
Redes de Computadores

(RCOMP – 2015/2016)

Encaminhamento IPv4.

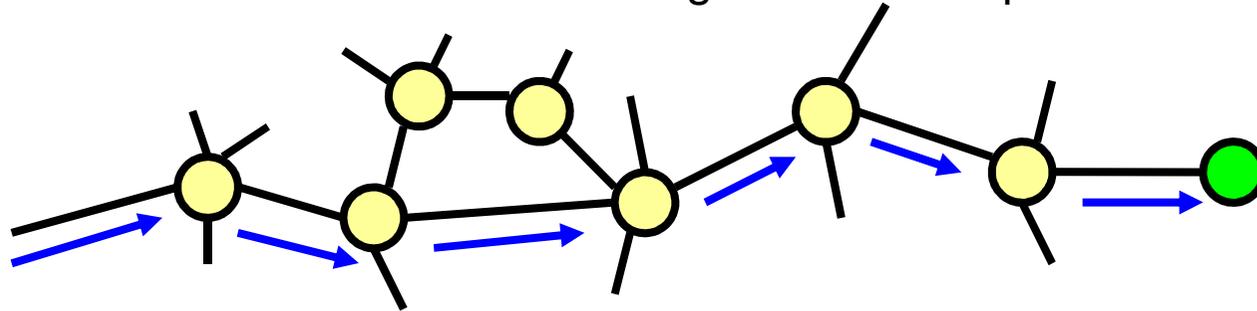
Encaminhamento estático e encaminhamento dinâmico.

Protocolos de encaminhamento: RIP, RIPv2, EIGRP e OSPF.

Sistemas autónomos e redistribuição de rotas.

Nós intermédios

Os nós intermédios assumem o papel principal em qualquer tipo de rede de comutação. As redes de comutação caracterizam-se pela retransmissão da informação entre sucessivos nós até chegar ao destino pretendido.



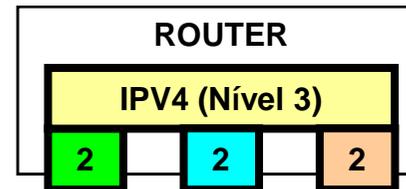
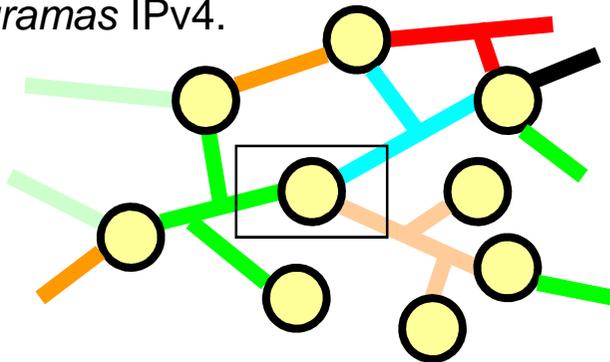
Os nós da rede que assumem essa missão de retransmissão são genericamente conhecidos como nós intermédios. No nível 2 do modelo OSI são habitualmente designados de comutadores ou *switches*.

Os *datagramas* do protocolo IPv4 também chegam ao destino graças aos nós intermédios, quando operam no nível de rede os nós intermédios são normalmente designados encaminhadores ou routers. A designação *gateway* também é por vezes usada.

Encaminhadores (routers)

Os encaminhadores são nós intermédios responsáveis pela retransmissão de pacotes do nível 3. Operam segundo um protocolo de rede, por exemplo IPv4.

Os encaminhadores possuem várias interfaces de rede (implementações nível1/2, eventualmente de tipos diferentes), usando essas interfaces recebem e retransmitem *datagramas* IPv4.

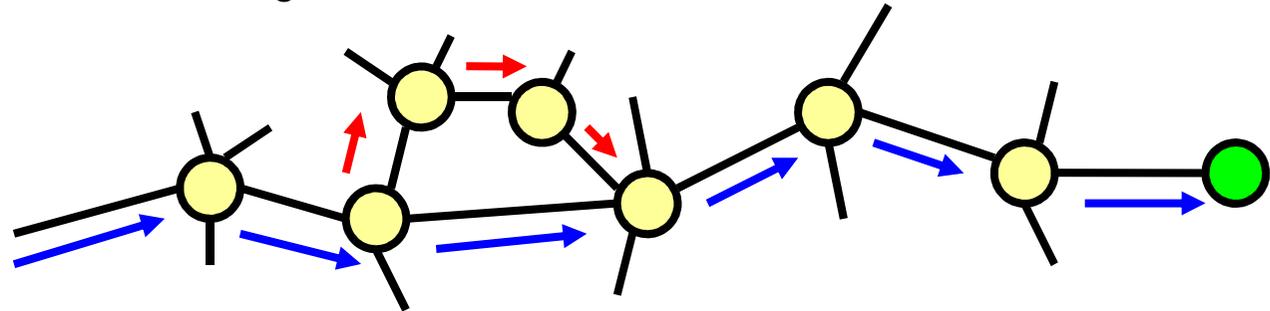


Quando um encaminhador recebe um *datagrama* para retransmitir analisa o endereço IPv4 de destino contido no cabeçalho. Com base nesse endereço tem de tomar uma decisão relativamente a “para onde enviar”.

No exemplo acima o encaminhador em destaque possui 3 interfaces de rede, mas um total de 8 encaminhadores vizinhos (diretamente ligados). Este encaminhador tem de decidir para qual dos oito destinos possíveis deve enviar o *datagrama*. O encaminhador vizinho para onde o *datagrama* vai ser enviado é conhecido como próximo-nó (*next-hop*).

Encaminhamento (*routing*)

A decisão que um encaminhador tem de tomar consiste em determinar para onde enviar um dado *datagrama*, ou seja determinar o *next-hop*. Esta decisão e a aplicação da mesma designa-se encaminhamento ou *routing*.



Cada encaminhador toma localmente a sua decisão escolhendo o *next-hop* apropriado. Para que o *datagrama* chegue ao destino é conveniente que todos os encaminhadores ao longo do percurso tomem as decisões corretas. Por vezes alguns erros podem ser corrigidos: 

Os encaminhadores interagem apenas com os encaminhadores vizinhos, esses são os únicos *next-hop* possíveis. Na figura ao lado o encaminhador central tem exatamente 8 encaminhadores vizinhos, ou seja 8 *next-hop* possíveis.

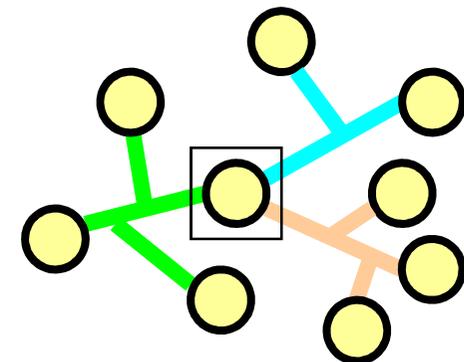


Tabela de encaminhamento (*routing table*)

Uma das principais razões do atual sucesso do protocolo IP é o facto de ser assegurado que um DATAGRAMA IP emitido em qualquer ponto da INTERNET será corretamente encaminhado até ao endereço de destino.

As decisões de encaminhamento, ou seja a escolha do próximo nó (*next-hop*) apropriado, são realizadas usando uma tabela conhecida por tabela de encaminhamento (ou “routing table”).

Cada linha da tabela de encaminhamento possui dois elementos fundamentais:

DESTINO	PRÓXIMO NÓ

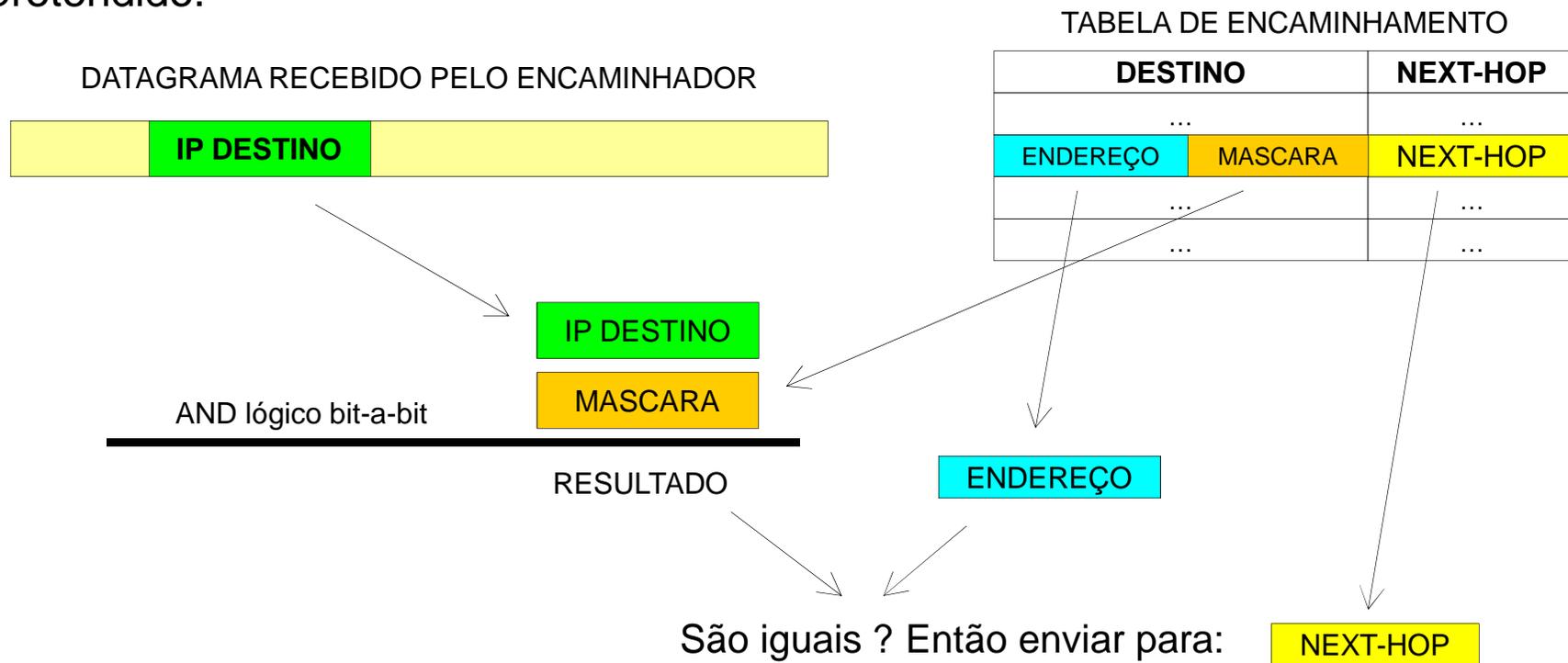
DESTINO – identificação do destino, ou seja um endereço IP associado a uma máscara de rede. Normalmente representa uma rede remota

PRÓXIMO NÓ – próximo encaminhador (*next-hop*) para onde devem ser enviados os dados quando se pretende que estes cheguem ao **DESTINO**. Trata-se do endereço IP do nó seguinte do percurso ou rota dos dados, é sempre um endereço IP de um nó vizinho.

Encaminhamento

Quando um encaminhador recebe um *datagrama* usa a coluna “DESTINO” da tabela de encaminhamento para determinar o *next-hop* adequado.

O endereço de destino do *datagrama* é confrontado sequencialmente com cada uma das linhas da tabela de encaminhamento até ser encontrado o DESTINO pretendido.



Redes Locais e Caminho por omissão

Para cada interface de rede a que um nó está ligado (redes locais) existe uma linha especial na tabela de encaminhamento em que o “PRÓXIMO NÓ” é a identificação interna dessa interface na rede local e não um endereço IP.

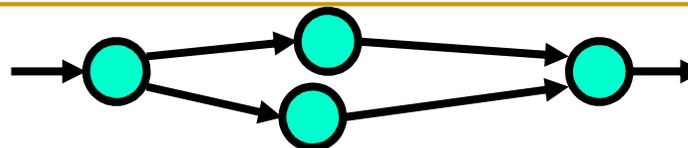
Numa tabela de encaminhamento não é possível ter identificados todos os destinos possíveis, usa-se uma linha no fim da tabela que serve para identificar todos os destinos não contemplados em linhas anteriores. Trata-se do caminho por omissão (*default route*). O *next-hop* correspondente é muitas vezes conhecido por *default gateway*.

Todos os nós de rede IP possuem uma tabela de encaminhamento, no caso mais simples apenas com duas entradas: “interface na rede local” e “caminho por omissão”.

Todos os endereços na coluna “PRÓXIMO NÓ” pertencem obrigatoriamente a redes locais diretamente ligadas por uma interface.

DESTINO	PRÓXIMO NÓ
192.168.10.0/24	INTERFACE ETHERNET 1
172.14.0.0/16	INTERFACE ETHERNET 2
194.121.12.0/24	172.14.5.100
0.0.0.0/0	192.168.10.200

Caminhos alternativos



Quando apenas existe um caminho possível para chegar ao nó de destino, as tabelas de encaminhamento com duas colunas são suficientes.

Em redes mais complexas como por exemplo as redes de trânsito que interligam zonas da INTERNET é vulgar e desejável (redundância e distribuição do tráfego) que existam vários caminhos alternativos para chegar a qualquer ponto.

Caminhos alternativos, significa que em determinados encaminhadores vão existir linhas da tabela de encaminhamento repetidas com o mesmo destino.

São necessários novos critérios para tomar a melhor decisão de escolha do caminho.

DESTINO	PRÓXIMO NÓ
192.168.10.0/24	INTERFACE ETHERNET 1
172.14.0.0/16	INTERFACE ETHERNET 2
194.121.12.0/24	172.14.5.100
194.121.12.0/24	192.168.10.2
0.0.0.0/0	192.168.10.200

Para permitir uma decisão no sentido de que seja usado o melhor caminho, a cada linha da tabela de encaminhamento são adicionados outros parâmetros que deverão quantificar o custo da sua utilização (caminho até ao destino).

Quando existem duas linhas com o mesmo DESTINO será usada a de menor custo. O custo é calculado em função de vários parâmetros resultado num valor designado métrica.

Encaminhamento dinâmico

A construção das tabelas de encaminhamento pode ser realizada manualmente (encaminhamento estático), contudo para redes extensas e complexas essa tarefa torna-se quase impossível e tem de ser automatizada.

As vantagens da existência de caminhos alternativos (redundância e distribuição do tráfego) apenas fazem sentido se as tabelas de encaminhamento mantiverem uma representação atualizada do estado da rede, isso não pode ser feito manualmente.

Para resolver estes problemas usam-se protocolos de encaminhamento dinâmico que permitem a construção automática das tabelas de encaminhamento. Estes protocolos envolvem a troca de informação de controlo entre os nós encaminhadores.

Existem dois tipos de protocolo de encaminhamento dominantes:

DISTANCE-VECTOR - cada nó divulga junto dos nós vizinhos a sua tabela de encaminhamento.

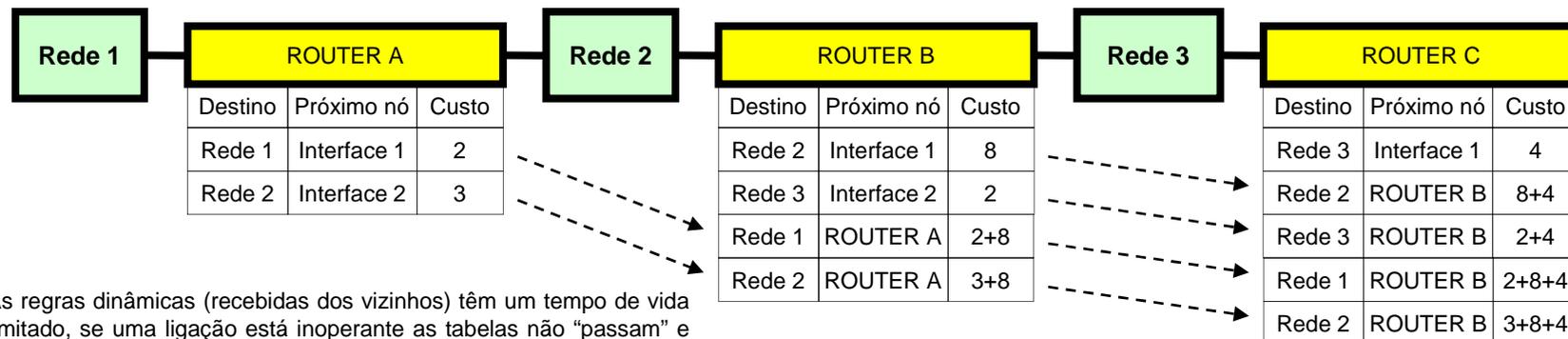
LINK-STATE - cada nó divulga junto dos nós vizinhos a lista de nós aos quais está diretamente ligado (vizinhos).

Algoritmos DISTANCE-VECTOR

Este algoritmo envolve a divulgação periódica entre nós vizinhos das respetivas tabelas de encaminhamento. Esta divulgação pode recorrer a uma simples emissão em BROADCAST.

Inicialmente cada nó possui uma tabela de encaminhamento em que constam apenas as redes a que está diretamente ligado (interfaces de rede), a cada uma das interfaces está associado um custo (distância).

Quando um nó recebe do vizinho uma tabela de encaminhamento adiciona ao custo de cada linha o custo da interface por onde a informação foi recebida e modifica o PROXIMO NÓ para corresponder ao endereço de origem dessa informação:



As regras dinâmicas (recebidas dos vizinhos) têm um tempo de vida limitado, se uma ligação está inoperante as tabelas não "passam" e as respetivas linhas acabam por ser eliminadas.

Algoritmos LINK-STATE

Nos algoritmos LINK-STATE as tabelas de encaminhamento são totalmente construídas em cada encaminhador. Para isso cada encaminhador tem de conhecer toda a rede.

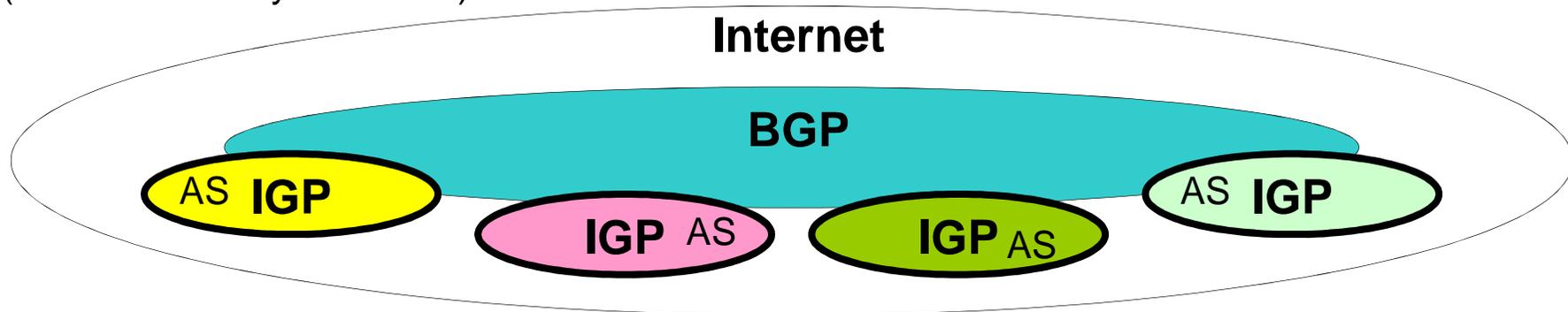
Cada nó de encaminhamento tem de conhecer os seus vizinhos diretos e controlar permanentemente o estado da ligação com cada um deles. Na posse dessa lista divulga-a por todos os encaminhadores da rede. Sempre que detetar uma alteração nos estados das ligação reconstrói a lista e divulga-a novamente.

Cada nó de encaminhamento recebe portanto mensagens de todos os outros nós contendo a identificação do nó de origem e dos respetivos vizinhos (as ligações entre nós só são aceites com reconhecimento mutuo). Com estas informações todos os encaminhadores ficam a conhecer as interligações de toda a rede.

Na posse do conhecimento de todas as interligações da rede, o nó pode agora autonomamente determinar a tabela de encaminhamento. Trata-se de um algoritmo simples de determinação dos caminhos mais curtos (menos nós intermédios).

Sistemas autónomos (AS) – Protocolos IGP e BGP

Para efeitos de encaminhamento a INTERNET está dividida em sistemas autónomos (AS), cada sistema autónomo integra um conjunto de redes IP geridas por uma mesma entidade, por exemplo um ISP. Os protocolos de encaminhamento usados no interior de um AS são independentes da restante INTERNET e dos AS vizinhos. Os protocolos de encaminhamento usados no interior de um AS são habitualmente designados de IGP (Interior Gateway Protocols).



O encaminhamento entre sistemas autónomos é atualmente definido pelo BGP (*Border Gateway Protocol*). Para interagir com o BGP, cada AS tem atribuído um ASN (*Autonomous System Number*) único que o identifica. Os ASN são atribuídos pelo IANA (*Internet Assigned Numbers Authority*), também responsável pela atribuição de endereços IPv4/IPv6 e nomes de domínio DNS. O IANA delega a administração de partes do sistema aos RIR (*Regional Internet Registries*).

Protocolos IGP

Os protocolos de encaminhamento usados no interior dos AS são designados “Interior Gateway Protocols”, a utilização de um ASN único, fornecido pelo IANA apenas é importante se o AS estiver em contacto com o BGP, caso contrário podem usar-se por exemplo os valores 64512 a 65534 que foram reservados para uso privado.

Principais Protocolos IGP

Na categoria DISTANCE-VECTOR: **RIP** (Routing Information Protocol) e o IGRP (Interior Gateway Routing Protocol).

Na categoria LINK-STATE: **OSPF** (Open Shortest Path First) e o IS-IS (Intermediate System to Intermediate System) .

Também existem protocolos mistos ou híbridos, o protocolo proprietário da CISCO “Enhanced Interior Gateway Routing Protocol” (**EIGRP**) possui características de ambas as categorias.

Protocolo RIPv1

- Cada router divulga a sua tabela de encaminhamento por *broadcast* (UDP) nas redes vizinhas. A divulgação ocorre de 30 em 30 segundos, ou em períodos variáveis ligeiramente superiores.
- Quando uma linha da tabela de encaminhamento não é refrescada durante 180 segundos, é marcada como não atingível (*hops*=16).
- Não divulga mascaras de rede, logo apenas suporta endereçamento classful.
- A métrica é o número de saltos (*hops*), é incrementada por cada router que retransmite a tabela. O número de *hops* máximo é 15, o valor 16 significa que o destino não é atingível.
- Não usa nenhum identificador de área ou AS, isso torna impossível a um router estar ligado a dois AS distintos que usem RIP.
- O protocolo é inseguro porque as informações são recebidas sem qualquer procedimento de autenticação.

Protocolo RIPv2

A versão 2 do protocolo RIP tenta colmatar algumas limitações da versão 1.

O RIPv2 foi desenvolvido de forma a ser parcialmente compatível com o RIPv1.

- Cada router divulga a sua tabela de encaminhamento usando *multicast* para o endereço 224.0.0.9 em lugar de *broadcast*.
- As tabelas de encaminhamento divulgadas incluem agora as mascaras de rede, por isso já suporta CIDR (*Classless Inter-Domain Routing*).
- Para manter a compatibilidade com o versão 1, o número máximo de saltos (*hops*) mantém-se (15 saltos).
- Suporta a utilização do algoritmo MD5 permitindo a autenticação baseada numa chave secreta pré-partilhada.

Protocolo OSPF

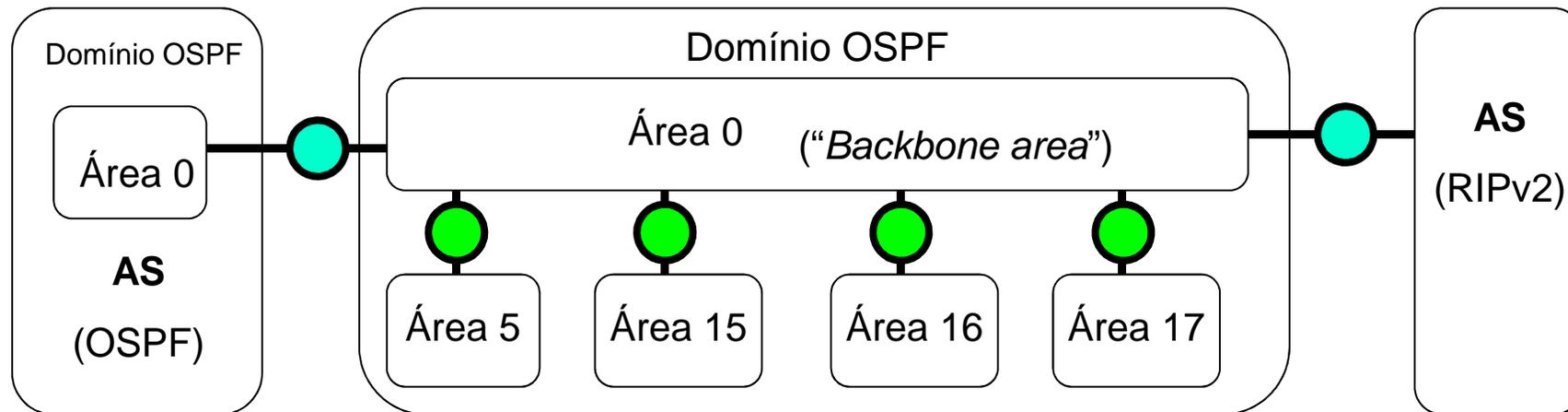
- Trata-se de um protocolo *link-state*, cada router tenta identificar os *routers* vizinhos, recorrendo a *broadcast* e *multicast* (224.0.0.5). Depois divulga a lista de vizinhos aos restantes *routers* recorrendo ao endereço 224.0.0.6.
- Cada router monitoriza o estado dos *routers* vizinhos, sempre que se produz alguma alteração repete a divulgação. As transações OSPF usam diretamente o protocolo IP, não recorrem ao UDP.
- Cada router utiliza a informação recebida para construir autonomamente a tabela de encaminhamento. A informação transacionada transporta mascaras de rede, por isso o OSPF suporta CIDR.
- Suporta autenticação entre routers, baseada em MD5 e HMAC-SHA.
- A métrica pode ser calculada de diversas formas, mas normalmente deriva da taxa de transmissão correspondente à ligação que dá acesso ao caminho.

Áreas OSPF

TIPOS DE ROUTERS OSPF

- ASBR (“Autonomous System Boundary Router”)
- ABR (“Area Border Router”)

O OSPF é um IGP, por isso não suporta o conceito de AS, sob o ponto de vista do OSPF tudo o que existe é o domínio OSPF. Sob o ponto de vista externo poderá ser um AS, mas não para o OSPF.



Pelas mesmas razões que a Internet está dividida em sistemas autónomos, também um domínio OSPF pode ser dividido em **áreas** onde o encaminhamento será tratado de forma independente umas das outras, contudo agora o protocolo é o mesmo em todas elas.

Protocolo EIGRP



O protocolo EIGRP é um melhoramento do protocolo IGRP desenvolvido pela Cisco para fazer face aos problemas do RIP. Na sua essência é um protocolo “distance-vector”, mas tem algumas características dos protocolos *link-state*.

Cada router mantém uma lista de *routers* vizinhos usando o envio periódico, em *unicast* / *broadcast* / *multicast*, da mensagem *hello*. **Vantagens:**

- é mantido um controlo mais apertado sobre o estado dos routers vizinhos permitindo um reflexo mais rápido do estado da rede nas tabelas de encaminhamento.
- as tabelas de encaminhamento são divulgadas aos routers vizinhos apenas quando ocorre alguma alteração, recorrendo ao endereço 224.0.0.10, não há divulgação periódica.

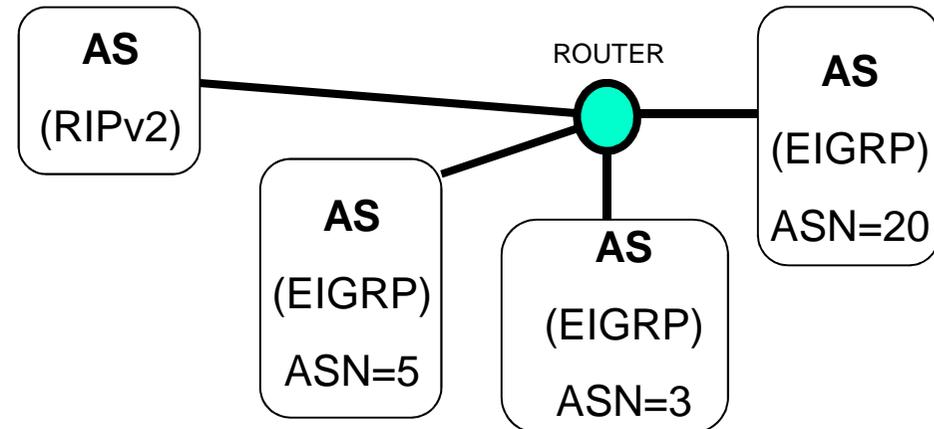
O protocolo EIGRP suporta CIDR e usa uma métrica complexa que envolve vários parâmetros, nomeadamente taxa de transmissão da interface, saturação dos nós, atraso na rede, fiabilidade da ligação e MTU.

Embora não seja usado para efeitos de métrica, também procede à contagem de *hops*, normalmente um número de *hops* superior a 100 classifica o destino como não atingível. O número máximo de *hops* pode ser ajustado até 224.

Sistemas autónomos EIGRP



O protocolo EIGRP permite a criação de sistemas autónomos de encaminhamento associando a cada um deles um número único (*Autonomous System Number*) que pode variar de 1 a 65535. Todas as informações do EIGRP têm um ASN associado, sendo tratadas de forma totalmente independente informações relativas a sistemas autónomos diferentes.



A vantagem do EIGRP usar os ASN é que um encaminhador pode estar ligado a vários sistemas autónomos EIGRP diferentes.

Os ASN do EIGRP não têm nenhuma relação direta com os ASN do BGP.

Encaminhamento entre Sistemas Autónomos

O objetivo da definição de sistemas autónomos (ou áreas OSPF) é isolar partes das redes sob o ponto de vista da gestão das tabelas de encaminhamento, as vantagens são:

- Administração mais simples uma vez que existem menos redes
- Tabelas de encaminhamento mais pequenas
- Menor tráfego de rede (propagação do protocolo limitada)

Os sistemas autónomos não são criados arbitrariamente, devem corresponder a partes isoladas das redes, muitas vezes com apenas com uma ligação aos restantes sistemas autónomos.

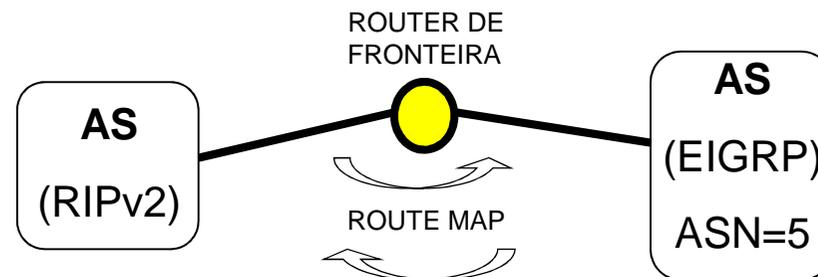
Para facilitar o encaminhamento no exterior do sistema autónomo é desejável que as redes IP de um sistema autónomo constituam um bloco CIDR único.

O encaminhamento entre sistemas autónomos pode ser conseguido pela inserção manual de regras de encaminhamento nas tabelas no interior de cada AS. Estas regras estáticas podem depois ser propagadas a todos os routers do AS pelo protocolo de encaminhamento usado no seu interior.

Redistribuição de Rotas

Para garantir o encaminhamento entre sistemas autónomos podem ser configuradas manualmente nos routers de fronteira regras estáticas que indiquem como chegar às redes de cada um dos sistemas autónomos, de preferência sob a forma de blocos CIDR únicos.

Uma alternativa é a “redistribuição de rotas” ou *route map*. Consiste em definir formas automáticas de copiar regras de encaminhamento entre dois AS vizinhos, essa operação é realizada no router de fronteira que faz parte de ambos os AS.



Uma das dificuldades na “redistribuição de rotas” coloca-se quando os AS vizinhos utilizam protocolos de encaminhamento diferentes. Devido à variedade dos tipos de métrica usado por cada um torna-se necessário muitas vezes arbitrar alguns valores.