Směrování

Směrovač - router

Aktivním prvkem pracujícím na síťové vrstvě je směrovač (router). Zajišťuje:

- Nalezení ideální cesty v síti – směrování paketů
- Provádí fragmentaci paketů
- Upravuje hlavičky všech paketů – hodnotu TTL, kontrolní součet, eventuálně položky pro fragmentaci nebo položky záhlaví
- Odesílá ICMP zprávy např. „vyčerpání“ - TTL je nula
- Provádí další činnosti – např. vytvoření tunelu IPsec pro VPN, pro potřeby DHCP pracuje jako „relay agent“, filtruje na třetí vrstvě pakety- přístupové seznamy ACL apod.

Základní činností je ideální směrování paketů. K tomu jsou potřeba informace a algoritmus směrování. Informace jsou ve směrovací tabulce.

Směrovací tabulka

Každý směrovač má směrovací tabulku. Údaje jsou získávány dle použité metody směrování (viz. dále). **Směrovací tabulka obsahuje tyto položky:**

- **Adresa sítě** (cílové)
- **Síťová maska** – upřesnění adresy sítě
- **Metrika (cena spoje)** – vyjádřena dostupnost sítě. Záleží na protokolu či způsobu záznamu, jak je určená. Např. u protokolu RIP je to pouze počet „skoků“ (hops) k cíli.
- **Administrative distance** – priorita záznamu. Pro stejnou síť může být více záznamu získaných různými způsoby (statický záznam má prioritu nejvyšší, protokoly dle typu)
- **Next hop** – kudy je síť dostupná. Uveden je port nebo IP adresa dalšího portu (IP next hop)
- **Typ záznamu** – původ informace o dostupnosti. Protokol nebo jiný způsob zadání (statický nebo defaultní směr)
- **Stáří (Age)** – stáří informace

Níže je výpis obsahu směrovací tabulky směrovače CISCO – **příkaz „sh ip route“**

```
ISP#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.31.7.0/30 is subnetted, 1 subnets
C       192.31.7.4 is directly connected, Serial2/0
D    192.168.1.0/24 [90/20514560] via 192.31.7.6, 00:01:41, Serial2/0
D    192.168.10.0/24 [90/20514560] via 192.31.7.6, 00:01:41, Serial2/0
D    192.168.20.0/24 [90/20514560] via 192.31.7.6, 00:01:41, Serial2/0
D    192.168.30.0/24 [90/20514560] via 192.31.7.6, 00:01:41, Serial2/0
```

Metody směrování
Metody směrování lze rozdělit následně:

- Statické
  - Statické směry
  - Defaultní směr
- Dynamické
  - Izolované
    - Metoda „horké brambory“
    - Metoda zpětného učení
    - Záplavové směrování
  - Distribuované
    - Vector Distance
    - Link State
  - Hierarchické

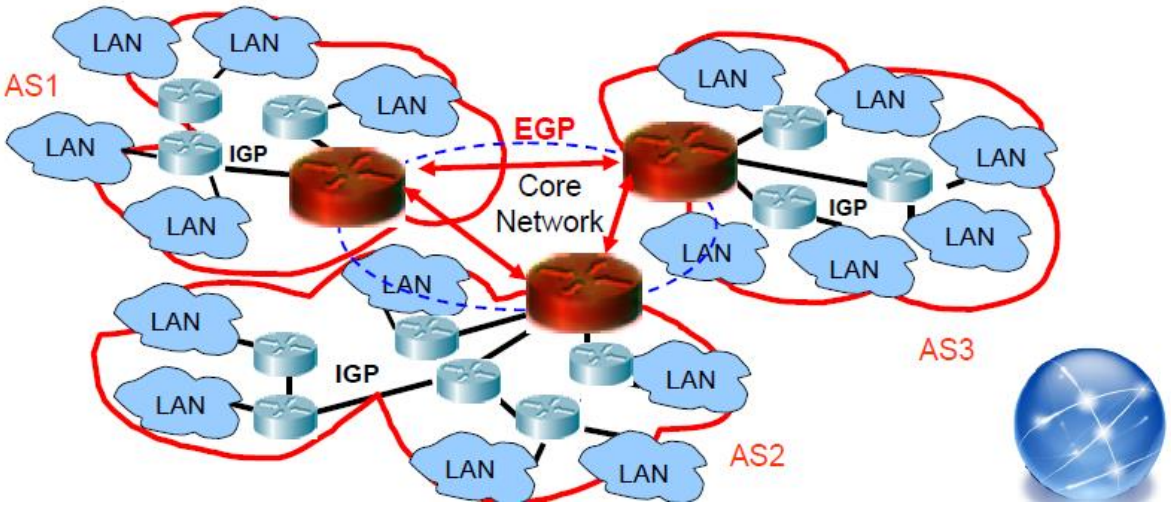
Hierarchické směrování

Internet je složité propojení sítí, kde **nelze zvládnout směrování bez hierarchického rozdělení**. Hierarchické rozdělení je založeno na **předávání „intervalových“ informací** mezi jednotlivými částmi struktury. Směrovací tabulky by nebyly schopny pojmout všechny informace o všech sítích. Proto se **informace agregují (sumarizují) do směrů** a předávají v této podobě.

Základním celkem je **autonomní systém (AS)** většinou dle ISP (filozofie odpovídá i struktuře přidělování IP adres po blocích). **Autonomní systém obsahuje páteřní část (backbone)** a jednotlivé **autonomní oblasti (AO).** Autonomní oblast je **základní části s jednou tzv. směrovací politikou** (např. příkaz pro zapnutí protokolu – „router ospf **192“ –** 192 je určení politiky a tím i oblasti). Použité směrovací protokoly jsou ze skupiny tzv. **IGP – Interior Gateway Protocols.**

Směrovače v této struktuře plní **různé role**. Rozlišujeme **hraniční směrovače (border routers)** umístěné **na hranici AO nebo páteřní sítě**. Ty si předávají agregované informace – intervalové. Směrovací protokoly jsou typu B**GP – Border Gateway Protocol**. Směrovače v **páteřní síti se nazývají „backbone“ routers nebo core routers**.

Pro **směrování mezi AS se používají EGP – Exterior Gateways Protocol**.



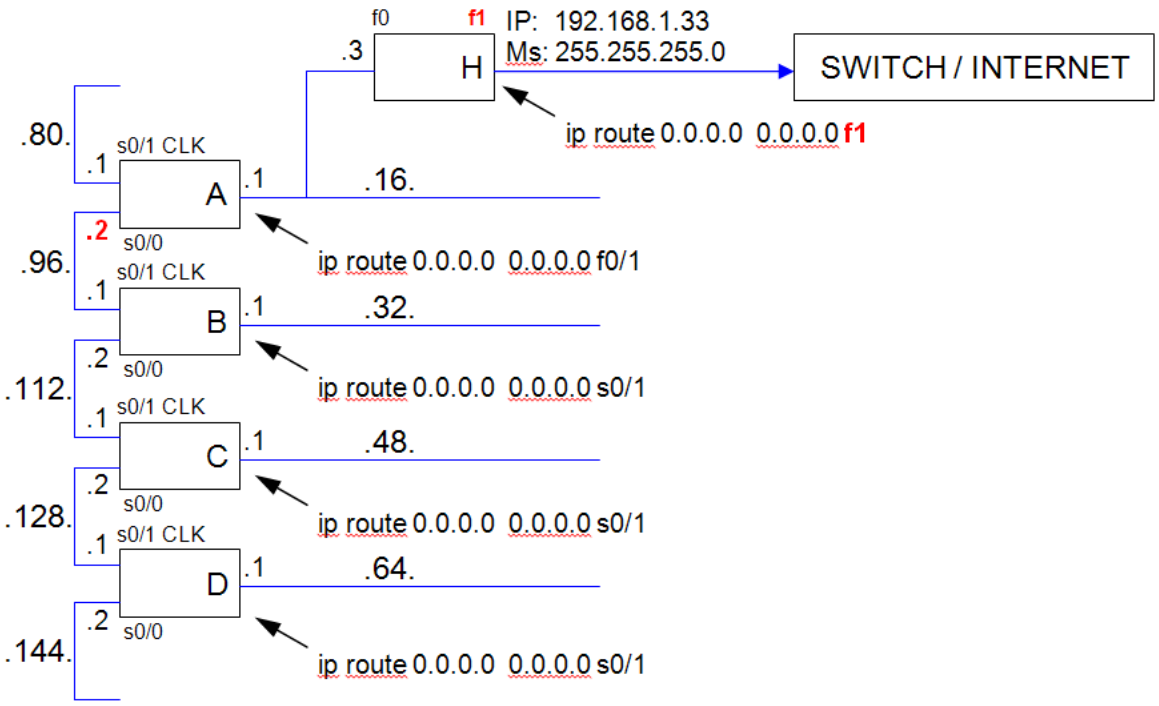
Statické směrování

Statické směry se používají například z bezpečnostních důvodů. Zajistí se vždy směrování určeným směrem. Zadání se musí **provést manuálně**. Statický směr **má přiřazenou nejvyšší „prioritu“ díky hodnotě Administrative Distance (AD).** Tuto hodnotu lze dle potřeby měnit (např. zadání st. směru - ip route 192.168.1.0 255.255.255.0 s0/1 **50 –** nová hodnota AD).

Protocol	Administrative distance
Directly connected route	0
Static route out an interface	1
Static route to next-hop address	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP	200
DHCP-learned	254
Unknown	255

Defaultní směr se používá pro zadání směru k „output gateway“ celé sítě. Zadá se pomocí nespecifikované IP adresy a masky, stejně jako statický směr např. -
„ ip route 0.0.0.0 0.0.0.0 s0/1“. Tento záznam platí pro všechny neznámé sítě (stejné jako u nepřímého směrování, postupuje se od konkrétního k obecnému a tento záznam je nejobecnější).

Níže je nastaveno defaultní směrování na směrovač H port f1.



Dynamické směrování

Izolované směrování

Informace o síti si směrovač **zjišťuje z datového provozu sám** bez vazby na okolí. Na změny v síti směrovač neumí reagovat nebo se promítnou až po dlouhém čase. Izolované směrování **se používá v sítích, kde se nelze spolehnout na správný a spolehlivý update informací** např. vojenské sítě.

Metoda horké brambory je založena na **co nejrychlejším odeslání paketu do všech volných směrů. Záplavové směrování** posílá paket **do všech směrů mimo rozhraní, ze kterého přišel**. V obou případech **dochází k nadbytečnému a nekoordinovanému provozu**. **Metoda zpětného učení** se **používá například u switchů v rámci dynamického plnění tabulky MAC adres.** Jedná se o jednoduché konfigurace sítí (viz. switching).

Distribuované směrování

Většina v současnosti používaných směrovacích protokolů je z této oblasti. Používají matematický **aparát teorie grafů** (podobným problémem je řešení jízdních řádů například MHD – jak se dostat nejrychleji ze stanice A do B). Jsou to protokoly **založené na**

- **Vector Distance Algoritmus (VDR)**
- **Link State Algoritmus (LSA)**

Vector Distance Routing

Směrovací protokoly založené na tomto algoritmu si předávají **informace mezi sousedy**. **Obraz sítě je založen na těchto informacích**. **Chyba, která vznikne, se šíří dál**. Používá se **Bellman–Fordův algoritmus**. Nejznámějším zástupcem je **protokol RIP**.

Routing Information Protocol – RIP

Patří mezi nejstarší směrovací protokoly. **Je jednoduchý a vhodný pro malé sítě**. Ve **verzi 1 umí pouze 15 „skoků" k cíli (16 je nedosažitelná síť**) – tzv. **malý diametr sítě**. **Verze 2 umí maskování a zvládne 127 skoků k cíli. RIP nepodporuje hierarchické směrování**.

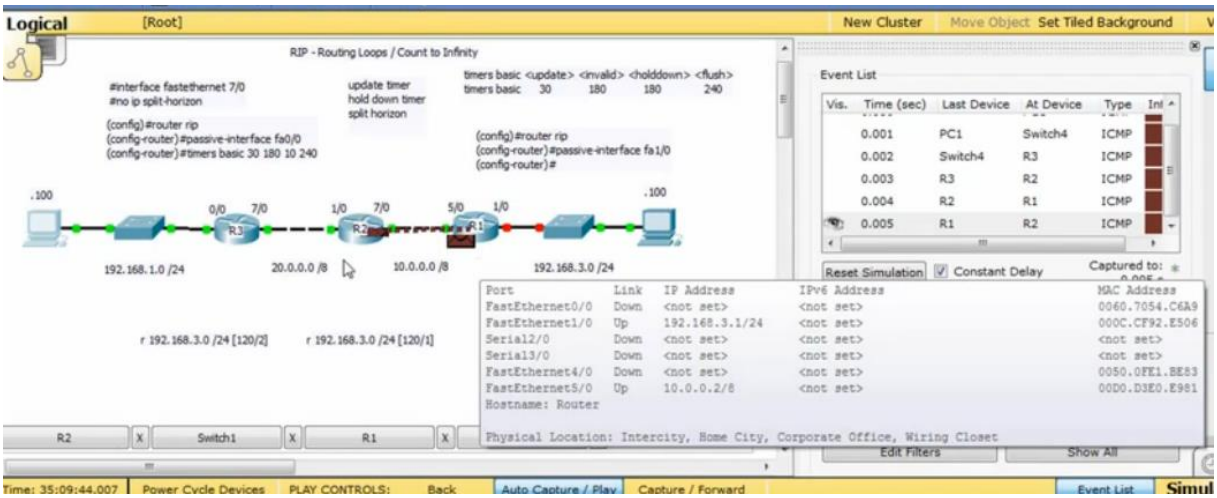
Cena spoje (metrika) je určena pouze počtem skoků (směrovačů) k cíli. **Neumí ocenit kvalitu spoje,** proto směruje pomalejší cestou, která má méně směrovačů. **Je vhodný pro homogenní sítě.**

Update informací je zasílán okamžitě při změně stavu sítě a dále v pravidelných cca 30 sec. intervalech formou broadcastu . Informace předávaná sekvenčně sousedy se pomalu šíří. **Konvergence změn je** tedy **pomalá**.

K přenosu update **používá nezajištěný protokol UDP** (v rámci LAN to ohledně chybovosti nevadí). **RIP nemá možnost autentizace (ověření identity)** a RIP update lze snadno podvrhnout.

Slabinou je vytváření přechodných směrovacích smyček. Při **nedostupnosti připojené sítě přebírá informace o dostupnosti od souseda**. K jeho záznamu přičte jedničku. Přestože se jedná o záznam původně získaný od něho. **Tímto i sousední směrovač přičítá v dalším**

kroku jedničku a smyčka je uzavřena. Po dosažení nejvyššího čísla je **síť označena jako nedostupná.**
Dále může dojít k **zacyklení update a pořád se pak bude počítat metrika dokola**. **Největším problémem je špatné směrování dat do smyčky a zahlcení sítě (traffic storm –** viz. níže video http://www.youtube.com/watch?feature=player_embedded&v=lTvCFEZJDhI**).**



Obranou proti vytváření přechodných směrovacích smyček je použití tzv.

- **„split horizon“– sousední směrovač není třeba informovat o těch cestách, které vedou přes něj** a o nichž nás sám již informoval. Proto se přenášejí jen části směrovací tabulky s odstraněnou informací o uvedených cestách. Neboli **směrovač nepropaguje informace o této síti do portu, ze kterého přišly.**

- „**poison reverse“**– je vylepšení metody split horizon. Má-li směrovač podezření na zacyklení přes vzdálenou síť, **prohlásí tuto síť za nedostupnou a (u RIP v1 – nastavení metriky 16) a vyčká**, až soustava začne konvergovat. Neboli **směrovač propaguje sítě, které se naučil z daného portu, nazpátek tím samým portem s označením vzdálenosti nekonečno (jako nedostupné)**

Link State Routing

Směrovací protokoly založené na tomto algoritmu **předávají informace všem směrovačům v síti prostřednictvím multicastového vysílání. Každý směrovač si vytváří obraz celé sítě sám.** Pro nalezení ideální cesty se používá **Dijkstrův algoritmus** z teorie grafů. **Nejznámější protokoly jsou OSPF (Open Shortest Path First) a EIGRP (Enhanced Interior Gateway Protocol – CISCO).** Dále je popsán OSPF, ale pro oba platí uvedené informace.

Open Shortest Path First – OSPF

Je „open“ verzí protokolu SPF. Specifikace jsou veřejně dostupné (IETF). **Každý uzel** (v tomto případě aktivní prvek - směrovač) **testuje dostupnost svých sousedů – stav linky.** Dále **sestavuje „link state paket“, ve kterém uvádí informace o dostupnosti svých sousedů – stav linky a její ohodnocení. Tyto pakety rozesílá všem uzlům (směrovačům) v síti okamžitě při změně stavu linky nebo po 30min**. Link state (dále LS) paketů je pět typů:

- **Hello** – zjištění okolních směrovačů – zjištění „sousednosti“
- **Databáze description** – popis DB
- **LS (Link State) request** – žádost informace o stavu linky

- **LS update** – aktualizace DB
- **LS acknowledgment** – potvrzení aktualizace

Všechny směrovače v síti mají úplnou informaci o spojích. Každý si vytváří aktuální stav **samostatně**. **Chyba se tedy projeví jen u něho. Informace o stavu jsou uloženy v LS databázi**.

Protokol OSPF **podporuje alternativní cesty**. Umí definovat různé cesty pro různé druhy provozu. Dále podporuje vyvažování zatížení částí sítě – „**load balancing**".

Podporuje **autentizaci – ověření a potvrzení identity**. Umožňuje proto šíření informací pouze autorizovaným směrovačům. **Zvládá i hierarchické směrování – autonomní systémy**.

Směrovací informace automaticky sumarizuje (OSPF summarizace). Sítě agreguje do směrů a směruje dle nejdelšího prefixu (tj. uplatnění pravidla – „ od konkrétního k obecnému").

Protokol má tyto vlastnosti:

- **Nízké nároky na pásmo** (v klidovém stavu beze změn)
- **Každá změna v síti generuje informaci** – link-state advertisement (LSA)
- **Rychlá konvergence** – šíření informace sítí
- **Cena je přiřazena všem odchozím cestám** – dle kvality cesty 1-65535 (64kbps sériová linka – 1562, Ethernet – 10, Fastethernet – 1)
- Směrovací rozhodnutí **je provedeno na základě celkové ceny** – dalších ovlivňujících faktorů nejen počet skoků k cíli.

Nevýhodou OSPF je jeho paměťová a výpočetní náročnost.

Pozn.: Pro ilustraci výpočtu metriky - příklad výpočtu EIGRP metriky (u OSPF obdobně)

$$M = \left[K_1 \cdot BW + \frac{K_2 \cdot BW}{256 - LOAD} + K_3 \cdot DELAY \right] \cdot \left[\frac{K_5}{RELIABILITY} + K_4 \right]$$

K_x – jsou konstanty (běžně K_1 a K_3 =1 a ostatní jsou nulové)

Skupinové směrovací protokoly

V LAN je zajištěno **skupinové vysílání pomocí multicast routeru a protokolu IGMP (IPv4).** Pro směrování skupinového vysílání v internetu jsou speciální směrovací protokoly. Nejznámějším je **protokol PIM – Protocol Independent Multicast**. **Data se šíří pomocí distribučního stromu.** Podle typu provozu má protokol PIM **různé módy:**

- **PIM – DM – Dense Mode** – pro vysokou hustotu adresátů
- **PIM – SM – Sparse Mode** – pro nízkou hustotu adresátů
- **PIM – BIDIR- Bidirectional PIM –** varianta pro obousměrné distribuční stromy
- **PIM – SSM – Source Specific Multicast –** rozlišení skupinové adresy a adresy zdroje (použití – internetové rádio a televize)