Obsah

Úvod
Metrika
Komunikace mezi OSPF směrovači
Navazování vztahů sousednosti
Výměna topologických informací mezi sousedy
Naplnění směrovací tabulky
Typy sítí
Hierarchie OSPF sítě
Spolupráce OSPF s dalšími směrovacími protokoly
Typy oblastí
Více o komunikaci mezi OSPF směrovači
Sumarizace adres
Autentikace
Srovnání interních směrovacích protokolů
Konfigurace OSPF na směrovačích Cisco

Úvod

Protokol OSPF (Open Shortest Path First) byl vytvořen organizací IETF přibližně v letech 1988 až 1991. Jeho nejnovější verze je definována v RFC2328. Tento protokol můžeme zařadit do skupiny směrovacích protokolů IGP - Interior Gateway Routing Protocols. Je tedy určen k použití uvnitř jednoho autonomního systému.

OSPF je typickým představitelem směrovacího protokolu typu **Link State**. Vytváří tedy v paměti směrovače kompletní mapu celé sítě, označovanou jako topologická databáze (někdy se jí říká Link State Database). Nad touto databází potom pomocí algoritmu označovaného jako Shortest Path First (SPF) provádí výpočty potřebné k nalezení nejvýhodnější cesty do jednotlivých sítí. Naproti tomu směrovací protokoly typu **Distance Vector** používají Bellman-Fordův algoritmus, kdy si sousední směrovače navzájem vyměňují své směrovací tabulky, ale topologii celé sítě neznají. Do skupiny Distance Vector protokolů můžeme zařadit např. protokoly RIP nebo IGRP.

Ve velmi zjednodušené podobě můžeme funkci protokolu OSPF popsat následovně :

1. Směrovač vysílá přes svá rozhraní tzv. Hello pakety. Pokud se dva navzájem propojené routery pomocí těchto paketů dohodnou na určitých společných parametrech, stávají se sousedy (neighbors).
2. Mezi některými ze sousedů se vytvářejí užší vazby. Tyto routery se pak označují jako přilehlé (adjacent).
3. Přilehlé routery si vzájemně vyměňují pakety obsahující LSA (Link State Advertisement) informace. Ty popisují stav rozhraní směrovače nebo seznam směrovačů připojených k dané síti.
4. Všechny směrovače si ukládají přijaté LSA do své lokální topologické databáze a zároveň je přeposílají na ostatní přilehlé směrovače. Tím se informace postupně rozšíří mezi všechny směrovače v síti. Výsledkem bude shodná topologická databáze na všech směrovačích.
5. Po naplnění databáze každý směrovač provede výpočet pomocí SPF (Dijkstrova) algoritmu. Jeho výsledkem bude nalezení nejkratší cesty do každé známé sítě a odstranění smyček v topologii sítě.
6. Na základě vypočtených dat je možné naplnit směrovací tabulku routeru.
7. Pokud dojde ke změně topologie sítě, směrovač na kterém ke změně došlo odešle přilehlým směrovačům informaci v podobě LSA datových položek v OSPF paketu. Ta se postupně rozšíří po celé síti a každý směrovač upraví svou topologickou databázi a provede nový výpočet SPF algoritmu.

Velkou výhodou protokolu OSPF proti starším směrovacím protokolům (např. RIP) je jeho schopnost pracovat v relativně velkých sítích. Dosáhlo se toho zavedením dvou úrovní hierarchie. Síť je rozdělené na takzvané oblasti (area). LSA se běžně šíří pouze uvnitř dané oblasti a také výpočet SPF algoritmu se spouští pro každou oblast samostatně. Z jedné oblasti do druhé se předávají pouze sumární informace. Změna topologie sítě v jedné oblasti tedy nevyvolá přepočet SPF algoritmu v ostatních oblastech.

Metrika

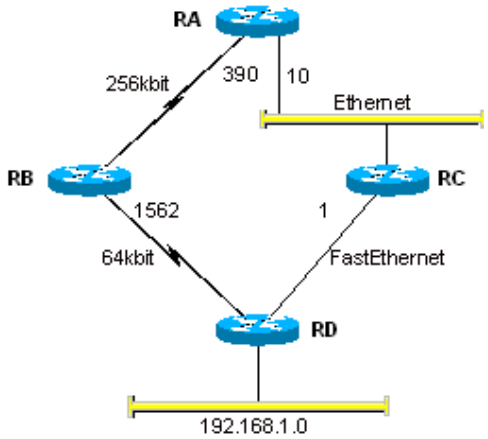
Každý směrovací protokol potřebuje kritérium podle kterého posoudí, která z více možných cest do cílové sítě je nejvýhodnější. Různé protokoly používají různá kritéria. Toto kritérium se označuje jako metrika. Například RIP používá počet přeskoků mezi routery nebo IGRP využívá kombinaci šířky pásma, zatížení, zpoždění a spolehlivosti linky.

Protokol OSPF používá metriku označovanou jako **cena (cost)**. To je číslo v rozsahu 1 až 65535, přiřazené ke každému rozhraní směrovače. Čím menší číslo, tím má cesta lepší metriku a bude tedy více preferována. Standardně je ke každému rozhraní přiřazena cena automaticky odvozená z šířky pásma daného rozhraní podle vztahu

cost = 100000000 / bandwidth v bps

Například linka 64kbps bude mít standardně cenu 100000000/64000=1562. Aby tento automatický mechanismus fungoval, je třeba mít u každého rozhraní správně přiřazený bandwidth. Dále je z uvedeného vztahu vidět, že linky FastEthernet a rychlejší budou mít shodně přiřazenou cenu 1. Proto některé implementace OSPF dovolují konstantu 100000000 změnit na vyšší. Dále je možné přiřadit cenu k rozhraní ručně a tím například upřednostnit pomalejší linku před linkou rychlejší.

Výsledná cena cesty ze směrovače do cílové sítě je pak dána součtem cen všech odchozích rozhraní po cestě. Například v obrázku 1 bude cena cesty ze směrovače RA do sítě 192.168.1.0 přes RB 390+1562=1952, zatímco cesta přes RC bude mít cenu 10+1=11 a bude mít tedy přednost. Pokud bychom na ethernetové rozhraní RA ručně přiřadili cenu 2000, dostane přednost cesta přes RB.



Obr.1 Výpočet ceny cesty

Komunikace mezi OSPF směrovači

Data která si mezi sebou vyměňují OSPF směrovače jsou přenášena prostřednictvím protokolu IP jako protokol číslo 89. Za IP hlavičkou následuje hlavička OSPF, která určuje typ OSPF paketu (Hello, Link State Request a pod). Pak přijdou informace specifické pro jednotlivé typy OSPF paketů. Ukázka enkapsulace OSPF protokolu v IP paketu a ethernetovém rámci je na obr.2.

```
Ethernet: Destination Adr=01005E000005 Source Adr=Cisco463E88 Type/Len=IP
IP: Length=68 TTL=1 Protocol= OSPF Source Address=192.168.1.1 Destination Address=224.0.0.5
OSPF: Version=2 Type=(1)Hello Length=48 Routed ID=192.168.1.1 Area ID=0.0.0.0
```

Obr.2 Enkapsulace OSPF protokolu v Ethernet rámci

Pakety protokolu OSPF si vyměňují vždy jen sousední zařízení. Proto je pole TTL v IP hlavičce nastaveno na hodnotu 1. OSPF používá při komunikaci po síti typu Ethernet adresy typu multicast. Tím je zajištěno, že rámce nesoucí OSPF pakety budou přijímat pouze směrovače podporující tento protokol a nebudou zbytečně přijímány pracovními stanicemi.

Navazování vztahů sousednosti

Dříve než bude možné mezi směrovači posílat směrovací informace, každý směrovač musí nalézt své sousedy. Použije k tomu Hello protokol, kdy každým rozhraním s nakonfigurovaným protokolem OSPF periodicky vysílá Hello pakety.

Přitom je nezbytná možnost jednoznačné identifikace jednotlivých směrovačů. K tomu se používá tzv. **Router ID**. Jako Router ID se použije nejvyšší IP adresa na loopback rozhraní nebo pokud není žádné takové rozhraní nakonfigurováno použije se nejvyšší IP adresa z libovolného rozhraní. Tato volba se provede vždy jen při zapnutí směrovače a pozdější změny IP adres na ní již nemají vliv.

Paket Hello protokolu je zobrazen na obrázku 3. Tyto pakety každý směrovač periodicky vysílá každým svým rozhraním (s nakonfigurovaným OSPF protokolem) v intervalu **HelloInterval**. Tento interval bývá na LAN sítích standardně 10s. Pokud směrovač nedostane od svého souseda Hello paket po dobu **DeadInterval**, předpokládá se, že spojení mezi směrovači je nefunkční. Obvyklá délka Dead intervalu bývá 4*Hello Interval, tedy na LAN síti 40s. Na WAN síti typu NBMA (viz. dále) se Hello Interval prodlužuje na 30s.

```
OSPF: Version: 2                    <02>
OSPF: Type:  Hello                  <01>
OSPF: Packet length: 48 [Bytes]     <0030>
OSPF: Router ID: 192.168.1.1
OSPF: Area ID: 0.0.0.0 [Backbone]   <00000000>
OSPF: Checksum: 0xF5F1
OSPF: Autype: 0[No authentication]    <0000>
OSPF: Authentication: 0x0000000000000000  <0000000000000000>
OSPF: The Hello Packet:
OSPF:   Network mask: 0xFFFFFF00
OSPF:   HelloInterval: 10 [seconds]  <000A>
OSPF:   Options: 0x02               <02>
OSPF:     ......1. E-bit
OSPF:     .....0.. MC-bit
OSPF:     ....0... N/P-bit
OSPF:     ...0.... EA-bit
OSPF:     ..0..... DC-bit
OSPF:   Router Priority: 1          <01>
OSPF:   RouterDeadInterval: 40 [seconds]  <00000028>
OSPF:   Designated Router: 192.168.1.1
OSPF:   Backup Designated Router: 192.168.1.2
OSPF:   Neighbor: 192.168.1.2
```

Obr.3 Formát OSPF Hello paketu

Každý Hello paket obsahuje pole Neighbor, ve kterém jsou Router ID všech již nalezených sousedů. Vztah sousednosti je mezi směrovači navázán ve chvíli, kdy v Hello paketu který dostal od svého souseda najde směrovač v tomto poli své vlastní Router ID. V té chvíli je ověřena obousměrná komunikace. Další podmínkou navázání vztahu sousednosti je to, že oba směrovače mají stejný Hello i Dead interval a dále že patří do stejné oblasti (Area ID) a do stejného typu oblasti (viz dále). Poté je sousední směrovač přidán do aktuálního seznamu sousedů.

Výměna topologických informací mezi sousedy

Dalším krokem v navazování komunikace mezi navzájem propojenými směrovači je vytvoření tzv. **adjacency**. Pouze směrovače které jsou navzájem přilehlé (adjacent) si mohou vyměňovat informace ze své topologické databáze. Cílem je dosáhnout shodnou databázi na všech směrovačích v oblasti.

Vše začne tím, že si směrovače vzájemně zašlou **Database Description Packet**. V něm je obsažen návrh náhodného sekvenčního čísla SEQ které bude použito pro další komunikaci. Ten směrovač, který má vyšší Router ID, bude zvolen jako Master a jím poslané sekvenční číslo bude v další komunikaci používáno.

Dále nejprve Master a poté i Slave směrovač odešle další Database Description Pakety, ve kterých si navzájem předají informace o svých topologických databázích. Tyto pakety jsou číslovány od dříve dohodnutého

sekvenčního čísla. Nyní oba směrovače porovnají popis databáze který dostali od svého souseda se svou vlastní databází. Pokud zjistí, že jim některé informace chybí nebo jsou zastaralé, vyžádají si příslušnou položku pomocí paketu typu **Link State Request** (LSR). Na něj soused odpoví paketem typu **Link State Update** (LSU), ve kterém zašle požadované informace. LSU paket je nutno potvrdit paketem **Link State Acknowledgement**. Nebude-li paket potvrzen, je po uplynutí timeoutu odeslán znova.

Podobný proces proběhne, pokud směrovač zjistí, že některý s jeho sousedů nadále není funkční (tedy že po dobu delší než Dead timer od něj nedostal Hello paket) nebo když pomocí Hello protokolu nalezne nového souseda. LSA s touto informací je třeba předat všem přilehlým směrovačům. Provede se to zasláním paketu typu LSU. Přilehlé směrovače tento LSU paket předají zase svým sousedům a tak se postupně informace rozšíří po celé oblasti.

S každou položkou v topologické databázi (LSA) je spojeno pole **Age** které je periodicky inkrementováno. Když jeho hodnota dosáhne **Maxage**, je LSA považováno za zastaralé a odstraněno z databáze. Proto jsou s periodou **LSRefreshTime** LSA rozesílána na všechny sousedy. Při přijetí LSA od sousedního routeru je pole Age vynulováno. Implicitní hodnota časovače MaxAge je v OSPF 1 hodina, pro časovač LSRefreshTime je to 30 minut.

Příklad paketu typu Link State Update a Link State Acknowledgement je na obrázku 4. V tomto příkladu propaguje směrovač s Router ID 1.0.0.2 informaci o sítích 1.0.0.4/32 a 200.0.0.0/24. Směrovač 1.0.0.3 přijatou informaci potvrzuje.

```
OSPF: Version: 2                    <02>
OSPF: Type:  Link State Update      <04>
OSPF: Packet length: 76 [Bytes]     <004C>
OSPF: Router ID: 1.0.0.2            <01000002>
OSPF: Area ID: 0.0.0.0 [Backbone]   <00000000>
OSPF: Checksum: 0x4C2F              <4C2F>
OSPF: Autype: 0[No authentication]    <0000>
OSPF: Authentication: 0x0000000000000000  <0000000000000000>
OSPF: The Link State Update packet:
OSPF:   Number of advertisements: 1  <00000001>
OSPF:   Link State Advertisment header No. 1
OSPF:     LS age: 46 [seconds]
OSPF:     Options: 0x22             <22>
OSPF:     LS type: 1 Router links    <01>
OSPF:     Link State ID: 1.0.0.4    <01000004>
OSPF:     Advertising Router: 1.0.0.4  <01000004>
OSPF:     LS sequence number: 0x80000006  <80000006>
OSPF:     LS checksum: 0x3E06       <3E06>
OSPF:     Length: 48 [bytes]        <0030>
OSPF:     Router links advertisement:
OSPF:     Bits: 0x00                <00>
OSPF:       Number of router links: 2  <0002>
OSPF:       Link No. 1
OSPF:         Link ID: 1.0.0.4      <01000004>
OSPF:         Link Data: 0xFFFFFFFF
OSPF:         Type:  Connection to a stub network
OSPF:         Number of TOS metrics: 0  <00>
OSPF:         Metric: 1             <0001>
OSPF:       Link No. 2
OSPF:         Link ID: 200.0.0.0
OSPF:         Link Data: 0xFFFFFF00
OSPF:         Type:  Connection to a stub network
OSPF:         Number of TOS metrics: 0  <00>
OSPF:         Metric: 1             <0001>

OSPF: Version: 2                    <02>
OSPF: Type:  Link State Acknowledgment   <05>
OSPF: Packet length: 64 [Bytes]     <0040>
OSPF: Router ID: 1.0.0.3            <01000003>
OSPF: Area ID: 0.0.0.0 [Backbone]   <00000000>
OSPF: Checksum: 0xAA43
OSPF: Autype: 0[No authentication]    <0000>
OSPF: Authentication: 0x0000000000000000  <0000000000000000>
OSPF: The Link State Acknowledgment packet:
OSPF:   Link State Advertisment header No. 1
```

```
OSPF:     LS age: 46 [seconds]
OSPF:     Options: 0x22            <22>
OSPF:     LS type: 1 Router links   <01>
OSPF:     Link State ID: 1.0.0.4   <01000004>
OSPF:     Advertising Router: 1.0.0.4  <01000004>
OSPF:     LS sequence number: 0x80000006  <80000006>
OSPF:     LS checksum: 0x3E06      <3E06>
OSPF:     Length: 48 [bytes]       <0030>
OSPF:   Link State Advertisment header No. 2
OSPF:     LS age: 1 [seconds]
OSPF:     Options: 0x22            <22>
OSPF:     LS type: 1 Router links   <01>
OSPF:     Link State ID: 1.0.0.2   <01000002>
OSPF:     Advertising Router: 1.0.0.2  <01000002>
OSPF:     LS sequence number: 0x80000009  <80000009>
OSPF:     LS checksum: 0xCB9C
OSPF:     Length: 84 [bytes]       <0054>
```

Obr.4 Link State Update a Link State Acknowledgement paket

Než se dva navzájem propojené směrovače stanou přilehlými, projdou jejich propojená rozhraní řadou stavů. Tento poměrně komplikovaný proces je popsán v následující tabulce.

Down	Počáteční stav před zahájením komunikace. Směrovač začíná vysílat Hello pakety
Attempt	Byl odeslán Hello paket. Tento stav je platný jen na NBMA sítích (viz dále)
Init	Byl přijat Hello paket od sousedního směrovače, dosud v něm však není uvedeno Router ID našeho routeru. Každý směrovač ve svých Hello paketech uvádí Router ID směrovačů, jejichž Hello již přijal
Two-Way	Obousměrná komunikace byla navázána. V přijatém Hello paketu je Router ID našeho routeru. Po dosažení tohoto stavu proběhne na broadcast sítích volba Designated routeru (viz dále)
Exstart	Směrovače si dohadují počáteční sekvenční čísla a domlouvají se, který z nich bude Master / Slave. Master router zahajuje další komunikaci
Exchange	Směrovače si vzájemně vymění Database Description pakety. Ty obsahují hlavičky LSA, popisujících jejich topologickou databázi
Loading	Nyní proběhne vlastní výměna informací z topologických databází. Jeden ze směrovačů požádá o informace paketem Link State Request. Druhý mu požadované informace zašle v paketu Link State Update. Paketem Link State Acknowledgement je příjem LSU paketu potvrzen
Full	Proces je dokončen a směrovače jsou vzájemně přilehlé (adjacent). Jejich topologické databáze jsou stejné. Toto je stav, ve kterém se rozhraní směrovače mají nacházet při správné funkci

Celý proces navázání vztahu mezi přilehlými směrovači je dokumentován na výpisu z protokolového analyzátoru.

Naplnění směrovací tabulky

Cílem fungování každého směrovacího protokolu je naplnění směrovací tabulky. Všechny k tomu potřebné informace jsou již shromážděny v topologické databázi směrovače. Můžeme je interpretovat jako graf, popisující strukturu sítě. Ke každé hraně grafu je přiřazena odpovídající cena. Nyní pomocí algoritmu SPF (Shortest Path First, někdy také označován jako Dijkstrův algoritmus) vypočteme kostru tohoto grafu, přičemž náš směrovač je jeho vrcholem. Cílem výpočtu je odstranit z grafu smyčky a získat jedinou nejvýhodnější cestu do každé sítě.

Z celé takto vypočtené cesty využijeme ve směrovací tabulce pouze "next hop", tedy adresu nejbližšího směrovače na který bude posílán provoz do cílové sítě. Dále do směrovací tabulky uložíme sumární cenu této cesty.

Může se stát, že do některé cílové sítě existuje více cest se stejnou celkovou cenou. V takovém případě záleží na konkrétní konfiguraci směrovače, jestli se z nich jedna vybere nebo budou používány všechny cesty současně a bude mezi nimi vyvažována zátěž.

Výpočet SPF algoritmu představuje pro směrovač poměrně velkou zátěž a je žádoucí, aby neprobíhal příliš často. K tomu by mohlo dojít například v případě, že některá z linek je nestabilní a opakovaně nabíhá a padá. Proto bývá definován minimální časový interval mezi dvěmi výpočty.

Typy sítí

Z hlediska fungování protokolu OSPF můžeme sítě rozdělit na několik typů. Na každém z nich funguje OSPF poněkud odlišným způsobem.

Broadcast sítě

Jako broadcast sítě označujeme ty sítě, které jsou schopny vzájemně propojit více než dva počítače a navíc zajišťují, že jeden vyslaný paket mohou přijmout současně všechny počítače. Typickými představiteli broadcast sítí jsou sítě typu Ethernet nebo FDDI.

Na jednom segmentu broadcast sítě může být připojeno i několik směrovačů. Kdyby se výše popsaným způsobem měly navazovat vztahy přilehlosti systémem každý s každým, vedlo by to k poměrně velkému režijnímu provozu na síti. Proto je jeden ze směrovačů na síti zvolen jako **pověřený směrovač (designated router, DR)**. Pro případ jeho výpadku je zvolen ještě **záložní pověřený směrovač (backup designated router, BDR)**. Každý ze směrovačů pak navazuje vztah přilehlosti pouze s DR a s BDR. V případě poruchy pověřeného směrovače jeho funkci převezme BDR (se kterým již všechny ostatní směrovače mají navázaný vztah) a je zvolen nový BDR. Pověřený směrovač také reprezentuje celý segment sítě navenek a pouze on předává informace do ostatních segmentů sítě.

Podle výše uvedené tabulky stavů se až do stavu Full dostává na broadcast sítí jen vztah mezi běžným směrovačem a DR/BDR. Vztah mezi ostatními směrovači které nejsou DR ani BDR zůstává na stupni Two-Way.

Každé rozhraní směrovače do broadcast sítě má přiřazenoý parametr **Router Priority**. To je osmibitové číslo, určující s jakou prioritou má být směrovač pro tento segment sítě zvolen DR/BDR. Priorita je oznámena sousedním routerům v Hello paketu. Směrovač s nejvyšší prioritou se stane DR, s nejbližší nižší BDR. Pokud je priorita nastavena na hodnotu 0, nemůže se daný směrovač stát DR ani BDR. V případě rovnosti priorit je zvolen směrovač s vyšším Router ID. Jako DR by se měl konfigurovat nejvýkonnější nebo nejméně zatížený směrovač na segmentu.

OSPF komunikace na broadcast síti probíhá pomocí multicast paketů. Používají se dvě multicast adresy : **224.0.0.5 AllSPFRouters** - tyto pakety přijímají všechny OSPF směrovače a **224.0.0.6 AllDesignatedRouters** - tyto pakety přijímá pouze DR a BDR.

Point to point sítě

Jako point to point jsou označovány sítě spojující pouze dva směrovače. Jejich typickým příkladedm jsou sériové linky. Na těchto sítích se nevolí DR/BDR a směrovače na point to point sítích se vždy stávají přilehlými. Pro komunikaci mezi nimi se používá pouze multicast adresa 224.0.0.5.

NBMA sítě

Zkratka NBMA znamená Non Broadcast Multi Access. Síť tohoto typu může propojit více než dva směrovače, není však schopna posílat broadcasty. Není tedy možné vyslat paket, který by byl přijat všemi směrovači současně. Jako příklad NBMA sítě můžeme uvést síť Frame Relay, ATM nebo X.25. Na NBMA síti se volí DR a

BDR a veškerá komunikace probíhá pomocí unicastů.

Není-li NBMA síť zapojena v topologii full mesh (každý uzel je propojený s každým), budou mít směrovače problémy s nalezením svých sousedů. Proto se seznam sousedních routerů zadává v konfiguraci. Také je třeba zajistit, aby směrovač zvolený jako DR měl možnost komunikovat se všemi ostatními směrovači (např. vhodnou konfigurací PVC nebo SVC okruhů) a samozřejmě také vhodnou volbou DR směrovače.

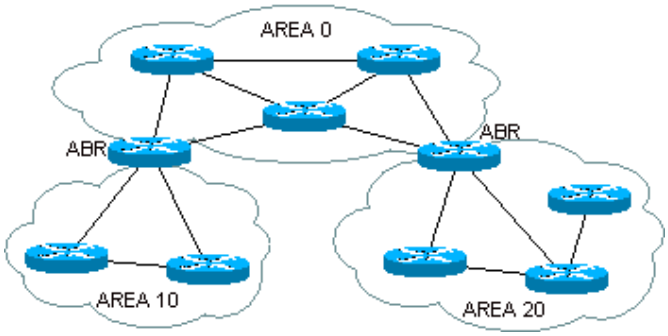
Point to multipoint sítě

Tato síť je vlastně zvláštním případem konfigurace NBMA sítě, kdy je síť chápána jako sada point to point linek. Proto nedochází k volbě DR ani BDR a komunikace probíhá pomocí multicastů.

Hierarchie OSPF sítě

V ustáleném stavu je množství informací vyměňovaných mezi OSPF směrovači poměrně malé. Periodicky se posílají jen nepříliš dlouhé Hello pakety a jednou za 30 minut proběhne link state refresh. Pokud však v síti dochází často ke změnám, musí se celou sítí šířit LSU pakety popisující tyto změny a jejich potvrzení. Navíc po každé změně je potřeba spustit nový výpočet SPF algoritmu. To všechno zatěžuje procesor směrovače i datové linky.

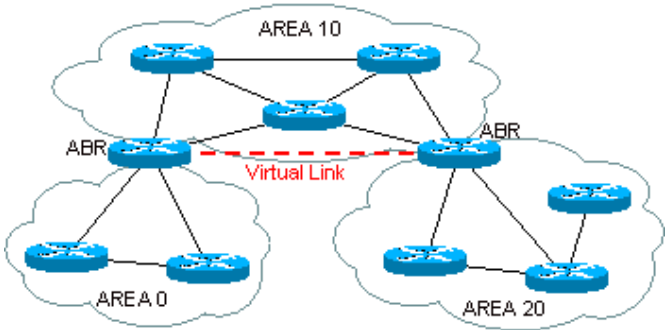
Proto je výhodné rozdělit síť do **oblastí (area)**. Šíření (flooding) Link State paketů je omezeno pouze na danou oblast a také SPF algoritmus běží pro každou oblast samostatně. Oblast je logická skupina směrovačů a linek mezi nimi. Směrovače v oblasti znají detailně pouze síť ve své oblasti a z ostatních oblastí dostávají jen souhrné informace. Oblasti jsou navzájem propojeny pomocí **hraničních směrovačů (Area Border Router, ABR)**. Příklad sítě rozdělené na více oblastí je na obrázku 5.



Obr.5 Síť složená z více oblastí

Každá oblast je označena 32 bitovým číslem, které může být ve dvou formátech. Buď jako běžné číslo (např. area 10) nebo ve formátu IP adresy (area 0.0.0.10).

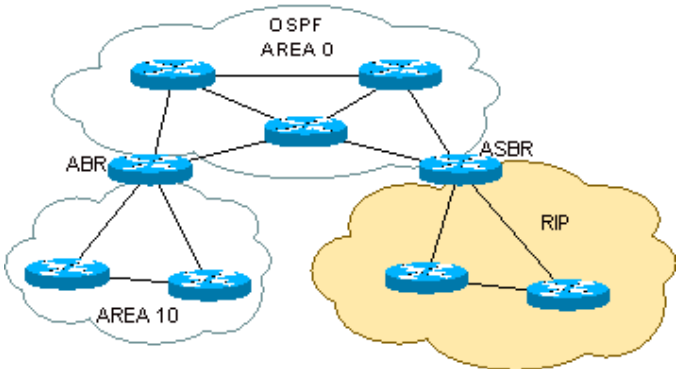
Zvláštní úlohu mezi oblastmi hraje area 0, někdy označována jako páteřní (backbone) oblast. Ta navzájem propojuje všechny ostatní oblasti. Veškerý provoz který teče z jedné oblasti do druhé musí procházet přes oblast 0 a každá oblast musí být přes ABR napojená na oblast 0. V některých případech - zvláště při dodatečných změnách v síti - může být obtížné tuto podmínku splnit. V takovém případě je možné použít **Virtual Link**. To je logické spojení mezi ABR oblasti 0 a ABR jiné oblasti, která k oblasti 0 nemohla být přímo připojena (viz. obrázek 6). Virtuální link je možné použít i v situaci, kdy oblast 0 z nějakých důvodů nemůže být spojitá. Pak se obě části oblasti 0 propojí virtuálním linkem. Ten však nesmí procházet přes více než jednu další oblast. V praxi je lepší se použití virtuálních linků vyhnout.



Obr.6 Virtual Link

Spolupráce OSPF s dalšími směrovacími protokoly

V reálné síti je někdy potřeba použít více než jeden směrovací protokol. Důvodem může být postupný přechod ze staršího protokolu k OSPF nebo to, že některá zařízení v síti OSPF nepodporují. V takovém případě budeme zřejmě potřebovat, aby sítě nalezené cizím směrovacím protokolem bylo možno předat do OSPF. Tomuto procesu se říká **redistribuce**. V praxi to bude vypadat tak, že na jednom směrovači poběží současně jak OSPF tak i jiný směrovací protokol (např. RIP). Tento směrovač se v OSPF terminologii označuje jako **hraniční směrovač autonomního systému (Autonomous System Boundary Router, ASBR)**.



Obr.7 ASBR

Když na ASBR nakonfigurujeme redistribuci, budou informace o sítích nalezených např. protokolem RIP dále předávány protokolem OSPF na ostatní směrovače jako tzv. **externí cesty**. Problémem přitom je navzájem nekompatibilní metrika různých směrovacích protokolů. Zatímco OSPF používá cenu, u RIPu je to počet přeskoků a podobně. Tyto metriky nelze mezi sebou porovnávat. Proto při redistribuci musíme nakonfigurovat, s jakou cenou budou sítě např. z RIPu do OSPF propagovány.

Protokol OSPF rozlišuje dva typy externích cest, které se označují jako E1 a E2. Standardně se používá typ E2, kdy cena cesty do externí sítě je dána pouze metrikou, se kterou byla síť do OSPF redistribuována a nezávisí již na cenách další cesy uvnitř OSPF autonomního systému. U typu E1 se cena, se kterou byla síť redistribuována, sčítá s cenou cesty uvnitř OSPF AS. Použití externí cesty typu E1 je vhodné v případě, že k dané externí síti existuje více než jedna cesta (přes více ASBR směrovačů).

Poznámka: pojem autonomní systém v tomto textu označuje část sítě, používající OSPF protokol. Nezaměňujte jej s autonomním systémem ve smyslu externího směrování.

Typy oblastí

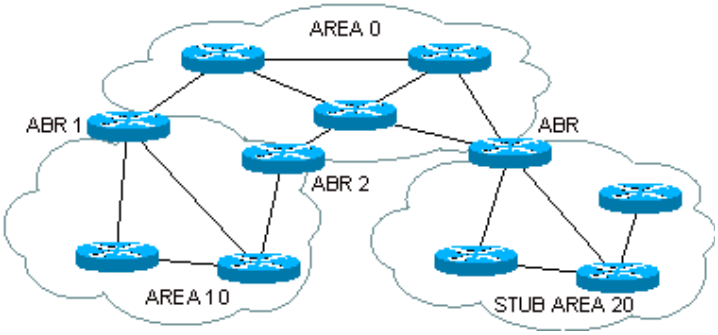
Stub area

Podle provozu procházejícího danou OSPF oblastí můžeme tyto rozdělit na **tranzitní** a **stub** oblasti. Tranzitní oblast je taková, kterou prochází provoz z jedné oblasti do druhé. Naproti tomu ve stub oblasti všechen provoz

začíná nebo končí, ale nikdy jí neprochází. Typickým příkladem tranzitní oblasti je area 0, může to ale být i jiná oblast pokud je v ní umístěn hraniční směrovač autonomního systému.

Pokud v OSPF síti nakonfigurujeme nějakou oblast jako stub, získá zvláštní vlastnosti. Nebudou do ní propagovány externí cesty, ale jen cesty nalezené OSPF protokolem v daném autonomním systému. Směrování do externích sítí je řešeno pomocí **default cesty**. Ta je do oblasti automaticky propagována z ASBR. Veškerý provoz do externích sítí tedy musí tímto ASBR procházet.

Výhodou stub oblasti je to, že se výrazně zmenší velikost topologické databáze na směrovačích v oblasti a tím se sníží požadavky na paměť i procesor směrovače. Jako stub je nejvhodnější definovat oblast, ze které vede jen jedna cesta ven. Je to možné i v případě že je cest více, pak ale nemusí pakety směrované do externích sítí procházet nejkratší cestou.



Obr.8 Stub area

Jako stub můžeme nakonfigurovat pouze oblast splňující určité podmínky :

- přes oblast nesmí procházet virtuální link
- v oblasti nesmí ležet ASBR, stub area tedy nesmí být tranzitní
- oblast 0 nesmí být stub
- všechny interní směrovače v oblasti musí být shodně nakonfigurovány jako stub

Totally stubby area

Koncepce Totally stubby area rozvíjí myšlenku stub oblasti ještě dále. Pokud z oblasti existuje jen jediná cesta ven, proč do ní propagovat cesty z ostatních oblastí stejného AS ? Do této oblasti tedy bude propagována pouze defaultní cesta. Ve směrovací tabulce směrovače v Totally stubby area nalezneme jen cesty uvnitř oblasti a defaultní cestu. Tento typ oblasti je rozšířením OSPF protokolu definovaným firmou Cisco.

Not so stubby area (NSSA)

V některých případech je nezbytné v oblasti, která by byla vhodným kandidátem na stub oblast, provádět redistribuci z jiného směrovacího protokolu. V té chvíli se však směrovač na kterém redistribuci provádíme stává ASBR. Jak bylo dříve uvedeno, ten ve stub oblasti ležet nesmí. Proto byla zavedena oblast typu NSSA, která má obdobné vlastnosti jako stub oblast, připouští však, aby z ní byly propagovány externí cesty.

Více o komunikaci mezi OSPF směrovači

Poté co jsme probrali základní pojmy OSPF směrovacího protokolu, můžeme se znovu vrátit k formátu paketů, které si směrovače mezi sebou předávají. Už jsme se zmínili o tom, že OSPF pakety mohou být pěti typů :

- **Hello pakety** vytvářejí a udržují vztah sousednosti mezi propojenými směrovači. Také slouží k volbě DR a BDR na broadcast sítích.
- **Database Description pakety** se uplatní při vytváření vztahu přilehlosti (adjacency) mezi směrovači. Popisují topologickou databázi odesílajícího směrovače, takže jeho soused ví, zda má odpovídající položky (LSA) ve vlastní databázi nebo je potřeba si je vyžádat.

- **Link State Request paket** pošle směrovač svému sousedovi tehdy, když zjistí (např. podle Database Description paketu) že mu některé LSA chybí nebo je zastaralé.
- **Link State Update paket** se používá pro šíření LSA po síti a také jako odpověď na Link State Request.
- **Link State Acknowledgement** potvrzuje LSA přijaté v Link State Update paketech. Každé LSA musí být explicitně potvrzeno, více LSA však může být potvrzeno v jednom Link State Acknowledgement paketu. V potvrzení se posílá jen hlavička LSA paketu.

LSA (Link State Advertisement) je datová struktura posílaná např. v Link State Update paketech. Popisuje stav rozhraní směrovače, jeho metriku, může také popisovat celý segment sítě nebo nést sumární informace o celé oblasti. Každé LSA je tvořeno hlavičkou a datovou částí. Údaje v hlavičce určují typ LSA (pole LS Type), identifikují směrovač, který je poslal (Advertising Router) a specifikují, kterou část databáze LSA popisuje (Link State ID). Dále jsou v hlavičce údaje, dovolující určit nejnovější instanci LSA - pole Age a Sequence Number. Datová část LSA se liší podle jeho typu.

```
OSPF:     LS age: 1 [seconds]
OSPF:     Options: 0x22             <22>
OSPF:     LS type: 1 Router links    <01>
OSPF:     Link State ID: 1.0.0.2    <01000002>
OSPF:     Advertising Router: 1.0.0.2  <01000002>
OSPF:     LS sequence number: 0x80000008  <80000008>
OSPF:     LS checksum: 0x63D1       <63D1>
OSPF:     Length: 84 [bytes]        <0054>
OSPF:     Router links advertisement:
OSPF:     Bits: 0x00                <00>
OSPF:       00000... Must Be Zero:
OSPF:       Must Be Zero: 0         <00>
OSPF:       Number of router links: 2  <0002>
OSPF:       Link No. 1
OSPF:         Link ID: 1.0.0.1      <01000001>
OSPF:         Link Data: 192.168.0.2
OSPF:         Type:  Point-to-point connection to another router
OSPF:         Number of TOS metrics: 0  <00>
OSPF:         Metric: 64            <0040>
OSPF:       Link No. 2
OSPF:         Link ID: 192.168.0.0
OSPF:         Link Data: 0xFFFFFF00
OSPF:         Type:  Connection to a stub network
OSPF:         Number of TOS metrics: 0  <00>
OSPF:         Metric: 64            <0040>
```

Obr.9 Příklad LSA typu 1

Podle způsobu použití se LSA dělí na řadu typů :

- **Router LSA (typ 1)** je posílán každým směrovačem. Popisuje stav jeho rozhraní a k němu přiřazenou metriku. Šíří se pouze uvnitř oblasti.
- **Network LSA (typ 2)** je odesílán jen z pověřeného směrovače (DR). Popisuje všechny směrovače připojené k jednomu segmentu sítě. Šíří se také jen uvnitř oblasti.
- **Network Summary LSA (typ 3)** posílá hraniční směrovač oblasti (ABR). Sumárně propaguje všechny sítě za danou oblast a případně také default cestu. Tento typ LSA je posílán z jednotnivých oblastí do oblasti 0 a také z oblasti 0 do ostatních oblastí.
- **ASBR Summary LSA (typ 4)** je podobné Network Summary LSA, popisuje cestu k ASBR směrovači.
- **AS External LSA (typ 5)** jsou vysílány z ASBR a popisují externí cesty redistribuované do OSPF autonomního systému. Šíří se do všech oblastí s výjimkou stub oblastí všech typů.
- **NSSA External LSA (typ 7)** vysílá ASBR v oblasti typu NSSA. Šíří se pouze uvnitř této oblasti a na ABR jsou konvertovány na LSA typu 5.

Sumarizace adres

Sumarizace znamená shrnutí několika IP sítí nebo subnetů do jediné sítě s kratší maskou. Například čtyři za sebou následující sítě typu C
192.168.4.0/24

192.168.5.0/24
192.168.6.0/24
192.168.7.0/24
můžeme zapsat jako 192.168.4.0/22. Podmínkou samozřejmě je, aby adresy následovaly za sebou a jejich počet odpovídal mocnině dvou. Do jedné sítě tedy můžeme sumarizovat např. 4, 8 nebo 16 sítí, ale ne 12. Tato technika se někdy označuje jako **supernetting**.

Sumarizaci adres je vhodné provádět na hranici oblasti nebo autonomního systému. Například je zbytečné aby ABR posílal do sousední oblasti všechny subnety které v oblasti existují, když stačí posílat jen jednu sumární cestu. Je ovšem nezbytné, aby v jiné části sítě neexistoval žádný subnet patřící do této sumární cesty. Proto je třeba IP adresy přidělovat tak, aby pozdější sumarizaci nebránily.

Protokol OSPF používá dva způsoby sumarizace. Prvním je sumarizace cest v rámci oblasti, prováděná na ABR. Druhým je sumarizace externích cest, ta probíhá na ASBR. Na Cisco směrovačích jsou oba způsoby sumarizace standardně vypnuty a je potřeba je explicitně nakonfigurovat.

Další věcí která se sumarizací souvisí je podpora různých subnet masek na jednotlivých rozhraních směrovače, v literatuře označované jako **Variable Length Subnet Mask (VLSM)**. Některé jednodušší směrovací protokoly (např. RIP) vyžadují, aby při subnetování sítě byla na všech subnetech stejná maska. Při předávání směrovacích informací totiž tyto protokoly neposílají aktuální subnet masku, ale berou masku podle některého rozhraní v příslušné síti nebo podle třídy IP adresy jestliže v dané síti žádné rozhraní nemají.

OSPF protokol posílá v LSA informaci o subnet masce a proto připouští, aby každý subnet měl masku jinou. To nám umožňuje například na spojovací point to point sítě použít masku /30 a neplýtvat tak IP adresami. Dále nám tato vlastnost dovoluje používat nespojité subnety, kdy dva subnety jedné sítě jsou navzájem odděleny jinou sítí. To by s RIP protokolem nebylo možné.

Autentikace

Potenciální útočník by mohl připojit na síť počítač s vhodným softwarem a začít generovat falešné OSPF pakety. Tím by mohl způsobit změny ve směrovacích tabulkách routerů a přerušit provoz v síti nebo dokonce nechat posílat cizí data na svůj počítač. Tomu je možné bránit autentikací OSPF paketů.

Autentikace může být dvojí. Můžeme použít heslo, které zadáme do konfigurace všech směrovačů. Tato metoda je jednoduchá, ale nepříliš bezpečná, protože heslo je možné na síti odposlechnout protokolovým analyzátorem. Druhou možností je kryptografická autentikace. Klíč a identifikátor se opět zadají na každém směrovači. Ten potom z obsahu OSPF paketu, klíče, identifikátoru a sekvenčního čísla vypočte md5 hash, který připojí k paketu. Samotný klíč se tedy nikdy neposílá přes síť. Tato metoda je díky sekvenčním číslům odolná i proti pozdějšímu přehrávání dříve odchycených paketů (replay attack).

Srovnání interních směrovacích protokolů

protokol	**RIP**	**RIP v2**	**OSPF**	**IGRP**	**EIGRP**
typ	distance-vector	distance-vector	link-state	distance-vector	hybrid
konvergence	pomalá	pomalá	rychlá	pomalá	rychlá
zatížení směrovače	malé	malé	velké	malé	malé
zatížení sítě	velké	velké	malé	velké	malé
VLSM	ne	ano	ano	ne	ano
metrika	počet hopů	počet hopů	cena	složená	složená
sumarizace	automatická, podle třídy IP adresy	automatická, je možné vypnout	ruční	automatická, podle třídy IP adresy	automatická, je možné vypnout
autentikace	ne	ano	ano	ne	ano

proprietární	ne	ne	ne	ano	ano

Konfigurace OSPF na směrovačích Cisco

Základní konfigurace OSPF
Konfigurace oblastí
Sumarizace, VLSM