrovací tabulce IPv6 nainstaloval tři trasy EIGRP do vzdálených sítí IPv6:

- 2001:DB8:CAFE:2::/64 via R3 (FE80:3) pomocí rozhraní Serial 0/0/1
- 2001:DB8:CAFE:3::/64 via R3 (FE80:3) pomocí rozhraní Serial 0/0/1
- 2001:DB8:CAFE:A002::/64 via R3 (FE80:3) pomocí rozhraní Serial 0/0/1

Všechny tři trasy používají R3, jako směrovač nástupce. Všimněte si, že směrovací tabulka používá jako adresu příštího hopu, adresu lokální linky. Vzhledem k tomu, že každý směrovač měl všechna rozhraní konfigurovaná s jedinečnou a odlišnou linkovou adresou, lze snadno rozpoznat, že další směrovač přes FE80::3, je směrovač R3.

Obrázek 2 zobrazuje směrovací tabulku IPv6 na R2.

Obrázek 3 zobrazuje směrovací tabulku na R3. Všimněte si, že R3 má dvě stejné ceny cest 2001:DB8:CAFE:A001::/64. Jedna cesta je přes R1 FE80::1 a druhá cesta je přes R2 FE80::2.

14.5 Shrnutí

14.5.1 Shrnutí

14.5.1.1 Aktivita třídy – Portfolio RIP a EIGRP

Portfolio RIP a EIGRP

Připravujete portfoliový soubor pro porovnání protokolů směrování RIP a EIGRP.

Přemýšlejte o síti se třemi propojenými směrovači s každým směrovačem, který poskytuje LAN pro počítače, tiskárny a další koncová zařízení. Grafika na této stránce zobrazuje jeden příklad takovéto topologie.

V tomto scénáři modelování činnosti budete vytvářet, adresovat a konfigurovat topologii pomocí ověřovacích příkazů a porovnávat/kontrastovat, výstupy protokolů RIP a EIGRP.

Dokončete otázky týkající se odrazu v PDF, doprovázející tuto činnost. Uložte svou práci a buďte připraveni sdílet své odpovědi s třídou. Uložte také kopii své práce pro pozdější použití v rámci tohoto kurzu nebo pro odkaz na portfolio.

14.5.1.2 Shrnutí

EIGRP je beztřídní vektorový směrovací protokol. Je rozšířením dalšího směrovacího protokolu IGRP, který je nyní zastaralý. EIGRP byl zpočátku vydán v roce 1992, jako protokol Cisco, který je k dispozici pouze u zařízení Cisco. V roce 2013 společnost Cisco vydala IETF základní funkcionalitu EIGRP, jako otevřeného standardu.

EIGRP používá zdrojový kód "D" pro DUAL ve směrovací tabulce. EIGRP má výchozí administrativní vzdálenost 90 pro vnitřní cesty a 170 pro trasy importované z externího zdroje, například výchozí trasy.

EIGRP je pokročilý směrovací protokol vzdáleného vektoru, který obsahuje funkce, které se nenacházejí v jiných protokolech směrování vektorů vzdálenosti, jako je RIP. Mezi tyto funkce patří: difuzní aktualizační algoritmus (DUAL), zřizování sousedních přidružení, spolehlivý přenosový protokol (RTP), částečné a ohraničené aktualizace a rovnoměrné a nerovnoměrné vyvážení zatížení.

EIGRP využívá PDM (protokolově závislé moduly), které jej umožňují podporovat různé protokoly 3. vrstvy, včetně protokolů IPv4 a IPv6. EIGRP používá jako transportní vrstvu protokol RTP, k dodávce paketů EIGRP. EIGRP využívá spolehlivé doručení pro aktualizace, dotazy a odpovědi. A používá nespolehlivé doručení pro Hello pakety a potvrzení. Spolehlivý protokol RTP znamená, že musí být vráceno potvrzení EIGRP.

Před odesláním aktualizací EIGRP, musí směrovač nejprve objevit své sousedy. To se provádí pomocí Hello paketů. Hodnoty Hello a Zadržení se nemusí shodovat se dvěma směrovači, aby se staly sousedy. Příkaz ***show ip eigrp neighbors***, se používá k zobrazení tabulky sousedů a ověření toho, že EIGRP vytvořil sousední sousedství.

EIGRP neposílá pravidelné aktualizace jako RIP. EIGRP odešle částečné nebo ohraničené aktualizace, které zahrnují pouze změny trasy a pouze těm směrovačům, které jsou touto změnou ovlivněny. Kombinovaná metrika EIGRP využívá šířku pásma, zpoždění, spolehlivost a zatížení pro určení nejlepší cesty. Ve výchozím nastavení se používá pouze šířka pásma a zpoždění.

V centru EIGRP je algoritmus DUAL (difuzní aktualizační algoritmus). DUAL konečný stav, se používá k určení nejlepší cesty a potenciálních cest zálohování do každé cílové sítě. Nástupcem je sousední směrovač, který se používá k předávání paketů pomocí nejlevnější trasy do cílové sítě. Dosažitelná vzdálenost (FD) je nejnižší vypočítaná metrika, pro dosažení cílové sítě prostřednictvím nástupce. Reálný nástupce (FS) je soused, který má záložní cestu

bez smyček do stejné sítě jako nástupce a také splňuje podmínku proveditelnosti. Podmínka proveditelnosti (FC) je splněna, když ohlášená vzdálenost sousedů (RD) do sítě je menší, než je vzdálenost mezi místním směrovačem a stejnou cílovou sítí. Uvedená vzdálenost je prostě vzdálenost sousedů od cílové sítě.

EIGRP je konfigurován pomocí příkazu ***router eigrp autonomní-systém***. Hodnota autonomního systému, je ve skutečnosti ID procesu a musí být stejná ve všech směrovačích v směrovací doméně EIGRP. Příkaz ***network***, je podobný příkazu použitému u RIP. Je to klasická síťová adresa, přímo připojených rozhraní na směrovači. Zástupní maska je volitelný parametr, který lze použít pouze pro zahrnutí specifických rozhraní.

15 KAPITOLA 8 – ROZŠÍŘENÉ KONFIGURACE A ŘEŠENÍ PROBLÉMŮ EIGRP

15.1 Rozšířené Konfigurace a Řešení Problémů EIGRP

15.1.1 Úvod

15.1.1.1 Úvod

EIGRP je univerzální směrovací protokol, který lze vyladit mnoha způsoby. Dvěma nejdůležitějšími možnostmi vylepšení, jsou schopnost shrnutí tras a schopnost implementovat vyvažování zátěže. Další možnosti ladění, zahrnují schopnost propagace výchozích časovačů jemného vyladění a zavádění autentizace mezi sousedy EIGRP, za účelem zvýšení bezpečnosti.

Tato kapitola se zabývá těmito dalšími funkcemi ladění a příkazy konfiguračního režimu pro implementaci těchto funkcí pro protokoly IPv4 a IPv6.

15.2 Rozšířené Konfigurace EIGRP

15.2.1 Automatické Shrnutí

15.2.1.1 Topologie Sítě

Před jemným laděním funkcí EIGRP, začněte základní implementací.

Obrázek 1, zobrazuje síťovou topologii použitou pro tuto kapitolu.

Obrázky 2, 3 a 4, ukazují konfigurace rozhraní IPv4 a implementace EIGRP na R1, R2 a R3.

Typy sériových rozhraní a jejich přidružené šířky pásma, nemusí nutně odrážet běžné typy připojení, které se dnes nacházejí v sítích. Šířka pásma sériových linek použitých v této topologii, pomáhá vysvětlit výpočet metriky směrovacího protokolu a proces optimálního výběru cesty.

Všimněte si, že příkaz ***bandwidth***, na sériových rozhraních, byl použit k úpravě výchozí šířky pásma 1,544 kb/s.

V této kapitole se směrovač ISP, používá jako brána směrovací domény k Internetu. Všechny tři směrovače používají technologii Cisco IOS 15.2.

15.2.1.2 Automatické Shrnutí EIGRP

Jednou z nejběžnějších metod ladění EIGRP, je povolení a zakázání automatického shrnutí trasy. Sumarizace trasy, umožňuje směrovači společně seskupovat sítě a propagovat je jako jednu velkou skupinu, pomocí jedné shrnuté trasy. Schopnost shrnout cesty je nutná, kvůli rychlému růstu sítí.

Okrajový směrovač je směrovač, který sedí na okraji sítě. Tento směrovač musí být schopen propagovat, všechny známé sítě ve své tabulce směrování, na propojovací síťový směrovač nebo směrovač ISP. Tato konvergence může mít za následek velmi rozsáhlé tabulky cest. Představte si, že jeden směrovač měl 10 různých sítí a musel inzerovat všech 10 položek trasy do spojovacího směrovače. Co kdyby měl tento směrovač také 10 sítí a musel inzerovat všech 20 směrů na směrovač ISP? Pokud by každý podnikový směrovač sledoval tento vzor, směrovací tabulka směrovače ISP by byla obrovská.

Sumarizace snižuje počet položek v aktualizacích směrování a snižuje počet položek v místních směrovacích tabulkách. To také snižuje využití šířky pásma, pro směrování aktualizací a rychlejší výsledky vyhledávání směrovací tabulky.

Chcete-li omezit počet směrovacích reklam a velikost směrovacích tabulek protokolů, jako je EIGRP, použijte automatické shrnutí na třídních hranicích. To znamená, že EIGRP rozpoznává podsítě, jako jedinou síť třídy A, B nebo C a vytvoří pouze jednu položku ve směrovací tabulce souhrnné trasy. Výsledkem je, že veškerá návštěvnost určená pro podsítě přechází touto cestou.

Obrázek ukazuje příklad toho, jak funguje automatické shrnutí. R1 a R2 jsou konfigurovány pomocí EIGRP pro IPv4 s automatickým shrnutím. R1 má ve své směrovací tabulce tři podsítě: 172.16.1.0/24, 172.16.2.0/24 a 172.16.3.0/24. Ve struktuře síťového adresování, jsou všechny tyto podsítě považovány za součást větší sítě třídy B, 172.16.0.0/16. Vzhledem k tomu, že EIGRP na směrovači R1, je konfigurován pro automatické shrnutí, po odeslání aktualizace směrování na R2 shrnuje tři podsítě /24, jako jedinou síť 172.16.0.0/16, což snižuje počet odeslaných aktualizací směrování a počet vstupů v směrovací tabulce IPv4 na R2.

Celá návštěvnost určená pro tyto tři podsítě, přechází po jedné cestě. R2 neudržuje cesty k jednotlivým podsítím a nejsou načteny žádné informace o podsítích. V podnikové síti nemusí být zvolená cesta, pro dosažení souhrnné trasy, tou nejlepší volbou pro provoz, který se pokouší dosáhnout každé jednotlivé podsíti. Jediný způsob, jak všechny směrovače najdou nejlepší trasy pro každou jednotlivou podsíť, je, aby sousedé odesílali informace o podsítích. V

takovém případě, by mělo být automatické shrnutí zakázáno. Pokud je automatické shrnutí zakázáno, aktualizace obsahují informace o podsítích.

15.2.1.3 Konfigurace Automatického Shrnutí EIGRP

EIGRP pro automatické shrnutí protokolu IPv4 je standardně deaktivováno od Cisco IOS 15.0. Předtím bylo automaticky povoleno. To znamenalo, že EIGRP prováděl automatické shrnutí vždy, když topologie EIGRP překročila hranici mezi dvěma různými hlavními třídními sítěmi.

Na obrázku 1, výstup z příkazu ***show ip protokols*** na R1 indikuje, že automatické shrnutí EIGRP je zakázáno. Tento směrovač běží s IOS 15.2. Proto je automatické shrnutí EIGRP ve výchozím stavu zakázáno. Obrázek 2, ukazuje aktuální směrovací tabulku pro R3. Všimněte si, že směrovací tabulka IPv4 pro R3 obsahuje všechny sítě a podsítě v směrovací doméně EIGRP.

Chcete-li povolit automatické shrnutí pro EIGRP, použijte příkaz ***auto-summary***, jak je znázorněno na obrázku 3:

R1 (config) # router eigrp as-number

R1 (config-router) # auto-summary

Žádná forma tohoto příkazu se nepoužívá k vypnutí automatického shrnutí.

Použijte kontrolu syntaxe na obrázku 4, abyste povolili automatické shrnutí pro R3.

15.2.1.4 Verifikace Automatického Shrnutí: show ip protocols

Na obrázku 1 si všimněte, že směrovací doména EIGRP má tři klasické sítě:

- Síť 172.16.0.0/16 třídy B, sestávající z podsítí 172.16.1.0/24, 172.16.2.0/24 a 172.16.3.0/30
- Síť 192.168.10.0/24 třídy C, sestávající z podsítí 192.168.10.4/30 a 192.168.10.8/30
- Síť 192.168.1.0/24 třídy C, která nemá podsíť

Výstup R1 z příkazu ***show ip protocols*** na obr. 2 ukazuje, že je nyní povoleno automatické shrnutí. Výstup také označuje sítě, které jsou shrnuty a na kterých rozhraních. Všimněte si, že R1 shrnuje dvě sítě v jeho aktualizacích směrování EIGRP:

- 192.168.10.0/24 odeslal na rozhraní GigabitEthernet 0/0 a Serial 0/0/0
- 172.16.0.0/16 vyslal na rozhraní Serial 0/0/1

R1 má podsítě 192.168.10.4/30 a 192.168.10.8/30 ve své směrovací tabulce IPv4.

Jak je uvedeno na obrázku 3, R1 shrnuje podsíť 192.168.10.4/30 a 192.168.10.8/30. Předává souhrnnou adresu 192.168.10.0/24 svým sousedům na rozhraní Serial 0/0/0 a GigabitEthernet 0/0. Vzhledem k tomu, že R1 nemá žádné sousedy EIGRP na rozhraní GigabitEthernet 0/0, souhrnnou aktualizaci směrování přijímá pouze R2.

Jak je uvedeno na obrázku 4, R1 má také podsítě 172.16.1.0/24, 172.16.2.0/24 a 172.16.3.0/30 ve své směrovací tabulce IPv4. R3 vybírá R1 jako nástupce k 172.16.0.0/16, protože má nižší dosažitelnou vzdálenost. Rozhraní R3 S0/0/0, které je připojeno k R1, používá výchozí šířku pásma 1,544 kb/s. Spojení R3 s R2 má vyšší dosažitelnou vzdálenost, protože rozhraní R3 S0/0/1, bylo nakonfigurováno s nižší šířkou pásma 1024 kb/s.

Všimněte si, že souhrnná aktualizace 172.16.0.0/16, není odeslána rozhraním R1 GigabitEthernet 0/0 a Serial 0/0/0. Je to proto, že tato dvě rozhraní, jsou členy stejné sítě 172.16.0.0/16 třídy B. Nesouhrnná aktualizace 172.16.1.0/24 směrování, je odeslána z R1 na R2. Souhrnné aktualizace se vysílají pouze v rozmanitých třídních sítích.

15.2.1.5 Verifikace Automatického Shrnutí: Tabulka Topologie

Na obr. 1, směrovače R1 a R2 pošlou R3, souhrnnou aktualizaci směrování EIGRP 172.16.0.0/16. Směrovací tabulky pro R1 a R2, obsahují podsítě sítě 172.16.0.0/16. Proto oba směrovače odesílají souhrnnou reklamu, přes jinou hlavní síť na R3.

Obrázek 2, ukazuje výstup z příkazu ***show ip eigrp topology all-links***, použitého pro zobrazení úplné tabulky topologie R3. To ověřuje, že R3 obdržel souhrnnou cestu 172.16.0.0/16 z obou R1 192.168.10.5 a R2 192.168.10.9. První vstup přes 192.168.10.5, je nástupcem a druhý vstup přes 192.168.10.9 je možným nástupcem. R1 je nástupcem, protože jeho propojení 1 544 kb/s na R3 má lepší metriku EIGRP na 172.16.0.0/16 směrovače R2, který používá pomalejší linku o kapacitě 1 024 kb/s.

Možnost ***all-links***, zobrazuje všechny přijaté aktualizace, zda se trasa kvalifikuje jako úspěšný nástupce (FS), nebo ne. V tomto případě se R2 kvalifikuje jako FS. Je považován za FS, protože jeho ohlášená vzdálenost (RD) 2,816, je menší než dosažitelná vzdálenost (FD) 2,170,112 na R1.

15.2.1.6 Verifikace Automatického Shrnutí: Směrovací Tabulka

Zkontrolujte směrovací tabulku a ověřte, zda byla Celková trasa přijata.

Obrázek 1, znázorňuje směrovací tabulku R3, před automatickým shrnutím a poté pomocí automatického shrnutí povoleného, pomocí příkazu ***auto-summary***. Všimněte si, že s povoleným automatickým shrnutím, směrovací tabulka R3, nyní obsahuje pouze síťovou adresu třídy B, 172.16.0.0/16. Nástupce, nebo směrovač dalšího skoku je, R1 přes 192.168.10.5.

Poznámka: Automatické shrnutí je pouze možností u protokolu EIGRP IPv4. V protokolu IPv6 neexistuje klasické adresování. Proto není potřeba automatického shrnutí EIGRP pro protokol IPv6.

Při povolení automatického shrnutí, je třeba také pochopit rozhraní Null. Obrázek 2, ukazuje směrovací tabulku pro R1. Všimněte si, že dvě zvýrazněné položky používají výstupní rozhraní Null0. EIGRP automaticky zahrnul celkovou cestu k Null0, pro dvě klasické sítě 192.168.10.0/24 a 172.16.0.0/16.

Rozhraní Null0, je virtuální rozhraní IOS, které je cestou nikam, běžně nazývané "bitový kbelík". Pakety, které odpovídají trase s výstupným rozhraním Null0, jsou vyřazeny.

EIGRP pro protokol, IPv4 automaticky obsahuje celkovou trasu Null0, pokud existují následující podmínky:

- K dispozici je, alespoň jedna podsít, která byla naučena přes EIGRP.
- Existují dva nebo více příkazů režimu konfigurace směrovače EIGRP, ***network***.
- Automatické shrnutí je povoleno.

Účelem souhrnné cesty Null0, je zabránit smyčkám směrování pro cíle, které jsou obsaženy ve shrnutí, ale ve směrovací tabulce skutečně neexistují.

15.2.1.7 Celková Trasa

Obrázek znázorňuje scénář, kdy by se mohla objevit směrovací smyčka:

1. R1 má výchozí trasu, 0.0.0.0/0 prostřednictvím směrovače ISP.

2. R1 vyšle aktualizaci směrování na R2 obsahující výchozí trasu.

3. R2 nainstaluje výchozí trasu z R1 do své směrovací tabulky IPv4.

4. Směrovací tabulka R2 obsahuje podsítě 172.16.1.0/24, 172.16.2.0/24 a 172.16.3.0/24 ve své směrovací tabulce.

5. R2 odešle souhrnnou aktualizaci do R1 pro síť 172.16.0.0/16.

6. R1 nainstaluje souhrnnou trasu pro 172.16.0.0/16 přes R2.

7. R1 obdrží paket pro 172.16.4.10. Protože R1 má cestu přes 172.16.0.0/16 do R2, předá paket do R2.

8. R2 obdrží paket s cílovou adresou 172.16.4.10 z R1. Paket neodpovídá žádné konkrétní trase, takže pomocí výchozí trasy ve směrovací tabulce R2, předá paket zpátky do R1.

9. Paket pro 172.16.4.10, je za smyčkovaný mezi R1 a R2, dokud TTL neuplyne a pak paket padne.

15.2.1.8 Celková Trasa

EIGRP používá rozhraní Null0, k zabránění těchto typů smyček směrování. Obrázek znázorňuje scénář, kdy trasa Null0, zabraňuje smyčce směrování znázorněné v předchozím příkladu:

1. R1 má výchozí trasu, 0.0.0.0/0 prostřednictvím směrovače ISP.

2. R1 vyšle aktualizaci směrování na R2, obsahující výchozí trasu.

3. R2 nainstaluje výchozí trasu z R1 do své směrovací tabulky IPv4.

4. Směrovací tabulka R2, obsahuje podsítě 172.16.1.0/24, 172.16.2.0/24 a 172.16.3.0/24 ve své směrovací tabulce.

5. R2 nainstaluje souhrnnou cestu 172.16.0.0/16 do Null0, ve své směrovací tabulce.

6. R2 vyšle souhrnnou aktualizaci do R1 pro síť 172.16.0.0/16.

7. R1 nainstaluje souhrnnou trasu pro 172.16.0.0/16 přes R2.

8. R1 obdrží paket za 172.16.4.10. Protože R1 má cestu přes 172.16.0.0/16 přes R2, předá paket R2.

9. R2 obdrží paket pro cílovou adresou 172.16.4.10 z R1. Paket neodpovídá žádné specifické podsíti 172.16.0.0, ale odpovídá souhrnné cestě 172.16.0.0/16 Null0. Pomocí trasy Null0 je paket vyřazen.

Souhrnná trasa na R2 pro rozhraní 172.16.0.0/16 na rozhraní Null0, odmítá všechny pakety, začínající na 172.16., ale nemají delší shodu s žádnou z podsítí: 172.16.1.0/24, 172.16.2.0/24 , nebo 172.16.3.0/24.

I když R2 má výchozí trasu 0.0.0.0/0, ve své směrovací tabulce, trasa Null0 je delší shoda.

Poznámka: Souhrnná trasa Null0 je odstraněna, pokud je příkazem ***no auto-summary*** deaktivována.

15.2.2 Manuální Shrnutí

15.2.2.1 Manuální Shrnutí Tras

EIGRP může být nakonfigurován tak, aby používal manuální souhrnné trasy, ať už je povoleno automatické shrnutí, nebo ne. Vzhledem k tomu, že protokol EIGRP, je beztřídní směrovací protokol a obsahuje masku podsítě v aktualizacích směrování, ruční shrnutí může obsahovat trasy supernet. Nezapomeňte, že supernet je agregace několika hlavních síťových adres.

Na obr. 1, jsou do směrovače R3, přidány dvě další sítě, pomocí rozhraní zpětné vazby: 192.168.2.0/24 a 192.168.3.0/24. Přestože jsou rozhraní zpětných vazeb virtuálními rozhraními, používají se k reprezentaci fyzických, sítí pro tento příklad.

Obrázek 2, ukazuje příkazy R3, které konfigurují dvě rozhraní zpětné vazby a konfiguraci, aby se umožnily obě rozhraní pro EIGRP.

Chcete-li ověřit, zda R3 odeslala aktualizační pakety EIGRP, na R1 a R2, jsou směrovací tabulky zkoumány na obou směrovačích.

Na obr. 3 jsou zobrazeny pouze příslušné cesty. Řídicí tabulky R1 a R2 zobrazují tyto přídavní sítě ve svých směrovacích tabulkách: 192.168.2.0/24 a 192.168.3.0/24. Namísto odeslání tří samostatných sítí, může R3 shrnout sítě 192.168.1.0/24, 192.168.2.0/24 a 192.168.3.0/24, do jedné cesty.

15.2.2.2 Konfigurace Manuálního Shrnutí Tras EIGRP

Určení souhrnné trasy EIGRP

Obrázek 1, ukazuje dvě manuální souhrnné trasy, které jsou na R3 konfigurovány. Tyto souhrnné trasy jsou vysílány ze Serial 0/0/0 a Serial 0/0/1 rozhraní, k sousedům R3.

Chcete-li určit souhrn těchto tří sítí, použije se stejná metoda pro určení souhrnných statických cest, jak je znázorněno na obrázku 2:

Krok 1. Napište sítě, které mají být shrnuty v binárním kódu.

Krok 2. Chcete-li najít sumarizaci masky podsítě, začněte s bitem nejvíc vlevo.

Krok 3. Prací zleva doprava, najděte všechny bity, které odpovídají po sobě.

Krok 4. Pokud narazíte na sloupec bitů, které neodpovídají, zastavte. Toto je souhrnná hranice.

Krok 5. Spočítejte počet odpovídajících bitů zleva, což je v tomto příkladu 22. Toto číslo se používá k určení masky podsítě pro souhrnnou trasu: /22 nebo 255.255.252.0.

Krok 6. Chcete-li zjistit síťovou adresu pro shrnutí, zkopírujte odpovídajících 22 bitů a přidejte všechny bity 0, do konce a vytvořte 32 bitů.

Výsledkem je souhrnná síťová adresa a maska 192.168.0.0/22.

Nakonfigurujte manuální shrnutí EIGRP

Chcete-li vytvořit manuální shrnutí EIGRP na konkrétním rozhraní, použijte následující příkaz konfigurace rozhraní:

Router (config-if) # ip summary-address eigrp číslo-as adresa-sítě maska-sítě

Obrázek 2, ukazuje konfiguraci pro šíření manuální souhrnné trasy, na rozhraní Serial 0/0/0 společnosti R3. Vzhledem k tomu, že R3 má dvě sousedy EIGRP, musí být manuální shrnutí EIGRP, nakonfigurováno jak na Serial 0/0/0, tak na Serial 0/0/1.

Použijte kontrolu syntaxe na Obr. 3, pro konfiguraci stejné manuální souhrnné trasy na rozhraní Serial 0/0/1, směrovače R3.

15.2.2.3 Verifikace Manuálního Shrnutí Tras

Obrázek ukazuje, že po sestavení souhrnné trasy směrových tabulek R1 a R2, již neobsahují jednotlivé sítě 192.168.1.0/24, 192.168.2.0/24 a 192.168.3.0/24. Místo toho zobrazují jednu souhrnnou trasu 192.168.0.0/22. Souhrnné trasy redukují počet celkových tras v směrovacích tabulkách, což činí vyhledávací postup směrovací tabulky účinnější. Souhrnné trasy vyžadují také menší využití šířky pásma, pro směrování aktualizací, protože jedna trasa může být odeslána namísto více individuálních tras.

15.2.2.4 EIGRP pro IPv6: Manuální Shrnutí Tras

Zatímco auto-sumarizace není k dispozici pro sítě EIGRP IPv6, je možné nakonfigurovat ručně shrnuté trasy pro protokol EIGRP IPv6.

Obrázek 1 znázorňuje topologii EIGRP IPv6 se čtyřmi adresami zpětné vazby nakonfigurovanými na R3. Tyto virtuální adresy, slouží k reprezentování fyzických sítí ve směrovací tabulce R3. Tyto sítě lze manuálně shrnout do protokolu EIGRP pro protokol IPv6.

Obrázek 2 ukazuje konfiguraci adres zpětné vazby IPv6 na R3. Pouze čtyři adresy zpětné vazby, jsou zobrazeny v topologii a nakonfigurovány na R3. Avšak pro tento příklad se předpokládá, že všechny podsítě sítě 2001:DB8:ACAD::/48, jsou dostupné přes R3.

Chcete-li nakonfigurovat EIGRP, pro manuální shrnutí protokolu IPv6, na konkrétním rozhraní EIGRP, použijte následující příkaz konfigurace rozhraní:

Router (config-if) # ipv6 summary-address eigrp číslo-as prefix/délka-prefixu

Obrázek 3 ukazuje konfiguraci šíření v EIGRP, pro ruční souhrnnou cestu IPv6 na R1 a R2 pro prefix 2001:DB8:ACAD::/48. Podobně jako EIGRP pro protokol IPv4, R3 obsahuje souhrnnou cestu k Null0, jako mechanismus prevence smyček.

Příjem ruční souhrnné trasy, lze ověřit prohlížením směrovací tabulky ostatních směrovačů, v doméně směrování. Obrázek 4 ukazuje trasu 2001:DB8:ACAD::/48, v směrovací tabulce R1.

15.2.3 Propagace Výchozí Trasy

15.2.3.1 Propagace Výchozí Statické Trasy

Propagace Výchozí Statické Trasy

Použití statické cesty na 0.0.0.0/0, jako výchozí trasy, není závislé na směrovacím protokolu. Statická výchozí trasa "quad-zero", může být použita se všemi aktuálně podporovanými směrovacími protokoly. Statická výchozí trasa je obvykle nakonfigurována na směrovači, který má připojení k síti mimo směrovací doménu EIGRP. Například k ISP.

Na obrázku 1, je R2 směrovač brány, který propojuje směrovací doménu EIGRP s internetem. Pokud je statická výchozí trasa nakonfigurována, je nutné tuto trasu rozšířit v celé doméně EIGRP, jak je znázorněno na obrázku 2.

Jedna metoda propagace statické výchozí trasy ve směrovací doméně EIGRP, je pomocí příkazu ***redistribute static***. Příkaz ***redistribute static***, pověří EIGRP, aby zahrnul statické cesty v aktualizacích EIGRP, do jiných směrovačů. Obrázek 3, ukazuje konfiguraci statické výchozí trasy a příkazu ***redistribute static***, na směrovači R2.

Obrázek 4 ověřuje, že výchozí trasa byla přijata směrovačem R2 a nainstalována do její směrovací tabulky IPv4.

15.2.3.2 Verifikace Propagace Výchozí Trasy

Na obrázku je zobrazena část směrovacích tabulek IPv4 pro R1 a R3.

Ve směrovacích tabulkách pro R1 a R3, si všimněte zdroje směrování a administrativní vzdálenost, nové výchozí trasy načtené pomocí EIGRP. Položka naučené výchozí trasy EIGRP, se identifikuje následujícím způsobem:

D - Tato trasa byla naučena z aktualizace směrování EIGRP.

***** - Trasa je kandidátem na výchozí trasu.

EX - Trasa je externí trasa EIGRP, v tomto případě statická trasa mimo směrovací doménu.

170 - Jedná se o administrativní vzdálenost externí trasy EIGRP.

Všimněte si, že R1 vybírá R3 jako nástupce výchozí trasy, protože má nižší dosažitelnou vzdálenost. Výchozí trasy poskytují výchozí cestu mimo směrovací doménu a jako shrnutí tras minimalizují počet položek ve směrovací tabulce.

15.2.3.3 EIGRP pro IPv6: Výchozí Trasa

Připomeňme si, že EIGRP, obsahuje samostatné tabulky pro protokoly IPv4 a IPv6. Proto musí být výchozí trasa protokolu IPv6, propagována samostatně, jak je znázorněno na obrázku 1. Podobně jako u protokolu EIGRP, pro protokol IPv4, je na směrovači brány (R2) nakonfigurována statická výchozí trasa, jak je znázorněno na obrázku 2:

R2 (config) # ipv6 route ::/0 serial 0/1/0

Prefix s délkou prefixu, odpovídají adrese 0.0.0.0 a masce podsítě 0.0.0.0, použité v protokolu IPv4. Obě jsou nulové adresy a s délkou prefixu /0.

Výchozí statická trasa protokolu IPv6, je redistribuována do domény EIGRP pro IPv6, pomocí stejného statického příkazu redistribuce použitého v protokolu EIGRP pro protokol IPv4.

Poznámka: Některé IOS mohou vyžadovat, aby statický příkaz redistribuce obsahoval parametry EIGRP, aby mohla být statická trasa redistribuována.

Ověření šíření výchozí trasy

Propagaci výchozí statické trasy IPv6, lze ověřit zkoumáním směrovací tabulky IPv6 na R1, pomocí příkazu ***show ipv6 route***, jak je znázorněno na obrázku 3. Všimněte si, že adresa nástupce, nebo adresa následující skoku není R2, ale R3. Je to proto, že R3 poskytuje lepší cestu k R2, při nižší metrice nákladů než R1.

15.2.4 Doladění Rozhraní EIGRP

15.2.4.1 Míra Využití Šířky Pásma EIGRP

Šířka pásma EIGRP pro IPv4

Ve výchozím nastavení, EIGRP využívá až 50 procent šířky pásma rozhraní, pro informace EIGRP. To zabraňuje tomu, aby proces zbytečně využíval linku a neumožňoval dostatečnou šířku pásma pro směrování běžného provozu.

Pomocí příkazu ***ip bandwidth-percent eigrp***, nakonfigurujte procento šířky pásma, které může rozhraní EIGRP použít.

Router (config-if) # ip bandwidth-percent eigrp číslo-as procenta

Na obr. 1, sdílí R1 a R2 velmi pomalou linku 64 kb/s. Konfigurace, která omezuje šířku pásma EIGRP, je znázorněna na obrázku 2. Příkaz ***ip bandwidth-percent eigrp***, využívá množství konfigurované šířky pásma (nebo výchozí šířku pásma) při výpočet procent, které může EIGRP použít. V tomto příkladu je EIGRP omezen na ne více než 40 procent šířky pásma propojení. Proto EIGRP nikdy nepoužívá více než 32 kb/s šířky pásma linky pro přenos paketů EIGRP.

Chcete-li obnovit výchozí hodnotu, použijte příkaz, ***no ip bandwidth-percent eigrp*** .

Použijte kontrolu syntaxe na obrázku 3, abyste omezili šířku pásma, kterou používá EIGRP mezi R2 a R3, na 75 procent šířky pásma.

Šířka pásma EIGRP pro protokol IPv6

Chcete-li nakonfigurovat procenta šířky pásma, které může rozhraní EIGRP použít pro IPv6 na rozhraní, použijte v konfiguračním režimu rozhraní příkaz, ***ipv6 bandwidth-percent eigrp***. Chcete-li obnovit výchozí hodnotu, použijte do tohoto příkazu ***no*** na začátek.

Router (config-if) # ipv6 bandwidth-percent eigrp číslo-as procenta

Obrázek 4, ukazuje konfiguraci rozhraní mezi R1 a R2 pro omezení šířky pásma, které používá EIGRP pro protokol IPv6.

15.2.4.2 Časovač Zadržení a Časovač Hello

Intervaly Hello a Časy zadržení s EIGRP pro IPv4

EIGRP používá protokol Hello, pro lehké vyvážení a monitorování stavu připojení jeho souseda. Doba zadržení udává směrovači, maximální čas čekáni směrovače, než obdrží příští Hello předtím, než prohlásí, že soused je nedosažitelný.

Hello intervaly a časy zadržení, jsou konfigurovatelné na bázi rozhraní a nemusejí odpovídat jiným směrovačům EIGRP, aby vytvořili nebo udržovali sousední prostory. Příkaz pro konfiguraci jiného intervalu Hello je:

Router (config-if) # ip hello-interval eigrp číslo-as sekundy

Pokud se změní interval Hello, ujistěte se, že hodnota časového limitu je stejná nebo delší než byla. V opačném případě sousední přidružení klesne, po uplynutí času zadržení a před dalším intervalem Hello. Pomocí následujícího příkazu nakonfigurujte jiný čas Zadržení:

Router (config-if) # ip hold-time eigrp číslo-as sekundy

Hodnota sekund pro časové intervaly Hello a Zadržení se může pohybovat od 1 do 65 535.

Obrázek 1 ukazuje konfiguraci na R1, která používá 50 sekundový interval Hello a 150 sekundový čas Zadržení. Žádný formulář nelze použít u obou těchto příkazů k obnovení výchozích hodnot.

Doba intervalu Hello a času Zadržení, nemusí odpovídat mezi dvěma směrovači, aby vytvořily sousedství EIGRP.

Intervaly Hello a Časy zadržení s EIGRP pro IPv6

EIGRP pro protokol IPv6, používá stejný interval Hello a čas Zadržení, jako EIGRP pro protokol IPv4. Příkazy režimu konfigurace rozhraní jsou podobné příkazům pro protokol IPv4:

Router (config-if) # ipv6 hello-interval eigrp číslo-as sekundy

Router (config-if) # ipv6 hold-time eigrp číslo-as sekundy

Obrázek 3, ukazuje konfigurace R1 a R2, s EIGRP pro IPv6.

15.2.4.3 Vyvážení Zátěže IPv4

Rovnoměrné vyvažování zátěže, je schopnost směrovače distribuovat odchozí provoz pomocí všech rozhraní, která mají stejnou metriku od cílové adresy. Vyrovnávání zatížení využívá segmenty sítě a šířku pásma efektivněji. Pro protokol IP používá software Cisco IOS, ve výchozím nastavení vyrovnávání zatížení, až se čtyřmi stejnými cestami.

Obrázek 1, ukazuje EIGRP pro topologii sítě IPv4. V této topologii má R3, dvě sítě EIGRP rovnocenných nákladů, pro síť mezi R1 a R2, 172.16.3.0/30. Jedna trasa je přes R1 na 192.168.10.4/30 a druhá trasa je přes R2 na 192.168.10.8/30.

Příkaz ***show ip protocols***, lze použít k ověření počtu cest stejných nákladů, které jsou nakonfigurovány na směrovači. Výstup na obrázku 2 ukazuje, že R3 používá výchozí čtyři cesty s rovnými náklady.

Směrovací tabulka udržuje obě cesty. Obrázek 3 ukazuje, že R3 má dvě sítě EIGRP s rovnými náklady pro síť 172.16.3.0/30. Jedna trasa je přes R1 na 192.168.10.5 a druhá trasa je přes R2 na 192.168.10.9. Když se podíváme na topologii na obr. 1, zdá se, že cesta přes R1 je lepší, protože na trase mezi R3 a R1, existuje spojení 1544 kb/s. Zatímco spojení na R2 má pouze 1024 kb/s. EIGRP však používá pouze nejpomalejší šířku pásma ve své kompozitní metrice, což je spojení mezi R1 a R2 o kapacitě 64 kb/s. Obě cesty mají stejnou vazbu 64 kb/s, jako nejpomalejší šířku pásma, což vede k tomu, že obě cesty jsou stejné.

Když je paket, přepínán procesem vyvažování zatížení na cestách s rovnými náklady, objevuje na základě paketů. Pokud jsou pakety rychle přepínány, vyvažování zatížení na trasách s rovnými náklady, vzniká na základě cíle. Služba Cisco Express Forwarding (CEF) může provádět paketové vyvažování zátěže a taky vyvažování cílových destinací.

Cisco IOS ve výchozím nastavení umožňuje vyvažování zátěže, až se čtyřmi stejnými cestami. Nicméně to může být změněno. Pomocí příkazu režimu konfigurace směrovače, ***maximum-paths***, je možné ve směrovací tabulce uchovat až 32 tras s rovnými náklady.

Router (config-router) # maximum-paths hodnota

15.2.4.4 Vyvážení Zátěže IPv6

Obrázek 1, ukazuje topologii sítě EIGRP pro IPv6. Sériové linky v topologii mají stejnou šířku pásma, která se používá v topologii IPv4 pro EIGRP.

Stejně jako předchozí scénář pro protokol IPv4, R3 má dvě cesty EIGRP s rovnými náklady pro síť mezi R1 a R2, 2001:DB8:CAFE:A001::/64. Jedna trasa je přes FE80::1 na R1 a druhá trasa je přes FE80::2 na R2.

Obrázek 2 ukazuje, že metriky EIGRP jsou stejné ve směrovací tabulce IPv6 a ve směrovací tabulce IPv4 pro sítě 2001:DB8:CAFE:A001::/64 a 172.16.3.0/30. Je to proto, že kompozitní metrika EIGRP je stejná pro IPv6 i IPv4.

Nerovnoměrné vyrovnávání zatížení nákladů

EIGRP pro protokoly IPv4 a IPv6, můžou také vyvážit provoz na různých trasách, které mají odlišné metriky. Tento typ vyvažování se nazývá vyvážení zatížení nerovnoměrných nákladů. Nastavení hodnoty pomocí příkazu ***variance***, v režimu konfigurace směrovače, umožňuje systému EIGRP, nainstalovat několik cest bez smyček s nerovnoměrnými náklady do místní směrovací tabulky.

Trasa naučená prostřednictvím protokolu EIGRP, musí splňovat dvě kritéria, aby se mohla nainstalovat do místní směrovací tabulky:

- Tato trasa musí být bez smyčky, být proveditelná nástupcem, nebo mít ohlášenou vzdálenost, která je menší než celková vzdálenost.
- Metrika trasy, musí být nižší než metrika nástupce, vynásobená rozptylem nakonfigurovaným na směrovači.

Pokud je například rozptyl nastaven na hodnotu 1, jsou v místní tabulce směrování nainstalovány pouze trasy se stejnou metrikou jako nástupce. Pokud je rozptyl nastaven na hodnotu 2, bude v místní směrovací tabulce nainstalována jakákoli trasa, naučená podle EIGRP, s metrikou, která je menší než, dvojnásobek metriky nástupce.

Chcete-li řídit, jak je provoz distribuován mezi cestami, pokud existuje více tras pro stejnou cílovou síť, které mají různé náklady, použijte příkaz ***traffic-share balanced***. Cena cesty je pak distribuována, úměrně k poměru nákladů.

15.2.5 Zajištění EIGRP

15.2.5.1 Přehled Autentifikace Směrovacího Protokolu

Autentifikace protokolu směrování

Správci sítí si musí být vědomi toho, že směrovače jsou ohrožené útokem, stejně jako zařízení koncového uživatele. Každý, kdo má paket sniffer, například Wireshark, může číst informace šířící se mezi směrovači. Obecně platí, že směrovací systémy, mohou být napadány narušením zařízení vrstevníka, nebo falšováním směrovacích informací.

Narušení vrstevníků, je méně kritické z obou útoků, protože protokoly o směrování se samy léčí, což způsobuje, že přerušení trvá jen o něco málo déle, než samotný útok.

Falšování informací o směrování, je méně jemným útokem, který je zaměřen na informace obsažené v protokolu směrování. Důsledky padělání informací o směrování jsou následující:

- Přesměrování provozu pro vytvoření smyček směrování

- Přesměrování provozu na monitorování nejisté linie
- Přesměrování provozu, abyste ho zlikvidovali

Metoda ochrany směrovacích informací v síti, je ověření paketů směrovacích protokolů pomocí algoritmu MD5. MD5 umožňuje směrovačům porovnávat podpisy, které by měly být všechny stejné, což potvrzuje, že je to z důvěryhodného zdroje.

Tři složky takového systému zahrnují:

- Šifrovací algoritmus, který je obecně veřejně známý
- Klíč použitý v šifrovacím algoritmu, což je tajemství sdílené směrovači, které ověřují jejich pakety
- Obsah samotného paketu

Na obrázku, klikněte na tlačítko Přehrát a zobrazte animaci o tom, jak každý směrovač ověří informace o směrování. Generátor informací o směrování, obecně vytváří podpis pomocí klíčových a směrovacích dat, které se chystá odeslat jako vstupy, do šifrovacího algoritmu. Směrovač, který přijímá směrovací data, pak může proces opakovat pomocí stejného klíče a stejných směrovacích dat, které obdržel. Pokud podpis, který přijímač vypočítá, je stejný jako podpis, který vypočítá odesílatel, aktualizace je ověřená a považovaná za spolehlivou.

Směrovací protokoly jako RIPv2, EIGRP, OSPF, IS-IS a BGP podporují různé formy autentizace MD5.

15.2.5.2 Konfigurace EIGRP s Autentifikací MD5

Ověření zprávy EIGRP zajišťuje, že směrovače přijímají směrování zpráv, pouze z jiných směrovačů, které mají stejný, předem sdílený klíč. Bez nakonfigurovaného ověření, pokud neoprávněná osoba zavede jiný směrovač s odlišnými nebo konfliktními informacemi o trase v síti, směrovací tabulky na legálních směrovačích se mohou poškodit a může dojít k útoku DoS. Při autentizaci do zpráv EIGRP, odesílaných mezi směrovači, se tedy zabraňuje někomu úmyslně, nebo náhodou přidat do sítě jiný směrovač a způsobit problém.

EIGRP podporuje autentizaci protokolování pomocí protokolu MD5. Konfigurace ověřování zpráv EIGRP, se skládá ze dvou kroků: vytvoření klíčenky a klíče a konfigurace autentizace EIGRP, pro použití této klíčenky a klíče.

Krok 1. Vytvořte klíčenku a klíč

Autentizace směrování vyžaduje klíč na klíčence k funkčnosti. Předtím, než může být ověření aktivováno, vytvořte klíčenku a alespoň jeden klíč.

A. V globálním konfiguračním režimu vytvořte klíčenku. Ačkoli lze konfigurovat více klíčů, tato část se zaměřuje na použití jediného klíče.

Router (config) # key chain jméno-klíčenky

B. Zadejte ID klíče. Identifikátor klíče je číslo, které se používá k identifikaci ověřovacího klíče v klíčence. Rozsah klíčů, je od 0 do 2 147 483 647. Doporučuje se, aby bylo číslo klíče stejné ve všech směrovačích v konfiguraci.

Router (config-keychain) # key klíč-id

C. Zadejte klíčový řetězec pro klíč. Řetězec klíče je podobný jako heslo. Směrovače, které si vyměňují ověřovací klíče, musí být nakonfigurovány pomocí stejného řetězce klíčů.

Router (config-keychain-key) # key-string text-řetězce-klíče

Krok 2. Nakonfigurujte ověřování EIGRP pomocí klíčenky a klíče

Nakonfigurujte protokol EIGRP, který provede ověřování zpráv pomocí dříve definovaného klíče. Dokončete tuto konfiguraci, na všech rozhraních povolených pro EIGRP.

A. V globálním konfiguračním režimu určete rozhraní, na kterém chcete konfigurovat ověřování zpráv EIGRP.

Router (config) # interface typ číslo

B. Povolte ověření zprávy EIGRP. Klíčové slovo md5 označuje, že hash MD5 má být použit pro ověřování.

Router (config-if) # ip authentication mode eigrp číslo-as md5

C. Určete klíčenku, která by měla být použita pro ověřování. Argument jméno-klíčenky určuje klíčenku, která byla vytvořena v kroku 1.

Router (config-if) # ip authentication key-chain eigrp číslo-as jméno-klíčenky

Každá klávesa má vlastní identifikační klíč, který je uložen lokálně. Kombinace ID klíče a rozhraní přidruženého ke zprávě, jednoznačně identifikuje ověřovací algoritmus a ověřovací klíč MD5, který se používá. Aktualizace klíčových řetězců a směrování jsou zpracovávány pomocí algoritmu MD5, k vytvoření jedinečného podpisu.

15.2.5.3 Příklad Autentifikace EIGRP

Pro autentizaci aktualizací směrování, musí být všechna rozhraní EIGRP nakonfigurována tak, aby podporovala autentizaci. Obrázek 1, ukazuje topologii protokolu IPv4 a která rozhraní jsou nakonfigurována s ověřením.

Obrázek 2, ukazuje konfiguraci směrovače R1, pomocí klíčenky ***EIGRP_KEY*** a řetězce klíčů ***cisco123***. Po nakonfigurování R1, budou ostatní směrovače přijímat autentizované směrovací aktualizace. Přidružení se ztrácí, dokud se sousedé nakonfigurují s autentizací směrovacího protokolu.

Obrázek 3 ukazuje podobnou konfiguraci pro směrovač R2. Všimněte si, že stejný klíčový řetězec, ***cisco123***, slouží k ověření informací pomocí R1 a nakonec R3.

Použijte kontrolu syntaxe na obr. 4, pro konfiguraci autentizace EIGRP na R3.

Konfigurace protokolu EIGRP pro ověření protokolu IPv6

Algoritmy a konfigurace pro ověřování EIGRP IPv6, jsou stejné jako EIGRP pro protokol IPv4. Jediným rozdílem je, že příkazy konfiguračního rozhraní směrovače, používají ***ipv6*** namísto ***ip***.

Router (config-if) # ipv6 authentication mode eigrp číslo-as md5

Router (config-if) # ipv6 authentication key-chain eigrp číslo-as jméno-klíčenky

Obrázek 5, ukazuje příkazy pro konfiguraci protokolu EIGRP, pro ověřování IPv6 na směrovači R1, pomocí ***EIGRP_IPV6_KEY*** a řetězce klíčů ***cisco123***. Podobné konfigurace by byly zadány na R2 a R3.

15.2.5.4 Verifikace Autentifikace

Po ověření pravosti zprávy EIGRP na jednom směrovači, již žádné sousední přidružení, které dosud nebyly nakonfigurovány pro ověření, nejsou sousedy. Například pokud rozhraní R1 Serial 0/0/0, bylo nakonfigurováno pro autentizaci MD5, ale R2 nebylo dosud nakonfigurováno, objevila se následující zpráva IOS na R1:

% DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.3.2 (Serial0/0/0) is down: authentication mode changed

Když je nakonfigurováno sousední sériové rozhraní 0/0/0 na R2, sousednost se obnoví a na R1 se zobrazí následující zpráva IOS:

% DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.3.2 (Serial0/0/0) is up: new adjacency

Podobné zprávy se zobrazují také na R2.

Přidružení se tvoří, pouze pokud jsou obě připojovací zařízení nakonfigurována, jak je znázorněno na obrázku 1. Chcete-li ověřit, zda byly správné přidružení EIGRP vytvořeny po konfigurování pro ověření, použijte na každém směrovači příkaz, ***show ip eigrp neighbors***. Obrázek 2 ukazuje, že všechny tři směrovače znovu nastavily sousední přidružení poté, co byly nakonfigurovány pro ověřování EIGRP.

Chcete-li ověřit sousední přidružení EIGRP pro protokol IPv6, použijte příkaz ***show ipv6 eigrp neighbors***.

15.3 Řešení Problémů EIGRP

15.3.1 Komponenty Řešení Problémů EIGRP

15.3.1.1 Základní Příkazy Řešení Problémů EIGRP

EIGRP se běžně používá ve velkých podnikových sítích. Řešení problémů souvisejících s výměnou informací o směrování je základním předpokladem správce sítě. To platí zejména pro správce, kteří se podílejí na zavádění a údržbě rozsáhlých podnikových sítí, které používají EIGRP jako protokol vnitřní brány (IGP). Existuje několik příkazů, které jsou užitečné při řešení potíží se sítí EIGRP.

Příkaz ***show ip eigrp neighbors*** ověří, zda směrovač rozpozná své sousedy. Výstup na obrázku 1, ukazuje dvě úspěšné sousední oblasti EIGRP na R1.

Na obr. 2 příkaz ***show ip route*** ověřuje, že směrovač zjistil trasu do vzdálené sítě prostřednictvím protokolu EIGRP. Výstup ukazuje, že R1 se prostřednictvím EIGRP dozvěděl o čtyřech vzdálených sítích.

Obrázek 3, ukazuje výstup z příkazu ***show ip protocols***. Tento příkaz ověří, že EIGRP zobrazuje aktuálně nakonfigurované hodnoty pro různé vlastnosti povolených směrovacích protokolů.

EIGRP pro protokol IPv6

Podobné příkazy a kritéria odstraňování problémů se vztahují také na protokol EIGRP pro protokol IPv6.

Následující jsou ekvivalentní příkazy, používané s protokolem EIGRP pro protokol IPv6:

- *Router # show ipv6 eigrp neighbors*
- *Router # show ipv6 route*
- *Router # show ipv6 protocols*

15.3.1.2 Komponenty

Obrázek ukazuje vývojový diagram pro diagnostiku problémů s připojením EIGRP.

Po konfiguraci protokolu EIGRP, je prvním krokem testování připojení k vzdálené síti. Pokud ping selže, potvrďte sousední přidružení EIGRP. Sousední přidružení, nemusí být vytvořeno z několika důvodů, včetně následujících:

- Rozhraní mezi zařízeními je nefunkční.
- Dva směrovače mají nesoulad s autonomními systémovými čísly EIGRP (ID procesů).
- Správná rozhraní nejsou pro proces EIGRP povolena.
- Rozhraní je nakonfigurováno jako pasivní.

Kromě těchto otázek existuje řada dalších, pokročilejších problémů, které mohou způsobit, že sousední sousedství nebudou tvořeny. Dva příklady jsou nesprávně nakonfigurované ověření EIGRP nebo nesprávné hodnoty K, které EIGRP používá pro výpočet své metriky.

Pokud je mezi dvěma směrovači vytvořena sousední sousedství EIGRP, ale stále existuje problém s připojením, může dojít k problému směrování. Některé problémy, které mohou způsobit problém s připojením pro EIGRP, zahrnují:

- Správné sítě nejsou propagovány na vzdálených směrovačích.
- Nesprávně nakonfigurované pasivní rozhraní, nebo ACL blokuje reklamy vzdálených sítí.
- Automatické shrnutí způsobuje nekonzistentní směrování v nesouvislé síti.

Pokud jsou všechny požadované trasy v směrovací tabulce, ale cesta, kterou provoz přebírá, není správná, ověřte hodnoty šířky pásma rozhraní.

15.3.2 Řešení Problémů ze Sousedy EIGRP

15.3.2.1 Konektivita 3. Vrstvy

Předpokladem pro sousední přidružení, mezi dvěma přímo propojenými směrovači, je propojení 3. vrstvy. Zkoumáním výstupu příkazu, ***show ip interface brief***, správce sítě může

ověřit stav a protokol propojovacích rozhraní. Ping z jednoho směrovače na jiný, přímo připojený směrovač, by měl potvrdit připojení IPv4 mezi zařízeními. Na obrázku je zobrazen krátký výstup příkazu, ***show ip interface brief***, pro R1. R1 ukazuje připojení k R2 a pingy jsou úspěšné.

Pokud je ping neúspěšný, zkontrolujte kabeláž a ověřte, zda jsou rozhraní připojených zařízení na společné podsíti. Zpráva protokolu, která uvádí, že sousedy EIGRP nejsou na společné podsíti, naznačuje, že na jedné ze dvou sousedních rozhraní EIGRP existuje nesprávná adresa IPv4.

15.3.2.2 Parametry EIGRP

Při odstraňování problémů se sítí EIGRP, je jednou z prvních věcí, které je třeba ověřit, že všechny směrovače, které se účastní sítě EIGRP, jsou nakonfigurovány se stejným autonomním systémovým číslem. Příkaz ***router eigrp číslo-as***, směrovače spustí proces EIGRP a následuje číslo, které je autonomním systémovým číslem. Hodnota argumentu ***číslo-as***, musí být stejná ve všech směrovačích, které jsou v směrovací doméně EIGRP.

Obrázek 1 ukazuje, že všechny směrovače by se měly účastnit autonomního systémového čísla 1. Na obrázku 2, příkaz ***show ip protocols*** ověřuje, že R1, R2 a R3 všechny používají stejné autonomní systémové číslo.

EIGRP pro protokol IPv6

Podobné příkazy a kritéria odstraňování problémů se vztahují také na protokol EIGRP pro protokol IPv6.

Následující příkazy jsou ekvivalentní příkazy, používané s protokolem EIGRP pro protokol IPv6:

- *Router (config) # ipv6 router eigrp číslo-as*
- *Router # show ipv6 protocols*

Poznámka: V horní části výstupu je "IP Směrování vědomé NSF", označuje Nonstop Forwarding (NSF). Tato možnost umožňuje partnerům EIGRP selhávajícího směrovače uchovat informace o směrování, které inzerovaly, a pokračovat v používání těchto informací, dokud selhání směrovače neobnoví normální provoz a nebudou schopny vyměnit informace o směrování.

15.3.2.3 Rozhraní EIGRP

Kromě ověření autonomního systémového čísla je nutné ověřit, zda se všechna rozhraní účastní sítě EIGRP. Příkaz ***network***, který je nakonfigurován v procesu směrování EIGRP, označuje, které rozhraní se účastní EIGRP. Tento příkaz se použije na klasickou síťovou adresu rozhraní, nebo na podsíť, pokud je zahrnutá zástupní maska.

Na obrázku 1, ukazuje příkaz ***show ip eigrp interfaces***, které rozhraní jsou povolena pro EIGRP na R1. Pokud nejsou pro EIGRP povolená propojená rozhraní, pak sousedé netvoří sousedství.

Na obrázku 2, je v části "Routing for Networks" v příkazu ***show ip protocols*** označena, která síť byla nakonfigurována. Všechna rozhraní v těchto sítích se účastní EIGRP.

Na obrázku 3, výstup z příkazu ***show running-config*** potvrzuje, že všechna rozhraní s těmito adresami nebo podsítěmi těchto adres, jsou povoleny pro EIGRP.

EIGRP pro protokol IPv6

Podobné příkazy a kritéria odstraňování problémů se vztahují také na protokol EIGRP pro protokol IPv6.

Následující jsou ekvivalentní příkazy používané s protokolem EIGRP pro protokol IPv6:

- *Router # show ipv6 protocols*
- *Router # show ipv6 eigrp interfaces*

15.3.3 Řešení Problémů ze Směrovací Tabulkou EIGRP

15.3.3.1 Pasivní Rozhraní

Jeden důvod, proč tabulky tras, nemusí odrážet správné trasy, je způsobeno příkazem ***passive-interface***. Při spuštění systému EIGRP v síti, zastaví příkaz ***passive-interface***, odchozí i příchozí směrování. Z tohoto důvodu se směrovače nestávají sousedy.

Chcete-li ověřit, zda je jakékoliv rozhraní na směrovači nakonfigurováno jako pasivní, použijte příkaz ***show ip protocols***, v privilegovaném režimu. Obrázek 1 ukazuje, že rozhraní R2 GigabitEthernet 0/0, je nakonfigurováno jako pasivní rozhraní, protože na tomto propojení nejsou žádní sousedi.

Jako přídavek v konfiguraci na rozhraní, které nemají žádné sousedy, může být z bezpečnostních důvodů povoleno pasivní rozhraní. Na obrázku 2 si všimněte, že stínování pro směrovací doménu EIGRP, se liší od předchozích topologií. Síť 209.165.200.224/27, je nyní zahrnuta v aktualizacích R2. Z bezpečnostních důvodů však správce sítě nechce, aby R2 vytvořil sousední přidružení EIGRP, se směrovačem ISP.

Obrázek 3, ukazuje přidání příkazu na R2, ***network 209.165.200.224/27***. R2 nyní inzeruje tuto síť na ostatní směrovače v směrovací doméně EIGRP.

Příkaz režimu konfigurace směrovače, ***passive-interface***, je nakonfigurován na Serial 0/1/0, aby se zabránilo tomu, že aktualizace R2, budou odeslány do směrovače ISP. Příkaz ***show ip eigrp neighbors*** na R2 ověřuje, že R2 nenastavil sousední přidružení s ISP.

Obrázek 4 ukazuje, že R1 má trasu do sítě 209.165.200.224/27, ve své směrovací tabulce IPv4 (R3 bude mít také trasu k této síti ve své směrovací tabulce IPv4). R2 však nemá sousední přidružení s ISP.

EIGRP pro protokol IPv6

Podobné příkazy a kritéria odstraňování problémů se vztahují také na protokol EIGRP pro protokol IPv6.

Následující příkazy, jsou ekvivalentní příkazy používané s protokolem EIGRP pro protokol IPv6:

Router # show ipv6 protocols

Router (config-rtr) # passive-interface typ číslo

15.3.3.2 Chybějící Tvrzení Sítě

Obrázek 1 ukazuje, že rozhraní R1, GigabitEthernet 0/1, je nyní nakonfigurováno s adresou 10.10.10.1/24 a je aktivní.

R1 a R3 stále mají sousední přidružení, ale ping ze směrovače R3 na rozhraní G0/1 10.10.10.1, na R2 je neúspěšný. Obrázek 2, ukazuje selhání testu připojení od R3 až do cílové sítě 10.10.10.0/24.

Na obrázku 3, pomocí příkazu ***show ip protocols***, na směrovači R1 ukazuje, že síť 10.10.10.0/24, není inzerována sousedům EIGRP.

Jak je znázorněno na obrázku 4, proces EIGRP na R1 je nakonfigurován tak, aby obsahoval reklamu sítě 10.10.10.0/24.

Obrázek 5 ukazuje, že nyní existuje trasa ve směrovací tabulce R3, pro síť 10.10.10.0/24 a dostupnost je ověřována pingem rozhraní GigabitEthernet 0/1 na R1.

EIGRP pro protokol IPv6

Podobné příkazy a kritéria odstraňování problémů se vztahují také na protokol EIGRP pro protokol IPv6.

Následující příkazy jsou ekvivalentní příkazy používané s protokolem EIGRP pro protokol IPv6:

Router # show ipv6 protocols

Router # show ipv6 route

Chcete-li do protokolu IPv6, přidat chybějící tvrzení sítě, použijte v konfiguračním režimu rozhraní příkaz:

Router (config-if) # ipv6 eigrp autonomní systém

Poznámka: Další způsob chybějící trasy může vyplývat z filtrování směrovače v příchozích, nebo odchozích aktualizacích směrování. Služba ACL, poskytuje filtrování pro různé protokoly a tyto seznamy ACL mohou ovlivnit výměnu zpráv směrovacího protokolu, které způsobují chybějící cesty ze směrovací tabulky. Příkaz, ***show ip protocols*** ukazuje, zda existují nějaké ACL, které jsou aplikovány na EIGRP.

15.3.3.3 Automatická Sumarizace

Další problém, který může pro správce sítě způsobit problémy, je automatické shrnutí EIGRP.

Obrázek 1, ukazuje odlišnou síťovou topologii, než jaká byla použita v celé této kapitole. Mezi R1 a R3 neexistuje žádné spojení. LAN sítě R1 má síťovou adresu 10.10.10.0/24, zatímco síť LAN R3 je 10.20.20.0/24. Sériová spojení mezi směrovači a R2 mají stejnou šířku pásma 1024 kb/s.

R1 a R3 mají pro EIGRP, rozhraní LAN a sériové rozhraní, jak je znázorněno na obrázku 2. Oba směrovače provádějí automatické shrnutí EIGRP.

EIGRP pro protokol IPv4, lze nakonfigurovat tak, aby automaticky shrnoval trasy na klasických hranicích. Pokud existují nesouvislé sítě, automatické shrnutí způsobuje nekonzistentní směrování.

Na obrázku 3, směrovací tabulka R2 ukazuje, že neobdrží jednotlivé cesty pro podsítě 10.10.10.0/24 a 10.20.20.0/24. Jak R1 a R3 automaticky shrnovaly tyto podsítě na 10.0.0.0/8 třídní hranici, při odesílání aktualizačních paketů R2. Výsledkem je, že R2 má ve směrovací tabulce dvě cesty s rovnými náklady na 10.0.0.0/8, což může mít za následek nepřesné směrování a ztrátu paketů. V závislosti na tom, zda se používá balancování zatížení podle paketů, cílů nebo CEF, pakety mohou nebo nemusí být předány správnému rozhraní.

Na obr. 4, příkaz ***show ip protocols*** ověřuje, že je provedeno automatické shrnutí na R1 a R3. Všimněte si, že oba směrovače shrnou síť 10.0.0.0/8, pomocí stejné metriky.

Příkaz ***auto-summary***, je ve výchozím nastavení deaktivován, ve verzích softwaru Cisco IOS verze 15 a novějších verzích verze 12.2. Ve výchozím nastavení je pro starší software povoleno automatické shrnutí. Chcete-li zakázat automatické shrnutí, zadejte do konfiguračního režimu směrovače EIGRP příkaz ***no auto-summary***.

Chcete-li tento problém vyřešit, mějte na R1 a R3 automatické shrnutí zakázáno:

R1 (config) # router eigrp 1

R1 (config-router) # no auto-summary

R3 (config) # router eigrp 1

R3 (config-router) # no auto-summary

Po automatickém shrnutí na R1 a R3, směrovací tabulka R2 nyní naznačuje, že přijímá jednotlivé podsítě 10.10.10.0/24 a 10.20.20.0/24 od R1 a R3, jak je znázorněno na obrázku 5. Přesné směrování a konektivita v obou podsítích, je nyní obnoveno.

EIGRP pro protokol IPv6

V síti IPv6 neexistují třídní sítě. Proto EIGRP pro protokol IPv6 nepodporuje automatické shrnutí. Všechna shrnutí musí být provedena pomocí manuálních souhrnných tras EIGRP.

15.4 Shrnutí

15.4.1 Shrnutí

15.4.1.1 Shrnutí

EIGRP je jeden ze směrovacích protokolů, běžně používaných ve velkých podnikových sítích. Modifikace funkcí EIGRP a odstraňování problémů je jednou z nejdůležitějších dovedností pro síťového inženýra, který se podílí na implementaci a údržbě rozsáhlých podnikových sítí, které používají EIGRP.

Sumarizace snižuje počet položek v aktualizacích směrování a snižuje počet položek v místních směrovacích tabulkách. To také snižuje využití šířky pásma pro směrování aktualizací a výsledky v rychlejších vyhledáváních směrovací tabulky. EIGRP pro automatické shrnutí protokolu IPv4 je standardně deaktivováno od Cisco IOS 15.0 a 12.2. Předtím bylo automaticky povoleno. Chcete-li povolit automatické shrnutí pro EIGRP, použijte příkaz ***auto-summary***, v režimu konfigurace směrovače. Pomocí příkazu ***show ip protokols*** ověřte stav automatického shrnutí. Zkontrolujte směrovací tabulku a ověřte, zda je automatické shrnutí funkční.

EIGRP automaticky obsahuje souhrnné cesty k Null0, aby se zabránilo smyčkám směrování, které jsou obsaženy v souhrnu, ale ve směrovací tabulce skutečně neexistují. Rozhraní Null0 je virtuální rozhraní IOS, které je cestou k nikam, běžně nazývaná "bitový kbelík". Pakety, které odpovídají trase s rozhraním ukončení Null0, jsou vyřazeny.

Chcete-li vytvořit manuální shrnutí EIGRP na konkrétním rozhraní, použijte následující příkaz konfigurace rozhraní:

Router (config-if) # ip summary-address eigrp číslo-as adresa-sítě maska-podsítě

Chcete-li nakonfigurovat EIGRP pro manuální shrnutí protokolu IPv6 na konkrétním rozhraní, použijte následující příkaz konfigurace rozhraní:

Router (config-if) # ipv6 summary-address eigrp číslo-as prefix/délka-prefixu

Jednou z metod propagace výchozí trasy v směrovací doméně EIGRP je použití příkazu ***redistribute static***. Tento příkaz informuje EIGRP, že tuto statickou cestu zahrnul do svých aktualizací EIGRP pro jiné směrovače. Příkaz ***show ip protocols*** ověřuje, že se statické cesty v doméně směrování EIGRP redistribuují.

Použijte příkaz konfigurace rozhraní, ***ip bandwidth-percent eigrp číslo-as procenta***, abyste mohli nakonfigurovat procenta šířky pásma, které může rozhraní EIGRP použít.

Chcete-li nakonfigurovat procenta šířky pásma, které může rozhraní EIGRP použít pro protokol IPv6, použijte příkaz ***ipv6-bandwidth-percent eigrp***. Chcete-li obnovit výchozí hodnotu, použijte ***no*** před tímto příkazem.

Hello intervaly a časy Zadržení, jsou konfigurovatelné na základě rozhraní v EIGRP a nemusejí odpovídat jiným směrovačům EIGRP, za účelem vytvoření nebo udržení sousedství.

Pro IP v EIGRP, software Cisco IOS ve výchozím nastavení používá vyvažování zátěže až ve čtyřech stejných cestách. Pomocí příkazu režimu konfigurace směrovačů, ***maximum-paths***, lze ve směrovací tabulce uložit až 32 tras s rovnými náklady.

EIGRP podporuje autentizaci protokolů pomocí protokolu MD5. Algoritmy a konfigurace pro ověřování u IPv4 jsou stejné jako u IPv6. Jediným rozdílem je, že příkazy pro konfiguraci rozhraní používají ***ip*** namísto ***ipv6***.

Router (config-if) # ipv6 authentication eigrp číslo-as md5

Router (config-if) # ipv6 authentication key-chain eigrp číslo-as jméno-klíčenky

Chcete-li ověřit, zda byly vytvořeny správné přídavné prvky EIGRP po nakonfigurování pro ověření, použijte příkaz ***show ip eigrp neighbors*** na každém směrovači.

Příkaz ***show ip route*** ověří, že směrovač zjistil trasy EIGRP. Příkaz ***show ip protocols***, slouží k ověření, zda EIGRP zobrazuje aktuálně nakonfigurované hodnoty.

16 KAPITOLA 9 - LICENCOVÁNÍ A OBRAZ IOS

16.1 Licencování a Obraz IOS

16.1.1 Úvod

16.1.1.1 Úvod

Cisco IOS (původně Internetwork Operating System), je software používaný na většině směrovačů a přepínačů Cisco. IOS je balíček směrování, přepínání, zabezpečení a dalších internetworking technologií, integrovaných do jediného více úlohového operačního systému.

Portfolio Cisco IOS, podporuje širokou škálu technologií a funkcí. Zákazníci si vybírají IOS na základě sady protokolů a funkcí podporovaných určitým obrázkem. Porozumění portfoliu sady funkcí Cisco, pomáhá při výběru správného IOS tak, aby vyhovoval potřebám organizace.

Cisco učinila významné změny v balení a licencování svých IOS při přechodu z IOS 12.4 na 15.0. Tato kapitola vysvětluje konvence pojmenování a balení IOS 12.4 a 15. Počínaje IOS 15, zavedla Cisco také nový formát balení a licenční proces. Tato kapitola popisuje proces získávání, instalace a správy softwarových licencí Cisco IOS 15.

Poznámka: Vydání IOS po 12.4 je 15.0. Neexistuje verze softwaru IOS 13 nebo 14.

16.2 Správa Systémových Souborů IOS

16.2.1 Pojmenování Konvencí

16.2.1.1 Rodiny a Vlaky Vydání Softwaru Cisco IOS

Software Cisco IOS, se vyvinul z jediného operačního systému platformy pro směrování, do sofistikovaného operačního systému, který podporuje velké množství funkcí a technologií, jako jsou VoIP, NetFlow a IPsec. Aby bylo možné lépe vyhovět požadavkům jednotlivých segmentů trhu, je software organizován do softwarových vlaků.

Rodina vydání softwaru, obsahuje několik verzí IOS a ty:

- Sdílejí kódovou základnu
- Používají se na příslušné hardwarové platformy
- Překrývání pokrytí podpory (protože jeden systém přichází do konce jeho životnosti, zavádí se a podporuje další operační systém)

Příklady vydání softwaru IOS v rámci rodiny vydání, zahrnují verze 12.3, 12.4, 15.0 a 15.1.

Spolu s každým vydáním softwaru, existují nové verze vytvořené pro implementaci oprav chyb a nové funkce. IOS označuje tyto verze jako vlaky.

Vlak Cisco IOS, se používá k dodávání verzí se společnou kódovou základnou do specifické sady platforem a funkcí. Vlak může obsahovat několik vydání, přičemž každé vydání je obrazem, kódové základny vlaku v okamžiku vydání. Vzhledem k tomu, že se na různých platformách nebo tržních segmentech mohou vztahovat různé rodiny vydání softwaru, mohou být v každém okamžiku aktuální vlaky.

Tato kapitola zkoumá vlaky IOS 12.4 a 15.

16.2.1.2 Cisco IOS 12.4 – Hlavní Vlaky a T Vlaky

Vlaky 12.4

Obrázek ukazuje migraci z verze softwaru 12.3 na 12.4. V rámci rodiny vydání softwaru, mohou existovat dva nebo více úzce souvisejících a aktivních vlaků. Například rodina vydání Softwaru 12.4 má dva vlaky, hlavní vlak 12.4 a vlaky 12.4T.

Vlak Cisco IOS Software 12.4, je považován za hlavní vlak. Hlavní vlak přijímá většinou opravy softwaru (chyby) s cílem zvýšit jeho kvalitu. Vydání hlavních vlaků, jsou také označeny jako vydání údržby (MD).

Hlavní vlak je vždy spojen s technologickým vlakem (T vlakem). T vlak, jako je 12.4T, obdrží stejné opravy chyb softwaru jako hlavní vlak. T vlak také obdrží nové funkce podpory softwaru a hardwaru. 12.4T je považováno za vydání včasného nasazení (ED).

Mohou existovat další vlaky, v závislosti na rodině vydání softwaru. Např. jiný vlak, který je k dispozici, je vlak poskytovatele služeb (vlak S). Vlak S bude obsahovat specifické funkce určené pro splnění požadavků poskytovatele služeb.

Všechny dětské vlaky hlavního vlaku (T, S atd.) Obvykle obsahují velké písmeno označující typ vlaku.

Hlavní vlak = 12,4

T vlak = 12,4T (12,4 + nové funkce podpory softwaru a hardwaru)

Až do rodiny vydání Softwaru 12.4, byly odděleny hlavní vlaky a vlaky T. Jinými slovy, z hlavního vlaku, T vlak se rozdělil a stal se samostatnou kódovou základnou, která obdržela nové funkce a podporu hardwaru. Nakonec se nový hlavní vlak vyvíjel ze zavedeného vlaku

T a cyklus začal znovu. Toto použití více vlaků bylo změněno pomocí softwaru Cisco IOS 15.

16.2.1.3 Cisco IOS 12.4 - Číslování Hlavních a T Vlaků

Konvence číslování vydání IOS se používá k identifikaci vydání softwaru IOS, včetně oprav chyb a nových softwarových funkcí. Příklad schématu číslování je zobrazen na obrázku pro hlavní vlaky i T vlaky:

- Schéma číslování softwaru pro hlavní vlak se skládá z čísla vlaku, identifikátoru údržby a identifikátoru obnovení. Například vydání Cisco IOS Software 12.4 (21a) je hlavní vlak. Vydání pro vlak T se skládá z čísla vlaku, identifikátoru údržby, identifikátoru vlaku a identifikátoru obnovení. Například, vydání Cisco IOS Software 12.4 (20) T1, patří do vlaku 12.4T.
- Každý identifikátor údržby hlavní linky softwaru 12.4, například 12.4 (7), obsahuje další softwarové a opravy údržby. Tato změna je označena číslem v závorce. Každé vydání údržby softwaru 12.4T, například 12.4 (20)T, zahrnuje stejné opravy softwaru spolu s dalšími funkcemi a podporou hardwaru.
- Společnost Cisco využívá obnovení jednotlivých verzí, aby integrovala opravy významných problémů. To snižuje možný dopad na zákazníky, kteří již nasadili a certifikovali jednotlivá vydání. Obnovení obvykle zahrnuje opravy omezeného počtu chyb softwaru, které jsou známé jako upozornění. Je označen malým písmenem uvnitř závorek hlavních vlaků, nebo konečným číslem v jiných vlacích. Například 12.4(21) obdržel několik oprav údržby a výsledné obnovení bylo pojmenováno 12.4(21a). Podobně 12.4(15)T8, je osmé obnovení 12.4(15)T. Každé nové obnovení postupně zvyšuje identifikátor obnovení a před dalším plánovaným jednotlivým vydáním, dodá další opravy softwaru v urychleném rozvrhu. Kritéria pro provedení změn v rekonstrukci jsou přísná.

Pro všechny vlaky 12.4, se používá jediná sada individuálních čísel vydání. Vydání 12.4 a 12.4T používají soubor individuálních čísel vydání, které jsou sdíleny v celé řadě vydání rodiny 12.4. Po verzi 12.4(6)T, následovalo 12.4(7)T a 12.4(8)T. To umožňuje správci sledovat změny zavedené v kódu.

Poznámka: Jakákoli náprava, která je opravena ve vydání T vlaku, by měla být implementována v příštím vydání.

16.2.1.4 Cisco IOS 12.4 – Balení Obrazu Systému

Před vydáním Cisco IOS Software 15.0, se Balení skládalo z osmi balíčků pro směrovače Cisco, jak je znázorněno na obrázku. Toto schéma balení, bylo zavedeno s hlavním vlakem Cisco IOS Software 12.3 a bylo později použito v jiných vlacích. Obraz Balení se skládá z osmi obrazů IOS, z nichž tři jsou považovány za prémiové balíčky.

Pět neprémiových balíčků je:

- **IP Base** - IP Base je vstupní úroveň Obrazu Cisco IOS Software
- **IP Voice** - konvergovaný hlas a data, VoIP, VoFR a IP telefonie
- **Rozšířené zabezpečení** - Zabezpečení a funkce VPN, včetně Cisco IOS Firewallu, IDS/IPS, IPsec, 3DES a VPN
- **Služby SP (poskytovatele služeb)** - přidává protokoly SSH/SSL, ATM, VoATM a MPLS do protokolu IP Voice
- **Enterprise Base** - Podnikové protokoly: Appletalk, IPX a podpora IBM

Poznámka: Počínaje vydáním rodiny produktů Cisco IOS Software 12.4, je ve všech obrazech k dispozici SSH.

Další tři prémiové balíčky, nabízejí další kombinace funkcí softwaru IOS, které řeší složitější síťové požadavky. Všechny funkce se slučují v balíčku Pokročilých Podnikových Služeb. Tento balíček integruje podporu pro všechny směrovací protokoly s možnostmi Voice, Security a VPN:

- **Pokročilé podnikové služby** - plné funkce softwaru Cisco IOS
- **Podnikové služby** - služby na základe podniku a poskytovatele služeb
- **Pokročilé služby IP** - Rozšířené zabezpečení, Služby poskytovatele služeb a podpora pro protokol IPv6

Poznámka: Cisco Feature Navigator, je nástroj používaný k nalezení správného operačního systému Cisco, v závislosti na potřebných funkcích a technologiích.

16.2.1.5 Cisco IOS 15.0 - M a T Vlaky

Po vydání softwaru Cisco IOS 12.4(24)T, bylo další vydání 15.0.

IOS 15.0 poskytuje několik vylepšení operačního systému včetně:

- Nové podpora funkcí a hardwaru
- Rozšířené konzistence funkcí s ostatními hlavními verzemi IOS

- Více předvídatelné nové vydání a obnovení plánů
- Proaktivní zásady podpory jednotlivých vydání
- Zjednodušené číslování vydání
- Jasnější pokyny pro nasazení a migraci softwaru

Jak je znázorněno na obrázku, Cisco IOS 15.0, používá odlišný model vydání, od tradičních oddělených hlavních vlaků a T vlaků 12.4. Namísto rozdělení se do samostatných vlaků bude hlavní 15 a T, mít prodloužené vydání údržby (EM) a standardní údržbu (T). S novým vydáním modelu IOS, jsou hlavní verze Cisco IOS 15 označovány jako M vlaky.

Počínaje 15.0, jsou nové verze ve formě vlaku T, dostupné přibližně dvakrát až třikrát ročně. Vydání EM je k dispozici přibližně každých 16 až 20 měsíců. T verze umožňují rychlejší dodávku funkcí Cisco před tím, než bude k dispozici další verze EM.

EM vydání obsahuje funkce a hardwarovou podporu všech předchozích vydání T. Díky tomu jsou k dispozici novější verze EM, které obsahují plnou funkčnost vlaku.

Stručně řečeno, výhody nového modelu vydání Cisco IOS zahrnují:

- Funkce dědičnosti ze softwaru Cisco IOS 12.4T a hlavní 12.4
- Nová funkce se vydává přibližně dva až třikrát ročně a postupně se přenáší z jediného vlaku
- EM se vydává přibližně každých 16 až 20 měsíců a obsahuje nové funkce
- T verze pro nejnovější funkce a hardwarovou podporu před příštím vydáním EM, bude k dispozici na Cisco.com
- Vydání obnovy údržby M a T, obsahuje pouze opravy chyb

16.2.1.6 Cisco IOS 15 – Číslování Vlaků

Konvence číslování vydání pro IOS 15 identifikuje konkrétní vydání IOS, včetně oprav chyb a nových softwarových funkcí, podobné předchozím rodinám IOS. Na obrázku jsou uvedeny příklady této konvence jak pro vydání EM, tak pro T.

Vydání Prodloužení údržby

Vydání EM je ideální pro dlouhodobou údržbu, což zákazníkům umožňuje, aby se kvalifikovali, nasadili a zůstávali na vydání po delší dobu. Hlavní vlak obsahuje funkce dodávané v předchozích verzích a přírůstkové vylepšení nových funkcí a podporu hardwaru.

První obnova údržby (pouze pro opravy chyb, žádné nové funkce nebo nová hardwarová podpora) vydání 15.0(1)M, je očíslována 15.0(1)M1. Následná údržba je definována přírůstkem čísla pro obnovení údržby (tj. M2, M3 atd.).

Standardní vydání údržby

Vydání T se používá, pro krátké verze aplikací, které jsou ideální pro nejnovější nové funkce a hardwarovou podporu před tím, než bude k dispozici další verze EM. Vydání T, poskytuje pravidelné opravy údržby a chyb, plus kritickou oprava podpory pro sítě, které ovlivňují chyby, jako jsou problémy se zprávami týkajícími se Produckt Security Incident Report Team (PSIRT).

První plánované vydání 15T je uvedeno jako 15.1(1)T. První obnovení údržby (pouze pro opravy chyb, žádné nové funkce nebo novou hardwarovou podporu) verze 15.1(1)T, bude očíslováno 15.1(1)T1. Následná vydání jsou definována přírůstkem čísla pro obnovení údržby (tj. T2, T3 atd.).

16.2.1.7 IOS 15 – Balení Obrazu Systému

Integrované Služby Směrovačů Cisco 2. Generace (ISR G2) 1900, 2900 a 3900, podporují služby na vyžádání prostřednictvím licencování softwaru. Proces služeb na požádání, umožňuje zákazníkům realizovat provozní úspory prostřednictvím, snadného uspořádání a správy softwaru. Při objednávce nové platformy ISR G2, je směrovač dodáván s jediným univerzálním softwarem Cisco IOS a licencí, která se používá k povolení konkrétních balíků sady funkcí, jak je znázorněno na obrázku 1.

V ISR G2 jsou podporovány dva typy univerzálních obrazů:

- **Univerzální obrazy s označením "universalk9" v názvu obrazu** - Tento univerzální obraz, nabízí všechny funkce softwaru Cisco IOS, včetně funkcí kryptografie s vysokým užitečným zatížením, jako například VPN, SSL VPN a IPsec.
- **Univerzální obrazy s označením "universalk9_npe" v názvu obrazu** - Silné vynucení šifrovacích funkcí, poskytovaných pomocí softwaru Cisco Software Aktivace, splňuje požadavky na export šifrovacích funkcí. Některé země však mají požadavky na import, které vyžadují, aby platforma nepodporovala žádnou silnou kryptografickou funkci, jako je kryptografie s užitečným zatížením. K uspokojení dovozních požadavků těchto zemí, nepodporuje univerzální obraz npe, žádné silné šifrování užitečného zatížení.

Se zařízeními ISR G2, byl výběr obrazů IOS snazší, protože všechny funkce jsou součástí univerzálního obrazu. Funkce jsou aktivovány licencováním. Každé zařízení je dodáváno s univerzálním obrazem. Technologické balíčky IP Base, Data, UC (Unified Communications) a SEC (Security), jsou povoleny v univerzálním obrazu, pomocí licenčních klíčů pro aktivaci softwaru Cisco. Každý licenční klíč je pro konkrétní zařízení jedinečný a získává se od společnosti Cisco, uvedením ID produktu a sériového čísla směrovače a aktivačního klíče (PAK). Služba PAK poskytuje společnost Cisco v době nákupu softwaru. IP Base je standardně nainstalována.

Obrázek 2, ukazuje doporučenou migraci pro další generace ISR, z IOS 12 na IOS 15.

16.2.1.8 Jména Souborů Obrazu IOS

Při výběru nebo upgradu směrovače Cisco IOS, je důležité vybrat správný obraz IOS se správnou sadou funkcí a verzí. Obrazový soubor je založen na konvenci speciálního pojmenování. Název souboru obrazu IOS, obsahuje více částí, z nichž každá má určitý význam. Je důležité pochopit tuto konvenci pojmenování, při upgradu a výběru softwaru Cisco IOS.

Jak je znázorněno na obrázku 1, příkaz ***show flash***, zobrazuje soubory uložené v paměti flash, včetně obrazových souborů systému.

Příklad obrazu softwaru IOS 12.4 je uveden na obrázku 2.

- **Jméno obrazu (c2800nm)** - Určuje platformu, na níž je obraz spuštěn. V tomto příkladu je platformou směrovač Cisco 2800 se síťovým modulem.
- **Advipservicesk9** - Určuje sadu funkcí. V tomto se odkazuje na sadu funkcí pro rozšířené služby IP, které zahrnují jak pokročilé balíky zabezpečení a poskytovatele služeb, tak i IPv6.
- **mz** - Označuje, kde se obraz spustí a zda je soubor komprimován. V tomto příkladu mz označuje, že soubor běží z paměti RAM a je komprimován.
- **124-6.T** - Formát souboru pro obraz 12.4(6)T. Jedná se o číslo vlaku, číslo vydání údržby a identifikátor vlaku.
- **Bin** - přípona souboru. Toto rozšíření označuje, že tento soubor je binární spustitelný soubor.

Obrázek 3, znázorňuje různé součásti systémového obrazového souboru systému IOS 15 na zařízení ISR G2:

- **Název obrazu (c1900)** - Určuje platformu, na níž je obraz spuštěn. V tomto příkladu je platformou směrovač Cisco 1900.

- **Universalk9** - Určuje označení obrazu. Dvě označení pro ISR G2 jsou universalk9 a universalk9_npe. Universalk9_npe, neobsahuje silné šifrování a je určen pro země s omezeními šifrování. Funkce jsou řízeny licencí a mohou být rozděleny do čtyř technologických balíčků. Jedná se o IP Base, Security, UC a Data.
- **mz** - Označuje, kde se obraz spustí a zda je soubor komprimován. V tomto příkladu mz označuje, že soubor běží z paměti RAM a je komprimován.
- **SPA** - Označuje, že soubor je digitálně podepsán společností Cisco.
- **152-4.M3** - Určuje formát souboru pro obrázek 15.2(4)M3. Jedná se o verzi IOS, která obsahuje hlavní vydání, drobné vydání, údržbu vydání a údržbu obnovy čísla. M označuje, že jde o rozšířené vydání údržby.
- **Bin** - přípona souboru. Toto rozšíření označuje, že tento soubor je binární spustitelný soubor.

Nejběžnější označení pro umístění paměti a kompresní formát je mz. První písmeno označuje místo, kde je obraz proveden na směrovači. Umístění může zahrnovat:

- f - flash
- m - RAM
- r - ROM
- l - přemístitelný

Formát komprese může být buď z pro zip, nebo x pro mzip. To je metoda, kterou Cisco používá, ke kompresi některých obrazů run-from-RAM, které jsou účinné při snižování velikosti obrazu. Je to samoobslužné rozbalení, takže když se obrázek načte do paměti RAM, bude první akce rozbalit.

Požadavky na paměť

Na většině směrovačů Cisco, včetně směrovačů integrovaných služeb, je IOS uložen v kompaktní paměti flash, jako komprimovaný snímek a je během bootování vložen do paměti RAM. Obrazy vydání Cisco IOS Software 15.0, dostupné pro Cisco 1900 a 2900 ISR, vyžadují 256MB flash a 512MB paměti RAM. Model 3900 ISR vyžaduje 256MB flash a 1GB paměti RAM. Nezahrnuje další nástroje pro správu, jako je Cisco CP. Podrobné informace naleznete v datovém listu produktu pro konkrétní směrovač.

16.2.2 Správa Obrazů Cisco IOS

16.2.2.1 Záložní Lokace a TFTP Servery

S rostoucí sítí mohou být obrazy a konfigurační soubory softwaru Cisco IOS, uloženy na centrálním serveru TFTP. To pomáhá řídit počet obrazů IOS a jejich revizi, stejně jako konfigurační soubory, které musí být zachovány.

Interní sítě produkují obvykle širokou oblast a obsahují více směrovačů. Pro každou síť je dobré zachovat záložní kopii obrazu softwaru Cisco IOS v případě, že obraz systému ve směrovači bude poškozen, nebo náhodně vymazán.

Široce distribuované směrovače potřebují zdrojové nebo záložní umístění pro obrazy softwaru Cisco IOS. Použití sítě TFTP serveru, umožňuje odesílání a stahování obrazů a konfigurací po síti. Síťový server TFTP může být jiným směrovačem, pracovní stanicí nebo hostitelským systémem.

16.2.2.2 Vytvoření Zálohy Obrazu Cisco IOS

Chcete-li udržovat síťové operace s minimálním prostojem času, je třeba mít k dispozici postupy pro zálohování obrazů Cisco IOS. To umožňuje správci sítě rychle zkopírovat obraz zpět do směrovače, v případě poškození nebo vymazání.

Na obr. 1, chce správce sítě vytvořit zálohu aktuálního obrazového souboru na směrovači (c1900-universalk9-mz.SPA.152-4.M3.bin) na server TFTP na adrese 172.16.1.100.

Chcete-li vytvořit zálohu obrazu Cisco IOS na server TFTP, proveďte následující tři kroky:

Krok 1. Zkontrolujte, zda je přístup k síťovému serveru TFTP. Ping serveru TFTP, testujte připojení, jak je znázorněno na obrázku 2.

Krok 2. Ověřte, zda má server TFTP dostatek místa na disku, pro přizpůsobení obrazu softwaru Cisco IOS. Pomocí příkazu ***show flash0:*** na směrovači, zjistíte velikost souboru obrazů Cisco IOS. Soubor v příkladu je dlouhý 68831808 bajtů.

Krok 3. Zkopírujte obraz na server TFTP, pomocí příkazu ***copy zdrojová-url cílová-url***, jak je znázorněno na obrázku 3.

Po zadání příkazu pomocí zadané zdrojové a cílové adresy URL, je uživatel vyzván k zadání názvu zdrojového souboru, adresy IP vzdáleného hostitele a názvu cílového souboru. Převod začne.

Pomocí kontroly syntaxe na obrázku 4 na R2, zkopírujte IOS na server TFTP.

16.2.2.3 Kopírování Obrazu Cisco IOS

Společnost Cisco důsledně vydává nové verze softwaru Cisco IOS, k vyřešení problémů a poskytování nových funkcí. Tento příklad používá protokol IPv6 pro přenos, který ukazuje, že TFTP lze také použít v sítích IPv6.

Obrázek 1, znázorňuje kopírování obrazu softwaru Cisco IOS ze serveru TFTP. Nový soubor s obrazem (c1900-universalk9-mz.SPA.152-4.M3.bin), bude zkopírován ze serveru TFTP na 2001:DB8:CAFE:100::99 do směrovače.

Při upgradu softwaru ve směrovači Cisco, postupujte takto:

Krok 1. Vyberte soubor obrazu Cisco IOS, který splňuje požadavky z hlediska platformy, funkcí a softwaru. Stáhněte soubor z cisco.com a přeneste jej na server TFTP

Krok 2. Ověřte připojení k serveru TFTP. Ping serveru TFTP ze směrovače. Výstup na obrázku 2 ukazuje, že server TFTP je přístupný ze směrovače.

Krok 3. Ujistěte se, že na směrovači, který je aktualizován, je dostatek místa. Množství volného místa flash paměti, lze ověřit pomocí příkazu ***show flash0:***. Porovnejte volné místo ve flash s novou velikostí souboru obrazu. Příkaz ***show flash0:*** na obrázku 3, slouží k ověření volné velikosti flash paměti. Volný prostor pro flash v příkladu, je 182 394 880 bajtů.

Krok 4. Zkopírujte soubor obrazu IOS ze serveru TFTP do směrovače, pomocí příkazu ***copy*** zobrazeného na obrázku 4. Po vydání tohoto příkazu se zadanými zdrojovými a cílovými adresami URL, bude uživatel vyzván k zadání adresy IP vzdáleného hostitele, Název zdrojového a cílového souboru. Přenos souboru bude zahájen.

16.2.2.4 Boot Systému

Chcete-li upgradovat na kopírovaný obraz IOS, po uložení tohoto snímku do paměti flash, nakonfigurujte směrovač tak, aby během bootování načetl nový obraz, pomocí příkazu ***boot system***. Uložte konfiguraci. Znovu načtěte směrovač a spustíte ho s novým obrazem. Po spuštění směrovače ověřte, zda byl nový obrázek načten. Použijte příkaz ***show version***.

Během spouštění, se spustí bootstrapový kód spouštěcí konfigurační soubor v NVRAM pro příkaz ***boot system***, který určuje název a umístění softwaru Cisco IOS a kde se má načíst. Několik příkazů ***boot system***, může být zadáno postupně, čímž se vytvoří plán zavádění odolný proti chybám.

Na obrázku 1, je příkaz ***boot system***, globální konfigurační příkaz, který uživateli umožňuje zadat zdroj pro načtení obrazu softwaru Cisco IOS. Některé dostupné možnosti syntaxe zahrnují:

Určete zařízení Flash jako zdroj obrazu Cisco IOS.

- *Router (config) # boot systém flash0://c1900-universalk9-mz.SPA.152-4.M3.bin*

Určete server TFTP jako zdroj obrazu Cisco IOS.

- *Router (config) # boot system tftp://c1900-universalk9-mz.SPA.152-4.M3.bin*

Pokud v konfiguraci nejsou žádné příkazy ***boot system***, směrovač je výchozí k načtení prvního platného obrazu Cisco IOS do paměti flash a jeho spuštění.

Jak je znázorněno na obrázku 2, příkaz ***show version***, může být použit k ověření souboru obrazu softwaru.

16.3 Licencování IOS

16.3.1 Licencování Softwaru

16.3.1.1 Přehled Licencování

Počínaje vydáním softwaru Cisco IOS verze 15.0, se změnil proces umožňující nové technologie v sadách funkcí IOS. Vydání softwaru Cisco IOS 15.0, obsahuje sady funkcí pro různé platformy, které zjednodušují proces výběru obrazů. To dělá tím, že poskytuje podobné funkce přes hranice platformy. Každé zařízení je dodáváno se stejným univerzálním obrazem. Technologické balíčky jsou povoleny v univerzálním obrazu, pomocí licenčních klíčů pro aktivaci softwaru Cisco. Funkce aktivace softwaru, umožňuje uživateli povolit licencované funkce a registrovat licence. Funkce Aktivace softwaru Cisco IOS, je sbírka procesů a komponent používaných k aktivaci sad funkcí vydání Cisco IOS, získáním a ověřením licencí.

Obrázek 1 ukazuje technologické balíčky, které jsou k dispozici:

- IP Base
- Data
- Unified Communications (UC)
- Bezpečnost (SEC)

Klepnutím na tlačítka na obrázku 2, se dozvíte více o technologických balíčcích.

Poznámka: Licence IP Base, je předpokladem pro instalaci licencí Data, Security a UC. U starších platforem směrovačů, které mohou podporovat verzi softwaru Cisco IOS 15.0, není k dispozici univerzální obraz. Je nutné stáhnout samostatný obraz, který obsahuje požadované funkce.

Licence na technologické balíčky

Licence na technologické balíčky jsou podporovány na platformách Cisco ISR G2 (směrovače Cisco série 1900, 2900 a 3900). Univerzální obraz Cisco IOS, obsahuje všechny balíky a funkce v jednom obrazu. Každý balíček je seskupením technologií specifických funkcí. Licenční balíčky s více technologiemi mohou být aktivovány na platformách ISR řady Cisco 1900, 2900 a 3900.

16.3.1.2 Proces Licencování

Když je nový směrovač dodán, je dodán s předinstalovaným obrazem softwaru a odpovídajícími trvalými licencemi pro balíky a funkce určené zákazníkem.

Směrovač je dodáván s licencí pro hodnocení, známou jako dočasná licence, pro většinu balíčků a funkcí podporovaných na daném směrovači. To umožňuje zákazníkům vyzkoušet nový softwarový balíček nebo funkci aktivací konkrétní hodnotící licence. Pokud zákazníci chtějí trvale aktivovat softwarový balíček nebo funkci na směrovači, musí získat novou softwarovou licenci.

Obrázek ukazuje tři kroky k trvalé aktivaci nového softwarového balíčku nebo funkce na směrovači.

16.3.1.3 Krok 1. – Pořízení Balíčku Softwaru, nebo Funkce k Instalaci

Krok 1. Pořízení balíčku nebo funkce, kterou chcete nainstalovat.

Prvním krokem je zakoupení potřebného softwarového balíčku nebo funkce. Může se jednat o přidání balíčku do služby IP Base, například zabezpečení.

Certifikáty pro nároky na software se používají pro licence, které vyžadují aktivaci softwaru. Certifikát obsahuje licenční klíč pro aktivaci produktu (PAK) a důležité informace týkající se licenční smlouvy koncového uživatele Cisco (EULA). Ve většině případů již společnost Cisco, nebo partner kanálu společnosti Cisco, aktivují licence objednané v době nákupu a neposkytují žádný certifikát o softwaru.

V každém případě obdrží zákazník k nákupu, PAK. PAK slouží jako potvrzení a slouží k získání licence. PAK je 11místný alfanumerický klíč vytvořený společností Cisco. Definuje Sadu funkcí přidruženou k PAK. Není vázán na konkrétní zařízení, dokud nebude vytvořena licence. Může být zakoupeno PAK, který generuje libovolný počet licencí. Jak je znázorněno na obrázku, pro každý balíček, IP Base, Data, UC a SEC je vyžadována samostatná licence.

16.3.1.4 Krok 2. – Získání Licence

Krok 2. Získat licenci.

Dalším krokem je získat licenci, která je vlastně licenční soubor. Licenční soubor, známý také jako licence pro aktivaci softwaru, se získává pomocí jedné z následujících možností:

- **Cisco License Manager (CLM)** - volná softwarová aplikace dostupná na adrese http://www.cisco.com/go/clm. Správce licencí společnosti Cisco je samostatná aplikace od společnosti Cisco, která pomáhá správcům sítě rychle zavádět více licencí softwaru Cisco v rámci svých sítí. Správce licencí, může objevovat síťová zařízení, prohlížet jejich licenční informace a získávat a nasazovat licence od společnosti Cisco. Aplikace poskytuje grafické uživatelské rozhraní, které zjednodušuje instalaci a pomáhá automatizovat získávání licencí, stejně jako provádět řadu licenčních úkolů z centrálního umístění. CLM je zdarma a lze jej stáhnout z CCO.
- **Portál registrace licencí společnosti Cisco** - tento webový portál pro získávání a registraci jednotlivých licencí softwaru, který je k dispozici na adrese http://www.cisco.com/go/license.

Oba tyto procesy vyžadují číslo PAK a jedinečný identifikátor zařízení (UDI).

PAK je obdržena během nákupu.

UDI je kombinací ID produktu (PID), sériového čísla (SN) a hardwarové verze. SN je 11místné číslo, které jednoznačně identifikuje zařízení. PID identifikuje typ zařízení. Pro tvorbu licencí se používají pouze PID a SN. Tento UDI, lze zobrazit pomocí příkazu ***show license udi***, který je zobrazen na obrázku 1. Tyto informace jsou k dispozici také na výsuvném zásobníku štítků, který se nachází na zařízení. Obrázek 2, ukazuje příklad vytažení štítku na směrovači Cisco 1941.

Po zadání příslušných informací obdrží zákazník e-mail, obsahující informace o licenci k instalaci licenčního souboru. Licenční soubor je textový soubor XML, s příponou lic.

16.3.1.5 Krok 3. – Instalace Licence

Krok 3. Nainstalujte licenci

Po zakoupení licence získá zákazník licenční soubor. Instalace trvalé licence vyžaduje dva kroky:

Krok 1. Chcete-li nainstalovat licenční soubor, použijte příkaz ***license install url-lokace-uložení***.

Krok 2. Znovu načtěte směrovač pomocí ***reload*** příkazu. Opětovné načtení není požadováno, pokud je aktivována evaluační licence.

Obrázek 1 ukazuje konfiguraci pro instalaci trvalé licence pro balíček zabezpečení na směrovači.

Poznámka: U směrovačů 1941, nejsou podporovány sjednocené komunikace.

Trvalá licence je licence, která nikdy nevyprší. Po instalaci trvalé licence na směrovači je dobré, aby tato funkce byla nastavena na dobu životnosti směrovače, a to i ve verzích IOS. Pokud je například na směrovači nainstalována licence UC, SEC nebo Data, jsou aktivovány další funkce této licence, i když je směrovač inovován na nové vydání IOS. Trvalá licence je nejběžnější typ licence používaný při zakoupení sady funkcí pro zařízení.

Poznámka: Produkce společnosti Cisco, před-instaluje příslušnou trvalou licenci na objednané zařízení, pro zakoupenou sadu funkcí. Pro povolení této licence na nový hardware není zapotřebí interakce s procesy aktivace softwaru Cisco IOS.

Pomocí kontroly syntaxe na obrázku 2, nainstalujte trvalý licenční soubor na směrovači R2.

16.3.2 Verifikace a Správa Licence

16.3.2.1 Verifikace Licence

Po instalaci nové licence, musí být směrovač restartován, pomocí příkazu ***reload***. Jak je znázorněno na obrázku 1, příkaz ***show version***, se používá po opětovném načítání směrovače k ověření, že byla nainstalována licence.

Příkaz ***show license***, na obrázku 2 slouží k zobrazení dalších informací o licencích softwaru Cisco IOS. Tento příkaz zobrazuje informace o licencích, které se používají k řešení problémů týkajících se licencí softwaru Cisco IOS. Tento příkaz zobrazí všechny licence nainstalované v systému. V tomto příkladu byly nainstalovány licence IP Base i Security. Tento příkaz také zobrazuje funkce, které jsou k dispozici, ale nejsou licencovány k provedení,

jako je například sada funkcí Data. Výstup je seskupen podle toho, jak jsou funkce ukládány do úložiště licencí.

Následuje stručný popis výstupu:

- **Funkce** - název funkce
- **Typ licence** - typ licence. Jako například Trvalé nebo Hodnocení
- **Stav licence** - stav licence. Jako například aktivní nebo v užívání
- **Počet licencí** - Počet licencí, které jsou k dispozici a jsou používány, pokud jsou započítány. Není-li započítáno, je licence neomezená.
- **Priorita licence** - priorita licence. Jako je vysoká nebo nízká

Poznámka: Podrobné informace o informacích zobrazených v příkazu show licence naleznete v referenční příručce k příkazům Cisco IOS 15.

16.3.2.2 Aktivace Hodnocení Licence – Right-To-Use(Právo Používat)

Proces vyhodnocovací licence, prošel třemi verzemi zařízení ISR G2. Nejnovější revize, počínaje verzemi Cisco IOS 15.0(1)M6, 15.1(1)T4, 15.1(2)T4, 15.1(3)T2 a 15.1(4)(RTU), se dělají po 60 dnech. Licenční hodnocení je dobré pro 60denní zkušební dobu. Po uplynutí 60 dnů tato licence automaticky přechází do licence RTU. Tyto licence jsou k dispozici v systému čestnosti a vyžadují, aby zákazník akceptoval smlouvu EULA. Licenční smlouva EULA se automaticky vztahuje na všechny licence softwaru Cisco IOS.

Příkaz globálního konfiguračního režimu, ***license accept end user agreement***, se používá pro konfiguraci jednorázového přijetí smlouvy EULA pro všechny balíky a funkce softwaru Cisco IOS. Po vydání příkazu a přijetí smlouvy EULA, se smlouva EULA automaticky vztahuje na všechny licence softwaru Cisco IOS a uživatel není vyzván k přijetí smlouvy EULA během instalace licence.

Obrázek 1 ukazuje, jak nakonfigurovat jednorázové přijetí smlouvy EULA:

Router (config) # license accept end user agreement

Obrázek 1 navíc zobrazuje příkaz k aktivaci licence RTU hodnocení:

Router # license boot module jméno-modulu technology-package jméno-balíčku

Použijte otazník namísto argumentů, které určují, které názvy modulů a podporované softwarové balíčky jsou k dispozici na směrovači. Názvy technologických balíčků pro platformy Cisco ISR G2 jsou:

- ipbasek9 - balíček IP Base Technology
- securityk9 - Balík bezpečnostních technologií
- datak9 - Balík datových technologií
- uck9 - balíček UC (není k dispozici v řadě 1900)

Poznámka: Pro aktivaci softwarového balíku je nutné opětovné načtení příkazu ***reload***.

Hodnotící licence jsou dočasné a slouží k vyhodnocení funkce nastavené na nový hardware. Dočasné licence jsou omezeny na konkrétní dobu používání (například 60 dní).

Znovu načtěte směrovač po úspěšné instalaci licence pomocí příkazu ***reload***. Příkaz ***show license*** na obrázku 2 ověří, že licence byla nainstalována.

Pomocí kontroly syntaxe na obrázku 3, přijměte smlouvu EULA a aktivujete licenci pro vyhodnocení datového balíčku RTU na směrovači 1900.

16.3.2.3 Záloha Licence

Příkaz ***license save***, se používá ke kopírování všech licencí v zařízení a jejich ukládání ve formátu vyžadovaném zadaným úložištěm. Uložené licence jsou obnoveny pomocí příkazu ***license install***.

Příkaz k zálohování kopie licencí na zařízení je:

Router # license save file-sys://lic-lokace

Pomocí příkazu ***show flash0:*** ověřte, zda byly licence uloženy (obrázek 1).

Umístění úložiště licencí může být adresář nebo adresa URL, která odkazuje na souborový systém. Použijte otazník pro zobrazení míst uložení podporovaných zařízením.

Použijte kontrolu syntaxe na obrázku 2 pro uložení všech licenčních souborů na směrovači R2.

16.3.2.4 Odinstalování Licence

Chcete-li zrušit aktivní trvalou licenci ze směrovačů řady Cisco 1900, 2900 a 3900, proveďte následující kroky:

Krok 1. Zakažte technologický balíček.

- Zakázat aktivní licenci příkazem:

Router (config) # license boot module jméno-modulu technology-package jméno-balíčku disable

- Znovu načtěte směrovač pomocí příkazu ***reload***. Pro obnovení softwarového balíčku je nutné znovu načíst.

Krok 2. Vymažte licenci.

- Vymažte licenci pro balíček technologií z úložiště licencí.

Router # license clear jméno-funkce

- Pro deaktivaci aktivní licence, použijte příkaz:

Router (config) # no license boot module jméno-modulu technology-package jméno-balíčku disabled

16.4 Shrnutí

16.4.1 Shrnutí

16.4.1.1 Shrnutí

Příklady softwarových verzí Cisco IOS zahrnují 12.3, 12.4, 15.0 a 15.1. Spolu s každým softwarem jsou k dispozici nové verze softwaru, které se používají k implementaci oprav chyb a nových funkcí.

Software Cisco IOS 12.4, obsahuje nové softwarové funkce a podporu hardwaru, které byly zavedeny do vlaku Cisco IOS Software 12.3T a dodatečné opravy softwaru. Hlavní vydání (nazývané také verze vydání údržby) neobsahují žádné velké písmeno v označení jejich vydání a dědí nové funkce a hardware softwaru Cisco IOS, od nižších číslovaných vydání T. V 12.4, hlavní vlak "M", dostal pouze opravy chyb. Technologie vlaku "T" obsahuje opravy, nové funkce a platformy. Vlak 12.4T poskytuje funkčnost softwaru Cisco IOS a přijetí hardwaru, které zavádí nové technologie, funkce a pokroky v oblasti hardwaru, které nejsou k dispozici v hlavním vlaku Cisco IOS Software 12.4.

V nové verzi Cisco IOS Software 15.0 je zavedena nová strategie. Rodina vydání Cisco IOS 15.0, se neodchyluje do samostatných vlaků M a T, ale do vydání M a T ve stejném vlaku. Například první vydání ve verzi Cisco IOS Software 15.0 je 15.0(1)M, kde M označuje prodloužené vydání údržby. Rozšířené vydání údržby, je ideální pro dlouhodobou údržbu. Ne všechny verze ve verzi Cisco IOS Software 15.0 budou prodloužená vydání údržby; Budou zde také standardní verze údržby, které získají nejnovější funkce a podporu hardwaru. Standardní vydání údržby bude mít v jejich označení velkou T.

Při výběru nebo upgradu směrovače Cisco IOS, je důležité vybrat správný obraz IOS se správnou sadou funkcí a verzí. Obrazový soubor Cisco IOS, je založen na speciální konvenci pojmenování. Název souboru obrazu Cisco IOS, obsahuje více částí, z nichž každýá má určitý význam. Příklad: c1900-universalk9-mz.SPA.152-4.M3.bin

Příkazy jsou k dispozici pro upgrade a ověření flash paměti. Příkaz ***show flash***, zobrazuje ukládání souborů v paměti Flash včetně obrazových souborů systému. Tento příkaz lze také použít k ověření volné velikosti paměti flash. Příkaz ***boot system***, je globální konfigurační příkaz, který uživateli umožňuje zadat zdroj pro Cisco IOS.

Používání sítě TFTP serveru, umožňuje odesílání a stahování obrazů a konfigurací po síti. Síťový server TFTP může být jiným směrovačem, pracovní stanicí nebo hostitelským systémem.

Počínaje vydáním softwaru Cisco IOS verze 15.0, změnila Cisco proces umožňující nové technologie v sadách funkcí IOS. Každé zařízení je dodáváno se stejným univerzálním obrazem. Technologické balíčky jako IP Base, Data, UC a SEC jsou povoleny v univerzálním obrazu pomocí licenčních klíčů pro aktivaci softwaru Cisco. Každý licenční klíč je pro konkrétní zařízení jedinečný a získává se od společnosti Cisco uvedením ID produktu a sériového čísla směrovače a aktivačního klíče pro produkt (PAK).

Aktivace licence není nutná pro předem nakonfigurované licence před použitím. IP Base je dodáván jako trvalá licence na všech zařízeních ISR-G2. Další tři technologické balíčky: Data, Security a UC, přicházejí s licencí pro hodnocení jako výchozí, ale může být zakoupena trvalá licence.

Instalace licence

Předpoklady:

- Získejte potřebné PAK, což je 11 místní ID, které lze doručit poštou nebo elektronicky
- Potřebujete mít platné uživatelské jméno/heslo společnosti Cisco
- Načtěte sériové číslo a PID pomocí příkazu, ***show license udi***, pro ukázkovou licenci nebo z přihrádky štítku směrovače

ZÁVĚR

Síťová komunikace, je v současnosti základním stavebním kamenem moderní doby. Možnosti vzdálené, nebo bezdrátové komunikace hrají zásadní roli ve firmách, podnicích a u většiny klientů. Kurz CCNA 3 Směrování a Přepínání Škálovatelných sítí, je jedním z nejvyhledávanějších výukových materiálů na světě. Protože společnost Cisco je obrovská společnost, která poskytuje a řeší veškerý síťový provoz, za použití jejich zařízení.

Cílem této práce, bylo přeložení učebních materiálů celého kurzu, pro usnadnění výuky studentů, z jazykovou bariérou. Samotnému překladu předcházelo, rozebrání všech důležitých aspektů a technologií, které patří k obsahu tohoto kurzu.

V rámci kurzu, se začínalo z popisem 2. vrstvy OSI modelu, na které fungují síťová zařízení, jako přepínače. Proto se startovalo od protokolu fungujícím na 2. vrstvě, Spanning Tree Protocol. Tento protokol, se používá kvůli zabezpečení redundance sítě, bez smyček. Dále jsem se věnoval protokolům, které vycházejí ze STP, ale mají specifická vylepšení. Jednalo se o protokoly RSTP a PVST+, které poskytují rychlejší konvergence sítě.

Jenomže, redundantní linky v síti, můžou způsobit smyčky, nebo si krást pro sebe šířku pásma. Aby se umožnilo sdílení zatížení fyzických linek, používá se metoda agregace linek. Která, vytváří jedno logické spojení z více fyzických. Je to jiná forma, než STP a v přepínaných sítích se často používá.

Jenomže v moderní době, jsou stále víc kladeny nároky na flexibilitu a tu umožňuje použití bezdrátových sítí WLAN. Bezdrátové sítě jsou méně nákladnou formou komunikace, i když na menší vzdálenosti. Ale z velkou podporou flexibility. To znamená, že každý klient z notebookem, nebo chytrým telefonem, se může připojit kdekoliv, kde se lokalizuje nějaký přístupový bod AP.

Dále jsem se věnoval dvěma dynamickým směrovacím protokolům, OSPF a EIGRP. Oba jsou směrovacími protokoly, používané ve velkých sítích z mnoha uživateli. Jejich správná konfigurace zabezpečí, bezpečnou a rychlou komunikaci.

Nakonec, každé zařízení Cisco, ke svému fungování, potřebuje operační systém, konkrétně IOS. Prošli jsme si verze IOS, které se nejběžněji používají na zařízeních Cisco. A ke správnému použití jsme si rozebrali, možnosti získání licencí, na tyto systémy.

I když je to velice rozsáhlý kurz, nebyl problém při překládání, protože výukové materiály, jsou psány velmi srozumitelně. A proto je potřeba s nimi spolupracovat, pro dosažení co nejlepších výsledků v tomto kurzu.

SEZNAM POUŽITÉ LITERATURY

[1] Online Curriculum: Scaling Networks. Cisco Networking Academy [online]. [cit. 2017-01-30]. Dostupné z: https://www.netacad.com/

[2] EMPSON, Scott. CCNP routing and switching portable command guide. 2nd edition. Indianapolis: Cisco Press, 2014, 391 p. ISBN 978-1-58714-434-9.

[3] LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-80-251-2359-1.

[4] CISCO NETWORKING ACADEMY na VUT v Brně FIT: Kurz CCNA Routing and Switching 3 [online]. Page last modified on June 28, 2016 [cit. 2017-01-30].Dostupné z :http://netacad.fit.vutbr.cz/index.php?n=CCNA

[5] SOSINSKY, Barrie A. Mistrovství - počítačové sítě [vše, co potřebujete vědět o správě sítí]. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.

[6] PAHLAVAN, Kaveh a Prashant. KRISHNAMURTHY. *Principles of wireless access and localization*. ISBN 978-0-470-69708-5.

[7] ZANDL, Patrick. *Bezdrátové sítě WiFi: praktický průvodce*. Brno: Computer Press, 2003. ISBN 80-7226-632-2.

[8] PEPELNJAK, Ivan. *EIGRP network design solutions*. Indianapolis, IN, USA: Cisco Press, c2000. ISBN 1-57870-165-1.

[9] Guides. *Router Alley* [online]. Aaron Balchunas, 2007 [cit. 2017-05-21]. Dostupné z: http://www.routeralley.com/guides.html

[10] HUCABY, Dave a Steve MCQUERRY. *Konfigurace směrovačů Cisco*. Brno: Computer Press, 2004. ISBN 80-7226-951-8.

[11] LAW, David. Agenda and General Information. *Ieee802* [online]. 2007, 1-19 [cit. 2017-05-21]. Dostupné z: http://www.ieee802.org/3/axay/public/jul_07/agenda_0707.pdf

[12] *Samuraj-cz* [online]. Brno: Petr Bouška, 2005 [cit. 2017-05-21]. Dostupné z: http://www.samuraj-cz.com/

[13] HALLAK, Danny. Etherchannel (Link Aggregation/ LACP/ PAGP). In: *Linkedin* [online]. Danny Hallak, 2015 [cit. 2017-05-21]. Dostupné z: https://www.linkedin.com/pulse/etherchannel-link-aggregation-lacp-pagp-dany-hallak

[14] NAYANAJITH, Rasika. 802.11 Frame Format. In: *Mrncciew* [online]. Dubai: Rasika Nayanajith, 2013 [cit. 2017-05-21]. Dostupné z: https://mrncciew.com/2013/04/24/802-11-frame-format/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ICT	Information and Communication Technologies
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
STP	Spanning Tree Protocol
VLAN	Virtual Local Area Network
VTP	VLAN Trunking Protokol
RSTP	Rapid Spanning Tree Protocol
RIP	Routing Information Protocol
OSPF	Open Shortest Path First
EIGRP	Enhanced Interior Gateway Routing Protocol
IOS	Internetwork Operating System
QoS	Quality of Services
WAN	Wirreles Area Network
IDS	Intrusion Detection System
IPS	In-Plane Switching
TTL	Time To Live
Dos	Denial of Srvice
ARP	Address Resolution Protocol
Trunk	Linka mezi 2 body
BPDU	Bridge Protocol Data Unit
MSTP	Multiple Spanning Tree Protocol
MST	Minimum Spanning Tree
STA	Spanning Tree Algorithm
BID	Bridge ID
CST	Computer Simulation Technology

FHRP	First Hop Redundancy Protocols
HSRP	Hot Standby Router Protocol
VRRP	Virtual Router Redundancy Protocol
GLBP	Gateway Load Balancing Protocol
ICMP	Internet Control Message Protocol
IRDP	ICMP Router Discovery Protocol
PAgP	Port Aggregation Protocol
LACP	Link Aggregation Control Protocol
RF	Radio Frequency
WPA	Wifi Protected Access
WPS	Wifi Protected Setup
AP	Access Piont
SSID	Service Set ID
WDS	Wirreles Domain Services
PoE	Proof of Entitlement
MCC	Meraki Cloud Controoller
WLC	Wirreles LAN Controler
WCS	Wirreles Controled Systems
ISR G2	Integrated Services Routers Generation 2
DS	Distribute Systém
BSS	Basic Service Set
BSA	Basic Service Area
ESS	Extended Service Set
ESA	Extended Service Area
RTS	Request to Send
CTS	Clear to Send

ACK	Acknowledgment frame
DCF	Distributed Coordinated Function
OFDM	Ortogonal Frequency Divided Multiplex
MFP	Management Frame Protection
MITM	Man in the Middle
TKIP	Time Key Integrity Protocol
AES	Advanced Encryption Standard
DR	Designated Router
BDR	Backup Designated Router
VLSM	Variable Lenght Subnet Mask
MD5	Message Digest 5
BMA	Broadcast Multiaccess
NBMA	Non-broadcast
LSA	Link-state Advertisement
LSDB	Link State Database
SPF	Sender Policy Framework
NSSA	Not so Stubby Area
ABR	Area Boundary Router
ASBR	Autonomous Systém Boundary Router
IETF	Internet Engineering
DUAL	Diffusing Update Algorithm
RTP	Reliable Transport Protocol
ATM	Asynchronous Transfer Model
TLV	Type-lenght-value
ISP	Internet Service Provider
FD	Feasible Distance

FS	Feasible Successor
RD	Reported Distance
AD	Advertisement Distance
FC	Feasible Condition
FSM	Finite State Machine
CEF	Cisco Express Forwarding
IGP	Interior Gateway Protocol
NSF	Nonstop Forwarding
ACL	Access list
EM	Vydání hlavní údržby
UC	Unified Communications
TFTP	Trivial File Transfer Protocol
PAK	Product Activation Key
CLM	Cisco License Manager
BSSID	Basic Service Set ID
PID	ID Produktu
UDI	Unique Device Identificator
RTU	Right-to-Use
ECNM	Enterprise Composite Network Model
WPAN	Wirreles Personal Area Network
WLSE	Wirreles LAN Solition Engine
LWAPP	Lightworth Control Point Protocol
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
PVST +	Per VLAN Spanning Tree Plus

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH