TUDO SOBRE ENDEREÇOS IP

Revisão: Endereços IP são números de 32 bits, geralmente representados em notação decimal (xxx.xxx.xxx.xxx). Cada número decimal (xxx) representa oito bits em binário, e por isso, pode assumir valores entre 0 e 255. O valor do primeiro número do endereço IP é que determina qual é a classe que este IP pertence, como ilustra a tabela abaixo:

Classe	Range	Alocação	
A	1-126	N.H.H.H	N = Network
B	128-191	N.N.H.H	H = Host
C	192-223	N.N.N.H	
D	224-239	Usado para MultiCast.	

Notas:

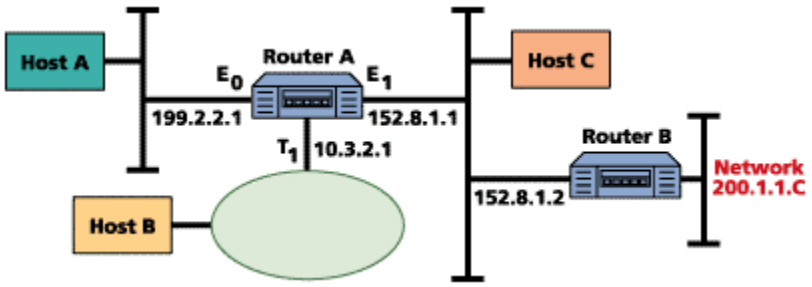
1) 127.0.0.0 é uma rede classe A reservada para uso como endereços de loopback (geralmente 127.0.0.1);

2) A rede 0.0.0.0 é reservada para uso como rota default;

3) Classes D são usados por grupos de hosts ou roteadores que dividem uma característica comum. (Ex. Todos os dispositivos OSPF respondem pacotes enviados para a rede 224.0.0.0)

4) Redes Classe E (240-248) existem, mas estão reservadas para uso futuro.

Então, sem fazer subnet, uma tabela de roteamento conterá informações de: a) números de rede; b) o próximo roteador (hop) usado para chegar até uma determinada rede; c) a interface no qual este próximo roteador é alcançável. Uma rede simples e sua respectiva tabela de roteamento "aprendida" usando protocolos de roteamento (RIP, IGRP, OSPF, BGP e etc.) é ilustrada abaixo:



C	199.2.2.0	Conectado Diretamente	Ethernet 0
C	10.0.0.0	Conectado Diretamente	Token-ring 1
C	152.8.0.0	Conectado Diretamente	Ethernet 1
I	200.1.1.0	via 152.8.1.2	Ethernet 1

A primeira coluna da tabela de roteamento refere-se como a rede foi descoberta. C significa conectado, ou seja estão no mesmo barramento (rede), e I indica que a rede foi descoberta através de um protocolo de roteamento (Ex: IGRP).

Cada interface de um roteador e dos hosts conectados a ele em uma rede precisam ter um endereço IP e uma mascara de subrede definida (muitos equipamentos assumem a mascara de subrede default se nenhuma for especificada). Os endereços IP e a mascara de subrede, derivam da tabela de roteamento pertencente a está rede.

Tabela de roteamentos podem ficar muito grandes. Roteadores de Backbone Internet podem possuir mais de 40.000 rotas definidas neles. Estes roteadores usam um método chamado CIDR (Classless InterDomain Rounting) para reduzir o número de entradas em suas tabelas de roteamento. Se imaginarmos, por exemplo, que todos endereços Classe C que começam com 194 são alocados para uso na Europa, isto reduziria significativamente o tamanho de uma tabela de roteamento nos roteadores de Internet da Embratel, pois haveria apenas uma rota para todas estas redes Classe C (194), invés de rotas definidas para cada uma destas redes. CIDR trabalha como se todas as redes cujo o primeiro octeto for 194 estão fisicamente alocadas na mesma área.

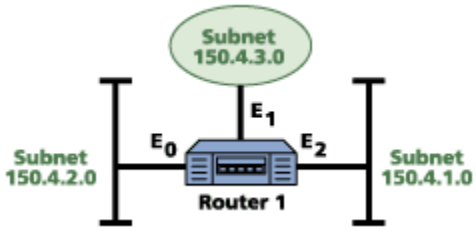
Endereços IP são usados para entregar pacotes de dados na rede (Intranet ou Internet), ou seja entregar os pacotes fim-a-fim. Isto significa que o endereço fonte e de destino permanecem constante enquanto os pacotes atravessam a rede. Toda vez que um pacote passa por um roteador, o roteador irá buscar em sua tabela de roteamento se há alguma rota ou entrada para o número de rede do IP de destino. Se existe uma rota ou entrada, o pacote é encaminhado ao próximo roteador (next hop) da rede de destino em questão (note que um roteador não necessariamente conhece o caminho completo da fonte ao destino – ele só conhece o próximo roteador que ele tem que encaminhar o pacote). Se não existe uma rota ou entrada, duas coisas podem acontecer, ou pacote é encaminhado para o roteador definido como default gateway ou o pacote não é encaminhado (drop).

Pacotes são encaminhados para um default gateway na crença que este roteador tenha mais informação de rede em sua tabela de roteamento e por isso será capaz de rotear o pacote corretamente para seu destino final. Isto ocorre geralmente em uma LAN com PCs conectados nela para Internet. Cada PC terá o roteador que a conecta a rede à Internet definido como default gateway.

Um default gateway em uma tabela de roteamento de um host é visto como: a rota default (0.0.0.0) será listada a rede de destino, e o endereço IP do default gateway será listado como o próximo hop.

Mascaras de Subrede

São usadas para dividir uma rede em uma porção de redes menores. Isto pode ser feito para reduzir o tráfico em cada subrede. Todas as subredes funcionam come se elas fossem redes independentes. A ilustração abaixo mostra como uma tabela de roteamento se parece quando submascaras são usadas.



Configuração das Interfaces no Router 1

Interface	Endereço IP	Mascara de Subrede
E0	150.4.2.1	255.255.255.0
E1	150.4.3.1	255.255.255.0
E2	150.4.1.1	255.255.255.0

A tabela de roteamento nota que a classe B (150.4.0.0) está subnetada, e reconhece cada subnet como uma entrada separada na tabela de roteamento.

Quando subredes são utilizadas, um endereço IP é interpretado assim:

[Endereço IP] = [Endereço de Rede][Endereço de Surede][Endereço do Host]

Isto mostra que quando uma rede é dividida em subredes, a parte do endereço IP reservada para endereços de host é dividida em duas partes: endereço de subrede e endereço de host.

Por exemplo se uma rede Classe B 129.47, o que sobra do endereçamento IP é dividido em endereço de subrede e endereço de host.

Submascara de rede é um mecanismo que define como a parte reservada para host do endereço IP será dividida em subrede e qual será a parte definida para host locais.

Para ver como uma mascara de subrede divide a parte de host em parte de subrede e de host locais, é necessário converter tanto o endereço IP como a mascara para binário. Depois aplicaremos uma operação lógica do tipo AND (significa que para o valor resultante ser 1, o valor do bit do IP e da mascara devem ser 1, caso contrário o resultado será 0). Olhe o exemplo:

Endereço IP : 201.222.5.121
Subnet Mask : 255.255.255.248

201.222.5.121 : 11001001.11011110.00000101.01111 001
255.255.255.248 : 11111111.11111111.11111111.11111 000

Subnet : 11001001.11011110.00000101.01111 000

201. 222. 5. 120

Assim, o endereço de subrede resultante é 201.222.5.120. Nesta mascara é dito que ter cinco bits no campo de subnet, que deixa três bits para definir hosts. Com três bits binários, há oito valores possíveis para host (0 à 7). Entretanto somente seis destes endereços podem ser usados por hosts nesta subrede. Isto ocorre porque o ultimo e o primeiro IP de uma rede ou subrede são reservados. O primeiro é reservado como identificador da própria subrede e o ultimo é o endereço de broadcast para aquela rede ou subrede.

Ainda em nosso exemplo, ilustraremos o acima descrito:

Endereço IP = 210.222.5.121
Mascara de Subrede = 255.255.255.248
Endereço de Subrede = 201.222.5.120
Endereços que podem ser usados na subrede = 201.222.5.121 - 201.222.5.126
Endereço de Broadcast na Suberede = 201.222.5.127

Uma maneira mais fácil de calcular seria, pelo ultimo octeto (que é a tarefa mais comum, subtraia-o de 256. O resultado dirá quantos endereços IP há nesta subrede.

Por exemplo, com a mascara de rede 255.255.255.224, tire 224 de 256 e você terá 32. Isto mostra que para uma mascara de subrede que termina com 224, você está dividindo a rede em subredes tem 30 endereços disponíveis em cada subrede (Lembre-se que o primeiro e o ultimo IP de cada subnet são reservados).

As Tabelas a seguir mostram quantos hosts por subrede e total de subredes quando uma mascara de subrede é aplica as classes B e C:

Classe B

Subnet Mask	#Subnets	#Hosts
255.255.192.0	4	16382
255.255.224.0	8	8190
255.255.240.0	16	4094
255.255.248.0	32	2046
255.255.252.0	64	1022
255.255.254.0	128	510
255.255.255.0	256	254
255.255.255.128	512	126
255.255.255.192	1024	62
255.255.255.224	2048	30
255.255.255.240	4096	14
255.255.255.248	8192	6
255.255.255.252	16384	2

Classe C

Subnet Mask	#Subnets	#Hosts
255.255.255.192	4	62
255.255.255.224	8	30
255.255.255.240	16	14
255.255.255.248	32	6
255.255.255.252	64	2

Alguns Request for Coments (RFC), avisam sobre o uso do primeiro e do ultimo endereço IP. Na prática o uso ou não desses endereços dependem do protocolo de roteamento em uso na rede e da implementação IP nos dispositivos de roteamento na rede.

RFCs na prática são somente um estudo e um guia – não um padrão sancionado oficialmente. Fabricantes são livres para implementar soluções diversas para os problemas apontados nos RFCs. Se sua rede usa hosts UNIX e como protocolo de roteamento RIP 1, você não pode usar o primeiro e o ultimo endereço da subrede. Se estiver usando roteadores Cisco com OSPF e EIGRP, você pode usar o primeiro e ultimo endereço. Se está usando Cisco e IGRP, você pode usar o primeiro mas não pode usar o ultimo. É claro há inúmeras aplicações onde isto irá funcionar e também onde não ira funcionar. O que se faz na pratica é deixar estes endereços reservados, mas se você possui poucos endereços, verifique no manual do fabricante do dispositivo que você usará e verifique se há alguma restrição.

O que define se um protocolo suporta o uso destes endereços corretamente é se o protocolo em uso envia informação de mascara de subrede em suas atualizações de rotas. RIP e outros protocolos que trabalham com o algoritmo do tipo vetor de distancia (distance vector) não funcionam, protocolos link state e/ou híbridos (OSPF, EIGRP) funcionam.

Suponha que você tem uma rede da Classe C 200.200.200.0, usando uma mascara de subrede 255.255.255.192 e uma interface de um roteador com o IP 200.200.200.195. Este IP está na rede que começa com 200.200.200.192. O endereço de broadcast para está subrede é 200.200.200.255, que também acontece de ser o endereço de broadcast para toda está rede Classe C. Se o valor da mascara de subrede não for enviada em atualizações de roteamento, um router remoto que tem a subrede 200.200.200.192 listada em sua tabela de roteamento pode não

saber se um pacote endereçado para 200.200.200.255 é para ser encaminhado somente dentro da subrede ou em toda rede Classe C.

Como se não bastasse, a outros problemas que precisam ser considerados, e que tornam seu entendimento difícil e de um estudo e conhecimento mais aprofundado.

Protocolos de Roteamento

Como a tabela de roteamento é o centro de uma rede roteada, foram implementados protocolos de roteamento para mante-las atualizadas automaticamente. Um protocolo de roteamento tem como objetivo notificar à todos os roteadores as redes que ele conhece e qualquer mudança que ocorra nesta rede (por exemplo, como resultado de uma falha em algum link da rede, o roteador aprenderia ou criaria uma rota para esta rede).

Protocolos que trabalham com vector de distancia (Distance Vector), como RIP e EIGRP enviam atualizações em tempos regulares (default de 30 segundos para RIP e 90 para EIGRP, embora isto possa ser configurável) que incluem informações de todas as rotas conhecidas pela tabela de roteamento. Para tabelas de roteamento muito grande, estas atualizações podem consumir uma banda considerável (se uma tabela de roteamento tem mais de mil rotas, irá consumir cerca de 128K de banda a cada vez que uma utilização for enviada). Estas atualizações são enviadas somente para os roteadores vizinhos.

Protocolos link state usam um mecanismo diferente. Estes protocolos enviam um pequeno pacote de hello a cada 30 segundos a todos os roteadores na rede como mensagem de keep-alive. Informação de rotas são enviadas sempre que alguma coisa mudar e somente serão enviados aos roteadores que precisaram mudar alguma coisa em sua tabela de roteamento. Estes protocolos podem ser um pouco melhores em consumo de banda, porém necessitam de maior processamento e memória dentro dos roteadores para operar bem.

Se um roteador aprende dois jeitos de chegar a uma subrede remota usando RIP, a rota com a métrica mais baixa, será selecionada e colocada na tabela de roteamento. Se as métricas são iguais, o roteador pode colocar as duas rotas na tabela de roteamento, contudo, usando RIP, só uma rota será usada.

Se um roteador aprende dois jeitos de chegar a uma subrede remota usando IGRP, a coisa fica diferente. Se as duas rotas tiverem métricas iguais, as duas são colocadas na tabela de roteamento e o tráfico é dividido entre as duas rotas. Se a métrica para as duas rotas está dentro de um valor pré definido, o tráfico será dividido entre elas na proporção do valor das métricas. Se a diferença entre os valores das métricas for muito maior do a variância pré definida, a rota com menor métrica será colocada na tabela de roteamento. A variância predefinida para IGRP é 1.

Dentro de uma rede você pode restringir a distribuição e aceitação de atualizações de rotas via interfaces passivas. Se a interface de um roteador é definida como passiva ela somente receberá atualizações mas não enviará nenhuma. Se você quer receber informações de atualizações de rotas apenas de alguns roteadores você pode usar o comando **neighbor** (somente roteadores Cisco), identificando o IP dos routers que você aceitará atualizações.

Em rede com multi-protocolos, pode haver mais de um protocolo de roteamento em uso. Se um roteador aprende uma rota através de dois protocolos de roteamentos diferentes, como ele vai selecionar a informação que será colocada na tabela de roteamento? Neste caso a comparação das métricas é sem uso pis o RIP por exemplo uso uma forma de calculo de métricas diferente do usado em IGRP que é diferente do usado em OSPF. O jeito que este problema é lidado em Ambientes Cisco é designar uma distancia administrativa para cada protocolo, e pegar as informações do protocolo com menor distancia administrativa. RIP tem uma distancia administrativa de 120. OSPF 110, EIGRP 100, IGRP 90, rotas estáticas tem distancia administrativa 1 e diretamente conectado a porta ou interface 0.

O próximo ponto a ser considerado são Sistemas Autonomos (AS) e áreas OSPF. Um AS é uma coleção de números de redes sobre uma administração comum. Por default, irão processar atualizações de rotas que originarem no nesmo AS, e desconsiderarão as atualizações vindas de outros ASes.

Então com um roteador IGRP, a hierarquia do Endereço IP começa com, número de AS, número de rede e numero de subrede.

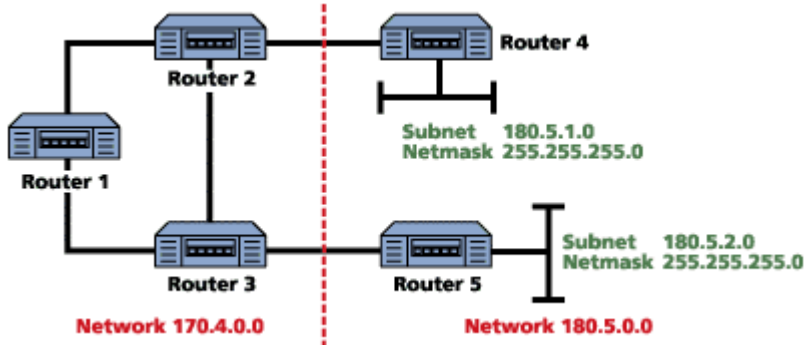
Com sistemas OSPF, uma outra hierarquia é apresentada, Área de Roteamento (Routing Area). Cada sistema OSPF tem ao menos uma área configurada. Como protocolos link state mantêm um banco de dados topológico de todos os números de rede, que é usado para calcular entradas para a tabela de roteamento. Para reduzir o tamanho deste banco de dados topológico e para faze-lo gerenciavel para uma rede grande, é usado a divisão de um sistema OSPF em múltiplas áreas, cada área é interconectada via Area 0 (Area Backbone).

Há a opção de usar VLSM (Variable Length Subnet Mask) com protocolos de roteamento híbridos ou link state. Com protocolos de vetor de distancia como RIP e IGRP, somente um valor de mascara de subrede pode ser usado em uma rede, valores de mascara não são enviados em atualizações de roteamento. Nesta situação, o protocolo de roteamento procura ver a mascara usada na interface que ela recebeu a atualização de roteamento e assume que a mascara está em uso na rede.

Em protocolos link state e híbridos, informação de mascara de subrede é enviada em atualizações de roteamento, que permite uma mascara de subrede diferente ser usada em diferentes parte da rede.

Um ponto que pode causar confusão, o que é resumo de rotas (route summarization) para protocolos vetor de distancia (Protocolos link state podem ser configurados para habilitar ou não resumo de rotas). O que resumo de rotas significa é quando um roteador conecta duas redes diferentes juntas, informação de subrede não é passada entre as duas redes. Isto é melhor ilustrado com um exemplo:

Uma rede configurada incorretamente para uso com protocolos vetor de distancia para resumo de rotas.



Nesta figura, a rede 180.5.0.0 com mascara 255.255.255.0. Por causa do resumo de rota router 2 e router 3 ambos propagaram 180.5.0.0 sem informação de mascara de subrede para o router 1. Router 1 terá por isso rotas de custos iguais para a rede 180.5.0.0. Qualquer pacote que o router 1 precise enviar para subrede 180.5.1.0 será dividido entre o router 2 e 3. Isto poderia causar a entrega de somente metade dos pacotes para um host nas redes 180.5.1.0 e 180.5.2.0.

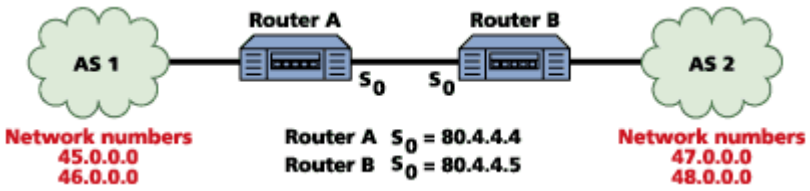
Os protocolos que foram discutidos até agora foram IGRP (Interior Gateway Routing Protocols) ou seja protocolos de roteamento de gateway interno. Protocolos externos também

existem. Estes protocolos foram inventados para regular que tráfico pode viajar entre diferentes AS e proteger cada um de bugs que possam surgir em um AS remoto. Os mecanismos que iremos examinar aqui são roteamento estático, EGP (Exterior Gateway Protocol) e o BGP (Border Gateway Protocol). Um AS é uma coleção de redes sob uma administração comum. Processos de roteamento como IGRP e OSPF são iniciados como número de AS na configuração do roteador e somente aceita atualizações de outros roteadores dentro do mesmo AS. Diferentes números de AS são usados na internet.

Roteamento Estático: Geralmente um administrador de rede com experiência vai buscar minimizar qualquer configuração manual. No caso de protocolos exteriores, isto pode ser diferente, pois o roteamento estático oferece um número de vantagens para fazer roteamento entre AS. Estas vantagens podem se resumir no seguinte:

- Flexibilidade completa sobre o aviso das subnets e a seus next hops;
- Nenhum trafego de protocolos de roteamentos viaja no link inter-AS;
- Como nenhum protocolo de roteamento está trafegando no link inter-AS, não há possibilidade de uma falha de um roteador em um AS afetar em outro AS.

Rotas estáticas não se adaptam a falhas de link, e configuração manual pode ser uma dor de cabeça para se manter. Por isso roteamento estático não é uma escolha para conectar redes que não há confiança em seus links. Vamos dizer que AS 1 possui as redes 45.0.0.0 e 46.0.0.0 e AS 2 as redes 47.0.0.0 e 48.0.0.0. Isto é ilustrado na figura:



Roteamento Estático entre ASes

Para completar o roteamento estático para conectar estes dois Ases, em roteadores Cisco, use os seguintes comandos:

```
RouterA(config)#ip route 47.0.0.0 255.0.0.0 80.4.4.5
RouterA(config)#ip route 48.0.0.0 255.0.0.0 80.4.4.5
RouterB(config)#ip route 45.0.0.0 255.0.0.0 80.4.4.4
RouterB(config)#ip route 46.0.0.0 255.0.0.0 80.4.4.4
```

Isto fala para cada AS como alcançar as redes no outro AS.

EGP – Exterior Gateway Protocol

Foi o primeiro exemplo de um protocolo de roteamento de gateway externo. EGP tem três componentes: Aquisição de Vizinho, Alcançabilidade do Vizinho e Informação de Roteamento.

A informação de roteamento do EGP é similar aos protocolos de vetor de distancia, mas ele omite a métrica para as rotas propagadas. EGP foi implementado desta forma pois ele foi projetado para internet, quando foi assumido que haveria rede central, com domínios de roteamento conectado à estes centro por um roteador. O maior problema quando usar EGP em uma rede mais generalizada é que, como não é feito uso de métricas, se há mais de um caminho para um destino, pacotes muito facilmente podem cair em loops de roteamento.

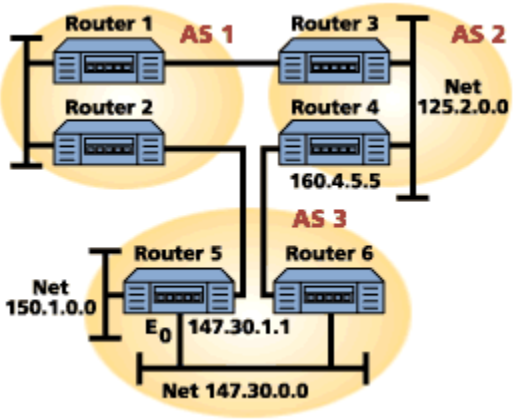
BGP – Border Gateway Protocol

Foi introduzido para melhor o desempenho sobre o EGP. A principal característica do BGP é que foi introduzido um protocolo de transporte confiável, para assegurar que as atualizações de roteamento foram recebidas. Também implementa um mecanismo de keepalive. Para assegurar que o roteador BGP conheça se os roteadores BGP na sua vizinhança apresentam falha. BGP não transmite métrica em suas mensagens de atualizações de roteamento, mas transmite um caminho para cada AS que lista os ASes a serem visitado no caminho para o AS de destino, evitando assim o problema de loop nos pacotes que acontece no EGP.

BGP trabalha com políticas de escolha de melhor caminho ou como alcançar determinado AS ou rede pré definidas. Uma política pode ser manualmente configurada e permite a um roteador BGP fazer uma lista das possíveis rotas para outro AS, selecionado o melhor caminho.

Configurando BGP

Nós podemos usar um exemplo para discutir como configurar BGP em um roteador. Neste exemplo vamos pegar o router6.



Configuração de Rede para o Exemplo BGP

- Definir BGP como processo de roteamento;
- Determinar as redes internas a este AS que serão propagadas as rotas;
- Definir o relacionamento que esses roteadores terão com os vizinhos;
- Atribuir pesos administrativos aos caminhos para controlar o processo de seleção de caminho.

Esta é uma configuração básica para BGP, entretanto há muitas outras configurações que podem ser implantadas.

Os seguintes comando são aplicados no router 6:

```
Router6(config)#router bgp 3
Router6(config-router)#network 147.30.0.0
Router6(config-router)#network 150.1.0.0
Router6(config-router)#neighbor 147.30.1.1 remote-as 3
Router6(config-router)#neighbor 160.4.5.5 remote-as 2
```

A primeira linha nesta configuração define BGP no AS 3 para o router 6. As próximas linhas definem as redes internas ao AS 3 que serão propagadas via BGP. A quarta linha define um vizinho interno, que está no mesmo AS. O processo BGP no router 6 irá agora trocar informações com um processo BGP definido no router 5. A quinta linha define um vizinho em um AS diferente no qual o router 6 irá trocar informação.

O efeito desta configuração é que o router 6 irá dividir informações sobre as redes 147.30.0.0 e 150.1.0.0 com os dois routers especificados via atualizações BGP.

A ultima coisa a fazer nesta configuração básica de BGP, é atribuir pesos administrativos para controlar o processo de seleção de caminho. No exemplo, um peso de 40000 é atribuído ao caminho para router 4.

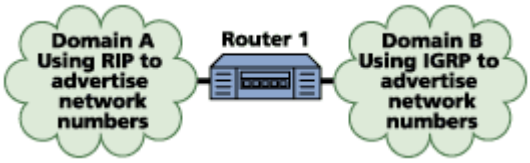
```
Router6(config-router)#neighbor 160.4.5.5 40000
```

Este peso administrativo pode variar entre 0 e 65535, e o default é 32768. O efeito de aumentar o peso para o router 4 é fazer menos atrativo quando R6 está calculando qual caminho usar.

Redistribuindo Informações de Rotas Entre Protocolos

Se você tiver a oportunidade de construir uma rede do zero, e pudesse projeta-la de tal modo que somente dispositivos que rodariam protocolos de roteamento fossem routers, você poderia escolher seu protocolo favorito e usá-lo exclusivamente. Embora tipicamente o que exista na prática é que a rede já existe rodando um protocolo de roteamento. Máquinas UNIX possuem algumas responsabilidades de roteamento em algumas redes. Como muitas máquinas UNIX suportam apenas RIP, e é improvável será a melhor escolha de protocolo de roteamento para uma rede de qualquer tamanho. A questão envolve quantos protocolos de roteamento podem coexistir em uma mesma rede, permanentemente ou em um período de migração.

A resposta é Redistribuição. Um router pode ser configurado para rodar mais de um protocolo e redistribuir informações de rotas entre os dois protocolos. A idéia é que haverá múltiplos domínios na rede, cada um operando com um protocolo diferente. Na fronteira ou borda entre esses dois domínios, um router tem a responsabilidade de rodar ambos protocolos e informar cada domínio sobre as outras redes no protocolo apropriado. Isso é ilustrado abaixo.



Um roteador de borda configurado para redistribuir entre RIP e IGRP

Neste exemplo, router 1 tem que rodar RIP e IGRP, então informar ao domínio A sobre as redes no domínio B com atualizações RIP , e informar ao domínio B sobre as redes no domínio A usando atualizações IGRP. O router desta figura será capaz de atribuir uma métrica para todas as rotas que ele redistribui de um domínio para o outro. Ele não pode traduzir métricas de um protocolo para o outro. A princípio isto pode ser visto como um problema, pois todas as redes são redistribuídas com o valor da mesma métrica, não importando onde elas e alocam no outro domínio. Na realidade isto não é problema, desde que para alcançar o domínio B do domínio A, todas as conexões passem através do mesmo router, então a parte inicial da “viajem” é identificar quando enviar pacotes entre domínios.

Neste exemplo, um pacote destinado para o domínio A, originando no domínio B, alcança o roteador 1. Router 1 tem então sua tabela de roteamento preenchida com entradas para as redes

no domínio A que foram calculadas usando atualizações RIP. O pacote então encontrará o melhor caminho para a rede de destino.

A seguir um exemplo de como um processo de roteamento poderia ser configurado no router 1, para redistribuir rotas entre dominios RIP e IGRP.

Dada uma configuração básica para IGRP e RIP, os comandos de redistribuição estão em negrito:

```
router igrp 12
timers basic 15 45 0 60
network 164.8.0.0
network 193.1.1.0
no metric holddown
metric maximum-hop 50
redistribute rip
default - metric 300 344 200 200 200

router rip
network 150.1.0.0
network 120.0.0.0
redistribute igrp 12
default-metric 3
```

Isto assume que o Domínio A tem redes 150.1.0.0 e 120.0.0.0 e Domínio B tem redes 164.8.0.0 e 193.1.1.0.

Os cinco valores no comando default-metric na seção router IGRP são as métricas que serão enviados em atualizações IGRP, para rotas aprendidas via RIP. Na seção router RIP, rotas aprendidas das atualizações IGRP será propagadas com a métrica 3.