ENCAMINHAMENTO NA INTERNET

No início havia a ARPANET e a SATNET e emergiu a Internet. A Internet funcionava como uma única rede que interligava computadores em centros de investigação e algumas redes locais. Os routers tinham o nome de gateways e a troca da informação de encaminhamento era feita através do protocolo GGP (Gateway to Gateway Protocol).

O GGP consistia num algoritmo distribuído shortest path em que as tabelas de encaminhamento continham o número mínimo de saltos entre a própria gateway e todas as outras da rede e esta informação era trocada entre as gateways vizinhas.

Com o aumento do número de gateways aumentava também a dimensão da tabela de encaminhamento, o número de actualizações, o número de quebra de linhas e o número de gateways a desligarem e ligarem. Tudo isto influenciava o aumento de comunicação entre as gateways para se adaptarem a cada uma das alterações.

Outro aspecto importante foi a crescente diversidade de construtores de equipamento e as gateways começaram a serem diferentes umas das outras. Isto dificultava a manutenção e a tolerância a falhas. Outra dificuldade é a de qualquer alteração no protocolo te agora de ser efectuada por muitas pessoas em diversas empresas, o que nem sempre é fácil de conciliar, por isso cada alteração a ser feita no protocolo teria de ser muito significativa.

Como o modelo de rede única não servia decidiu-se adoptar um modelo hierárquico. A Internet foi dividida entre diversos Sistemas Autónomos com a atribuição de um número único a cada um desses sistemas. A Arpanet e Satnet foram incluídas no mesmo Sistema Autónomo e passaram a ser conhecidas como o Core, que servia de espinha dorsal a toda a rede. Os restantes Sistemas Autónomos eram chamados de Stubs (toco) e ligavam directamente ao Core. A comunicação entre os diversos Stubs era feita através do Core. Os nós que interligavam Sistemas Autónomos distintos eram chamados de gateways externas. Como estas gateways necessitavam de trocar informação foi criado o EGP, Exterior Gateway Protocol. Os nós dentro do mesmo Sistema Autónomo eram chamados de gateways internas e o protocolo de comunicação entre elas foi chamado de IGP, Interior Gateway Protocol.

Em 1982 a IGP escolhida era equivalente ao GGP anterior à divisão da Internet em Sistemas Autónomos. Neste início do século XXI o termo IGP significa uma classe de protocolos dos quais os mais conhecidos são o RIP, OSPF e IGRP. O termo EGP significa uma classe de protocolos dos quais o EGP é um protocolo que tem uma forte concorrência com o BGP-4 (Border Gateway Protocol versão 4) que é neste momento o EGP preferido.

Sistemas Autónomos

A Internet é um conjunto de sistemas autónomos interligados cada um deles com o seu algoritmo de encaminhamento e gestão. Um Sistema Autónomo (Autonomous System – AS) na Internet é um conjunto de redes IP sob a gestão de uma única identidade como por exemplo um Internet Service Provider (ISP) ou uma organização muito grande com diversas ligações redundantes à Internet.

É atribuído um endereço AS único a cada sistema autónomo para uso no encaminhamento BGP (Border Gateway Protocol). Este endereço é atribuído pela mesma autoridade que atribui os endereços IP (Internet Assigned Numbers Authority - IANA). Os endereços AS são a 16 bits e dividem-se em públicos, de 1 a 64511 (0001-FBFF) e privados de 64512 a 65535 (FC00-FFFF) que podem ser usados dentro da própria instituição.

Há diversos tipos de sistemas autónomos Multihomed AS, Stub AS e Transit AS.

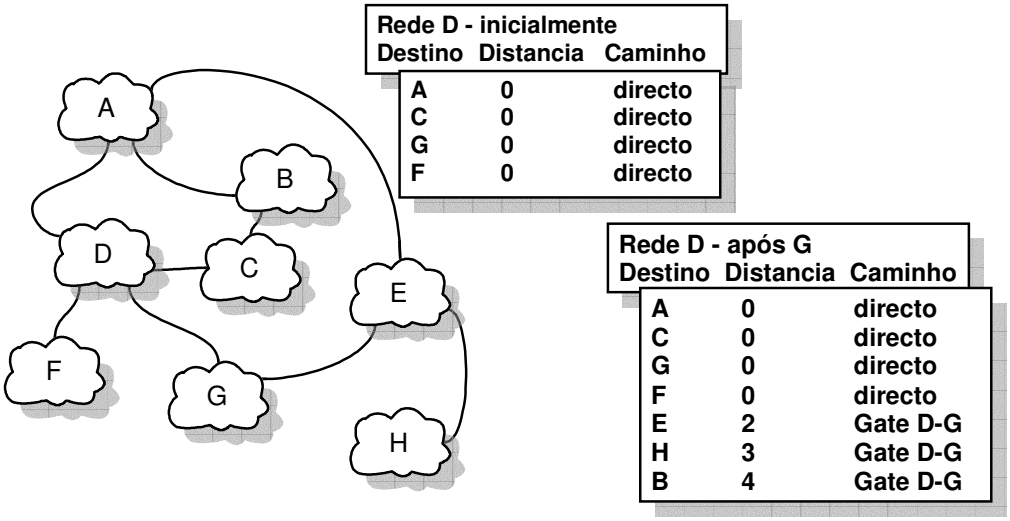
Stub AS – Os Sistemas Autónomos que estão ligados à Internet através de um único ponto de saída. Também são chamados de “single-homed”

Transit AS – São Sistemas Autónomos Multihomed que permitem tráfego originário fora desse Sistema Autónomo poder passar através dele para outro Sistema Autónomo diferente. Os ISP são sistemas deste tipo. O contrário deste tipo de sistemas são os Non-Transit AS que não permitem tal tráfego.

Multihomed AS – Sistemas Autónomos que estão ligados a dois ou mais ISP, Transit AS.

Existem diversos protocolos de encaminhamento dentro de um sistema autónomo, no interior, com um seu equivalente para o exterior. São classificados como IGP (Interior Gateway Protocol) e EGP (Exterior Gateway Protocol).

GGP – Gateway to Gateway Protocol



Rede D - inicialmente

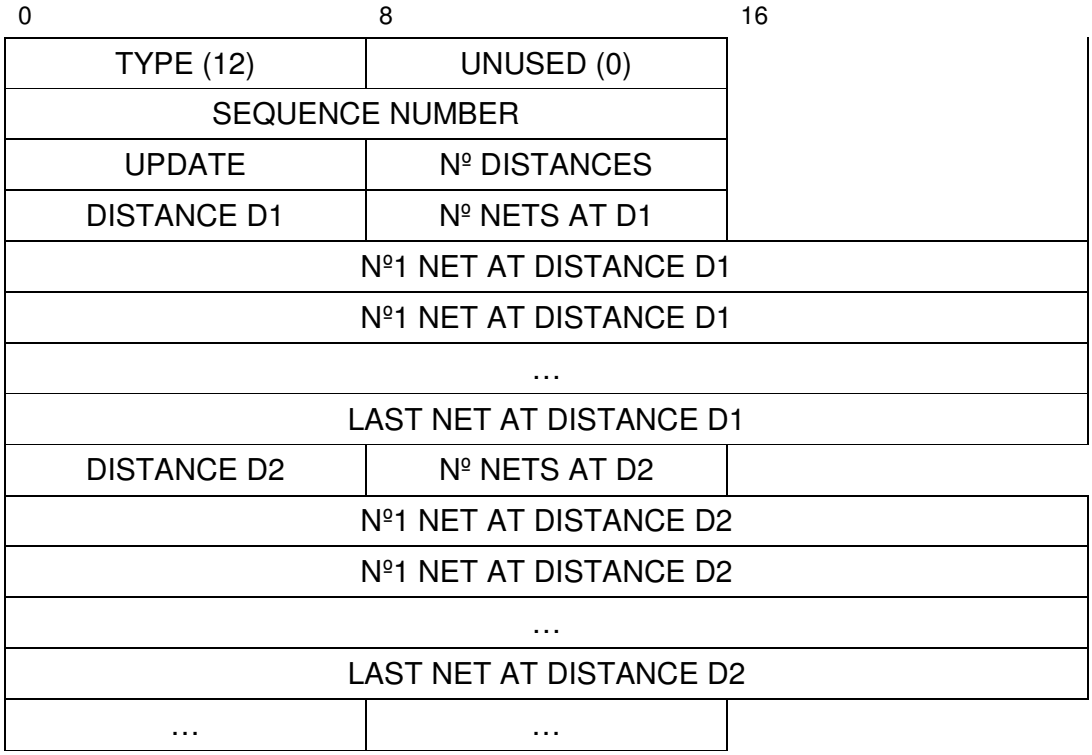
Destino	Distancia	Caminho
A	0	directo
C	0	directo
G	0	directo
F	0	directo

Rede D - após G

Destino	Distancia	Caminho
A	0	directo
C	0	directo
G	0	directo
F	0	directo
E	2	Gate D-G
H	3	Gate D-G
B	4	Gate D-G

- Facilidade de expansão de gateways
- Distancia medida em saltos (HOPS)
- Faz publicidade acerca das redes que consegue alcançar e preço
- Resposta a alterações na topologia é muito demorada
- Mensagens
  - Routing Update
  - Positive Acknowledge
  - Negative Acknowledge
  - Echo Request
  - Echo Reply
- A troca de conhecimento tende a aumentar cada vez mais a troca de informação
- Todas as gateways entram na conversa
- Encaminhamento
  - As gateways trocam informação de estado das ligações
  - Cada gateway tem um conhecimento global da topologia
  - Uma alteração obriga a recalcular os caminhos mais curtos (Dijkstra)
  - O algorítmo converge
- Deixou de ser utilizado em 1988 no núcleo principal da Internet

Formato do pacote GGP para a troca de informação de encaminhamento entre os nós, gateways, da rede.



Interior Gateway Routing Protocols

As Gateways interiores podem ser configuradas de um modo manual ou automático. Em qualquer dos casos é necessário que reajam a alterações de topologia, que possam suportar diversos protocolos de encaminhamento porque alguns são incompatíveis entre si e as gateways podem ser de fabricantes distintos.

Das implementações existentes de protocolos de encaminhamento interno temos o RIP, HELLO e OSPF.

RIP

O RIP foi desenvolvido pela Xerox Corporation no inicio dos anos 80 para ser utilizado nas redes Xerox Network Systems (XNS). É o protocolo intra domínio mais comum, sendo suportado por praticamente todos os fabricantes de routers e disponível na grande maioria das versões do UNIX.

Um das vantagens é a facilidade de configuração. O algoritmo não necessita de grande poder de computação ou capacidade de memória nos routers ou computadores.

O protocolo RIP funciona bem em pequenos ambientes, porem apresenta serias limitações quando utilizado em redes grandes. Limita o número de saltos entre hosts a 15 (16 é considerado infinito). O protocolo converge lentamente, ou seja, leva relativamente muito tempo para que alterações na rede fiquem conhecidas por todos os nós. Esta lentidão pode causar loops de encaminhamento, por causa da falta de sincronismo nas informações dos nós.

O protocolo RIP é também um grande consumidor de largura de banda, pois, a cada 30 segundos, faz um broadcast da sua tabela de encaminhamento, com informações sobre as redes e sub-redes que alcança.

O RIP determina o melhor caminho entre dois pontos, levando em conta somente o número de saltos (hops) entre eles. Esta técnica ignora outros factores que fazem diferença nas linhas entre os dois pontos, como: velocidade, utilização das mesmas (tráfego) e outras métricas que podem fazer diferença na determinação do melhor percurso entre dois pontos.

Ao iniciar o protocolo RIP o nó envia um pedido para actualizar as informações de encaminhamento e aguarda as respostas. Os sistemas já

configurados respondem com as suas tabelas de encaminhamento. A tabela de encaminhamento de cada nó é enviada com uma determinada frequência.

São acrescentados novos nós, e ligações, as métricas são alteradas e também se eliminam nós e ligações de modo a garantir uma visão mais real da topologia.

Existem duas maneiras de remover nós e ligações. A primeira acontece quando o gateway para um destino indica que o percurso possui mais do que 15 saltos. A segunda é o RIP assumir que uma gateway não está operacional se ela não enviar informações de actualização durante um período excessivo de tempo.

- Vector - distance algorithm
- Máquinas Passivas - escutam publicidade das gateways
- Máquinas Activas - escutam e enviam publicidade das gateways
- Distancia é em saltos (HOPS)
- Duas máquinas directas, estão à distância de um salto
- Número Máximo de saltos 16
- Não detecta loops
- UNIX – routed (realização do protocolo RIP no sistema 4BSD UNIX)
- Guardam-se sempre os melhores caminhos evita oscilações entre caminhos com a mesma distancia
- Troca de informação de 30 em 30 segundos
- Esquece um caminho se não souber nada, após 180 segundos
- Split Horizon Update - Alterações não vão por onde vieram
- Boas notícias voam, as más arrastam-se

IGRP (Interior Gateway Routing Protocol)

O IGRP também foi criado no inicio dos anos 80 pela Cisco Systems Inc., detentora de sua patente. O IGRP resolveu grande parte dos problemas associados ao uso do RIP para encaminhamento interno.

O algoritmo utilizado pelo IGRP determina o melhor caminho entre dois pontos dentro de uma rede examinando a largura de banda e o atraso das redes entre nós. O IGRP converge mais rapidamente que o RIP, evitando loops de encaminhamento, e não tem a limitação de 15 saltos entre nós.

Com estas características, o IGRP viabilizou a implementação de redes grandes, complexas e com diversas topologias.

EIGRP (Enhanced IGRP)

A Cisco aprimorou ainda mais o protocolo IGRP para suportar redes grandes, complexas e criticas, e criou o Enhanced IGRP.

O EIGRP combina protocolos de encaminhamento baseados no Distance-Vector Routing com os mais recentes protocolos baseados no algoritmo de Link-State. Diminui o tráfego entre nós por limitar a troca de informações de encaminhamento àquilo que foi alterado.

Uma desvantagem do EIGRP, assim como do IGRP, é que ambos são de propriedade da Cisco Systems, não sendo amplamente disponíveis fora dos equipamentos deste fabricante.

HELLO

Este protocolo usa uma métrica de encaminhamento baseada em atrasos e não em contadores de hops.

O protocolo HELLO provê duas funções: a sincronização dos relógios de um conjunto de equipamentos e o cálculo pelos equipamentos participantes dos caminhos de menor atraso. As mensagens HELLO trazem consigo marcas de tempo, ou timestamps, além das informações de encaminhamento propriamente ditas.

A ideia básica do HELLO é simples: cada equipamento participante mantém uma tabela da sua melhor estimativa do relógio das máquinas vizinhas. Antes de transmitir um pacote, a máquina adiciona a sua marca de tempo através da cópia do valor corrente do seu relógio. Quando um pacote chega, o receptor calcula o atraso da ligação. Para isso, o receptor subtrai a marca de tempo contida no pacote recebido do valor corrente estimado para o relógio do vizinho. Periodicamente, as máquinas fazem um polling aos vizinhos para restabelecer as estimativas dos relógios.

O protocolo Hello é utilizado em redes distribuídas (DCN -Distributed Computer Network) e em redes locais. Nas redes distribuídas o encaminhamento de datagramas é determinado completamente por endereços Internet. Cada host contém duas tabelas:

Tabela de Hosts, que é usada para determinar a ligação para cada um dos outros hosts na rede local.

Tabela da Rede, que é usada para determinar o gateway para cada uma das outras redes locais. Esta tabela contém uma entrada para cada uma das redes vizinhas que podem estar ligadas à rede local, ocasionalmente também entradas de outras redes que não são vizinhas. Cada entrada contém o número da rede, assim como também o identificador do gateway que liga a essa rede.

A função do encaminhamento é apenas a de procurar o número da rede na tabela da rede, e encontra a identificação da gateway, depois devolve a identificação da porta do processo de saída da rede da tabela de hosts.

- Métrica é o tempo de trânsito
- Sincroniza os relógios
- Cada máquina calcula os melhores caminhos
- A troca de informação baseia-se em timestamp e routing
- Para evitar oscilações, só se altera os caminhos utilizados se a diferença de tempo for grande
- Juntando EGP, RIP e Hello, e algumas regras, obtém-se o gated – UNIX (suporta diversos protocolos e não apenas o RIP)

OSPF

Foi desenvolvido pelo IETF (Internet Engineering Task Force) como substituto para o protocolo RIP. Caracteriza-se por ser um protocolo intra domínio, hierárquico, baseado no algoritmo Link-State e foi especificamente projectado para operar com redes grandes. Outras características do protocolo OSPF são:

• A inclusão de encaminhamento por tipo de serviço (TOS - type of service routing). Por exemplo, um acesso FTP poderia ser feito por um link de satélite, enquanto que um acesso a um terminal poderia evitar este link, que tem um grande tempo de atraso, e ser feito através de outra ligação;

• O fornecimento de balanceamento de carga, que permite ao administrador especificar múltiplos percursos com o mesmo custo para o mesmo destino. O OSPF distribui o tráfego igualmente por todas as rotas;

• O suporte de percursos para hosts, sub-redes e redes especificas;

• A possibilidade de configuração de uma topologia virtual de rede, independente da topologia das ligações físicas. Por exemplo, um administrador pode configurar um link virtual entre dois nós mesmo que a ligação física entre eles passe através de uma outra rede;

• A utilização de pequenos "hello packets" para verificar a operação dos links sem ter que transferir grandes tabelas. Em redes estáveis, as maiores actualizações ocorrem uma vez em cada 30 minutos.

O protocolo ainda especifica que todos os anúncios entre nós sejam autenticados (nem sempre é). Permite mais de uma variedade de esquema de autenticação e que diferentes áreas de encaminhamento utilizem esquemas diferentes de autenticação;

Duas desvantagens deste protocolo são a sua complexidade, e maior necessidade de memória e poder computacional, característica inerente aos protocolos que usam o algoritmo de Link-State.

O OSPF suporta, ainda, encaminhamento hierárquico de dois níveis dentro de um Sistema Autónomo, possibilitando a divisão do mesmo em áreas de encaminhamento. Uma área de encaminhamento é tipicamente uma colecção de uma ou mais sub-redes intimamente relacionadas. Todas as áreas de encaminhamento precisam de estar ligadas ao backbone do Sistema Autónomo, no caso, a Área 0. Se o tráfego necessitar de atravessar duas áreas, os pacotes são primeiramente encaminhados para a Área 0 (o backbone). Isto pode não ser eficiente, uma vez que não há encaminhamento inter áreas enquanto os pacotes não alcançam o backbone. Chegando à Área 0, os pacotes são encaminhados para a Área de Destino, que é responsável pela entrega final. Esta hierarquia permite a consolidação dos endereços por área, reduzindo o tamanho das tabelas de encaminhamento. Redes pequenas, no entanto, podem operar utilizando uma única área OSPF.

- Divulgado de modo a não ser necessário pagar direitos
- Escolhe tipo de serviço
- Fiável
- Rápido
- Distribuição de tráfego (load balancing)

- As redes podem ser divididas em sub-redes; áreas
- Troca de informação entre gateways é autenticada
- Host-specific e network-specific routes
- Utiliza o SPF - Shortest Path First
- Conceito de designated-gateway e utilização de broadcast
- Diminui número de mensagens
- Permite ligações virtuais entre gateways, ainda que não coincidam com as físicas
- Divulga informação que foi adquirida externamente

Exterior Gateway Routing Protocols

Das implementações existentes de protocolos de encaminhamento externo temos o EGP (Exterior Gateway Protocol) e o BGP.

EGP - Exterior Gateway Protocol

- As alterações propagam-se
- Saber se um vizinho está vivo: por tentativas
- Alterações contínuas levam a destabilizar algoritmos de vector-distance
- Não interpreta as distâncias recebidas pelo routing update

  não pertencem ao mesmo sistema autónomo
- Apenas são divulgadas as redes que são totalmente atingíveis dentro desse sistema autónomo
- Restringe a topologia a uma árvore sem ligações adicionais entre sistemas autónomos
- Conectividade universal falha caso o núcleo principal falhe
- Só se utiliza um caminho entre sistemas autónomos
- Dificuldade na escolha de caminhos alternativos

0	8	16	24
VERSION	**TYPE (1)**	**CODE (0)**	STATUS
CHECKSUM		AUTONOMOUS SYSTEM Nº	
SEQUENCE NUMBER		**Nº INT. GATEWAYS**	**Nº EXT. GATEWAYS**
IP SOURCE NETWORK			
GATEWAY 1 IP ADDRESS (sem prefixo de rede)			
Nº DISTANCES			
DISTANCE D11	Nº NETS AT D11		
NETWORK 1 AT DISTANCE D11			
NETWORK 2 AT DISTANCE D11			
…			
DISTANCE D12	Nº NETS AT D12		
NETWORK 1 AT DISTANCE D12			
NETWORK 2 AT DISTANCE D12			
…			
…			
GATEWAY n IP ADDRESS (sem prefixo de rede)			
Nº DISTANCES			
DISTANCE Dn1	Nº NETS AT Dn1		
NETWORK 1 AT DISTANCE Dn1			
NETWORK 2 AT DISTANCE Dn1			
…			

Os campos Type e Code geram os seguintes mensagens EGP:

⇒ Neighbor acquisition
- Acquisition Request - pede a um nó para ser vizinho
- Acquisition Confirm - confirmação do nó que aceita o convite
- Acquisition Refuse - o nó (a gateway) recusa o convite
- Cease Request - terminar a relação de vizinho
- Cease Confirm - aceita, confirma, o fim da relação

⇒ Neighbor reachability
- Hello - Está aí alguém ? Confirma a relação!
- I Heard You - Olá cá estou eu! Relação confirmada.

⇒ Routing Update
- Poll Request - pede tabela de encaminhamento
- Routing Update - envia a tabela (network reachability)

⇒ Error Response
- Error - resposta a uma mensagem incorrecta

O campo de STATUS tem o seguinte significado:

0 – Indeterminado

1 – Operacional

2 – Inactivo

O bit mais significativo (+128) indica mensagem não solicitada

A utilização do EGP como protocolo externo de comunicação entre gateways tornou-se inadequada devido aos seguintes factos:

⇒ Falta de Autenticação. É fácil difundir informação errada de encaminhamento, por descuido de configuração, do protocolo ou por malícia.

- ⇒ Falta de política de encaminhamento. O uso da distância mínima como métrica não introduz no encaminhamento alterações de tráfego ou outra
- ⇒ Loops de encaminhamento e topologia. O EGP foi desenhado inicialmente para uma topologia simples, tipo árvore, e torna-se impraticável com as estruturas complexas usadas hoje com muitas malhas.
- ⇒ Dimensão da mensagem e fragmentação. A troca de informação entre nós implica a transmissão de muita informação, de uma tabela de encaminhamento muito grande. Esta dimensão superou a dimensão dos datagramas e por isso necessita de ser fragmentada. Como é o IP que faz a fragmentação e o agrupar da informação só é feito com todos os fragmentos presentes, a probabilidade de perder informação é grande o que provoca retransmissões.

Em Junho de 1989 foi criado o BGP do qual a versão 4 é a que se utiliza presentemente.

BGP – Border Gateway Protocol

O BGP (Border Gateway Protocol) é um dos protocolos de encaminhamento centrais da Internet. Mantém uma tabela de endereços IP que relaciona a atingibilidade entre sistemas autónomos, e considera-se um protocolo tipo path vector. De modo a diminuir a dimensão das tabelas de encaminhamento organiza a rede em agregados, em classes de rede. Este protocolo também pode ser utilizado dentro de grandes instituições privadas, ou no agrupar de diversas redes OSPF (Open Shortest Path First).

Os utilizadores terminais da Internet não utilizam o BGP, mas os ISP (Internet Service Provider) têm de o utilizar. Por isso o BGP é um dos protocolos mais importantes da Internet.

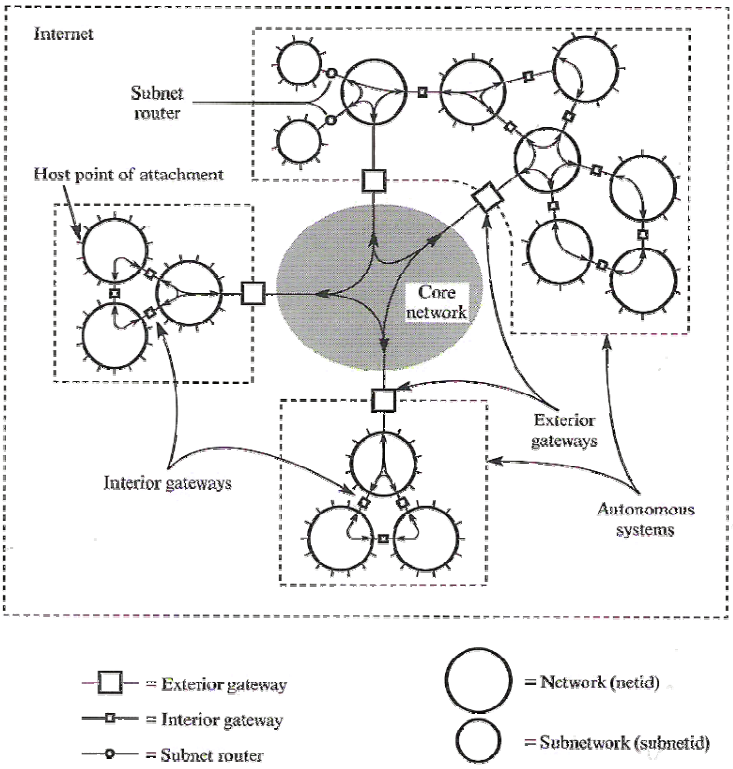
Através da sessão de TCP no porto 179 são inseridos manualmente nas tabelas de encaminhamento dos routers os nós que utilizam o BGP. Este protocolo é único uma vez que utiliza o próprio TCP como camada de Transporte.

O BGP é constituído por duas partes, o Interior Border Gateway Protocol (IBGP) e Exterior Border Gateway Protocol (EBGP). O IBGP é utilizado dentro de um único sistema autónomo enquanto que o EBGP é utilizado entre sistemas autónomos.

Todos os routers que dentro de um sistema autónomo participam do protocolo BGP têm de estar configurados de tal modo que cada router esteja ligado a todos os outros, em malha. Como o número de ligações aumenta por cada router que se insere nessa malha existem modos de minimizar o peso associado, são elas as Confederações (Confederations) e Route Reflectors.

O Route Reflector reduz as ligações. Apenas um router (ou dois por causa da redundância) é configurado como route reflector e todos os outros apenas necessitam de estar ligados a ele(s) (peer). Obtém-se assim uma hierarquia de routers.

A Confederação é utilizada em grande redes em que estas possam estar subdivididas noutras redes autónomas mais pequenas onde se utiliza o Route Reflector.



Devido ao grande número de nós que estão ligados nos diversos sistemas autónomos surgem situações de alguns deles irem a baixo e voltarem novamente a funcionar, ou linhas que deixam de ter continuidade para depois voltarem a tê-la ou até devido a configurações desajustadas ou erradas.

Estas situações podem provocar flutuações maiores na rede e causar uma certa instabilidade. Para evitar oscilações na rede o BGP introduz um efeito de amortecimento (dampening). Isto consegue-se com o auxílio de constantes de tempo que agem em conformidade com o sucedido. Se um nó de repente ficar inacessível, ele sai das tabelas de encaminhamento, mas se de seguida voltar a estar acessível, aguarda-se um tempo determinado, pois caso vá de novo abaixo não terá influência sobre a nova configuração. Se se mantiver operacional após esse tempo então é colocado novamente nas tabelas de encaminhamento. Outras quebras consecutivas fazem com que o tempo de espera cresça exponencialmente.

Este amortecimento também se torna útil quando a rede fica sujeita a um ataque do tipo Denial of Service, em que as ligações não são estabelecidas por alegada falta de recursos.

O grande número de redes e routers originam tabelas de encaminhamento muito grandes. Essa situação será resolvida com o funcionamento do IPV6 que assegurará um espaço de endereçamento maior e consequente melhoria na gestão dos agregados.

Quando se inicia o BGP, os nós envolvidos neste protocolo trocam cópias completas das suas tabelas. A partir daí apenas trocam eventualmente as diferenças que ocorrem, o que minimiza a comunicação de longas tabelas. Se o nó for abaixo terá de recomeçar todo o processo de novo quando voltar a estar activo.

A unidade básica de encaminhamento do BGP é o BGP path, um caminho para um conjunto de confederações (prefixos CIDR). Os caminhos, BGP path, estão catalogados com diversos atributos, path attibutes, dos quais se salientam o AS_PATH e NEXT_HOP.

O AS_PATH é a lista dos Sistemas Autónomos a serem atravessados para se chegar ao Sistema Autónomo de destino. É possível saber se há loops criados verificando se o número AS onde está o nó existe nas tabelas que são recebidas; se faz parte do AS_PATH. Ou seja, há um loop, se ao escolher um determinado percurso ele passa novamente pelo próprio nó. Este processo torna-se complexo quando se utiliza também a agregação, quando diversos percursos são substituídos por um único, Route Reflector.

Também é possível ter percursos que evitem um determinado Sistema Autónomo.

Sempre que o anúncio de um BGP Path atravessa um Sistema Autónomo, o NEXT_HOP é alterado para o endereço IP do router de fronteira (boundary router). No caso de atravessar o mesmo Sistema Autónomo o NEXT_HOP não é alterado. Assim em cada Sistema Autónomo o NEXT_HOP é sempre o endereço IP do primeiro router (de fronteira) do próximo Sistema Autónomo, ainda que seja necessário atravessar diversos routers para lá chegar.

Dentro do Sistema Autónomo o algoritmo de encaminhamento calcula o ar o percurso para encaminhar os pacotes para os routers de fronteira. Há assim uma distinção entre o que se passa dentro dos sistemas autónomos, IBGP e fora deles EBGP. Os NEXT_HOP são alterados nas sessões EBGP mas permanecem inalterados nas sessões BIGP.

As condições essenciais para estes protocolos são a do BIGP atingir um router que está para lá da fronteira do AS e as sessões do BEGP estarem ligadas directamente umas às outras dentro do próprio AS.

Como o NEXT_HOP contém o endereço IP do router de fronteira do próximo Sistema Autónomo o algoritmo de encaminhamento do Sistema Autónomo tem de chegar a uma solução para atingir esse router de fronteira. Isto significa que os algoritmos de encaminhamento têm de ter pelo menos um hop a mais para saírem do seu domínio.

O BGP não encaminha tráfego dentro do Sistema Autónomo (entre sessões BIGP), mas encaminha tráfego entre sessões BEGP e entre BEGP e BIGP. Todos os BGP têm de estar logicamente ligados ponto a ponto. Quando se recebe um BGP de actualização de percursos, é necessário enviar esta alteração a todos os outros nós BGP dentro do Sistema Autónomo.

Assimilação de Conceitos

- CIDR – Classless Inter-Domain Routing
- VLSM – Variable Length Subnet Masks
- ISP – Internet Service Provider
- DoS – Denial of Service
- IGP
- IGRP
- HELLO
- OSPF
- EGP
- RIP
- BGP-4
- http://www2.rad.com/networks/2002/bgp/bgpall.htm
- http://www2.rad.com/networks/2002/bgp/index.htm
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/bgp.htm
- http://www.tutorgig.com/ed/Internet_protocol_suite
- http://penta.ufrgs.br/redes296/cidr/tutorial.html

Para Aprofundar

- Signaling System 7 – para rede telefónica, comparar com o BGP
- RFC 1058
- RFC 1583
- RFC 1771, 1772, 1773