

Тема № 5. ДИНАМИЧНА МАРШРУТИЗАЦИЯ

Протоколи за динамична маршрутизация – вътрешни (IGP) и външни (EGP); дистанционно-векторни (distance-vector) или следящи състоянието на връзката (link-state).

МАРШРУТИЗИРАНЕ – процесът на придвижване на един пакет с информация от един физически сегмент на мрежата до друг физически сегмент се нарича маршрутизация (routing). Маршрутизирането управлява процеса на изпращане на логически адресираните (от IP протокола) пакети с информация от техния източник до получателя им с помощта на междинни устройства, наричани маршрутизатори (routers).

Маршрутизиращата таблица (routing table or RIB – Routing Information base) представлява структура от данни в табличен вид, в която се съхранява информацията, необходима за маршрутизирането на пакетите в мрежата (Internet). Всеки пакет съдържа информация за неговия източник (source address) и за неговата цел (destination address), а самата маршрутна таблица съдържа следната информация:

1. **Назначение** – IP адресът на следващото местоназначение (следващия hop). Това е (next hop) IP адресът, до който ще се изпрати пакетът;
2. **Метрика** – определя разстоянието до всеки маршрут, така че да може да се избере най-ефективния такъв;
3. **Маршрути** – съдържа директно свързани подмрежи, индиректно свързани подмрежи (такива, които не са директно свързани към възела, но до които може да се достигне през няколко hop-a);
4. **Интерфейс** – изходният мрежов интерфейс, който трябва да се използва за препращане на пакета към крайното му местоназначение.

В маршрутизиращата таблица се поддържа списък на най-добрите маршрути до различни мрежи. За определяне на най-добрия маршрут се използват мерни единици, наречени **метрики**. Те представляват оценка или стойност на даден параметър на мрежовата връзка.

Най-често използвани метрики за оценка на възможните маршрути на изпращане на пакетите са hop count, delay, bandwidth, reliability и communication cost.

Най-често, маршрутизиращите таблици имат следния вид:

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	192.168.11.1	0.0.0.0	UG	1024	0	0	wlp3s0
192.168.11.0	0.0.0.0	255.255.255.0	U	0	0	0	wlp3s0
192.168.122.0	0.0.0.0	255.255.255.0	U	0	0	0	virbr0

Маршрутизиращата таблица се попълва от програмното осигуряване на TCP/IP стека. При инициализацията на маршрутизатора, то автоматично попълва няколко записа в маршрутизиращата таблица, като по този начин се създава така наречената **минимална маршрутизираща таблица**.

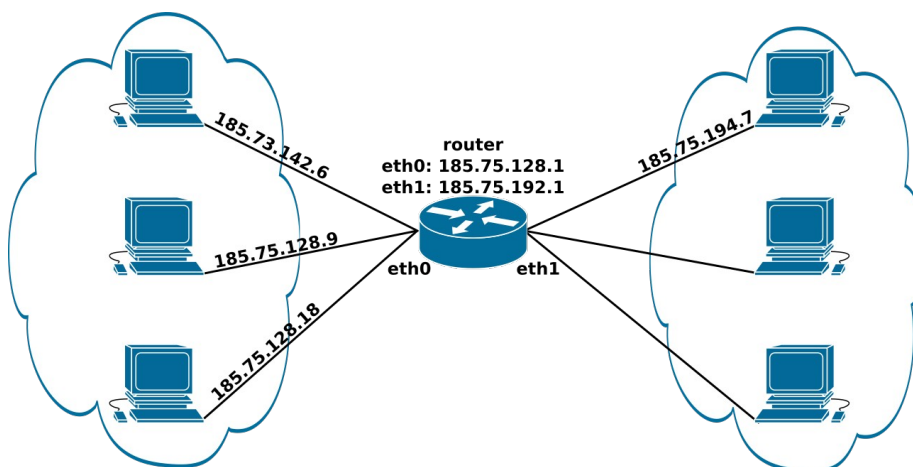
В нея се намират следните записи:

- записите на непосредствено свързаните мрежи и маршрутизатори;
- записите за специалните адреси loopback, multicast и broadcast;
- маршрути към:
 - локалния интерфейс localhost;
 - локална подмрежа;
 - отдалечена подмрежа;
 - multicast адрес;
 - маршрута по подразбиране (default).

Съдържанието на маршрутизиращата таблица може да бъде показано с някоя от командите:

```
# ip route  
# route show
```

Записите имат дървовидна структура, тоест едни записи могат да бъдат включени в други записи. Не е възможно да има частично пресичане. Границите на адресното пространство, в което действат тези записи, се изравняват с неговите размери. Маршрутната таблица се ползва само в случаите, когато трябва да се определи как да бъдат доставени пакетите.



фиг. 1 Примерна топология

Например, маршрутизиращата таблица за H_1 , първият възел, най-горе от лявата мрежа от топологията, показана на фигура 1, ще има следния вид:

Address	Mask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	185.75.128.1	185.75.142.6	20

127.0.0.1	255.0.0.0	127.0.0.1	127.0.0.1	1
185.75.128.0	255.255.224.0	185.75.142.6	185.75.142.6	20
185.73.142.6	255.255.255.255	127.0.0.1	127.0.0.1	20
185.75.255.255	255.255.255.255	185.75.142.6	185.75.142.6	20
224.0.0.0	240.0.0.0	185.75.142.6	185.75.142.6	20
255.255.255.255	255.255.255.255	185.75.142.6	185.75.142.6	1

ДИНАМИЧНО МАРШРУТИЗИРАНЕ

Динамичното маршрутизиране използва маршрутизиращи протоколи за автоматично построяване на маршрутизиращата таблица. При възникване на промяна в топологията на свързване поради отпадане на един или няколко маршрута, маршрутизаторите обновяват своята маршрутна таблица и намират алтернативен път за доставяне на пакетите до тяхното местоназначение. Повечето протоколи за динамично маршрутизиране попадат в един от двата класа – на дистанционно-векторните протоколи ([distance-vector protocols](#)) или на протоколите със следене на състоянието на връзката (link-state). Едни от най-често използваните алгоритми за динамично маршрутизиране са [алгоритъма на Белман-Форд](#) и [алгоритъма на Дийкстра](#).

DISTANCE-ВЕКТОР (С ДИСТАНТЕН ВЕКТОР) ПРОТОКОЛИ

Протоколите с дистантен вектор (distance-vector protocols) най-често използват като мерна единица за оценяване на маршрутите броя преходи (hop count) до крайната цел и са разновидност на алгоритъма на Belman-Ford за изчисляване на маршрутите. При тях:

- маршрутите се анонсират като вектори;
- посока (на маршрута) – адреса на следващия възел (next hop) и интерфейса, през който се излиза;
- метрика (metrics) – броя възли, през които трябва да се премине за да се достигне до местоназначението на пакета (hop count).

Дистанционно-векторните протоколи за лесни за конфигуриране, затова често се използват.

През различни периоди на развитие на Internet са прилагани различни протоколи от този клас, Routing Information Protocol – RIP v1 и RIP v2; Xerox Networking System's RIP – XNS RIP; Novel IPX RIP; Cisco Internet Gateway Routing Protocol – IGRP, DEC DNA Phase IV; Apple Talk Routing Table Maintenance Protocol – RTMP

При поставяне на нов маршрутизатор, използващ дистанционно-векторен протокол за маршрутизиране, той построява и обявява своя маршрутизираща таблица. Всеки маршрутизатор изгражда и поддържа маршрутна таблица, в която всеки ред съдържа адрес на местоназначение, следващата стъпка към това местоназначение по най-добрия засега маршрут и дължината на този маршрут (метриката);

Обща черта на тези протоколи е използването на маршрутизиращ алгоритъм в тях,

който периодично изпраща до всички съседни маршрутизатори обновявания на тяхната маршрутизираща таблица чрез използване на broadcast адрес.

Тези периодични обновявания се изпращат след изтичането на определен период от време, обикновено между 10 (за AppleTalk) и 90 секунди (за Cisco IGRP). Поради твърде малкия интервал на обновяване е възможно при линии с тясна честотна лента (bandwidth) да се получи задръстване на линията. От друга страна, твърде голям интервал на разпращане на обновяванията ще доведе до неприемливо голям период от време, необходим за конвергенция на информацията.

Предимства на тези протоколи

1. лесни за конфигуриране;
2. не товарят паметта и процесора.

Недостатъци:

1. информацията се изпраща само до съседните маршрутизатори (намиращи се в същия физически сегмент), което води до много бавна конвергенция (времето, за което мрежата се приспособява към промените в нейната топология и преизчислява маршрутните таблици);
2. тези периодични изпращания на маршрутните таблици отнемат от честотната лента, предоставяна на потребителите;
3. имат изключително ниска скорост на сходимост на алгоритмите – добрите новини се разпространяват бързо, но лошите достигат прекалено бавно до всички маршрутизатори.

ПРОТОКОЛИ СЪС СЛЕДЕНЕ НА СЪСТОЯНИЕТО (LINK-STATE) НА ВРЪЗКАТА

Тези протоколи носят в себе си маршрутната информация до всички възли в мрежата. Тя съдържа само маршрутите до директно свързаните с маршрутизатора мрежи и тяхното състояние. Предимства на тези протоколи са:

1. намален размер на изпращаната информация, което води до по-ефикасен обмен на данни;
2. могат да използват multicast или unicast адресиране, което също намалява общия мрежови трафик;
3. информацията се предава от маршрутизатор към маршрутизатор, които само я копират, без да я променят.

Динамичните протоколи със следене на състоянието на връзката са базирани на алгоритъма на Дийкстра за намиране на най-късия път (shortest path). Такива протоколи са:

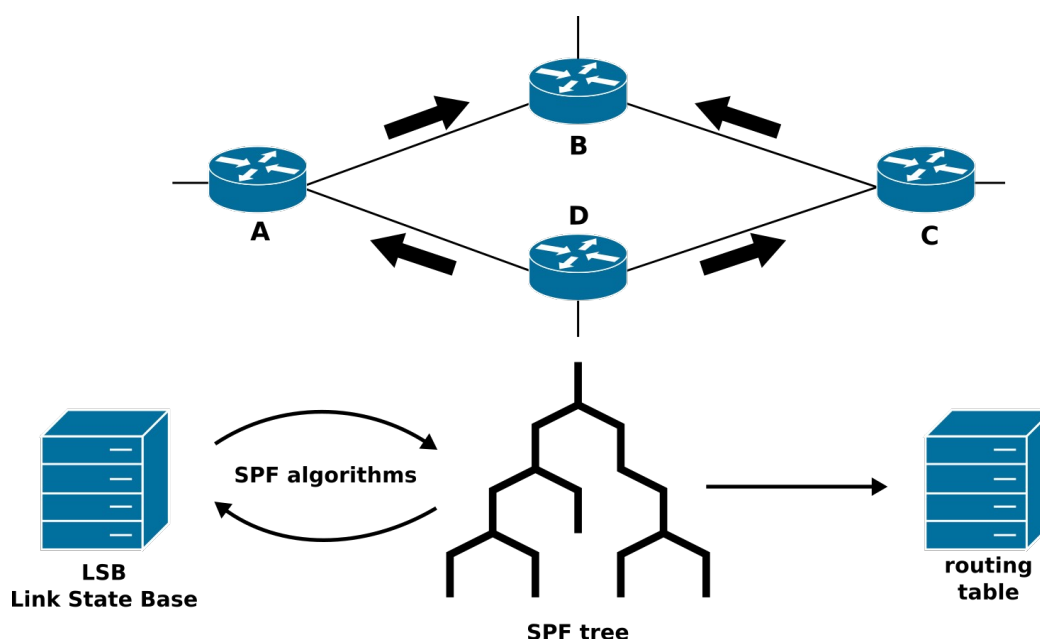
- Open Shortest Path First (OSPF);
- Intermediate System to Intermediate System (IS-IS) на ISO;

- Optimized Link State Routing Protocol (OLSR) – RFC 3626.

Всеки маршрутизатор разполага с пълната топология на мрежата и посредством разновидност на алгоритъма на Дийкстра изчислява най-кратките пътища до всеки възел от мрежата. Поради тази причина, тези алгоритми изискват много повече планиране, конфигуриране, памет и процесорна мощ, отколкото дистанционно-векторните протоколи, но за сметка на това са значително по-мощни и подходящи за използване в големи мрежи.

Протоколите със следене на състоянието на връзката извършват пет основни действия при изчисляването на маршрутната таблица:

1. откриване на съседните маршрутизатори и техните мрежови адреси;
2. измерване на стойностите на връзките до тях;
3. създаване на пакети с информация за състоянието на връзките;
4. изпращане на тези пакети до всички останали маршрутизатори;
5. изчисляване на най-късия път до всеки маршрутизатор в мрежата.



Фиг. 2 Схема на действие на маршрутизиращ протокол със следене на състоянието на връзките

Като краен резултат от горните действия имаме събрана и разпространена до всички маршрутизатори информация за цялата топология на мрежата.

SPF алгоритъм – има за цел да конструира дърво с минимална обща дължина между всичките n възела.

Както вече беше казано преди, динамичните протоколи за маршрутизация се разделят на два класа – вътрешни (интериорни) и външни (екстериорни) протоколи.

1. Вътрешни протоколи – Routing Information Protocol – RIP v1 и RIP v2; Xerox Networking System's RIP – XNS RIP; Novel IPX RIP; Cisco Internet Gateway Routing Protocol – IGRP, DEC DNA Phase IV; Apple Talk Routing Table Maintenance Protocol – RTMP;
2. Външни протоколи – Border Gateway Protocol (BGP).

RIP v1 & RIP v2

RIP v1 – RFC 1058. Routing Information Protocol

RIP v2 – RFC 2453. RIP version 2

Използваната метрика в този протокол е hop count – разстоянието в брой стъпки до местоназначението на изпращания пакет, максималния брой хопове, който може да бъде преминал в една мрежа е 15. За обмен на маршрутна информация при този протокол се използва порт 520 с транспортен протокол UDP (port 520/UDP).

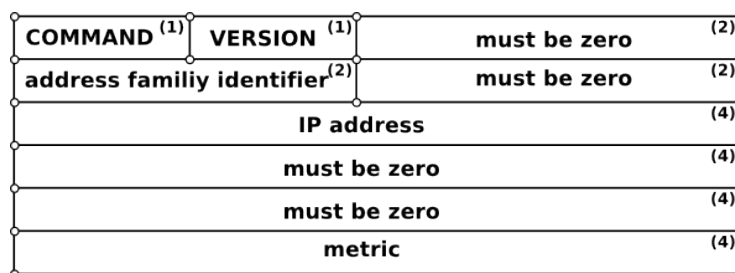
Този протокол е подходящ за използване при малки мрежи, в които относително рядко се правят промени в топологията. Всеки ред от маршрутната таблица съдържа:

- информация за направлението;
- (адресът на) следващата стъпка към това направление;
- метриката.

RIP timers:

1. На всеки 30 sec изпраща копие от маршрутизиращата таблица към съседните маршрутизатори;
2. hold down timer – 180 sec. Това е таймерът за невалиден маршрут;
3. flush timer – съобщение за изтриване на маршрут – пътя се изтрива окончателно от маршрутната таблица.

RIP v1 header



фиг. 3 Формат на заглавната част на RIP пакет

Всеки ред от заглавната част е с дължина 32 бита (4 октета). Размерът на всяко поле е посочен в октети в кръгли скоби, след името на полето. Последните 6 полета (от

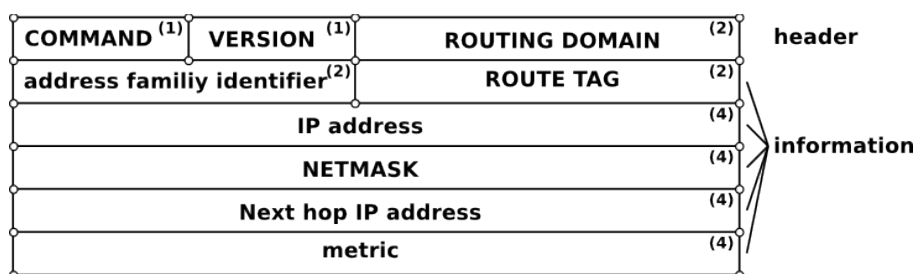
address family identifier до metric) могат да се появят общо 25 пъти в дейтаграмата. IP address е обикновеният 4 октетен internet адрес. Специалният адрес 0.0.0.0 се използва за описване на маршрута по подразбиране (default route). Идентификатора на адресното семейство за IP протокола е 2. Полето за метрика трябва да съдържа стойност между 1 и 15, определяйки текущата метрика за маршрута или да съдържа 16, ако местоназначението е недостъпно. Максималният размер на дейтаграмата на един RIP пакет е 512 октета (IP и UDP заглавните части не се броят). Всяка дейтаграма съдържа команда, номер на версия и възможни аргументи. Когато трябва да се маршрутизира дейтаграма, първо нейният адрес на местоназначение се проверява в списъка с възли на мрежи за да се провери дали съвпада с някоя позната подмрежа или номер на мрежа. Ако няма съвпадение при тези проверки, дейтаграмата се изпраща по маршрута по подразбиране.

RIP v1 не поддържа мрежови маски, респективно безкласова адресация (CIDR). В полетата, означени с етикет „address“ могат да се съдържат следните стойности:

1. адрес на възел от мрежа;
2. номер на подмрежа;
3. номер на мрежа;
4. 0, ако пакета ще се изпраща по подразбиращия се маршрут.

RIP v2

Заглавната част на протокола RIP v2 има следния вид:



фиг. 4 Заглавна част от дейтаграма на протокола RIP v2

И тук информацията от последните 6 полета може да се повтори 25 пъти в една дейтаграма. Ако таблицата е по-голяма, тогава се попълват няколко RIP v2 пакета.

Полето **command** указва дали пакетът съдържа заявка или отговор.

Полето **version** указва версията на протокола.

Полетата **routing domain** и **routing tag** не се изпълват в първата версия на протокола RIP и се запълват с 0.

Полето **address family** се попълва с 2, ако следва IP адрес или се попълва с 0, ако следва заявка за цяла маршрутна таблица.

Протоколът RIP v1 изпраща цялата информация на съответния broadcast адрес на

мрежата, докато при втората версия на протокола, RIP v2, информацията се изпраща на multicast адрес 224.0.0.9.

RIPng (RFC 2080) е разширение на RIP v2, което поддържа протокола IPv6.

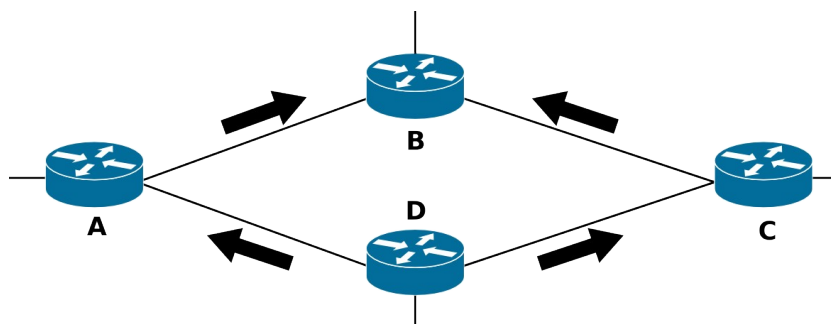
ПРОТОКОЛ OSPF

RFC 2328 – OSPF v2 за IPv4

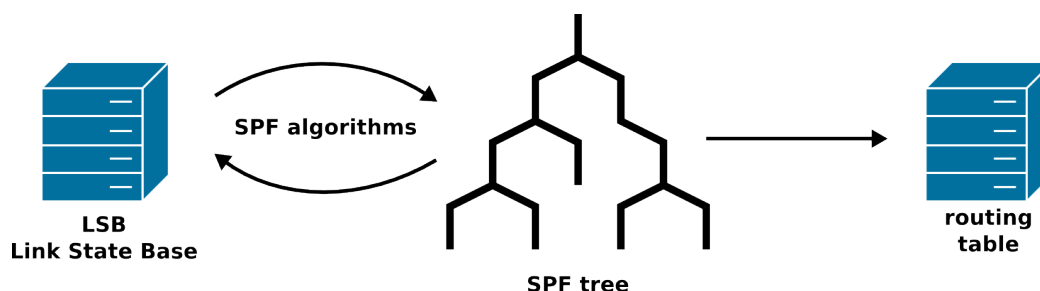
- динамичен протокол за маршрутизация;
- със следене състоянието на връзката;
- за вътрешна маршрутизация в автономни системи;
- OSPF – използва се в големи корпоративни мрежи; IS-IS се използва обикновено от доставчици на Internet; OLSRP – използва се за мобилни и безжични мрежи

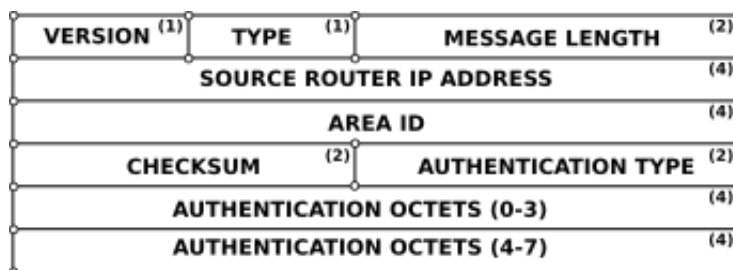
ХАРАКТЕРИСТИКИ

- топология – граф, възлите на който са маршрутизаторите, а клоните – комуникационните връзки между тях.



- на клоните се присвояват стойности, обратно-пропорционални на скоростта на линиите => по-бързата връзка има по-малка стойност;
- с помощта на алгоритъма на Дийкстра се изчислява „дървото на най-късия път“ (shortest path tree) по най-ниската стойност за всеки маршрут;
- информацията за състоянието на връзката се поддържа на всеки маршрутизатор под формата на база от данни LSDB – LinkState DataBase – мрежова топология и пълния граф на мрежата.



OSPF header

фиг. 5

Протоколът OSPF ...

ПРОТОКОЛ BGP

RFC 1771 – дефинира актуалната, 4^{-та} версия на протокола.

Border Gateway Protocol (BGP) е основният протокол за маршрутизация в Internet. Поддържа таблица от IP мрежи (префикси), които определят достижимостта на мрежите между автономните системи. BGP е протокол с вектор на пътищата ([path vector protocol](#)). Той е динамичен протокол за маршрутизация и не поддържа метриката, използвана от вътрешните протоколи за маршрутизиране, а взема решението за определяне на маршрута на основата на пътя между отделните автономни системи и възприетите мрежови политики и правила за маршрутизиране. Актуалната версия на протокола е версия 4, която поддържа безкласова адресация (CIDR) и обединяването (агрегация) на маршрути, с което се намалява размера на самите маршрутни таблици. Последната версия на протокола (BGP 4/4+) е стандартизирана в RFC 4271.

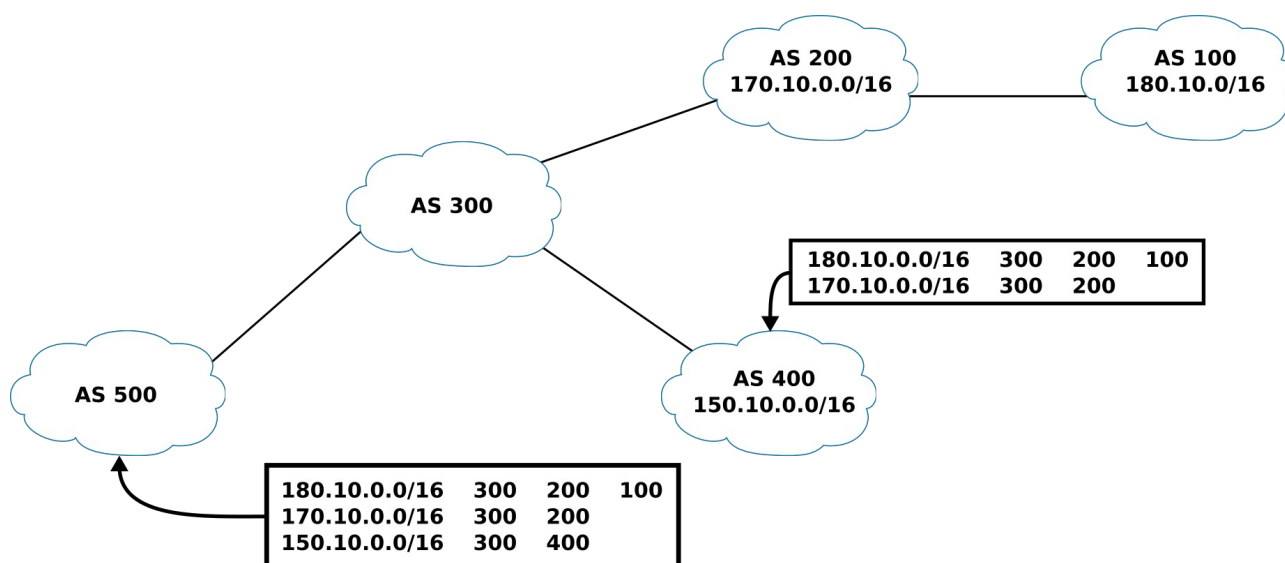
Основен протокол. Използва се при:

1. наличие на множество изходни точки, свързани към един доставчик на Internet;
2. наличие на множество маршрути през различни доставчици и нужда от управление на трафика, изпращан по тези връзки;
3. нужда от интелигентно управление на маршрутизацията в нашата мрежа, надхвърляща използването на маршрут по подразбиране;
4. ако мрежата ни се използва за транзит на трафик от други мрежи;

Съществуват 4 типа BGP маршрутизатори:

1. BGP маршрутизатори говорители – обикновените маршрутизатори, работещи с протокол BGP, без конфигурирани по тях специализирани функции;
2. Равноправни (съседни) BGP маршрутизатори – такива са свързаните към общ сегмент от мрежата маршрутизатори;
3. Вътрешни равноправни BGP маршрутизатори – равноправни възли в една автономна система;

4. Външни равноправни BGP маршрутизатори – съседни BGP маршрутизатори от различни автономни системи.



Съседните BGP маршрутизатори (neighbors или peers) се задават ръчно в конфигурационните файлове. Между тях се установява сесия по протокола TCP на порт 179. Всеки BGP възел периодично изпраща до своите съседи 19-байтови съобщения (keep-alive packets) за поддържане на връзката между тях. Протоколът BGP е единствен между маршрутизиращите протоколи, който използва като транспортен протокол TCP, което до някаква степен го прави и приложен протокол. След като се установи TCP сесия между съседните BGP маршрутизатори, те обменят маршрутната информация помежду си. Може да бъде обменена пълната маршрутната таблица или част от нея – това зависи от сключените споразумения между отделните автономни системи, от прилаганите политики или филтри в тях и тен. При промяна в маршрутната таблица, BGP маршрутизаторите изпращат на съседите си само променените маршрути. При протокола BGP не се изпращат периодични обновления (routing updates) и се обявява (advertise) само оптималния маршрут до дадено местоназначение.

BGP атрибути

BGP атрибутите са характеристики, използвани от BGP маршрутизаторите за определяне на най-добрия път до дадено местоназначение.

1. Тежест (weights);
2. локален приоритет (local preferences);
3. метричен атрибут (metric atribut или MED – Multi-Exit Discriminator);
4. Източник (origin);
5. Път към AS (AS_Path);
6. Следващ скок (next hop);
7. Общност (community).

Критерии за избор на маршрут

Критериите се сравняват по реда, в който са написани:

1. ако пътят води към следващ скок (next hop), който е недостъпен, той се отхвърля;
2. предпочитат се маршрути с най-голяма тежест;
3. при еднакви тежести на маршрутите се предпочитат тези с най-голям локален приоритет;
4. при еднакви локални приоритети се предпочитат маршрути, които са с BGP източник, изпълняван на дадения маршрутизатор;
5. ако няма маршрути, които да са с BGP източник на дадения маршрутизатор, тогава се предпочитат маршрути с най-къс списък на атрибута AS_path;
6. при еднакви атрибути AS_path се избира маршрут, имащ по-нисък ранг на тип източник (IGP имат по-нисък ранг от EGP, а EGP имат по-нисък ранг от incomplete);
7. при еднакви рангове на източниците се предпочитат пътища с най-малък MED атрибут;
8. ако атрибутът MED е еднакъв – предпочитат се външните маршрути пред вътрешните;
9. Ако все още маршрутите са равнопоставени, тогава се избира маршрут през най-близкия IGP съсед.

QUAGGA ROUTING SUITE

IPv4	IPv6	
zebra		-- kernel interface, static routes; zserv serv;
ripd	ripngd	-- RIPv1/RIPv2 за IPv4; RIPng за IPv6
ospfd	ospf6d	-- OSPF v2 и OSPF v2;
bgpd		-- BGP v4+;
isisd		-- IS-IS protocol за IPv4 и IPv6;
babeld		-- BABEL wireless mesh routing;
olrdsd		-- OLSR wireless mesh routing;
ldpd		-- MPLS Label Distribution Protocol'
bfdd		-- Bidirectional Forwarding Detection'

Quagga предоставя поддръжка на OSPFv2, OSPFv3, RIPv1 и v2, RIPng и BGP4 за Unix, Linux etc.

Архитектурата quagga съдържа основен демон – zebra, който служи като абстрактно ниво на лежащите под него ядро на linux и предоставя API на zserv върху Unix или TCP поток на клиентите на quagga.

Демоните на quagga се конфигурират през командна интерфейс (CLI), наречен vty. Има и допълнителен инструмент – vtysh, действащ като frontend към тези демони.

```
yum install quagga
```

```
setsebool -P zebra_write_config 1
```

тази команда е само за centos 7. указва на selinux да позволява на демона zebra да записва конфигурацията си

```
cp /usr/share/doc/quagga-xxxxx/zebra.conf.sample /etc/quagga/zebra.conf
```

```
service zebra start
```

```
chkconfig zebra on
```

```
vttysh
```

промпта се променя на:

```
site_A-RTR#
```

```
site_A-RTR# configure terminal
```

тук конфигурираме дневника на маршрутизатора

```
site_A-RTR# log file /var/log/quagga/quagga-log
```

