EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY

17300/B/2011/2722772762

SMEROVANIE V SIEŤACH IP

Bakalárska práca

2011 **Martin Solčanský**

EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY

SMEROVANIE V SIEŤACH IP

Bakalárska práca

Študijný program: Hospodárska informatika

Študijný odbor: 9.2.10 Hospodárska informatika

Školiace pracovisko: Katedra aplikovanej informatiky

Školiteľ: prof. Ing. Peter Závodný, CSc.

Bratislava 2011 **Martin Solčanský**

Čestné vyhlásenie

Čestne vyhlasujem, že záverečnú prácu som vypracoval samostatne a že som uviedlol všetku použitú literatúru.

Dátum: **.....**

(podpis študenta)

Rád by som sa poďakoval prof. Ing. Petrovi Závodnému, CSc.za odbornú pomoc a podnetné návrhy, ktoré mi poskytol k práci.

ABSTRAKT

SOLČANSKÝ, Martin: *Smerovanie v sieťach IP*. – Ekonomická univerzita v Bratislave. Fakulta hospodárskej informatiky; katedra aplikovanej informatiky. – prof. Ing. Peter Závodný, CSc. – Bratislava: FHI EU, 2011, 38s.

Hlavným cieľom práce je ukázať rôzne metódy smerovania v sieťach IP ako aj zhodnotiť výhody a nevýhody použitia jednotlivých smerovacích protokolov, ktoré pre svoju činnosť využívajú rôzne smerovacie algoritmy. To si vyžadovalo splnenie aj čiastkových cieľov v podobe vymedzenie základných rozdielov medzi statickým a dynamickým smerovaním, preskúmanie spôsobu fungovania hlavných smerovacích algoritmov používaných smerovacími protokolmi a porovnanie vybraných smerovacích protokolov, ich vývoj, výhody a nevýhody, činnosť a spôsob komunikácie.

Práca je rozdelená do 5 kapitol. Obsahuje 6 obrázkov a 1 tabuľku.

Prvá kapitola sa zameriava na 2 základné spôsoby smerovania, a to dynamické a statické, a ich princípu fungovania.

Ďalšia časť charakterizuje rôzne smerovacie algoritmy, ich základné princípy hľadania cesty v sieti, výhody a nevýhody. Potom sa venujeme konkrétnym smerovacím protokolom, ich vývoju, použitému smerovaciemu algoritmu, spôsobu komunikácie, ich výhodám a nevýhodám.

Záverečná kapitola sumarizuje všetky podstatné fakty, ktoré dané smerovacie metódy opisujú, a na základe ktorých sa dajú porovnať ich celkové výhody a nevýhody použitia v sieťach IP.

Kľúčové slová:

smerovanie, smerovacie protokoly, smerovacie algoritmy

ABSTRACT

SOLČANSKÝ, Martin: *Routing in IP networks.* – University of Economics in Bratislava. Faculty of Economic Informatics; Department of Applied Informatics. – prof. Ing. Peter Závodný, CSc. – Bratislava: FEI EU, 2011, 38p.

The main objective of this thesis is to show different ways of routing in IP networks and also to compare benefits of routing protocols which operate using different routing algorithms. That called for fulfilment of partial goals such as definition of the fundamental differences between static and dynamic routing, review of the main routing algorithms used by routing protocols and to compare the selected routing protocols, their development, advantages and disadvantage and the way they communicate each other.

The thesis is divided into 5 chapters. It contains 6 pictures and 1 table.

First chapter focuses on two basic methods of routing and their working principles.

The next part describes the various routing algorithms, the basic principle of seeking the path in the network, and their advantages and disadvantages. Then we look at specific routing protocols, their development, routing algorithms they use and their pros and cons.

The final chapter summarizes all the important facts about routing methods on which it is possible to compare their overall advantages and disadvantages of use in IP networks.

Key words:

routing, routing protocols, routing algorithms

Obsah

Úvod 2
1 Smerovanie v sieťach 3
1.1 Statické smerovanie 3
1.2 Dynamické smerovanie 4
1.2.1 Autonómne systémy 6
1.3 Algoritmus vektora vzdialenosti - Distance Vector Algorithm 8
1.4 Algoritmy stavu linky – Link state algorithms 11
1.4.1 Dijkstrov algoritmus najkratšej cesty 13
1.5 Distribuovaný Aktualizačný algoritmus 14
2 Smerovacie protokoly 18
2.1 Smerovací protokol RIP 18
2.2 Smerovací protokol OSPF 20
2.3 Smerovací protokol EIGRP 25
3 Cieľ práce 30
4 Metodika práce 30
5 Výsledky práce 31
Záver 36
Použitá literatúra 37

Úvod

Začiatky smerovania sa datujú do šesťdesiatych rokov minulého storočia, kedy boli počítače ešte skoro na začiatku svojej doterajšej cesty. Máloktorá inštitúcia vtedy mala k dispozícii aspoň jeden počítač a preto nejaká celosvetová sieť Internet vtedy skôr predstavovala futuristickú víziu ako teraz všade prítomnú realitu. Aj napriek tomu, že si to vtedy vedelo predstaviť len málo ľudí, dnes je Internet súčasťou každodenného života väčšiny z nás. Odborníci sa zhodujú že počítačové siete a smerovanie už existuje približne tých štyridsať rokov.

V tak veľkej sieti ako je Internet, s nespočetným množstvom ciest musí byť zabezpečená redundancia ciest do kritických uzlov v sieti, kvôli možným haváriám, ktoré by mohli v sieti nastať. To by malo určite neželané následky ďalekosiahleho významu. Ak ale existuje viac možných ciest ako sa dostať z jedného miesta sieti do druhého, odkiaľ zistíme koľko týchto ciest existuje? Určite budeme potrebovať nejaký spôsob alebo mechanizmus, ktorý tieto cesty v sieti do vzdialených uzlov nájde za nás. Keď sme už našli všetky cesty z jedného miesta v sieti do druhého logicky musí mať každá táto cesta inú vzdialenosť. Ako zistíme ktorá z nich je najkratšia? V tom nám opäť pomôže teória grafov a matematický aparát, ktorých teoretické poznatky využívajú smerovacie algoritmy aby našli tú najkratšiu respektíve najlepšiu cestu. Časom z týchto techník vznikli smerovacie protokoly a hardwarové zariadenia, smerovače, ktoré smerovacie protokoly implementujú a používajú na smerovanie správ v sieti. Smerovanie je tou najdôležitejšou a najkomplikovanejšou funkciou v sieťach IP. Smerovanie má v dnešnej dobe enormný význam nakoľko je sieť Internet postavená na smerovanom protokole IPv4, ktorý potrebuje služby smerovačov a smerovacích protokolov, bez ktorých by nebola doručená žiadna správa v sieti. Asi ani netreba hovoriť o význame Internetu a internetových technológiách a o tom, akú významnú úlohu plnia v dnešnom ekonomickom prostredí. Banky, telefónne siete, obchody, firmy, jednotlivci. Celá spoločnosť je súčasťou Internetu.

V tejto práci sa budeme zaoberať statickým a dynamickým smerovaním. Ďalej sa budeme venovať už iba dynamickému smerovaniu a rôznym algoritmom, ktoré používa pričom každý z nich pracuje na inom princípe a využíva iné prostriedky na dosiahnutie nájdenia cesty v sieti a výberu najlepšej z nich. Následne nato sa pozrieme na základné protokoly, ktoré tieto algoritmy implementujú a porovnáme si tieto vybrané smerovacie protokoly, ich vývoj, výhody a nevýhody, činnosť a spôsob komunikácie.

1 Smerovanie v sieťach

Smerovanie v sieťach môže pracovať dvoma základnými spôsobmi. Buď sa využívajú nakonfigurované statické cesty, alebo si cesty v sieti vypočítavajú smerovače dynamicky prostredníctvom niektorého z dynamických smerovacích protokolov. Pomocou týchto dynamických smerovacích protokolov vykonávajú smerovače takzvané rozpoznávanie ciest, po ktorých následne posielajú sieťové pakety. Staticky nakonfigurované smerovače nemajú žiadny vnútorný mechanizmus na rozpoznávanie ciest v sieti a preto dokážu smerovať pakety iba na základe vopred manuálne definovaných ciest.

1.1 Statické smerovanie[1]

Najjednoduchšiu formu smerovania predstavuje vopred nakonfigurované statické cesty. To znamená, že všetky činnosti a úlohy spojené so šírením a rozpoznávaním ciest má na starosti osoba zodpovedná za správnu činnosť počítačovej siete, ktorou je administrátor takejto siete. Smerovač teda v tomto prípadne iba hľadá zhodu medzi cieľovou IP adresou paketu, ktorý má smerovať a IP adresou siete vo svojej smerovacej tabuľke (z ang. Routing Table), ktorá je vopred prednastavená.

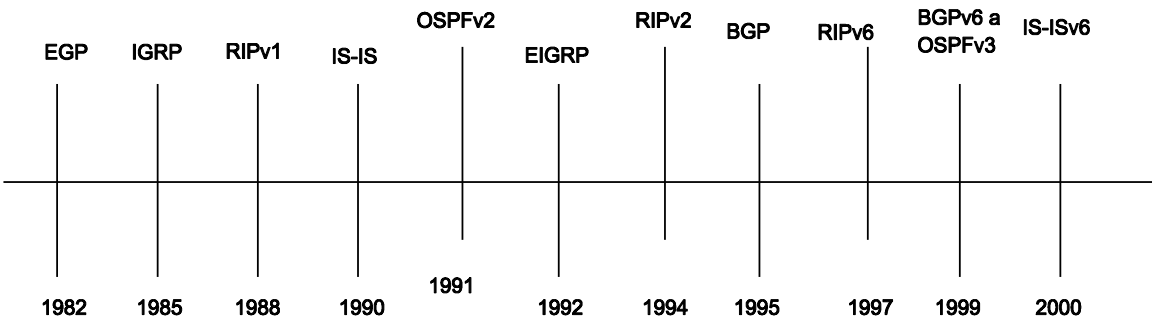
Statické smerovanie má veľa výhod medzi ktoré jednoznačne patrí vyššia efektivita využívania prostriedkov smerovača a aj prenosových prostriedkov. Pri statickom smerovaní sa využíva podstatne menšia šírka pásma ako pri dynamickom smerovaní , nespotrebuje sa žiaden strojový čas procesora smerovača a iba veľmi málo pamäti. Aj keď má statické smerovanie nesporné výhody, má aj svoje nedostatky, ktoré sa pokúsime vysvetliť na nasledujúcom príklade. Predstavme si jednoduchú sieť, kde je redundancia, teda z určitého miesta v sieti napríklad z miesta A sa do miesta B vieme dostať dvomi cestami. Smerovač má vo svojej tabuľke sieťovým administrátorom zadefinovanú tú lepšiu cestu, ktorá je pre prenos správ efektívnejšia. Druhá cesta zostáva tým pádom nevyužitá. Ak by došlo k havárii lepšej linky, správy z uzla A do uzla B by nebolo možné doručiť. Smerovač by nebol schopný akokoľvek zaznamenať pád tejto linky a reagovať nato nájdeným novej cesty, v našom prípade horšej druhej cesty, ktorá by ale aspoň nahradila prerušenú prevádzku, pokiaľ by tak neurobil sieťový administrátor. Takáto údržba siete je možná vo veľmi malých sieťach ale vo väčšom prostredí je prakticky nemožná.

[1] Spracované podľa: SPORTACK, M. 2004. *Směrování v sítích IP*. Brno: Computer Press, 2004. 351 s. ISBN 80-251-0127-4. [1]

Statické smerovanie sa stále využíva aj v praxi, kde ale tvorí skôr doplnok k dynamickým smerovacím protokolom. Veľmi užitočné bývajú statické cesty pri extranetových spojeniach s inými firmami, s ktorými obchodujeme cez IP protokol

1.2 Dynamické smerovanie[2]

Dynamické smerovacie protokoly sa používali v sieťach už na začiatku 80.rokov. Prvá verzia smerovacieho protokolu RIP (Rounting Information Protocol) bola vypustená v roku 1982, ale niektoré základne algoritmy, ktoré obsahovala boli po prvý krát použité v sieti ARPANET v roku 1969. Postupným vývojom, ako sa siete stávali väčšie a komplexnejšie, tak vznikla aj potreba smerovacích protokolov a ich neustále sa prispôsobovanie sa potrebám sietí. Ako sme už spomenuli jeden z prvých smerovacích protokolov bol protokol RIP. Počas svojho vývoja mal veľa pomenovaní nakoľko veľa firiem malo svoju vlastnú proprietárnu verziu RIP až pokým nebol v roku 1988 vypustený otvorený štandard s názvom RIP. Uplatnenie nájde predovšetkým v menších sieťach. V súčasnosti sa používa už jeho druhá verzia s označením RIPv2. Pre potreby rozsiahlejších sietí boli vyvinuté komplexnejšie smerovacie protokoly ako OSPF (Open Shortest Path First) ako aj protokol IS-IS (Intermediate System-to-Intermediate System). Tieto protokoly boli vyvinuté ako otvorené štandardy, čo znamená, že hociktoré implementácie sieťových zariadení od rôznych výrobcov spolu budú spolupracovať, vďaka dodržovaniu špecifikácii štandardov. Popri otvorených štandardoch vznikali ale aj uzatvorené protokoly, ktoré boli vlastníctvom firmy, ktorá ich vyvinula. Jedným z takýchto protokolov je EIGRP (Enhenced Interiour Gateway Protocol) od spoločnosti Cisco, ktorá je, dá sa povedať, veľmocou a lídrom na trhu so sieťovým zariadením a sieťovými technológiami ako takými. Vývoj jednotlivých protokolov v čase môžeme vidieť na obrázku 1.



Obr.1: Vývoj jednotlivých protokolov v čase[2]

[2] Spracované podľa Cisco Networking Academy CCNA Curriculum 4.0 r.2008 [4]

Sieť Internet sa skladá z takzvaných prepojovaných sietí. Na smerovanie medzi takýmito sieťami sa používa smerovací protokol BGP (Border Gateway Protocol).Problematiku prepojovaných sietí si objasníme v ďalšom texte.

Vďaka markantnému rozšíreniu internetu a ľahkovážnemu prideľovaniu IP adries došlo behom krátkeho času k vyčerpaniu podstatnej časti adresného priestoru súčasne najviac používaného internetového protokolu verzie 4 a preto museli byť prijaté dočasné a dlhodobé opatrenia aby sa dočasne spomalilo úplné vyčerpaniu Ipv4 adries a bol vyvinutý nový protokol. Medzi dočasné opatrenia patrilo určite zavedenie sieťových masiek s variabilnou dĺžkou(VLSM - Variable length subnet mask) ako aj podpora beztriedneho smerovania v smerovacích protokoloch(CIDR – Classless inter-domain routing) . Dlhodobé opatrenie bolo a stále je vývoj novej generácie internetového protokolu verzie 6, ktorý ma podporovať až 128 bitový adresný priestor . Každý spomenutí smerovací protokol ma svoju verziu pre internetový protokol novej generácie. My sa však budeme zaoberať iba smerovacími protokolmi, ktoré smerujú protokol IP verzie 4, ktorá je v súčasnosti najpoužívanejšia v sieti Internetu.

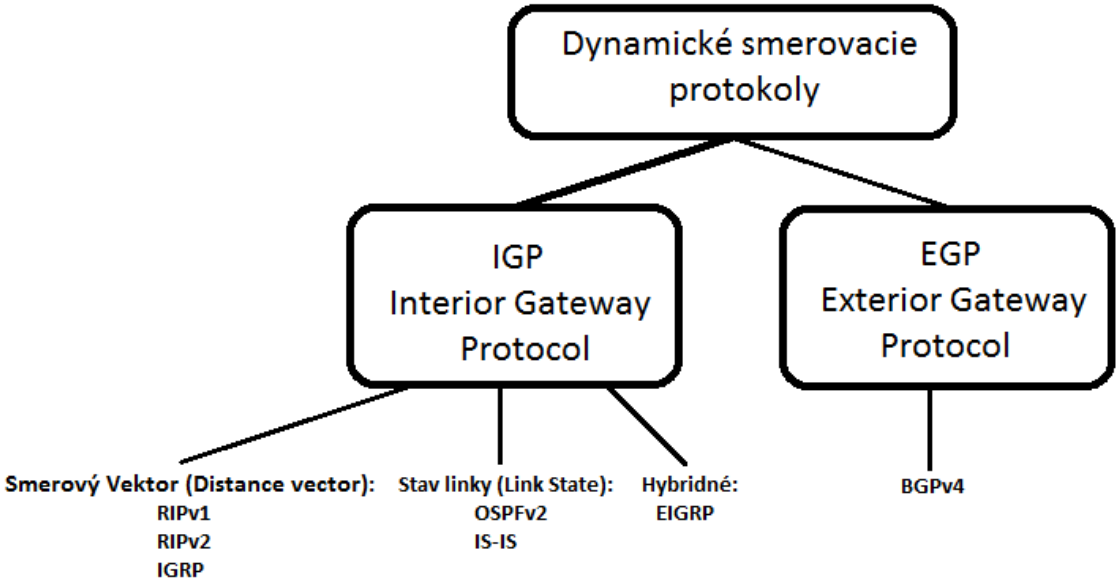
Smerovacie protokoly sa používajú na uľahčenie výmeny smerovacích informácií medzi smerovačmi. Protokoly umožňujú smerovačom dynamicky zdieľať informácie o vzdialených sieťach a automaticky si tieto informácie ukladať do svojich smerovacích tabuliek. Protokol usúdi, ktorá z ciest do vzdialenej lokácie je najlepšia a pridá si ju do svojej tabuľky. Jedna z hlavných predností smerovacích protokolov oproti statickému smerovaniu je, že smerovače sú schopné si tieto informácie vymieňať a hneď ako nastane nejaká zmena v topológii siete, havária alebo zmena cesty do určitej lokácie, sú schopné na túto zmenu zareagovať a prispôsobiť sa jej.

Smerovací protokol pozostáva zo sady procesov, smerovacieho algoritmu a správ, ktoré sa používajú na výmenu smerovacích informácií a zaplnenie smerovacej tabuľky cestami, ktoré protokol vybral ako najlepšie.

Hlavné úlohy smerovacieho protokolu sú:

- Objavovanie existencie vzdialených sietí
- Udržovanie aktuálnych informácií o cestách v smerovacej tabuľke
- Určenie najlepšej cesty do vzdialených sietí
- Hľadanie novej cesty ak je aktuálna cesta nedostupná

Nato aby smerovacie protokoly určili najlepšiu cestu z jednej siete do druhej používajú takzvanú metriku. Je to vlastne ohodnotenie danej cesty podľa určitých kritérií. Napríklad v protokole RIP sa používa ako metrika počet skokov(hop count), teda počet smerovačov, ktoré sú na ceste zo zdroja do cieľa. Iné protokoly ako OSPF zase používajú šírku pásma na určenie najkratšej cesty. Smerovacie protokoly, ktoré sa bežne používajú a ich delenie si môžeme ukázať na nasledujúcom obrázku.(Poznámka:



Obr.2: Delenie smerovacích protokolov[3]

1.2.1 Autonómne systémy

Autonómne systémy(Autonomous systems - AS) tiež známe ako smerovacia doména sú kolekcie smerovačov pod jednou spoločnou správou. Typický príkladom je interná firemná sieť a sieť poskytovateľa internetového pripojenia. Firemná sieť je pod správou firmy a ISP do nej nijako nezasahuje a ani firma nemá žiaden vplyv na správu siete ISP. Nakoľko je sieť Internet postavená na koncepte autonómnych systémov sú potrebné dva druhy smerovacích protokolov.

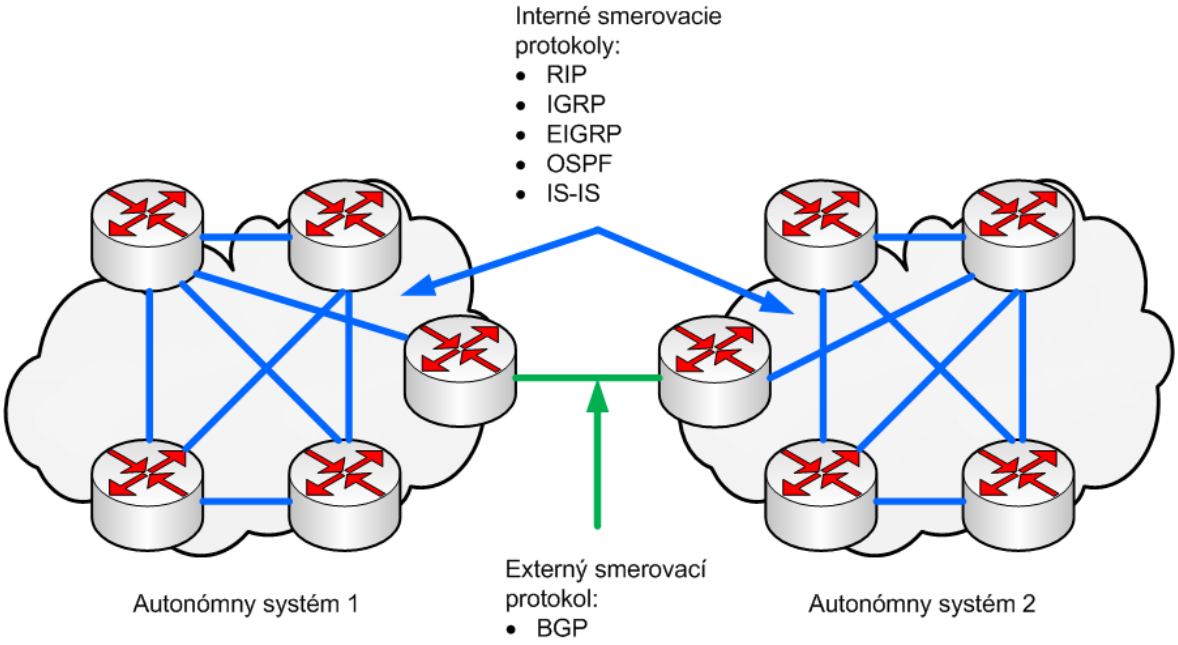
[3] Spracované podľa Cisco Networking Academy CCNA Curriculum 4.0 r.2008 [4]

Tieto sú:

- Interné smerovacie protokoly(Interiour Gateway Protocols - IGP)
- Externé smerovacie protokoly(Exterior Gateway Protocols - EGP)

Interné smerovacie protokoly sa používajú v rámci smerovacej domény, teda siete pod správou jednej organizácie. Bežne pozostáva autonómny systém z viacerých individuálnych entít ako sú rôzne firmy, školy, a iné inštitúcie. IGP sa používa na smerovanie v rámci autonómneho systému ako aj v jednotlivých sieťach, z ktorých pozostáva. Medzi Interné smerovacie protokoly protokolu IP radíme protokoly ako RIP, IGRP(Interiour Gateway Protocol) predchodca EIGRP, ďalej samotný EIGRP, OSPF a IS-IS.

Na druhej strane oproti interným smerovacím protokolom stoja externé smerovacie protokoly(Exteriour Gateway protocol - EGP), ktoré sú navrhnuté pre používanie medzi odlišnými autonómnymi systémami, ktoré sú pod kontrolou rozličných entít. Najrozšírenejší a najschopnejší smerovací protokol EGP je BGP(Border Gateway Protocol), ktorý používa aj dnešná sieť Internetu. BGP je smerovací protokol vektora vzdialenosti, ktorý môže používať rôzne atribúty na meranie ceny cesty. Na úrovni smerovania medzi poskytovateľmi internetu nie vždy záleží na nájdení najkratšej alebo najrýchlejšej cesty. Na obrázku 3 môžeme vidieť rozdiel medzi IGP a EGP.



Obr.3: Rozdiel medzi IGP a EGP[4]

[4] Spracované podľa Cisco Networking Academy CCNA Curriculum 4.0 r.2008 [4]

1.3 Algoritmus vektora vzdialenosti - Distance Vector Algorithm[5]

Distance Vector Algorithm (DVA) teda smerovanie pomocou vektora vzdialenosti je jedným z dvoch základných smerovacích algoritmov používaných v interných smerovacích protokoloch(Interior Gateway Protocol - IGP). Idea algoritmu vzdialenosti je veľmi jednoduchá. Každý smerovač periodicky zasiela svojím susedom svoju smerovaciu tabuľku. Smerovacia tabuľka je tvorená položkami usporiadaných trojíc - cieľom, adresou nasledujúceho smerovača na ceste do cieľa a vzdialenosťou do cieľa danou počtom smerovačov na tejto ceste, takzvaný počet skokov(Hop Count). Ak smerovač získa od svojho suseda kópiu jeho smerovacej tabuľky, ku všetkým cestám pripočíta jeden skok a potom ju porovná s aktuálnymi cestami vo svojej smerovacej tabuľke. Ak je táto nová cesta kratšia, pôvodná je ňou nahradená s uvedením nasledujúceho smerovača na ceste do cieľa. Tento postup je veľmi ľahko implementovateľný, a preto je, predovšetkým v podobe protokolu RIP, veľmi rozšírený. Algoritmus funguje veľmi dobre v relatívne malých sieťach. V sieťach väčšieho rozsahu je problém s jeho konvergenciou a hrozí nebezpečenstvo vzniku nekonzistencie, zacyklenia sa a počítania do nekonečna.

Algoritmus vektora vzdialenosti je založený na tabuľke najlepších ciest ku každému cieľu. Na výber najlepšej cesty sa používa meradlo zvané metrika. Takzvaná cena cesty alebo aj náklady na cestu. V sieťach so smerovaním vektora vzdialenosti sa bežne používa metrika, ktorá vyjadruje počet uzlov(smerovačov) cez ktoré musí správa prejsť aby sa dostala do cieľového uzla. V komplexnejších sieťach sa používajú smerovacie algoritmy stavu linky, kde metrika reprezentuje celkové oneskorenie správy, cenu posielania, alebo iné veličiny, ktoré môžu byť minimalizované. Hlavnou požiadavkou je schopnosť reprezentovať metriku ako sumu cien pre individuálne prechody alebo tiež preskoky (Hops).

Nech D(i,j) reprezentuje metriku najlepšej cesty z entity i do entity j. Nech d(i,j) reprezentuje cenu priameho prechodu z entity i do entity j. Ak i a j nie sú bezprostrední susedia d(i,j) je nekonečno. Najlepšie ohodnotenie je popísané nasledovne:

D(i,i) = 0 pre všetky i
D(i,j) = min[d(i,k) + D(k,j)] inak k

[5] Spracované podľa údajov: HEDRICK, C. 1988. *Routing Information Protocol*. [7]

Je realitou, že smerovače a linky medzi nimi často padajú a obnovujú sa späť do prevádzky. K ošetreniu tohto javu je nutné teoretický algoritmus trocha pozmeniť. Teoretický algoritmus si vyžaduje nejakých bezprostredných susedov. Ak sa zmení topológia, môže sa zmeniť aj počet okolitých susedov. Algoritmus je závislý na tom, že smerovače oznamujú susedom, keď sa ich metrika zmení. V prípade spadnutia smerovača neexistuje spôsob susedom oznámiť zmenu.

Na ošetrenie problémov tohto druhu sa používajú časovače. V protokole RIP každý smerovač zasiela aktualizačné správy všetkým susedom každých 30 sekúnd. Ak od smerovača nedostane 180 sekúnd aktualizačnú správu, predpokladá sa, že spadol smerovač alebo sieť. Potom sa cesta označí ako neplatná. Ak obdrží od nejakého suseda správu, že má platnú cestu do cieľa, neplatnú cestu nahradí za platnú.

RIP spolu s niekoľkými protokolmi tejto triedy, používajú na označenie suseda, ktorý má neplatnú cestu do určitej siete, špecifickú metrickú hodnotu, ktorá indikuje nedostupný cieľ. Táto hodnota je väčšia ako najväčšia platná očakávaná hodnota. V protokole RIP sa za nekonečno považuje hodnota 16, ktorá je implicitne prednastavená.

Hlavným nedostatkom v smerovaní s vektorom vzdialenosti je problém pomalej konvergencie, niekedy označovaný aj ako problém počítania do nekonečna. Je dokázané, že algoritmus vektora vzdialenosti konverguje k správnym hodnotám smerovacej tabuľky v konečnom čase. No negarantuje, že tento čas bude dostatočne malý na to aby bol algoritmus použiteľný. Je to vlastne model komunikačného systému. Písmená zodpovedajú smerovačom a spoje sieťam. Všetky linky majú ocenenie 1, okrem linky z C do D, ktorá má ocenenie 10. Úvahy robíme vzhľadom na cieľovú sieť. Je zrejmé:

D: priamo spojené, metrika 1
B: cez D, metrika 2
C: cez B, metrika 3
A: cez B, metrika 3

Predpokladajme, že linka z B do D spadne. Zmeny sa začnú vtedy, keď B oznámi, že cesta do D nie je použiteľná. Vznikne problém, pretože A aj C si stále myslia, že môžu ísť do cieľa cez B s cenou 3. V ďalšej iterácii B začne tvrdiť, že môže ísť do cieľa cez C s cenou 4. Samozrejme, že nemôže. A a C začnú postupne zvyšovať ceny ciest do cieľa cez seba

navzájom. Systém síce bude konvergovať ale potrvá mu to nejaký čas. Tomuto problému sa hovorí počítanie do nekonečna.

čas ------>

D: priamo, 1		priamo, 1		priamo, 1		priamo, 1		...	priamo, 1		priamo, 1	...
B: padnuté		C,	4	C,	5	C,	6		C,	11	C,	12
C: B,	3	A,	4	A,	5	A,	6		A,	11	D,	11
A: B,	3	C,	4	C,	5	C,	6		C,	11	C,	12

Keď sieť spadne, je potrebné počítanie do nekonečna, čo najskôr zastaviť. Preto je nekonečno zvolené ako kompromis medzi veľkosťou siete a rýchlosťou konvergencie. RIP navrhnutý pre siete s diametrálnou veľkosťou maximálne 15 skokov čiže 16 je už nedostupná sieť.

Pre zvýšenie stability smerovania s vektorom vzdialenosti sa používajú nasledovné mechanizmy:

- Rozdelenie horizontu (Split Horizon)
- Rozdelenie horizontu s pozmenením spätnej cesty (Split Horizon with Poisoned Reverse)
- Vyvolané aktualizácie (Triggered Updates)

Z vyššie uvedeného príkladu vyplýva, že A aj C sa navzájom klamú. Môže sa to ošetriť tak, že sa zisťuje odkiaľ je informácia o zmene poslaná. Potom je vhodné neposielať informácie o cieľovej sieti tomu susedovi, od ktorého je cesta naučená. Jednoduché rozdelenie horizontu neposiela žiadne správy o ceste tým susedom, od ktorých je cesta naučená. Rozdelenie horizontu s pozmenením spätnej cesty zabezpečuje, aby metrika aktualizovanej položky smerovacej tabuľky posielanej smerovaču, od ktorého smerovacia informácia spôsobila jej aktualizovanie, bola nastavená na 16.

Rozdelenie horizontu zabezpečuje prevenciu pred smerovacími slučkami, ktoré vyvolávajú dva smerovače. Avšak je možné, že budú zviazané tri smerovače a budú sa navzájom klamať. V tom prípade rozdelenie horizontu nemôže zastaviť slučku. Táto slučka sa zastaví len ak metrika dosiahne nekonečno. Ďalším mechanizmom, ktoré podporujú rýchlosť konvergencie siete sú vyvolané aktualizácie. Vždy keď sa zmení metrika pre

konkrétnu cestu, smerovač takmer okamžite pošle aktualizačnú správu, aj napriek tomu že ešte časovač pre pravidelné poslanie správy nevypršal.

Predpokladajme, že cesta do cieľa N ide cez smerovač G. Potom, pri príchode aktualizácie z G, prijímací smerovač vyhodnotí cestu a ak je lepšia ako stará, tak prijímací smerovač pošle aktualizáciu všetkým smerovačom priamo pripojeným k nemu. Vznikne kaskádové šírenie vyvolaných aktualizácií. Predpokladajme, že smerovač označí cestu do N ako neplatnú. G pošle vyvolanú aktualizáciu všetkým susedom. Potom jediný sused, ktorého cesta do N ide cez G si aktualizuje cestu ako jediný a pošle vyvolanú aktualizáciu. Takto si ju všetky časti systému, ktoré majú cestu do N, nastavia na nekonečno.

Samozrejme, že môže nastať prípad, kedy pri šírení vyvolaných aktualizácií príde pravidelná aktualizačná správa, založená na zlej ceste. Môže to spôsobiť nestabilitu systému a stratenie zostatku zlej cesty. Ale pokiaľ sa vyvolané aktualizácie šíria dostatočne rýchlo, je to dosť nepravdepodobné.

1.4 Algoritmy stavu linky – Link state algorithms

Algoritmy stavu linky (ďalej LSA) sú pomenovaním pre globálne smerovacie algoritmy. Pri globálnom smerovaní má každý smerovač kompletnú informáciu o všetkých smerovačoch v sieti a stave zaťaženia v sieti. Smerovače zasielajú informácie len o priamo pripojených linkách a neposielajú celú smerovaciu tabuľku. Vhodné sú najmä pre veľké prostredia, ktoré sa často menia. Využívajú sa hlavne v smerovacích protokoloch používaných v sieťach IP.[6]

Pri algoritmoch stavu linky, každý smerovač vykonáva nasledujúce kroky:

Identifikácia smerovačov, ktoré sú k nim fyzicky pripojené a získanie ich IP adries. Keď smerovač začne pracovať, pošle do siete takzvané "Hello" pakety aby nadviazal kontakt s okolitými smerovačmi. Každý smerovač, ktorý obdrží tento paket, odpovie so správou, ktorá obsahuje jeho jedinečný identifikátor (v IP sieťach IP adresu).

Smerovač ďalej meria čas oneskorenia (prípadne iné dôležité parametre siete ako priemerné zaťaženie) paketov od susedných smerovačov. Dosiahne to tak, že rozpošle do

[6] DIMARZIO, J. 2002. *Sams Teach Yourself Routing in 24 Hours.* QUE Publishing, 2002. 400p. ISBN 0672323648 [3]

siete echo pakety pre všetkých susedov. Každý sused, ktorý obdrží takýto paket, odošle ako odpoveď echo reply packet. Čas medzi odoslaním echo paketu a prijatím reply paketu vydelí smerovač dvomi a tak odhadne oneskorenie. Tento čas však okrem času potrebného na prenos obsahuje aj čas potrebný na spracovanie paketu a odoslanie odpovede.

Vysielanie informácií, ktoré smerovač zistil od iného smerovača a zároveň prijatie informácií od týchto smerovačov. V tomto kroku si smerovače teda navzájom vymenia informácie a získajú tak prehľad o topologickom stave siete. Toto sa deje pomocou záplavového algoritmu. Informácie si navzájom vymieňajú tzv. link-state paketmi (LSP). Tieto pakety majú nasledovnú štruktúru:

- ID smerovača
- ID jedného zo susedných smerovačov
- váha linky medzi nimi
- sekvenčné číslo
- TTL - time to live

Ďalej sa LSP paketom venujeme v časti smerovacieho protokolu OSPF.

Ak smerovač obdrží LSP, pokúsi sa ho uložiť vo svojej LSP databáze. Ak takýto LSP už v databáze existuje, nevykoná nič. Inak ho uloží do databázy a jeho kópiu rozošle všetkým svojim susedom, okrem iného aj to, kto bol zdrojom daného paketu. Tieto pakety môžu byť posielané periodicky, pri zmene stavu liniek alebo pri kombinácii predošlého.

Nasleduje výpočet najlepšej cesty medzi dvomi uzlami siete. Na tento výpočet sa používa najčastejšie Dijkstrov algoritmus najkratšej cesty, algoritmus SPF(sortest path first). V tomto algoritme smerovač na základe informácií, ktoré zozbieral, zostaví graf danej siete najkratších ciest do každého uzla v sieti. V tomto grafe sú znázornené umiestnenia smerovačov a ich vzájomné prepojenia. Každé toto spojenie je ohodnotené váhou(nákladmi na cestu). Táto váha môže byť funkciou oneskorenia na danej linke, priemerného zaťaženia alebo môže označovať počet skokov(Hops) medzi uzlami siete. Ak sa medzi počiatočným a cieľovým uzlom nachádza 2 a viac možných ciest, smerovač pomocou tohto algoritmu určí cestu s najmenšou váhou. Treba však spomenúť, že v prípade ak by existovali dve alebo aj viac rovnakých ciest, ktoré by mali rovnakú váhu, algoritmus dokáže sieťovú záťaž rovnomerne rozložiť medzi všetky cesty. Ďalej si

popíšeme kroky, ktorými Dijkstrov algoritmus nájde najkratšiu cestu do ostatných uzlov siete.

1.4.1 Dijkstrov algoritmus najkratšej cesty

Pri výpočte najkratšej cesty postupuje Dijkstrov algoritmus nasledovne:

1. V grafe siete, ktorý vytvoril smerovač si určí zdrojový a cieľový uzol. Označme si ich U_1 a U_2. Z tohto grafu je následne zostrojená tzv. "matica susedov". Súradnice v tejto matici určujú váhu medzi zodpovedajúcimi uzlami. Napríklad [i, j] určuje váhu linky medzi U_i a U_j. Ak medzi týmito uzlami neexistuje priame spojenie, váha spojenia v tejto matici nadobudne hodnotu nekonečna.
2. Smerovač si vytvorí záznamy stavov (status record set) pre každý uzol v sieti. Každý záznam obsahuje 3 polia:
    - Pole predchodcu - obsahuje predchádzajúci uzol
    - Pole dĺžky - obsahuje súčet váh od zdrojového uzla až po tento uzol
    - Pole návestia - obsahuje stav uzla. Každý uzol môže nadobúdať jeden z dvoch možných stavov: "permanentný" alebo "pokusný."
3. Smerovač inicializuje parametre týchto záznamov pre všetky uzly a nastaví ich dĺžku na nekonečno a ich návestie na "pokusný".
4. Smerovač nastaví T-uzol. V našom prípade, ak U_1 je zdrojový T-uzol, smerovač nastaví jeho návestie na "permanentný". Toto návestie sa už nezmení.
5. Smerovač upraví všetky záznamy pre všetky uzly s návestím "pokusný", ktoré sú priamo spojené s týmto T-uzlom.
6. Smerovač ďalej prezrie všetky uzly s návestím "pokusný" a vyberie ten, ktorého spojenie s U_1 má najmenšiu váhu. Tento uzol sa potom stane ďalším T-uzlom.
7. Ak tento uzol nie je cieľový uzol U_2, smerovač sa vráti do bodu 5.
8. Ak tento uzol je cieľový uzol U_2, smerovač vyberie jeho predchádzajúci uzol zo záznamov a takto pokračuje, kým sa nedostane naspäť do U_1. Takto dostane zoznam uzlov, ktoré určujú najlepšiu cestu z U_1 do U_2. [7]

Smerovacie algoritmy sú robustnejšie ako algoritmy s vektorom vzdialenosti a ako sme mohli vidieť používajú aj zložitejšie mechanizmy pri hľadaní ciest. Nenastáva pri nich problém pomalej konvergencie ani počítanie do nekonečna, pretože fungujú na inom

[7] Spracované podľa: RAZAVI, R. *How Routing Algorithms Work* [6]

základe ako smerovanie s vektorom vzdialenosti. Viac sa dozvieme v časti, v ktorej budeme hovoriť o smerovacom protokole OSPF.

1.5 Distribuovaný Aktualizačný algoritmus

Distribuovaný Aktualizačný algoritmus (z ang.Diffusing Update Algorithm - DUAL) bol prvýkrát predstavený E.W.Dijkstrom a C.S.Scholtenom v roku 1980.Napriek tomu že na vývoji tohto algoritmu pracovalo veľa odborníkov, významné zásluhy patria najmä J.J. Garcia-Luna-Aceves. Distribuovaný Aktualizačný algoritmus je hlavnou súčasťou protokolu EIGRP(Enhenced Interiour Gateway Routing Protocol), ktorý sa používa na smerovanie paketov v sieťach Internetu a zaraďuje sa medzi hybridné smerovacie protokol. V skutočnosti je to však obdoba smerovanie s vektorom vzdialenosti, kde sú iným spôsobom ošetrené slučky, ktoré môžu vzniknúť pri smerovaní. Filozofia algoritmu DUAL hovorí, že aj dočasné slučky škodia a následne znižujú rýchlosť siete. Je použitý ako náhrada za Bellman-Ford algoritmus alebo Ford-Fulkerson algoritmus, ktorý je používaný v smerovacích protokoloch založených na vektore vzdialeností.[8].

Tento algoritmus obsahuje väčšinu logiky, potrebnú pre výpočty a porovnávanie ciest v sieťach požívajúcich protokol EIGRP. Konkrétne tak sleduje väčšinu ciest oznámených susednými smerovačmi a pomocou zloženej metriky ich vzájomne porovnáva. Vybraná cesta nesmie obsahovať žiadne slučky a musí mať najnižšie náklady, distribuovaný aktualizačný algoritmus ju následne zapíše do smerovacej tabuľky, kde slúži pre posielanie datagramov v sieti[9].

Aby distribuovaný aktualizačný algoritmus pracoval správne musia byť splnené tieto podmienky:

1. Uzol zaznamená existenciu susedných uzlov v konečnom čase, inak s nimi stratí spojenie.
2. Všetky správy operačnej linky sú doručené v poriadku, v správnom poradí a v konečnom čase.
3. Všetky správy o zmene v cenách ciest, zlyhaniach v sieti a nájdení nových susedov sú spracované v konečnom čase a v poradí, v ktorom nastali.

Protokol EIGRP používa na zabezpečenie týchto troch podmienok protokol RTP[8].

[8] DOYLE, J. – CARROLL, J. 2006. *Routing TCP/IP* [9]
[9]Spracované podľa: SPORTACK, M. 2004. *Směrování v sítích IP.* Brno: Computer Press, 2004. 351 s. ISBN 80-251-0127-4. [1]

Pred tým ako sa začneme zaoberať samotným algoritmom si musíme vysvetliť určité pojmy.

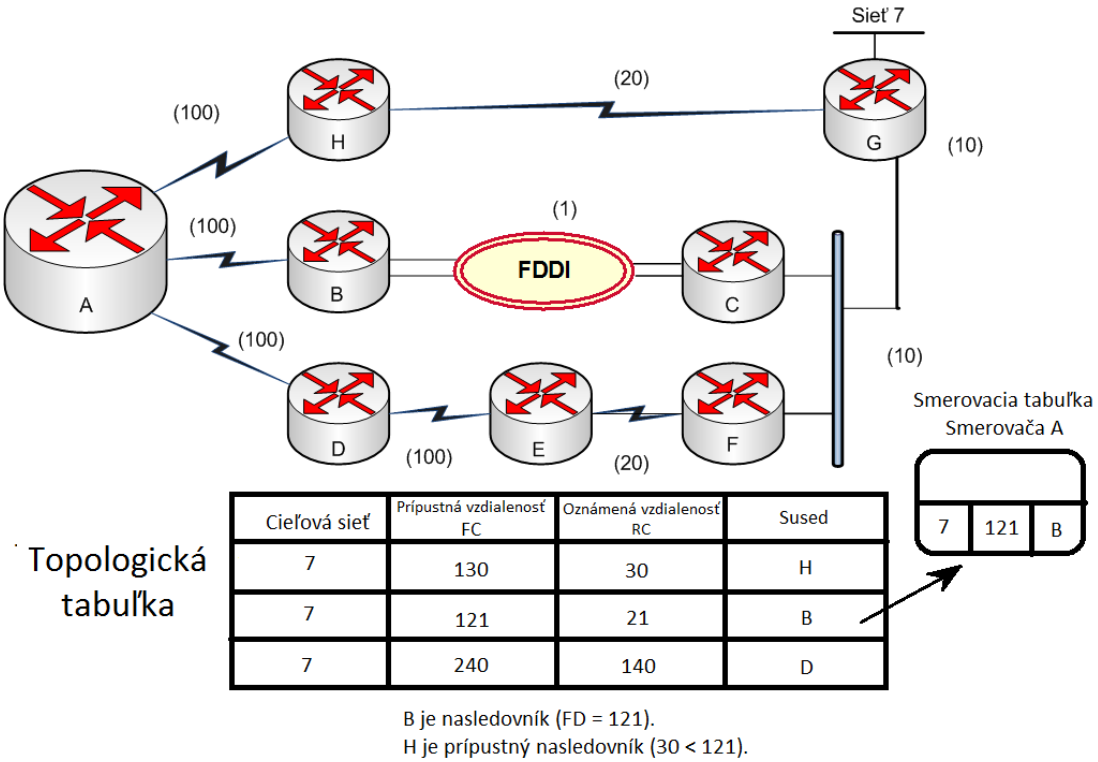
- Prípustná vzdialenosť (Feasible distance-FD) je najnižšia hodnota metriky teda vzdialenosti medzi všetkými cestami, pomocou ktorej sa dá dosiahnuť určitá podsieť. Oznámená vzdialenosť(Reported distance - RD) je vzdialenosť cesty, oznámená susedným smerovačom.
- Podmienka prípustnosti (Feasibility condition - FC) hovorí o tom, že pokiaľ do danej podsiete existuje viacej ciest, ide o stav, kedy je oznámená vzdialenosť nižšia ako prípustná vzdialenosť.
- Následnícka cesta alebo tiež aj následník je cesta, ktorá má spomedzi všetkých ciest najnižšiu hodnotu metriky do danej podsiete.
- Prípustný následník (Feasible Succesor - FS) je cesta, ktorá nie je následníckou cestou, ale spĺňa podmienku prípustnosti. V prípade výpadku následníckej cesty ju môžeme použiť bez rizika vzniku slučky.
- Aktívna cesta označuje cestu, ktorá stratila nasledovníka a nemá ani prípustného nasledovníka, a smerovač hľadá alternatívne cesty aby nastala konvergencia siete.
- Pasívna cesta označuje cestu, ktorá je následnícka.[10]

Činnosť algoritmu sa pokúsime opísať v nasledujúcom texte. Uvažujme o prípade kedy je prerušené spojenie s nasledovníkom. Algoritmus DUAL sa snaží znovu dosiahnuť konvergenciu siete. Nahliadne do topologickej tabuľky či sa v nej nenachádza nejaký prípustný nasledovník.

Ak je nájdený prípustný nasledovník jeho status je okamžite zmenený a stáva sa z neho nasledovník(následnícka cesta) a protokol EIGRP informuje o tejto zmene svojich susedov. Táto cesta sa následne používa na smerovanie datagramov do nedostupnej siete, čím sa opätovne dosiahla konvergencia siete a prenos je obnovený. Tento postup, kedy je smerovač sám schopný konvergovať a nepotrebuje spoluprácu ostatných smerovačov v sieti sa nazýva takzvaný lokálny výpočet (local computation). Lokálny výpočet má svoju výhodu v tom že nezaťažuje procesor smerovača pretože všetci prípustný nasledovníci sú vypočítaný pred tým ako výpadok siete nastal. Príklad vidíme na obrázku 4. Ak primárna

[10]ODOM, W. – HEALY, R. – MEHTA,N. 2009. *Směrování a přepínání sítí*. 3.vydanie. Brno: Computer Press, 2009. 879 s. ISBN 978-80-251-2520-5. [2]

cesta (smerovač D) nie je dostupná, predvolený prípustný nasledovník smerovač H preberie primárnu cestu.



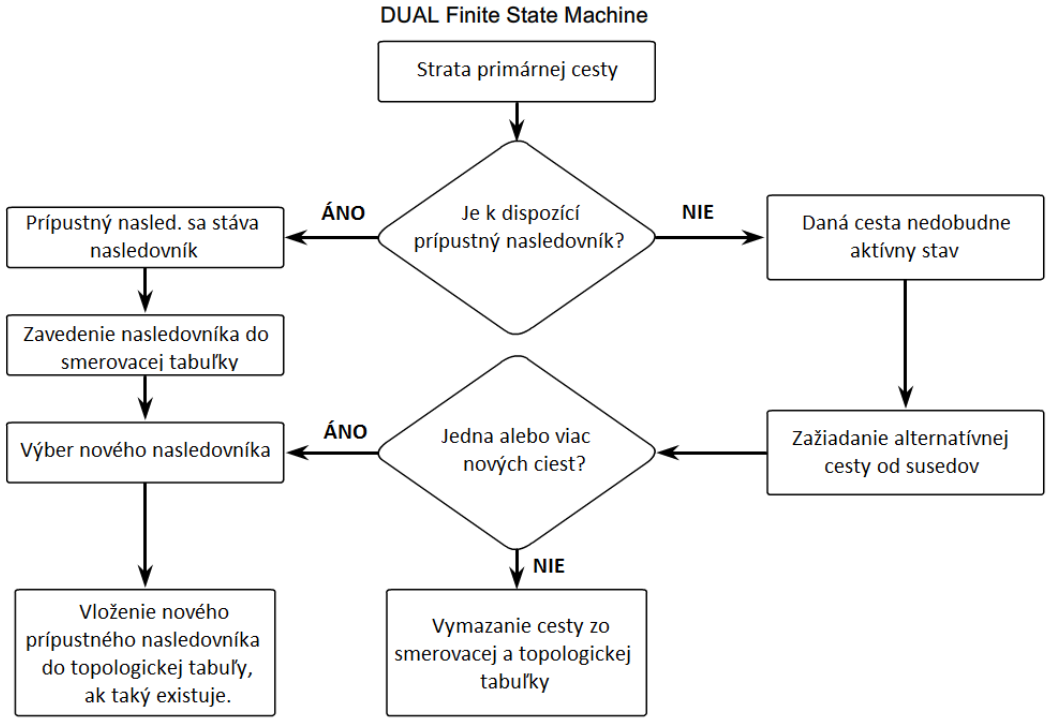
Obr.4: Výber prípustného nasledovníka[11]

Ak nie je nájdený prípustný nasledovník, smerovač začne takzvané difúzne počítanie (diffusing computation), kedy rozpošle správy všetkým svojím susedným smerovačom o padnutej ceste v sieti a žiada od nich náhradnú cestu do danej lokality. Nedostupná cesta zmení svoj stav na aktívny. Ak susedia majú informácie o dopytovanej ceste, odpovedia smerovaču. Ak susedia nemajú informácie o dopytovanej ceste, rozpošlú požiadavku všetkým svojím susedom. Ak susedný smerovač nemá alternatívnu cestu do danej lokality a nemá ani žiadneho ďalšieho suseda, pošle správu dopytovanému smerovaču, v ktorej nastaví vzdialenosť cesty na nekonečno, čo znamená že daný smerovač tiež cestu nemá. Dopytovaný smerovač čaká pokiaľ nedostane odpovede od všetkých susedov, z ktorých si potom vyberie cestu s najlepšiu hodnotu metriky a zvolí ju za svoju primárnu cestu do danej siete. Príklad vidíme na obrázku č.1.Ak primárna cesta cez smerovač B nie je k dispozícii a tak isto aj prípustný nasledovník smerovač H, smerovač A pošle požiadavku na alternatívnu cestu do siete 7 smerovaču D. V tomto prípade smerovač D odpovie a poskytne smerovaču A alternatívnu cestu do siete

[11] AZIZ, Z. – LIU, J. – MARTEY, A. – SHAMIM, F. 2004. *Troubleshooting IP Routing Protocols.* [10]

7.Smerovač A následne dosiahne stav konvergencie a nahradí pôvodnú cestu do siete 7 cez smerovač B novou cez smerovač D.[12]

Činnosť distribuovaného aktualizačného algoritmu si môžeme naznačiť stavovým diagramom na obrázku 5[13]



Obr.5: Činnosť distribuovaného aktualizačného algoritmu[13]

[12] Spracované podľa: AZIZ, Z. – LIU, J. – MARTEY, A. – SHAMIM, F. 2004. *Troubleshooting IP Routing Protocols* [10]
[13] Spracované podľa Cisco Networking Academy CCNA Curriculum 4.0 r.2008 [4]

2 Smerovacie protokoly

2.1 Smerovací protokol RIP[14]

V priebehu rokov sa smerovacie protokoly vyvíjali aby uspokojili narastajúci dopyt čoraz viac a viac komplexnejších sietí. Prvý z široko rozšírených protokolov, populárny pre svoju jednoduchú implementáciu do prostredia ale aj jeho nenáročnú údržbu sa stal protokol RIP(Routing information protocol).RIP pôvodne vyvinula spoločnosť Xerox a nazvala ho GWINFO(Gateway information protocol). Následne nato bol univerzitou v Berkeley implementovaný ako systémový démon s názvom "route-dee" do jej softwarovej distribúcie(BSD unixu) ale pod drobnými vylepšeniami a čiastočnými zmenami. Mnohí ďalší výrobcovia nasledovali a spravili si svoje jemne odlišné ale implementácie protokolu RIP, ktoré aj napriek malým odlišnostiam nevedeli spolupracovať. Na základe toho sa združenie IETF(Internet Engineering Task Force) rozhodlo vytvoriť smerovací protokol s identickým názvom RIP, ktorý by definoval štandard, podľa ktorého by boli ich implementácie schopné spolupracovať a bola by tak zabezpečená všeobecná kompatibilita v sieťach.

Protokol RIP je postavený na smerovacích algoritmoch vektora vzdialenosti, ktoré boli teoreticky popísané už v rokoch 1957 až 1962. Algoritmy vektora vzdialenosti sa niekedy nazývajú aj algoritmy Bellaman – Ford alebo Ford – Fulkerson po ich autoroch, ktorý ich popísali v diele Toky v sieťach(Flows in Networks). Protokol používa na ohodnotenie vzdialeností medzi jednotlivými uzlami v sieti metriku, nazývanú tiež aj cena. Táto cena je vlastne počet preskokov medzi jednotlivými uzlami(Hops). Je to jediná metrika, ktorá sa v protokole RIP používa na ohodnotenie ciest.

Informácie o cestách v sieti si smerovače preposielajú pomocou RIP paketov, ktoré využívajú na prenos protokol UDP. Ako vieme protokol UDP nezaručuje spoľahlivé doručenie svojich správ ale je menej náročnejší na prevádzku v sieti. To mali na mysli aj tvorcovia protokolu RIP, aby čo možno najmenej zahltili prenosové médium nutnou komunikáciou, ktorú protokol vyžaduje pre svoj chod. Informácie v jednotlivých destináciách v sieti sú udržiavané v smerovacej tabuľke, kde každý záznam obsahuje:

- Pole s cieľovou IP adresou
- Pole s metrikou vektora vzdialenosti(počet skokov)
- Pole s IP adresou najbližšieho preskoku

[14] Spracované podľa: SPORTACK, M. 2004. *Směrování v sítích IP*. Brno: Computer Press, 2004. 351 s. ISBN 80-251-0127-4. [1]

- Pole s príznakom zmeny cesty
- Časovače cesty

Treba pripomenúť, že protokol RIP podľa štandardu uchováva vždy iba jednu cestu do určitého cieľa a to tú najlepšiu, teda s najmenším počtom preskokov. Určite je jasné načo slúžia prvé dve polia. Prvé je adresa do možného cieľa a druhé je vzdialenosť v skokoch, ktorá tomuto cieľu prislúcha. Pole s IP adresou najbližšieho preskoku je IP adresa sieťového rozhrania susedného smerovača, ktorému musí byť správa poslaná ak chceme aby dorazila do uzla s cieľovou IP adresou, teda tomu smerovaču, ktorý nám dal o tejto ceste vedieť a zároveň je aj najkratšia. Pole s príznakom zmeny indikuje nedávnu zmenu tejto cesty, teda či k nej boli obdržané od susedov nejaké zmeny. Polia s časovačmi sú pre protokol RIP veľmi dôležité nakoľko sú to jediné mechanizmy pre udržanie konvergencie siete. Protokol na základe nich posiela pravidelné aktualizačné správy, rozhoduje sa či pozastaviť smerovanie cez danú cestu pokiaľ pre ňu neobdržal istý čas nové správy a keď sa aj po určitom čase nič o danej ceste nedozvie, vyradí ju zo smerovacej tabuľky úplne. Protokol RIP používa tri druhy časovačov. Prvý z nich je časovač platnosti cesty a druhý, časovač vyprázdnenia cesty. Tieto dva smerovače má každá z ciest v smerovacej tabuľke a slúžia na sledovanie aktuálnosti danej cesty v smerovacej tabuľke. Smerovač platnosti cesty je štandardne nastavený na 180 sekúnd. Pokiaľ nie je počas tejto doby obdržaná žiadna aktualizačná správa k danej ceste, smerovač nastaví vzdialenosť tejto cesty ako nekonečno(nedosiahnuteľnosť), ktoré v protokole RIP symbolizuje číslo 16 a spustí časovač vyprázdnenia cesty, ktorý odpočítava ďalších 90 sekúnd. Ak sa smerovač neobdrží žiadne aktualizácie ani do vypršania časového limitu časovača vyprázdnenia cesty, cesta je odstránená zo smerovacej tabuľky úplne. V opačnom prípade , teda ak by bola k danej ceste obdržaná aktualizácia v inkriminovanom čase, cesta by opäť nadobudla platnosť. Okrem časovača platnosti cesty a vyprázdnenia cesty je ešte jeden časovač, ktorý je iba jeden pre daný uzol, teda celý smerovač protokolu RIP a to aktualizačný časovač. Jeho úloha je inicializovať zaslanie aktualizačných správ každých 30 sekúnd. Uzly RIP si pri aktualizácií posielajú obsah celej smerovacej tabuľky, čo je rozdiel oproti protokolom so stavom linky alebo hybridným protokolom, ktoré posielajú iba nutné aktualizácie. Nepochybne sa týmto spôsobom plytvá využiteľnou šírkou pásma, ale napriek tomu protokol RIP nemá žiadne informácie o topológie siete a smerovačoch v nich, musí posielať v aktualizačných správach všetky cesty zo svojej tabuľky. Okrem tohto nedostatku má smerovanie vektora vzdialenosti problémy aj s rýchlosťou konvergencie siete a hlavne

po páde niektorej z liniek alebo smerovačov. Vzniká tu takzvaný problém počítania do nekonečna, kedy sa vďaka časovému oneskoreniu smerovače začnú navzájom klamať a vypočítavajú nesprávne metriky. Vznik takejto situácie je popísaný v časti Algoritmus vektora vzdialenosti aj s mechanizmami, ktoré sa používajú ako prevencia, ktorá má predísť takejto situácii. Avšak aj napriek tomu môže takáto situácia nastať.

Protokol RIP má nepochybne stále svoje miesto v menších sieťach, kde jeho služby plne postačujú požiadavkám siete. Vo väčších prostrediach je však už dávno nepoužiteľný hlavne kvôli svojmu obmedzeniu preskoku cez 16 uzlov, čo je maximum veľkosti cesty, pomalej konvergencii, záťaži na médium objemom posielaných smerovacích informácií, pevne stanovenej metrike a aj nízkej bezpečnosti celého protokolu. Protokolu navyše chýba aj vyrovnávania záťaže nakoľko sa s ním v pri vývoji nepočítalo a ani by nebolo možné, nakoľko protokol RIP z možných ciest do daného uzla vyberie a uloží iba tú najlepšiu aj keď existuje viacej možných. Niektoré implementácie iných výrobcov však sú schopné podporovať aj viac ciest do jedného cieľa.

2.2 Smerovací protokol OSPF [15]

Už na začiatku osemdesiatych rokov, začínalo byť jasné, že smerovacie protokoly s vektorom vzdialenosti neudržia krok s rýchlim rozvojom Internetu a vytváraním rozsiahlejších a rozsiahlejších sietí a musia byť nahradené novými smerovacími technikami. Tak začali postupne od rôznych výrobcov vznikať protokoly založené nie na vektore vzdialenosti medzi dvoma uzlami ale na stave linky medzi týmito uzlami. Nakoľko však nebol žiaden z týchto protokolov otvorený štandard, rozhodlo sa združenie IETF takýto štandard vytvoriť. Preto vytvorilo špeciálnu skupinu odborníkov zameranú na vytvorenie nového smerovacieho protokolu s názvom OSPF(Open shortest path first). Základ funkcionality protokolov stavu linky tvorí Dijkstrov algoritmus najkratšej cesty, algoritmus SPF(Sortest path first). Tento algoritmus je bližšie popísaný v časti Algoritmy stavu linky.

Protokol OSPF bol prvotne vyvíjaný ako smerovací protokol, ktorý mohol smerovať iba jeden smerovaný protokol a tým bol protokol IP. To znamená, že OSPF nie je schopný smerovať žiadny iný smerovaný protokol ako napríklad IPX od firmy Novell alebo AppleTalk od firmy Apple. Pre doručovanie svojich správ po sieti využíva priamo

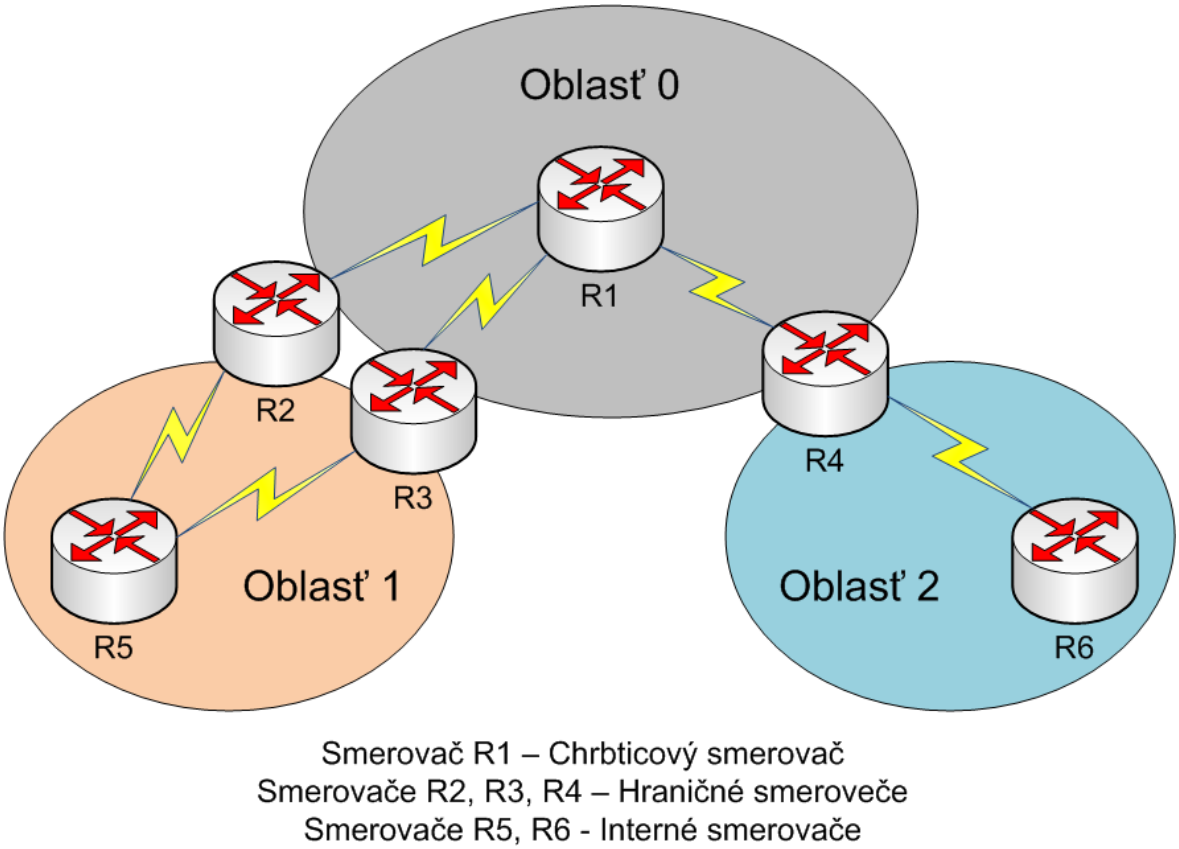
[15] Spracované podľa: SPORTACK, M. 2004. *Směrování v sítích IP*. Brno: Computer Press, 2004. 351 s. ISBN 80-251-0127-4. [1]

protokol IP a svoje pakety vkladá do paketov IP. Tým pádom nie sú potrebné žiadne ďalšie protokoly ako TCP, UDP a podobne.

Združenie IETF si pri vývoji protokolu OSPF za najdôležitejšie ciele stanovilo lepšiu škálovateľnosť siete a rýchlu konvergenciu siete. Tieto ciele boli dosiahnuté tým, že sieť bola rozdelená na takzvané oblasti(areas). Oblasť je tvorená sieťovo prepojenými koncovými systémami, smerovačmi a prenosovými prostriedkami. Každá oblasť má stanovené číslo, ktoré je súčasťou konfigurácie každého smerovača. Jednotlivé rozhrania smerovačov s rovnakým číslom sú potom súčasťou tej istej oblasti. Tieto oblasti by mali byt vytvorené s ohľadom napríklad na prevádzku v danej sieti a v žiadnom prípade nie náhodne, ale tak aby spolu funkčne súviseli.

Podľa príslušnosti v jednotlivých oblastiach rozlišujeme tri typy smerovačov.

- Interné smerovače
- Hraničné smerovače oblastí
- Chrbticové smerovače



Obr.6: Oblasti protokolu OSPF a rôzne typy smerovačov[16]

[16] Prameň: FRIEBE, A. 2009. *OSPF, Part 7*. 2009 [8] Vlastné spracovanie

Na obrázku vidíme jednotlivé typy smerovačov. Smerovače, ktoré majú viacej sieťových rozhraní môžu patriť do viac ako jednej oblasti. Hraničný smerovač je práve takýmto smerovačom, pričom prepája vlastnú oblasť s chrbticovou oblasťou 0. Smerovač s minimálne jedným rozhraním patriacim do oblasti 0 nazývame chrbticovým. Ak smerovač prepája hociktorú nenulovú oblasť s nulovou oblasťou je zároveň hraničným aj chrbticovým smerovačom. Interný smerovač je taký, ktorého všetky rozhrania patria do tej istej oblasti, ktorá je nenulová.

Medzi týmito troma typmi smerovačov prebiehajú dva typy smerovania paketov. Tým prvým je smerovanie v rámci oblastí a druhým smerovanie medzi oblasťami. Smerovanie v rámci oblastí je preposielanie iba medzi smerovačmi určitej oblasti pričom správy nevychádzajú za hranice danej oblasti. Pri smerovaní medzi oblasťami prebieha preposielanie správ medzi smerovačmi z rôznych nenulových oblastí. Toto preposielanie však musí prebiehať cez chrbticovú oblasť 0, čo znamená že nenulové oblasti nikdy nesmú spolu priamo komunikovať. Toto hierarchické obmedzenie umožňuje sieťam OSPF výbornú škálovateľnosť.

Ako kritérium pre porovnávanie možných ciest do cieľa protokol OSPF používa metriku označovanú ako cena(cost).Cena môže nadobúdať číslo od 1 do 65535 a je priradená implicitne ku každému sieťovému rozhraniu smerovača a jeho veľkosť závisí od šírky pásma daného rozhrania podľa vzťahu.

cena = 100 000 000 / šírka pásma v bps

Teda čím väčšia šírka pásma, tým menšia cena a tým aj lepšia cesta. Cenu konkrétnej cesty tvorí súčet cien všetkých rozhraní cez ktoré daná cesta vedie. Ako môžeme vidieť protokol OSPF používa metriku založenú na šírke pásma. Táto metrika sa však dá aj explicitne nastaviť. Odporúča sa však ponechať implicitné hodnoty cien. Ak by však sieť pozostávala napríklad iba z homogénnych prenosových technológií, šírka pásma by bola pre každé sieťové rozhranie rovnaká a tým by sa nakoniec počet skokov stal jediným faktorom tvorby ceny medzi danými uzlami.

Protokol OSPF používa pre komunikáciu medzi smerovačmi sadu piatich rôznych typov paketov. Každý z týchto paketov sa potom vkladá do hlavičky OSPF, pomocou ktorej smerovače OSPF, informuje o type paketu, ktorý daná správa obsahuje, a na základe ktorej sa smerovače rozhodnú či ju majú danú správu prijať alebo zahodiť. Jednotlivými

poľami hlavičky OSPF sa nebudeme zaoberať. Pre komunikáciu používa protokol OSPF týchto päť typov správ, z ktorých každý zabezpečuje určitú špeciálnu funkciu:

- Kontaktné pakety hello
- Pakety s popisom databázy
- Pakety s požiadavkou stavu linky
- Pakety s aktualizáciou stavu linky
- Pakety s potvrdením stavu linky

Kontaktné pakety hello slúžia na nadviazanie takzvaných "susedností" s okolitými smerovačmi. Tieto pakety sú súčasťou komunikačného protokolu hello, ktorý protokol OSPF používa, za účelom rozpoznania susedov a dohodnutí sa na určitých hodnotách, ktorá musia byt jednotné aby sieť OSPF správne fungovala. Konkrétne na maske siete, intervale posielania paketov hello(hello interval) a dobe, ktorá keď uplynie bez obdržania odpovede od určitého smerovača, môže byť určitá cesta vyhlásená za neplatnú(dead interval).

Ďalším typom správ je paket s popisom databáz(database description, DD), ktoré si dva susedné smerovače vymieňajú pri inicializácií relácie priľahlosti. Paket popisuje obsah databázy stavu liniek, ktorú daný smerovač obsahuje, neprenáša však konkrétnu databázu. Niekedy môže byť obsah databázy dosť rozsiahli, vtedy sa použije pre doručenie viac paketov s popisom databázy.

Na vyžiadanie konkrétnej časti z databázy stavu liniek slúži tretí typ paketov s požiadavkou stavu linky(link-state request, LSR).Ak smerovač zistí z obdržaného paketu s popisom databázy, že sused pozná lepšiu cestu do určitého uzla, pošle susedovi požiadavku stavu linky a vyžiada si od neho podrobnejšie informácie o stave danej linky.

Sused na túto požiadavku stavu linky odpovedá zaslaním aktualizačného paketu stavu linky(link-state update, LSU), v ktorom budú požadované informácie. Aktualizačné pakety stavu linky musia byť potvrdené posledným typom paketov s potvrdením stavu linky(link-state acknowledgement, LSAck).Ak nebude prijatie paketu LSU potvrdené do určitej doby, bude paket LSU znovu zaslaný. Podobný postup by nastal ak by smerovač zistil, že niektorí z jeho susedov už nie je dostupný, teda ak už vypršal limit dead intervalu a smerovač od suseda nedostal žiadny hello paket alebo ak by smerovač objavil pomocou protokolu hello nového suseda. Pakety LSA treba doručiť každému priľahlému smerovaču,

ktoré šíria túto správu tím istým spôsobom ďalej, až sa správa rozšíri po celej oblasti. Toto šírenie sa nazýva "záplava". Táto záplava sa uskutočňuje v rámci konkrétnej oblasti, a nikdy nezasahuje do druhej oblasti. Vďaka tejto skutočnosti jednotlivé oblasti siete OSPF rýchlo konvergujú a strata konvergencie jednej oblasti neovplyvní konvergenciu druhej. Fakt je, že dané smerovače v rámci jednej oblasti poznajú iba topologickú štruktúru svojej oblasti. Jednotlivé oblasti si potom medzi sebou preposielajú súhrnné smerovacie informácie pomocou hraničných a chrbticových smerovačov daných oblastí. Takto súbežne konvergujú rôzne oblasti siete OSPF, až dosiahnu konvergenciu celej siete. Na rozdiel od protokolu RIP, kde konvergencia nastávala pomaly z dôvodu postupnej konvergencie celej siete, protokol OSPF využíva rozdelenie celej siete na menšie oblasti, ktoré skonvergujú pomerne rýchlo.

Protokol OSPF má jednu zvláštnosť oproti iným smerovacím protokolom a to takú, že informácie o zmene stavu linky, ktoré preposiela ak zaznamená zmenu v sieti, nemôže daný smerovač po obdržaní hneď použiť a porovnať s informáciami, ktoré má vo svojej smerovacej tabuľke. Problém je v tom že tieto informácie sú z pohľadu, ktorý má odosielajúci smerovač na sieť. Smerovač, ktorý túto správu prijal si musí vytvoriť vlastný pohľad a preto musí znovu spustiť Dijkstrov algoritmus najkratších ciest a zostaviť si strom najkratších ciest. Následne môže porovnať či obdržaná správa ovplyvnila cesty v smerovacej tabuľke.

V protokole OSPF sa nestretneme s problémami, ktoré mohli nastať v sieti so smerovacím protokolom RIP ako počítanie do nekonečna. Nakoľko sa však pakety LSU šíria formou záplavy môže nastať situácia, kedy príde do smerovača viac ako jedna aktualizačná správa so stavom linky. Protokol je vybavený kontrolným mechanizmom, ktorý nám v takomto prípade vždy vyberie a spracuje iba najnovší z nich. Toto je zabezpečené pomocou hlavičky aktualizačného paketu, kde sa skontroluje pole s vekom , poradové číslo a kontrolný súčet paketu. V niektorých sieťach s malou šírkou pásma liniek môže protokol spôsobovať pri prvotnej konvergencií zvýšenú záťaž na sieť kvôli zvýšenému posielaniu správ. Toto môže predstavovať určitý problém, ktorý je ale kompenzovaný rýchlou konvergenciou. Nechýba takisto podpora vyrovnávania záťaže, kedy pri existencií viacerých najlepších ciest do jedného uzla protokol rovnomerne rozloží záťaž po týchto cestách. Protokol OSPF sa radí medzi funkčne najbohatšie smerovacie protokoly, vďaka tejto vlastnosti je však aj pomerne zložitý a vyžaduje skúsenosti sieťových administrátorov. Dobré postavená sieť OSPF sa však odmení rýchlou konvergenciou, stabilitou a výkonom.

2.3 Smerovací protokol EIGRP[17]

Protokol EIGRP(enhenced interiour gateway routing protocol) je proprietárny smerovací protokol, ktorý vyvinula firma Cisco. Úspech tohto protokolu ako aj jeho predchodcu, protokolu IGRP umožnil firme Cisco vstup medzi popredné firmy dodávajúce produkty na trh s internetovými technológiami. Protokol EIGRP sa radí medzi takzvané hybridné smerovacie protokoly, nakoľko v sebe spája funkcionalitu z protokolov stavu linky a smerovacích protokolov s vektorom vzdialenosti. Firma cisco vyvinula tento protokol práve aby využila priestor na trhu a zaplnila biele miesto, pričom využila najlepšie vlastnosti smerovania s vektorom vzdialenosti a smerovania so stavom linky.

Protokol EIGRP zdedil od protokolov s vektorom vzdialenosti používanie metriky na ohodnotenie vzdialenosti medzi jednotlivými uzlami. Nepoužíva však jednoduchú metriku založenú iba na počte skokov medzi smerovačmi ako je to napríklad v protokole RIP. Používa takzvanú zloženú metriky, ktorá pozostáva zo šírky pásma, odozvy(oneskorenia), spoľahlivosti linky, a zaťaženia linky. Bežne však protokol používa na výpočet metriky iba šírku pásma a odozvu linky, ktorá tvorí takzvaný základný vzorec. Základný a kompletný vzorec, podľa ktorého sa vypočítava zložená metrika môžeme vidieť na obrázkoch.

Základný vzorec na výpočet metriky:

$$metrika = [K1 * \check{s}\acute{i}rka\ p\acute{a}sma\ +\ K3 * odozva\ linky]$$

Kompletný vzorec na výpočet metriky:

$$metrika = \left[K1 * \check{s}\acute{i}rka\ p\acute{a}sma\ + \frac{(K2 * \check{s}\acute{i}rka\ p\acute{a}sma)}{256 - za\check{t}a\check{z}enie} + \ K3 * odozva\ linky\right] * [K5/(spo\check{l}ahlivos\check{t} + K4)]$$

Jednotlivé koeficienty K1 až K5 vyjadrujú váhu(dôležitosť), ktorá sa pripisuje danej veličine a predstavuje pre sieťového administrátora formu škálovateľnosti metriky a prispôsobenie konkrétnym podmienkam v danej sieti. Takéto prispôsobenie metriky je určite výhodou oproti statickej metrike skokov v protokole RIP, aj keď treba spomenúť, že sa v protokole RIP môžeme zmeniť váhu metriky a to tak, že vzdialenosť medzi uzlami

[17] Spracované podľa: SPORTACK, M. 2004. *Směrování v sítích IP.* Brno: Computer Press, 2004. 351 s. ISBN 80-251-0127-4. [1]

nebude mať hodnotu jedného skoku, ale 2 a viacerých. Toto sa však doporučuje iba ak naozaj vieme čo robíme. Ďalšiemu opisu vzorca sa nebudeme vzhľadom na obsiahlosť témy venovať. Črty, ktorými sa protokol EIGRP podobá na protokoly so stavom linky je reakcia na zmenu topológie siete, aktualizácia ciest v sieti a ich oznamovanie, o ktorých si povieme v nasledujúcom texte.

Hlavnými cieľmi protokolu EIGRP je čo možno najkratšia konvergencia siete a jej stabilita. Tú protokol dosahuje pomocou zavedenia nového algoritmu DUAL, ktorý je bližšie popísaní v časti distribuovaný aktualizačný algoritmus. Pomocou tohto algoritmu protokol EIGRP zisťuje či sú v cestách, ktoré príjme od svojich susedov nejaké slučky alebo nie a takisto pomocou neho získava informácie o alternatívnych cestách bez zbytočného čakania na aktualizácie od susedov. Celkovo protokol EIGRP prináša radu nový technológii, ktoré môžeme rozdeliť do nasledovných skupín:

- Rozpoznávanie a obnovovanie susedov
- Spojovaný prenosový protokol RTP
- Difúzny aktualizačný algoritmus DUAL
- Modularita protokolu

Protokol EIGRP sa na rozdiel od smerovacích protokolov s vektorom vzdialeností pri údržbe smerovacej tabuľky nespolieha výhradne na časovače, ale využíva neustálu komunikáciu medzi smerovačmi EIGRP, pomocou ktorej sa uskutočňujú nasledujúce činnosti:

- Dynamicky sa rozpoznávajú nové smerovače zapojené do siete
- Rozpoznanie ciest, ktoré sú nedosiahnuteľné alebo mimo prevádzky
- Spätné rozpoznanie predtým nedosiahnuteľných smerovačov

Proces rozpoznania nastáva pomocou zasielania kontaktných HELLO paketov všetkým svojim susedom v určitých pravidelných intervaloch. Pomocou týchto paketov vznikne medzi susedmi vzťah nazývaný priľahlosť. Priľahlé smerovače si potom medzi sebou vymieňajú smerovacie informácie a smerovacie metriky. Pokiaľ susedia prijímajú HELLO pakety medzi sebou navzájom, svedčí to o platnosti danej cesty. Ak však prestanú takéto

správy prichádzať, smerovač spustí proces algoritmu DUAL. V ďalšom texte sa budeme rôznym typom paketov venovať bližšie.

Ďalšou novou vlastnosťou protokolu EIGRP je že zaisťuje bezpečný prenos svojich rôznych paketov na rozdiel od protokolu RIP. Ten dosahuje pomocou celkom nového protokolu RTP(Reliable transport protocol), ktorý bol takisto vyvinutí spoločnosťou cisco špeciálne pre potreby protokolu EIGRP. Nutnosť vývoja tohto protokolu sa odvíja priamo od ďalšej novej vlastnosti protokolu EIGRP a to je jeho modularita. Zámer firmy Cisco bol totižto vyvinúť protokol, ktorý je nezávislý na smerovanom protokole a umožňuje smerovať aj iné smerované protokoly okrem protokolu IP ako sú napríklad IPX od firmy Novell alebo AppleTalk od firmy Apple. Preto museli vyvinúť celkom nový protokol, ktorý nie je závislí na sade TCP/IP. Aj keď treba poznamenať, že RTP má velmi veľa spoločných črtou s protokolom TCP a UDP. Vďaka modularite EIGRP môže byť modul smerovaného protokolu hocikedy zmenený na iný požadovaný smerovaný protokol.

Protokol EIGRP pracuje s pomerne veľkým množstvom informácii, lebo musí sledovať skoro aktuálny stav siete. Tieto informácie o stave siete uchováva v tabuľkovej podobe. Kvôli proprietárnej povahe protokolu EIGRP nie sú informácie o všetkých používaných tabuľkách k dispozícii. Popíšeme si teda iba 3 najpodstatnejšie a tieto sú:

- Tabuľka susedov
- Smerovacia tabuľka
- Tabuľka sieťovej topológie

V tabuľke susedov sa sledujú susedstvá medzi smerovačmi, ktoré tvoria základ pre väčšinu smerovacích aktualizácií a konvergenciu siete. Zapisujú sa sem informácie o stave priľahlých susedných uzlov EIGRP. Ak smerovač rozpozná nový uzol, do tabuľky sa zapíše nová položka s adresou a rozhraním suseda. Tabuľka susedov ďalej slúži ako nástroj na sledovanie paketov, ktoré dorazili od konkrétneho suseda. Pre každý riadok je pre každý paket vyhradené pravé jedno políčko kam sa zapisuje jeho poradové číslo. Ak nejaký paket od niektorého zo susedov nedorazí, jeho políčko zostane prázdne. Tabuľka týmto spôsobom podporuje spoľahlivé doručovanie paketov.

Smerovacia tabuľka obsahuje pre každý cieľový uzol jednu položku, ktorá obsahuje najkratšiu cestu do daného uzla, ktorá bola vypočítaná algoritmom DUAL. Ku každému uzlu pritom protokol EIGRP môže zaznamenať v smerovacej tabuľke maximálne až 6 možných ciest. Ak by smerovač zistil zmenu v hociktorej položke tabuľky okamžite

nato upozorní svojich susedov, ktorý vykonajú potrebné kroky aby zistili či ich táto zmena ovplyvnila

Informácie, ktoré sú potrebné pre výpočet vektorov vzdialeností do jednotlivých uzlov sú uložené v tabuľke sieťovej topológie. Tieto informácie obsahujú už spomínane veličiny na výpočet metriky ako šírka pásma, celkové zaťaženie, spoľahlivosť(danej linky), zaťaženie(danej linky), ale aj iné ako sú maximálna veľkosť prenosovej jednotky(MTU), oznámená vzdialenosť, prípustná vzdialenosť a zdroj cesty. Pojmy oznámená a prípustná vzdialenosť sú opísané v kapitole algoritmu DUAL. Zdroj cesty je identifikačné číslo smerovača, pomocou ktorého sa dá identifikovať pôvod smerovacích informácií v sieti. Každá položka ďalej obsahuje rozhranie cez ktoré je daný ciel dosiahnuteľný a či je daná položka nasledovník alebo prípustný nasledovník. Pojmy nasledovník a prípustný nasledovník sú bližšie popísané v časti algoritmu DUAL. Treba ešte spomenúť, že vďaka modularite, ktorá bola spomenutá už skôr, môže protokol EIGRP smerovať viac smerovaných protokolov súčasne a tým pádom si musí pre každý smerovaný protokol viesť jeho smerovaciu tabuľku, tabuľku susedov a aj topologickú tabuľku.

Pre komunikáciu a udržovanie svojich tabuliek používa protokol EIGRP týchto päť typov paketov:

- Kontaktné pakety HELLO
- Potvrdzovacie
- Aktualizačné
- Opytovacie
- Odpovedacie

Pakety HELLO ako sme si už povedali slúžia na rozpoznávanie nových susedných smerovačov EIGRP v sieti, ale aj pre udržovanie aktuálnosti súčasne používaných ciest a sú posielané v určitých časových intervaloch. Veľkosť tohto intervalu závisí od šírky pásma, ktoré sa používa rozhranie medzi dvoma susednými uzlami. Čím väčšia šírka pásma tým menší časový interval. Veľkosti časových intervalov pre bežne používané šírky pásma sú implicitne prednastavené, ale v prípade potreby ich možno zmeniť, čo môže byť určité osožné pre lepšiu škálovateľnosť protokolu. Predstavme is teraz situáciu že smerovač prestane dostávať správy(hocijaké nie len hello) pre určitú cestu po dobu časového intervalu HELLO. Táto cesta prejde do takzvanej udržiavacej doby(hold-time), ktorá je implicitne prednastavená na 3-násobok intervalu HELLO. Ak počas tejto doby

smerovač neprijme k danej ceste žiadne správy spustí sa nad touto cestou proces algoritmu DUAL.

Na spoľahlivé doručenie paketov EIGRP, ktoré to vyžadujú sa používajú potvrdzovacie pakety. Sú to vlastne pakety HELLO, ktoré neprenášajú žiadne dáta iba potvrdzujú prijatie určitých paketov. Niekedy sa nazývajú aj ACK pakety (acknowledgement).

Aktualizačné pakety sa používajú na prenos smerovacích informácií do jednotlivých známych uzlov. Môžu nastať 2 rôzne situácie, kedy sa posielajú aktualizačné pakety. Prvý prípad je ak smerovač zaznamená zmenu nejakej zo sledovaných ciest a druhý ak smerovač zaznamená prítomnosť nového smerovača v sieti. V prvom prípadne smerovač okamžite po zaznamenaní zmeny rozpošle viacsmerovú aktualizačnú správu všetkým známym susedom. V druhom prípade zašle smerovač kompletný výpis svojej topologickej tabuľky novému susedovi, ktorá sa môže skladať aj z viacerých aktualizačných správ.

Opytovacie a odpovedacie pakety sa používajú ak smerovač potrebuje od jedného alebo viac susedov určité informácie napríklad vypadne spojenie s určitou cestou a smerovač zašle jednosmerný alebo viacsmerový opytovací paket svojim susedom a čaká na príjem odpovedacích paketov. Opytovacie, odpovedacie a aktualizačné pakety sa posielajú vždy spoľahlivo, teda vyžadujú potvrdenie prijatia takéhoto paketu.

Ako sme mohli vidieť protokol EIGRP v sebe spája vlastnosti oboch skupín smerovacích protokolov. Preto sa nedá jednoznačne zaradiť ani do jednej z týchto skupín. Pokladá sa za funkčne bohatí, robustný smerovací protokol napriek tomu je však jeho konfigurácia pomerne veľmi jednoduchá. Medzi nevýhodu však určite patrí jeho proprietárnosť a skutočnosť, že je dostupný iba na zariadeniach firmy Cisco.

3 Cieľ práce

Hlavným cieľom práce je ukázať rôzne metódy smerovania v sieťach IP ako aj zhodnotiť výhody a nevýhody použitia jednotlivých smerovacích protokolov, ktoré pre svoju činnosť využívajú jednotlivé smerovacie algoritmy. To si vyžadovalo splnenie aj čiastkových cieľov v podobe:

- vymedzenie základných rozdielov medzi statickým a dynamickým smerovaním
- preskúmanie spôsobu fungovania hlavných smerovacích algoritmov používaných smerovacími protokolmi
- porovnanie vybraných smerovacích protokolov, ich vývoj, výhody a nevýhody ,činnosť a spôsob komunikácie

4 Metodika práce

Hlavným predmetom skúmania tejto práce boli rôzne metódy smerovania v sieťach IP. Základne rozdiely medzi jednotlivými metódami a ich spôsobe fungovania. Rozobrali sme základné algoritmy smerovania v počítačových sieťach ich činnosť a funkcionalitu. Následne sme si ukázali tri smerovacie protokoly, z ktorých každý implementoval iný druh smerovacie algoritmu. Hlavnou metódou použitou v tejto práci bola komparácia, pomocou ktorej sme sa snažili porovnávať jednotlivé smerovacie metódy, ich algoritmy a protokoly a ukázať ich hlavné výhody a nevýhody, s ktorými sme sa pri spracovávaní problematiky stretli. Zdrojmi pre prácu boli knižné publikácie, predovšetkým publikácia Ip Routing Fundamentals, Mark A.Sportack z vydavateľstva Ciscopress, ale aj iné knižné publikácie , odborné články a špecifikácie. V práci sú pre lepšiu predstavivosť daných problémov použité pri jednotlivých témach obrázky alebo tabuľky.

5 Výsledky práce

Ukázali sme si dva druhy smerovaní. Tým prvým je smerovanie statické, kedy sa vlastne nepoužíva žiaden smerovací protokol a všetky cesty v smerovači musia byť nastavené explicitne a aj explicitne udržiavané v prípade akejkoľvek zmeny v topológie siete alebo výpadku smerovača je sieťový administrátor jediný, ktorý je schopný túto zmenu zaregistrovať a vykonať potrebné zmeny. Statické smerovanie má svoje opodstatnenie a to v hlavne menších sieťach, kde nie sú redundantné linky, a tento druh smerovania sa vyplatí kvôli nulovému zaťaženiu prenosových liniek komunikáciou smerovačov, ale aj minimálnym zaťaženým smerovača a to konkrétne jeho výpočtovej jednotky a využitie pamäte. Statické smerovanie má aj ďalšie výhody a tým je bezpečnosť danej siete. Firmy tak napríklad využívajú jedinú staticky zadefinovanú cestu na pripojenie firmy do siete Internet, ktorá vedie cez zabezpečený server, ktorý kontroluje sieťový prenos v oboch smeroch a poskytuje tak ochranu pred možnými útokmi.

Druhý spôsob je použiť v smerovačoch dynamické smerovanie, ktoré budú zabezpečovať smerovacie protokoly založené na smerovacích algoritmoch. V tejto práci sme rozobrali činnosť troch najbežnejších druhov interných smerovacích protokolov, ktoré využívajú smerovací algoritmus vektora vzdialenosti, stavu linky alebo hybridné smerovanie spojením toho najlepšieho z prvých dvoch.

Smerovacie algoritmy vektora vzdialenosti posielajú svojim bezprostredne okolitým susedným smerovačom pravidelne kópie svojich smerovacích tabuliek. Smerovač po obdržaní tabuľky pripočíta ku každej ceste svoj hodnotu vektora vzdialenosti a opäť ju pošle ďalej bezprostredným susedom. Tento proces prebieha medzi susednými smerovačmi vo všetkých smeroch. Smerovače týmto spôsobom zistia vzdialenosti medzi jednotlivými uzlami v danej sieti. Na konci tohto procesu smerovače skonvergovali a vedie vzdialenosti do jednotlivých uzlov siete, ale nevedia nič o topológií siete ani o susedných smerovačoch. Konvergencia, ktorá je pre smerovanie v sieti vitálne dôležitá, je pri smerovaní s vektorom vzdialenosti ľahko ohroziteľná kvôli časovým stratám pri konvergovaní ako aj celkovo pomalej konvergencií týchto sietí. Problém s konvergenciou spôsobujú havárie liniek alebo smerovačov, kedy sa môžu začať smerovače navzájom klamať a počítať do nekonečna. Vtedy je sieť zraniteľná môže dochádzať k nekonzistnému smerovaniu alebo aj nekonečným slučkám v smerovaní. Ich výhodou je na druhú stranu však ich jednoduchá konfigurácia, údržba a prevádzka. Preto smerovacie

protokoly s vektorom vzdialenosti nájdu svoje uplatnenie iba v menších až veľmi malých sieťach, kde je len málo redundantných ciest a pomerne malé nároky na výkonnosť siete.

Algoritmy stavu linky si na rozdiel od algoritmov s vektorom vzdialenosti vymieňajú komplexné informácie o danej sieti, udržiavajú si databázu s topológiou siete a majú prehľad aj o ostatných smerovačoch v sieti. Tieto informácie si vymieňajú pomocou správ oznámení o zmene stavu linky takzvaných LSA paketov. Jednotlivé smerovače si zo všetkých prijatých paketov LSA vytvoria databázu topologických údajov a následne spustia algoritmus najkratších ciest, ktorý nájde najkratšie cesty do jednotlivých uzlov siete a podľa nich sa potom aktualizuje smerovacia tabuľka. Zmeny v topológii siete spôsobené haváriou alebo pridaným nových zariadení sú rozpoznané vďaka okamžitému rozposlaniu paketov LSA. Tento proces neprebieha periodicky, ale iba v prípade zmeny a neposielajú sa všetky smerovacie informácie, ale signalizuje sa iba zmena. Dochádza tu teda k rýchlej konvergencií a minimálnemu zaťaženiu siete komunikáciou smerovačov, čo je veľký rozdiel oproti smerovaniu s vektorom vzdialenosti, kde sú posielané všetky smerovacie informácie. Namiesto riadenia aktualizácii pevne stanovenými časovačmi sa tu využíva riadenie udalosťami. Smerovanie so stavom linky je preto použiteľné v sieťach ľubovoľnej veľkosti a zaručuje hladký a stabilný chod aj pri nečakaných zmenách v topológii a hlavne rýchlu konvergenciu. Okrem toho poskytuje oveľa lepšiu škálovateľnosť siete ako protokoly s vektorom vzdialenosti alebo staticky nakonfigurované cesty. Aj cez nepopierateľne vynikajúce vlastnosti, funkcie a flexibilitu smerovania stavu linky sa môžeme stretnúť s určitými problémami. A to najme behom prvotnej konvergencie siete, kedy môže v sieti nastať záplava prenosových prostriedkov siete. Tým pádom by zostávala len veľmi mála šírka pásma na prenos sieťových informácií nakoľko by väčšina šírky bola zahltená komunikáciou smerovačov. Aj keď je táto záplava iba dočasná, môže byť však veľmi citeľná. To aký vplyv bude mať záplava na sieť závisí v prvom rade od šírky pásma liniek, pričom pri veľmi malých šírkach je postihnutie záplavou značné. V druhom rade záleží od počtu smerovačov v danej sieti, od ktorých počtu sa odvíja aj množstvo komunikácie. Najhorší prípad teda nastáva ak používame linky s malými šírkami pásma a v sieti pozostáva z veľkého počtu smerovačov. Ďalší problém by niekto mohol vidieť vo zvýšenej záťaži výpočtovej jednotky a pamäte smerovača a treba teda zabezpečiť výkonnejší hardware za vyššie náklady. Týmto problémom sa však dá predísť dobrým návrhom siete. Pred samotným budovaním sa odporúča vypracovať návrh analyzujúci požiadavky, ktoré bude musieť daná sieť spĺňať a tak dosiahnuť optimálne vlastnosti celej siete s ohľadom na budúce rozšírenia danej siete. Ďalšie mínus by mohla byť aj

konfigurácia smerovacích protokolov využívajúcich smerovanie stavu linky, ktoré je hlavne v rozsiahlejších sieťach pomerne zložitý proces a vyžaduje si kompetentných a skúsených sieťových administrátorov. Naopak v smerovacie algoritmy s vektorom vzdialenosti ako aj hybridné smerovacie protokoly sa vyznačujú jednoduchou konfiguráciou.

Ako posledný druh smerovania v sieťach IP sme si ukázali takzvané hybridné smerovanie, ktoré v sebe spája najlepšie vlastnosti z algoritmov stavu linky a vektora vzdialenosti. Protokoly tohto druhu sú preto označované aj ako vyvážené. Miesto konvenčnej metriky, ktorú využívajú protokoly vektora vzdialenosti, používajú rozšírenú a presnejšiu metriku, ktorá lepšie odzrkadľuje vzdialenosť dvoch uzlov ako aj stav linky medzi nimi. Rýchla konvergencia je u tohto druhu smerovania docielená, vďaka vyhýbaniu sa réžii spojenej s pravidelnými aktualizáciami celej smerovacej tabuľky ako v smerovaní s vektorom vzdialenosti. Hybridné smerovanie teda nepracuje s pravidelnými aktualizáciami a namiesto toho je riadené udalosťami, ako smerovanie so stavom linky. Vďaka tomu je väčšina šírky pásma liniek použiteľná pre prenos správ. Hybridné smerovanie potláča všetky nevýhody smerovania so smerovým vektorom a stavu linky. V tejto triede smerovania existujú aj otvorené smerovacie protokoly, no dominantné postavenie tu más protokol EIGRP od firmy Cisco. Jeho proprietárnosť a fakt, že je dostupný iba na smerovačoch od firmy Cisco je určite nevýhoda nakoľko by zariadenia v našej sieti museli byť od jediného výrobcu. Toto však nemusí byť vždy na škodu a niekto by toto samozrejme nemusel považovať za nevýhodu.

Najdôležitejšou úlohou pri návrhu siete je určite výber smerovacieho protokolu. Videli sme tri hlavné druhy smerovacích algoritmov, na ktorých funkcionalite sú postavené smerovacie protokoly. Aby sme sa však vedeli správne porovnať, ktorý smerovací protokol je najvhodnejší a najoptimálnejší pre našu danú sieť, v ktorej by mal byť nasadení, musíme mať určité kritéria výkonnosti, podľa ktorých by sme ich vedeli dobre porovnať. Takýmito kritériami sú napríklad doba konvergencie, ktorá sa nedá presne určiť nakoľko je závislá od rôznych faktorov a jej doba sa teda nedá presne predpovedať. Faktory, ktoré ju ovplyvňujú sú napríklad:

- Vzdialenosť smerovača od miesta zmeny topológie v sieti(počet preskokov)
- Počet smerovačov sieti s dynamickým smerovaním
- Šírka pásma prenosového média a jeho prevádzkové zaťaženie
- Zaťaženie jednotlivých smerovačov

Tieto nedostatky sa dajú znížiť práve dobrým návrhom našej siete a výberom smerovacieho protokolu, ktorý bude optimalizovať potreby našej siete. Ďalším kritériom hodnotenia, od ktorého je priamo závislá aj doba konvergencie je spôsob akým protokol vypočítava cestu. Efektivita výpočtu cesty je následne závisí od ďalších faktorov ako napríklad:

- Množstvo ciest, ktoré si protokol vypočítava a ukladá do jedného cieľa
- Akým spôsobom sú riadené aktualizácie smerovacích informácií
- Aká metrika je použitá na výpočet nákladov alebo vzdialenosti cesty

Niektoré protokoly ako napríklad RIP si ukladajú iba jednu cestu do daného cieľa a to tú najlepšiu. Iné napríklad ako OSPF a EIGRP si uchovávajú viac ciest. Týmto spôsobom si protokoly zabezpečia v prípade možného výpadku linky alebo smerovača okamžitú náhradu za nefunkčnú cestu. To ale spôsobuje zväčšenie objemu smerovacích informácií a využitie väčšieho množstva pamäte smerovača. Treba však podotknúť, že existencia náhradníka za danú cestu nemusí priamo ovplyvniť dobu konvergencie siete, ale aspoň je udržaná konzistentnosť smerovania a prenos informácií nie je prerušený. Konvergencia siete môže nastať aj neskôr.

Spôsob aktualizácie smerovacích údajov je ďalší faktor, ktorý nepochybne zaváži pri vypočítavaní ciest a aj samotnej konvergencie siete. Jednoduché aktualizácie pomocou časovačov sú ľahko implementovateľné aj značne obmedzené a plynú z nich dva dôsledky. Prvým je, že veľká časť aktualizácií bude posielaná zbytočne nakoľko sa posiela aj to čo nie je treba a dochádza k plytvaniu šírky pásma aj prostriedkov smerovača. Druhým dôsledkom je, že vďaka časovačom sa môže zbytočne predlžovať doba konvergencie. Aktualizácie riadene udalosťami sú v tomto prípade určite efektívnejšie a hospodárnejšie ako časovače, pretože konvergencia siete je potrebná iba ak niekde v sieti nastala zmena.

Ďalšou nepochybne podstatnou vlastnosťou smerovacieho protokolu je metrika, ktorú používa na porovnanie vzdialeností ciest medzi danými uzlami. Primitívna vzdialenosť v podobe preskokov medzi uzlami siete, ktorú využíva protokol RIP už dávno nepostačuje čo i len trošku väčším sieťam. Neodzrkadľuje fyzickú vzdialenosť medzi dvoma uzlami ani šírku pásma, ktorá je dostupná. Navyše je zaťažená maximálnym počtom preskokov 16. To určuje aj maximálnu veľkosť siete medzi najvzdialenejšími uzlami siete.

Protokoly so smerovaním na základe stavu linky a hybridné protokoly používajú už podstatne zložitejšie metriky. Výpočty ciest prebiehajú na základe viacerých faktorov ako napríklad:

- Aktuálne zaťaženie siete
- Dostupná šírka pásma
- Odozva pri šírení signálu v prenosovom médiu
- Odhad nákladov pre dané sieťové spojenie(šírka pásma, ktoré poskytuje daná prenosová technológia)

Prehľadné porovnanie smerovacích protokolov podľa typu smerovania, používanej metriky, maximálneho počtu skokov, rýchlosti konvergencie, spôsobu a času aktualizácie a algoritmu, ktorý protokol používa, môžeme vidieť v tabuľke.

Tabuľka 1: Súhrnné porovnanie vlastností protokolov[18]

Protokol	RIP	EIGRP	OSPF
Typ smerovania	vektor vzdialenosti	hybridný	stav linky
Metrika	počet skokov	zložená	náklady(cena)
Maximálny počet skokov	15	224	nie je
Konvergencia	pomalá	veľmi rýchla	rýchla
Čas aktualizácie	30 sekúnd	iba keď nastane zmena	iba keď nastane zmena
Aktualizuje sa	celá tabuľka	iba zmeny	iba zmeny
Algoritmus	Bellman-Ford	DUAL	Dijkstra

[18] Spracované podľa: BALCHUNAS, A. *Routing Protocol Comaparison v 1.01*. 2007 [5]

Záver

V práci sme poukázali na význam smerovania v dnešnom svete počítačových sietí, charakterizovali sme základné smerovacie techniky, algoritmy a protokoly, ktoré sa využívajú v bežnej praxi. Cieľom práce bolo ukázať základné princípy a funkcionalitu, spôsob akým jednotlivé protokoly a algoritmy pracujú, ich výhody a nevýhody. Povedali sme si o dvoch základných spôsoboch smerovania, a to statickom a dynamickom. Ďalej sme sa venovali už iba dynamickému smerovaniu a úlohám, ktoré plní v počítačovej sieti. Následne sme si rozobrali podstatu fungovania smerovacích algoritmov, ktoré používajú rôzne techniky pomocou, ktorých hľadajú cesty v sieti a vyberajú spomedzi nich tú najlepšiu resp. najkratšiu. V práci sme si ukázali algoritmy využívajúce vektor vzdialenosti, stav linky a hybridný smerovací algoritmus. Pokračovali sme smerovacími protokolmi, ktoré v sebe implementujú funkcionalitu smerovacích algoritmov. Konkrétne sme si hovorili o troch smerovacích protokoloch, z ktorých bol každý reprezentantom iného typu smerovacieho algoritmu. Ukázali sme si ako postupujú v procese konvergencie siete. V každej časti textu sme sa pokúsili poukázať na klady a zápory, ktoré daný spôsob smerovania, smerovací algoritmus alebo protokol má a navzájom sme ich porovnávali. Vo výsledkoch práce sme zosumarizovali všetky podstatné informácie na základe ktorých sa dajú jednotlivé smerovacie metódy, algoritmy a protokoly porovnať. Uviedli sme ich podstatné výhody a nevýhody, ktorými disponujú a v akom prostredí je vhodné ich použiť. Výsledky práce poskytujú prierezový pohľad a vystihujú základne problémy, s ktorými sa v problematike v smerovania v sieťach IP môžeme stretnúť.

Použitá literatúra

KNIHY

1) SPORTACK, M. 2004. *Směrování v sítích IP.* Brno: Computer Press, 2004. 351 s. ISBN 80-251-0127-4.
2) ODOM, W. – HEALY, R. – MEHTA,N. 2009. *Směrování a přepínání sítí*. 3.vydanie. Brno: Computer Press, 2009. 879 s. ISBN 978-80-251-2520-5.
3) DIMARZIO, J. 2002. *Sams Teach Yourself Routing in 24 Hours.* QUE Publishing, 2002. 400p. ISBN 0672323648

ELEKTRONICKÉ PRAMENE

4) Cisco Networking Academy CCNA Curriculum 4.0. 2008. [online]. [cit. 20.12.2010] Dostupné na internete: <http://www.cisco.com/web/learning/netacad/index.html>
5) BALCHUNAS, A. *Routing Protocol Comaparison v 1.01*. 2007 [online] [cit. 4.5.2011]
   Dostupné na internete:
   <http://www.routeralley.com/ra/docs/routing_protocol_comparison.pdf>
6) RAZAVI, R. *How Routing Algorithms Work.* [online] [cit. 15.3.2011]
   Dostupné na internete: <http://computer.howstuffworks.com/routing-algorithm2.htm>
7) HEDRICK, C. 1988. *Routing Information Protocol*. 1988 [online] [cit. 15.3.2011] Dostupné na internete: <http://www.faqs.org/rfcs/rfc1058.html>
8) FRIEBE, A. 2009. *OSPF, Part 7.* 2009 [online] [cit. 12.4.2011]
   Dostupné na internete: <http://globalknowledgeblog.com/technology/cisco/routing-switching/ospf-part-7/>
9) DOYLE, J. – CARROLL, J. 2006. *Routing TCP/IP*. [online]. Indianapolis: Cisco Press, 2006. 913 p. [cit. 10.3.2011]
   Dostupné na internete:
   <http://books.google.sk/books?id=JjdF2yWqJAwC&pg=PR4&lpg=PR4&dq=Routing+TCP/IP,+Jeff+Doyle,+Jenniffer+DeHaven+Caroll&source=bl&ots=CeSDoj5xAa&sig=ATjzvleHGNksdRwBNVipdCYd4CQ&hl=sk&ei=nLvDTezfLYOaOsPN7LEE&sa=X&oi=book_result&ct=result&resnum=2&ved=0CCkQ6AEwAQ#v=onepage&q&f=false> ISBN 1-58705-202-4>
10) AZIZ, Z. – LIU, J. – MARTEY, A. – SHAMIM, F. 2004. *Troubleshooting IP Routing Protocols.* [online] Indianapolis: Cisco Press, 2004. 877p. [cit. 5.3.2011]

Dostupné na internete:
<http://books.google.sk/books?id=hlQKDmkJL_wC&printsec=frontcover&dq=Troubleshooting+IP+routing+protocols&hl=sk&ei=xr_DTci9Ls2ZOt7Eic4E&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCoQ6AEwAA#v=onepage&q&f=false>