

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

**PROCESSO DE ROTEAMENTO
E SEUS PROTOCOLOS**

SORAYA CHRISTIANE S. DE SOUSA

NATAL/RN
2010

SORAYA CHRISTIANE S. DE SOUSA

**PROCESSO DE ROTEAMENTO
E SEUS PROTOCOLOS**

Monografia apresentada ao curso de
Especialização em Redes de Computadores da
Faculdade Natalense para o Desenvolvimento do
Rio Grande do Norte como requisito parcial para
a obtenção do título de Especialista em Redes de
Computadores.

Orientador:

Alúzio Ferreira da Rocha Neto, M.Sc.

NATAL/RN

2010

SORAYA CHRISTIANE S. DE SOUSA

**PROCESSO DE ROTEAMENTO
E SEUS PROTOCOLOS**

Monografia apresentada a Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte e aprovada em ____ de _____ de _____, pela banca examinadora composta pelos seguintes membros:

M.Sc. Aluizio Ferreira da Rocha Neto (Orientador)

Membro examinador

Membro examinador

Natal/RN

2010

Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Souza, Soraya Christiane S. de
Processo de roteamento e seus protocolos / Soraya Christiane S. de
Souza. – Natal: FARN, 2008.
46 f.

Orientador: Aluísio Ferreira de Rocha Neto (Msc.)
Monografia (Especialização em Redes de Computadores) –
Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Roteamento de Redes – Monografia. 2. Protocolo de Redes –
Monografia. 3. Previdência Privada – Monografia. 4. Redes de
Computadores – Monografia. I. Título.

RN/FARN/BC

CDU 004.7

RESUMO

Este trabalho tem como finalidade entender como e através de quem ocorre o processo de roteamento e seus protocolos, desenvolvendo uma compreensão de como um roteador aprende redes remotas e determina o melhor caminho para essas redes. Ao examinar os protocolos, tem-se uma melhor perspectiva dos conceitos propriamente ditos e um entendimento de como é possível implementar, verificar, identificar e solucionar problemas das operações de roteamento cada vez mais comuns nos cenários de rede.

Palavras-chave: roteamento, protocolos, redes, solucionar problemas.

ABSTRACT

This work has to purpose understand the process of routing and protocols, developing an understanding how a router learn remote networks and determines the best path for these networks. By examining the protocols, we have a better understanding of the concepts themselves and an understanding of how you can implement, verify, identify and troubleshoot the operations routing increasingly common in network scenarios.

Keywords: routing protocols, networks, troubleshoot.

SUMÁRIO

1	INTRODUÇÃO	9
1.1	PROBLEMA DA PESQUISA	9
1.2	OBJETIVOS	9
1.2.1	Objetivos Específicos	10
1.3	JUSTIFICATIVA	10
2	REFERENCIAL TEÓRICO	11
2.1	CAMADA DE REDE.....	11
2.2	COMO OS PACOTES DE DADOS SÃO GERENCIADOS	16
2.3	O ROTEADOR COMO ELEMENTO CENTRAL DA REDE	20
3	PROTOCOLOS DE ROTEAMENTO.....	23
3.1	ROTEAMENTO ESTÁTICO E DINÂMICO	23
3.2	CLASSIFICAÇÃO DOS PROTOCOLOS DE ROTEAMENTO DINÂMICO.....	26
3.3	METRICA E DISTÂNCIA ADMINISTRATIVA	31
3.4	PROTOCOLOS DE ROTEAMENTO VETOR DISTÂNCIA	33
3.4.1	RIP	35
3.4.2	IGRP	37
3.4.3	EIGRP	38
3.5	PROTOCOLOS DE ROTEAMENTO LINK STATE	41
3.5.1	OSPF	42
4	CONSIDERAÇÕES FINAIS	45
	REFERÊNCIAS BIBLIOGRÁFICAS	46

LISTA DE FIGURAS

Figura 1: Camada de Rede. Fonte: (CCNA Discovery, 2010).	12
Figura 2: Independência dos Meios Físicos. Fonte: (CCNA Discovery, 2010).	15
Figura 3: Descarte dos pacotes sem rotas. Fonte: (CCNA Discovery, 2010).	18
Figura 4: Encaminhamento de pacotes através dos roteadores. Fonte: (CCNA Discovery, 2010)	21
Figura 5: Diversidade de roteadores. Fonte: (CCNA Discovery, 2010).	22
Figura 6: Comparação entre roteamento estático e dinâmico. Fonte: (CCNA Exploration, 2010).	24
Figura 7: Protocolos de Roteamento Comuns. Fonte: (CCNA Exploration, 2010).	25
Figura 8: Tipos de Protocolos de Roteamento. Fonte: (CCNA, 2008).	26
Figura 9: Comparação do modo de funcionamento entre Vetor de Distância e Link State. Fonte: (CCNA, 2008).	27
Figura 10: Distância Administrativa dos Protocolos de Roteamento. Fonte: (CCNA Exploration, 2010).	32
Figura 11: Vantagens e Desvantagens dos Protocolos Vetor Distância. Fonte: (CCNA Discovery, 2010).	35
Figura 12: Comparação entre as versões do RIP. Fonte: (CCNA, 2008).	37
Figura 13: Comparação entre protocolos Distância Vetor e Link State. Fonte: (CCNA, 2008).	42

1 INTRODUÇÃO

É incrível o quão rápido as redes e em especial a Internet se tornou parte integral da vida diária das pessoas. As redes de dados, que anteriormente transportavam informações entre empresas, ganharam um novo propósito, o de melhorar a qualidade de vida de pessoas em toda parte.

As redes atuais têm um impacto significativo, pois alteram a forma como elas vivem, trabalham e se divertem. Cada vez mais, as pessoas utilizam a comunicação em todos os lugares e daí a importância de se ter uma tecnologia eficiente e confiável a qual permita que as redes estejam disponíveis quando e onde forem necessárias.

Assim, as redes de computadores – e, em um contexto mais amplo, a Internet – permite a cada pessoa se comunicar, colaborar e interagir de maneira jamais vista. Usa-se a rede de várias formas, aplicativos Web, telefonia IP, videoconferência, jogos interativos, comércio eletrônico, educação e muito mais.

No centro está o roteador que conecta uma rede a outra. Por isso, ele é tão importante. Ele é responsável pela entrega de pacotes em redes diferentes.

Logo, a efetividade da comunicação das redes interconectadas depende, amplamente da capacidade dos roteadores de encaminhar pacotes da maneira eficiente, de forma a atender às demandas das redes atuais, seja ao assegurar disponibilidade 24 horas por dia, 7 dias por semana, garantir serviços integrados, qualidade de serviço ou atenuar o impacto de worms, vírus e outros ataques a rede, permitindo ou negando o encaminhamento de pacotes.

1.1 PROBLEMA DA PESQUISA

A importância dessa pesquisa é entender o que são os roteadores, seu papel na rede, como atuam no processo de roteamento e de que forma interagem com os protocolos dinâmicos para garantir a efetividade dos serviços e das redes convergentes atuais.

1.2 OBJETIVOS

O objetivo principal deste trabalho é entender a importância do processo de roteamento em uma rede de computadores, seus atores principais e os protocolos responsáveis pela efetivação desse processo.

1.2.1 Objetivos Específicos

Para atingir o objetivo principal, as seguintes etapas foram seguidas:

- Conhecer o que é um roteador;
- Como ele funciona e de que fatores dependem o processo de roteamento;
- Entender quais as características relacionadas a cada protocolo de roteamento dinâmico.

1.3 JUSTIFICATIVA

À medida que as empresas crescem e evoluem, o mesmo acontece com suas necessidades na rede. A rede seja ela corporativa ou pessoal é largamente utilizada para respaldar as atividades empresariais, seja no suporte a aplicações críticas, ao suportar o tráfego de uma rede convergente ou a necessidade de um controle centralizado.

E esse controle fundamental é desenvolvido em grande parte pelos equipamentos de borda como os roteadores, que impedem que cargas de broadcast congestionem os canais principais de comunicação e garantam a eficiência dos serviços de rede, que proporcionam serviços com priorização, redundância nas rotas, falhas, maximização da largura de banda, comunicação e até segurança, ao proteger a rede contra ataques. Sendo portanto um assunto de grande importância a ser discutido ao longo deste trabalho.

2 REFERENCIAL TEÓRICO

2.1 CAMADA DE REDE

A camada de rede, ou Camada 3 do modelo de referência OSI, fornece serviços para realizar trocas de fragmentos individuais de dados na rede entre dispositivos finais identificados. Para realizar este transporte de uma extremidade à outra, a camada 3 utiliza quatro processos básicos:

- Endereçamento
- Encapsulamento
- Roteamento
- Desencapsulamento

Primeiro, a camada de rede precisa fornecer o mecanismo de endereçamento destes dispositivos finais. Se fragmentos individuais de dados precisam ser direcionados a um dispositivo final, este dispositivo precisa ter um endereço único. Em uma rede IPv4, quando este endereço é atribuído a um dispositivo, o dispositivo passa a ser chamado de host.

Em segundo lugar, a camada de rede precisa fornecer o encapsulamento. Além da necessidade dos dispositivos serem identificados com um endereço, os fragmentos individuais (as PDUs da camada de rede) também devem conter estes endereços. Durante o processo de encapsulamento, a camada 3 recebe a PDU da camada 4 e acrescenta um cabeçalho ou rótulo da camada 3 para criar uma PDU da camada 3. Ao fazer referência à camada de rede, esta PDU é chamada de pacote. Quando se cria um pacote, o cabeçalho deve conter, entre outras informações, o endereço do host para o qual ele está sendo enviado. Este endereço é chamado de endereço de destino. O cabeçalho da camada 3 também contém o endereço do host de origem. Este endereço é chamado de endereço de origem (CCNA *Exploration*, 2010).

Depois que a camada de rede completa seu processo de encapsulamento, o pacote é enviado para a camada de enlace de dados a ser preparada para o transporte através do meio físico.

Em seguida, a camada de rede precisa fornecer serviços para direcionar estes pacotes a seu host de destino. Os hosts de origem e de destino nem sempre estão conectados à mesma rede. De fato, o pacote pode ter que viajar através de muitas redes diferentes. Ao longo do

caminho, cada pacote precisa ser guiado através da rede para chegar a seu destino final. Os dispositivos intermediários que conectam as redes são chamados roteadores. E o papel deles é selecionar o caminho e direcionar os pacotes a seus destinos. Este processo é conhecido como roteamento.

Durante o roteamento através de uma rede, o pacote pode atravessar muitos dispositivos intermediários. Cada rota do pacote para chegar ao próximo dispositivo é chamada de salto. Conforme o pacote é direcionado, seu conteúdo (a PDU da camada de transporte) permanece intacto até a chegada ao host de destino.

Finalmente, o pacote chega ao host de destino e é processado na camada 3. O host examina o endereço de destino para verificar se o pacote estava endereçado para este dispositivo.

Se o endereço estiver correto, o pacote é desencapsulado pela camada de rede e a PDU da camada 4 contida no pacote é passado para o serviço apropriado da camada de transporte.

Diferente da camada de transporte (camada 4 do OSI), que gerencia o transporte de dados entre os processos em execução em cada host final, os protocolos de camada de rede especificam a estrutura e o processamento dos pacotes usados para carregar os dados de um host para outro. O funcionamento sem consideração aos dados das aplicações carregadas em cada pacote permite que a camada da rede leve pacotes para diversos tipos de comunicações entre múltiplos hosts (CCNA *Exploration*, 2010).

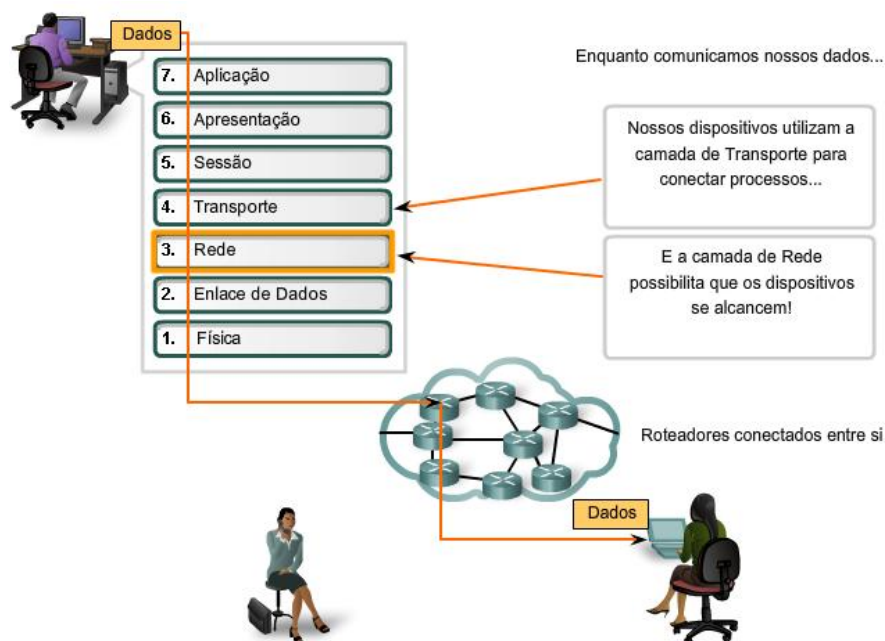


Figura 1: Camada de Rede. Fonte: (CCNA Discovery, 2010).

Entre os protocolos implementados na camada de rede que transportam os dados de usuários incluem:

- *Internet Protocol version 4 (IPv4)*
- *Internet Protocol version 6 (IPv6)*
- *Novell Internetwork Packet Exchange (IPX)*
- *AppleTalk*
- *Connectionless Network Service (CLNS/DECNet)*

O *Internet Protocol* (IPv4 e IPv6) é o protocolo mais usado para transporte de dados da camada 3. O *Internet Protocol* foi elaborado como um protocolo com baixo *overhead*. Ele somente fornece as funções necessárias para enviar um pacote de uma origem a um destino por um sistema de redes. O protocolo não foi elaborado para rastrear e gerenciar o fluxo dos pacotes. Estas funções são realizadas por outros protocolos de outras camadas. Dentre as características básicas do IPv4 tem-se que ele é um protocolo:

- Sem conexão - Nenhuma conexão é estabelecida antes do envio dos pacotes de dados.
- Melhor Esforço (não confiável) - Nenhum cabeçalho é usado para garantir a entrega dos pacotes.
- Independente de Meios Físicos - Opera independentemente do meio que transporta os dados.

Um exemplo de comunicação sem conexão é enviar uma carta a alguém sem notificar o destinatário com antecedência. As comunicações de dados sem conexão funcionam sob o mesmo princípio. Os pacotes IP são enviados sem notificar o host final de que eles estão chegando (CCNA *Exploration*, 2010)..

Os protocolos orientados a conexão, como o TCP, requerem que sejam trocados dados de controle para estabelecer a conexão, assim como campos adicionais no cabeçalho da PDU. Em razão do IP ser sem conexão, ele não requer uma troca inicial de informações de controle para estabelecer uma conexão entre as extremidades antes do envio dos pacotes, nem requer campos adicionais no cabeçalho da PDU para manter esta conexão. Este processo reduz muito o cabeçalho IP.

Entretanto, a entrega de pacotes sem conexão pode resultar na chegada dos pacotes ao destino fora de sequência. Se a entrega de pacotes foi feita fora de ordem ou ocorreu a falta de

pacotes, isso criará problemas para a aplicação que usarão os dados e os serviços das camadas superiores terão que resolver estas questões.

O protocolo IP não onera o serviço IP ao não proporcionar confiabilidade. Em comparação com um protocolo confiável, o cabeçalho IP é menor. O transporte destes cabeçalhos menores requer menos *overhead*. Menos *overhead* significa menos atraso na entrega. Esta característica é desejável para um protocolo da camada 3 (CCNA *Exploration*, 2010)..

Assim, missão da camada 3 é transportar os pacotes entre os hosts, e ao mesmo tempo sobrecarregar a rede o menos possível. A camada 3 não tem preocupações nem ciência sobre o tipo de comunicação contida dentro de um pacote. Esta responsabilidade é papel das camadas superiores, conforme necessário. As camadas superiores podem decidir se a comunicação entre serviços precisa de confiabilidade e se esta comunicação pode tolerar os requisitos de confiabilidade do *overhead*.

O IP geralmente é considerado um protocolo não confiável. Neste contexto, não confiável não significa que o IP trabalhe adequadamente algumas vezes e não funcione bem outras vezes. Isso também não quer dizer que ele não seja adequado como protocolo de comunicação de dados.

O significado de não confiável é simplesmente que o IP não possui a capacidade de gerenciar e recuperar pacotes não entregues ou corrompidos. Como os protocolos de outras camadas conseguem gerenciar a confiabilidade, o IP consegue funcionar com grande eficiência na camada de rede. Se fosse incluído um cabeçalho de confiabilidade no protocolo da camada 3, as comunicações que não requerem conexões ou confiabilidade seriam sobrecarregadas com o consumo de largura de banda e o atraso produzido por este cabeçalho.

No conjunto TCP/IP, a camada de transporte pode escolher entre TCP ou UDP, com base nas necessidades de comunicação. Assim, com todo o isolamento de camadas proporcionado pelos modelos de rede, deixar a decisão sobre confiabilidade para a camada de transporte torna o IP mais adaptável e fácil de se acomodar com diferentes tipos de comunicação.

Logo, o cabeçalho de um pacote IP não inclui campos necessários para uma entrega de dados confiável. Não há confirmações da entrega de pacotes. Não há controle de erros para os dados. Também não existe nenhuma forma de rastreamento de pacotes, e por isso não há possibilidade de retransmissão. A camada de rede também não fica sobrecarregada com as características do meio físico em que os pacotes serão transportados. O IPv4 e o IPv6 operam

independentemente do meio físico que transporta os dados nas camadas inferiores da pilha de protocolo.

Conforme mostra a figura 02, qualquer pacote IP individual pode ser passado eletricamente por cabo, como os sinais ópticos nas fibras, ou sem fio como sinais de rádio. É responsabilidade da camada de Enlace de Dados do OSI pegar um pacote IP e prepará-lo para transmissão pelo meio físico de comunicação. Isso quer dizer que o transporte de pacote IP não está limitado a nenhum meio físico particular.

Porém, existe uma característica de grande importância do meio físico que a camada de rede considera: o tamanho máximo da PDU que cada meio físico consegue transportar. Esta característica é chamada de *Maximum Transmission Unit (MTU)*. Parte das comunicações de controle entre a camada de enlace de dados e a camada de rede é o estabelecimento de um tamanho máximo para o pacote. A camada de enlace de dados envia a MTU para cima, para a camada de rede. A camada de rede determina então o tamanho de criação dos pacotes (CCNA *Exploration*, 2010).

Em alguns casos, um dispositivo intermediário (geralmente um roteador) precisará dividir o pacote ao enviá-lo de um meio físico para outro com uma MTU menor.

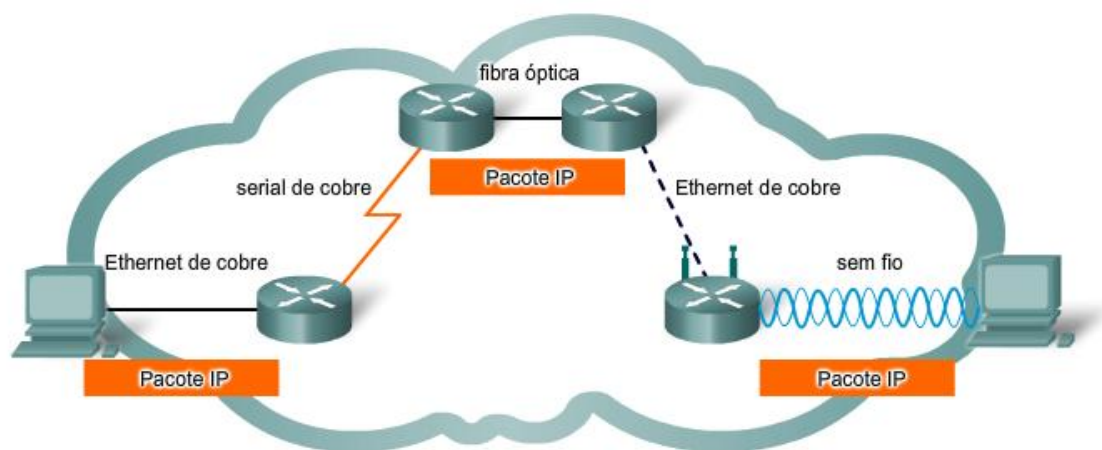


Figura 2: Independência dos Meios Físicos. Fonte: (CCNA Discovery, 2010).

Também na camada de rede, outro aspecto importante são os protocolos. Os protocolos roteados transportam dados através de uma rede e os protocolos de roteamento permitem que os roteadores escolham o melhor caminho para os dados, da origem ao destino.

As funções de um protocolo roteado abrangem:

- Incluir qualquer conjunto de protocolos de rede que forneça informações suficientes em seu endereço de camada de rede para que um roteador o encaminhe ao próximo dispositivo e, por fim, ao seu destino.
- Definir o formato e o uso dos campos em um pacote.

O *Internet Protocol (IP)* e o *Internetwork Packet Exchange (IPX)* da Novell são exemplos de protocolos roteados (XAVIER, 2004).

Já os roteadores usam protocolos de roteamento para trocar tabelas e compartilhar informações de roteamento. Em outras palavras, os protocolos de roteamento permitem que os roteadores direcionem protocolos roteados.

Assim, nas funções de um protocolo de roteamento incluem:

- Fornecer processos para o compartilhamento de informações de rota .
- Permitir que os roteadores comuniquem-se uns com os outros para atualizar e manter as tabelas de roteamento.

Exemplos de protocolos de roteamento que suportam o protocolo roteado IP incluem Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP) e Enhanced IGRP (EIGRP) (XAVIER, 2004).

2.2 COMO OS PACOTES DE DADOS SÃO GERENCIADOS

Dentro de uma rede ou sub-rede, os hosts se comunicam uns com os outros sem necessidade de qualquer dispositivo intermediário da camada de rede. Quando um host precisa se comunicar com outra rede, um dispositivo intermediário ou roteador atua como gateway para a outra rede.

Como parte de sua configuração, um host possui um gateway padrão definido. Este endereço de gateway é o endereço da interface de um roteador que está conectado à mesma rede do host. É importante observar que não é possível para um host específico conhecer o endereço de todos os dispositivos da Internet com o qual ele poderá ter que se comunicar. Logo, para comunicar-se com um dispositivo em outra rede, o host usa o endereço deste gateway ou gateway padrão para encaminhar um pacote para fora de sua rede local.

O roteador também precisa de uma rota que defina para onde encaminhar o pacote logo em seguida. Isso é chamado de endereço do próximo salto. Se uma rota estiver disponível para o roteador, ele encaminhará o pacote para o roteador de próximo salto que oferece o caminho para a rede de destino.

Como foi observado, a função da camada de rede é transferir os dados do host que os originou para o host que os utilizará. Durante o encapsulamento no host de origem, um pacote IP é construído na camada 3 para transportar a PDU da camada 4. Se o host de destino estiver na mesma rede do host de origem, o pacote será entregue entre os dois hosts no meio físico local sem a necessidade de um roteador.

Entretanto, se o host de destino e o host de origem não estiverem na mesma rede, o pacote poderá transportar uma PDU da camada de transporte através de muitas redes e muitos roteadores.

Conforme isso ocorre, as informações nele contidas não são alteradas por nenhum roteador quando as decisões de encaminhamento são tomadas. A cada salto, as decisões de encaminhamento são baseadas nas informações do cabeçalho do pacote IP. O pacote e seu encapsulamento da camada de rede também permanecem praticamente intactos através de todo o processo, desde o host de origem até o host de destino.

Se a comunicação for entre os hosts de redes diferentes, a rede local entregará o pacote desde a origem até seu roteador de gateway. O roteador examina a porção de rede do endereço de destino do pacote e encaminha o pacote para a interface apropriada. Se a rede de destino for diretamente conectada a este roteador, o pacote será encaminhado diretamente ao host. Se a rede de destino não for diretamente conectada, o pacote será encaminhado para um segundo roteador que será o roteador de próximo salto.

Então, o encaminhamento do pacote será responsabilidade deste segundo roteador. Muitos roteadores ou saltos ao longo do caminho poderão processar o pacote antes da chegada ao destino.

O gateway, também conhecido como gateway padrão, é necessário para enviar um pacote para fora da rede local. Se a porção de rede do endereço de destino do pacote for diferente da rede do host de origem, o pacote terá que ser roteado para fora da rede original. Para que isso ocorra, o pacote é enviado para o gateway. Este gateway é a interface de um roteador conectado à rede local. A interface do gateway possui um endereço da camada de rede que corresponde ao endereço de rede dos hosts. Os hosts são configurados para reconhecer este endereço como o gateway.

Nenhum pacote pode ser encaminhado sem uma rota. Quer o pacote tenha origem em um host ou esteja sendo encaminhado por um dispositivo intermediário, o dispositivo precisa ter uma rota para identificar para onde encaminhar o pacote.

Um host precisa encaminhar um pacote para o host na rede local ou para o gateway, conforme apropriado. Para encaminhar os pacotes, o host precisa ter rotas que representem estes destinos.

Um roteador toma uma decisão de encaminhamento para cada pacote que chega à interface de gateway. Este processo de encaminhamento é chamado de roteamento. Para encaminhar um pacote para uma rede de destino, o roteador requer uma rota para essa rede. Se não existir uma rota para a rede de destino, o pacote não poderá ser encaminhado e será descartado, conforme representa a figura 3.

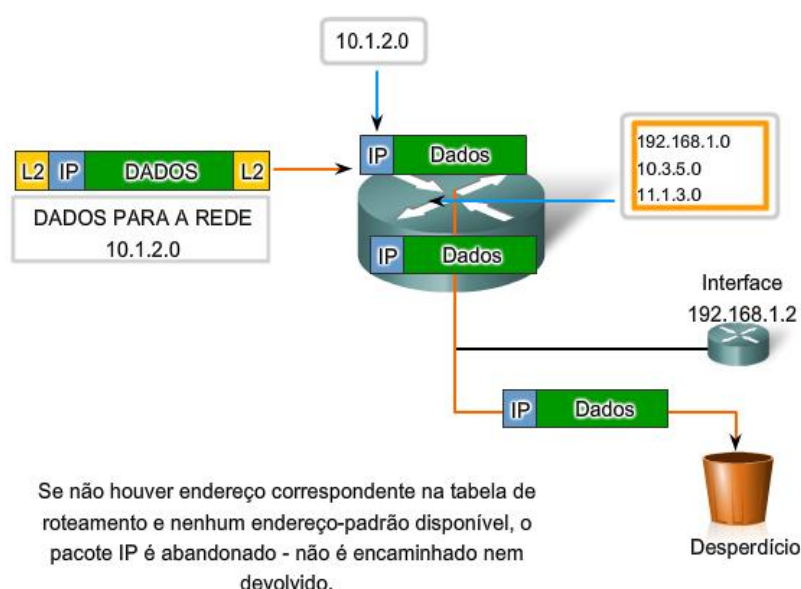


Figura 3: Descarte dos pacotes sem rotas. Fonte: (CCNA Discovery, 2010).

A rede de destino pode estar a alguns roteadores ou saltos de distância do gateway. A rota para essa rede indicaria somente o roteador de próximo salto para o qual o pacote deve ser encaminhado, e não o roteador final. O processo de roteamento usa uma rota para mapear o endereço da rede de destino para o próximo salto, e então encaminhar o pacote para o endereço deste próximo salto.

Uma rota para pacotes de destinos remotos é acrescentada com o uso do endereço do gateway padrão como o próximo salto. Embora isso geralmente não seja feito, um host também pode ter suas rotas acrescentadas manualmente por meio de configurações.

Assim como os dispositivos finais, os roteadores também adicionam rotas para redes conectadas à sua tabela de roteamento. Quando a interface de um roteador é configurada com um endereço IP e uma máscara de sub-rede, a interface torna-se parte dessa rede. Agora, a

tabela de roteamento inclui essa rede como uma rede diretamente conectada. Porém, todas as outras rotas precisam ser configuradas ou adquiridas por meio de um protocolo de roteamento. E para encaminhar um pacote, o roteador precisa saber para onde enviá-lo. Esta informação está disponível na forma de rotas em uma tabela de roteamento.

Assim, a tabela de roteamento armazena informações sobre redes conectadas e remotas. As redes conectadas estão diretamente ligadas a uma das interfaces do roteador. Estas interfaces são os gateways para os hosts em diferentes redes locais. As redes remotas são redes que não estão diretamente conectadas. As rotas para essas redes podem ser configuradas manualmente no roteador pelo administrador da rede, ou então apreendidas automaticamente com o uso de protocolos de roteamento.

Embora seja essencial para todos os roteadores ter um conhecimento abrangente das rotas, a manutenção da tabela de roteamento por configuração estática manual nem sempre é possível. Por isso, são utilizados os protocolos de roteamento dinâmico.

Os protocolos de roteamento são o conjunto de regras pelas quais os roteadores compartilham dinamicamente suas informações de roteamento. Conforme os roteadores apreendem as alterações ocorridas na rede nas quais atuam como gateways, ou apreendem as alterações nos links entre os roteadores, estas informações são passadas para outros roteadores.

Quando um roteador recebe informações sobre novas rotas ou alteração de rotas, ele atualiza sua própria tabela de roteamento e, por sua vez, passa essas informações para outros roteadores.

Desse modo, todos os roteadores possuem tabelas precisas que são atualizadas dinamicamente e podem aprender rotas para redes remotas que se localizam a muitos saltos de distância. Têm-se como protocolos de roteamento amplamente conhecidos:

- *Routing Information Protocol (RIP)*
- *Enhanced Interior Gateway Routing Protocol (EIGRP)*
- *Protocolo OSPF*

Embora eles forneçam tabelas de roteamento atualizadas aos roteadores, existem custos. Primeiro, a troca de informações de rotas adiciona *overhead*, que consome a largura de banda da rede. Este *overhead* pode ser um problema, especialmente para os links de baixa largura de banda entre os roteadores (XAVIER, 2004).

Em segundo lugar, as informações de rotas que um roteador recebe são processadas intensivamente por protocolos como EIGRP e OSPF, para criar as entradas na tabela de roteamento. Isso significa que os roteadores que empregam estes protocolos precisam ter capacidade de processamento suficiente tanto para implementar os algoritmos dos protocolos como para realizar em tempo hábil o roteamento e o encaminhamento dos pacotes.

O roteamento estático não produz nenhum *overhead* na rede e insere as entradas diretamente na tabela de roteamento, não requerendo nenhum processamento por parte do roteador. O custo do roteamento estático é administrativo: a configuração e manutenção manuais da tabela de roteamento o que asseguram um roteamento eficiente, para redes pequenas e menos complexas, já para grandes redes é inviável do ponto de vista operacional (XAVIER, 2004).

2.3 O ROTEADOR COMO ELEMENTO CENTRAL DA REDE

O roteamento é uma função da camada 3 do modelo OSI. É o processo de localizar o caminho mais eficiente entre dois dispositivos. Sendo o dispositivo primário que o executa, o roteador.

O roteador tem duas funções-chave: manter tabelas de roteamento e verificar se os outros roteadores conhecem as alterações na topologia da rede. Esta função é executada com o uso de um protocolo de roteamento para comunicar informações de rede a outros roteadores.

Quando os pacotes chegam a uma interface, o roteador deve usar a tabela de roteamento para determinar para onde enviá-los. O roteador comuta os pacotes para a interface apropriada, adiciona as informações de enquadramento necessárias à interface e transmite o quadro (CHAPPELL, 2007).

Ele é na verdade um computador com uma finalidade especial que desempenha um papel fundamental no funcionamento de qualquer rede de dados. E ele é o principal responsável por interconectar redes:

- Determinando o melhor caminho para enviar pacotes
- Encaminhando pacotes para o destino

Os roteadores executam o encaminhamento de pacotes, aprendendo as redes remotas e mantendo informações de roteamento.

O roteador é a junção ou a interseção que conecta várias redes IP. A decisão primária de encaminhamento dos roteadores se baseia nas informações de Camada 3, o endereço IP de

destino. A tabela de roteamento do roteador é usada para localizar a melhor correspondência entre o IP de destino de um pacote e um endereço de rede na tabela de roteamento. Ela acabará determinando a interface de saída que deve encaminhar o pacote, e o roteador encapsulará esse pacote no quadro de enlace de dados apropriado a essa interface de saída.

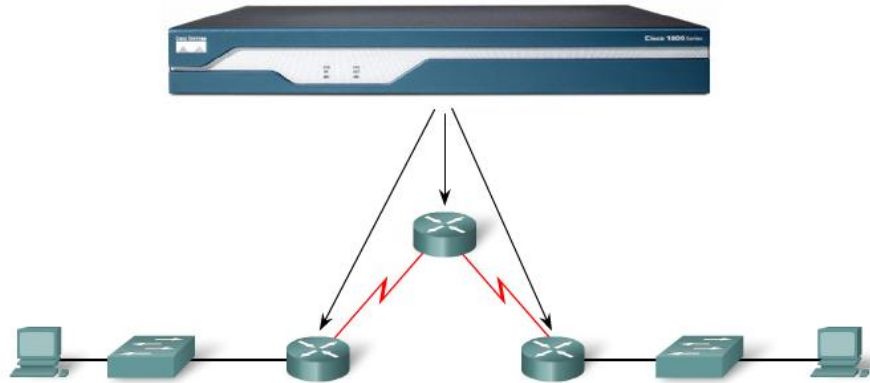


Figura 4: Encaminhamento de pacotes através dos roteadores. Fonte: (CCNA Discovery, 2010)

O roteador proporciona acesso a outras redes privadas, como também a Internet. Além de cumprir outras funções úteis.

- Oferece contenção de broadcast
- Conectam lugares remotos
- Proporciona segurança melhorada (com NAT e ACL)

Estando disponíveis em diversas formas, tamanhos, interfaces e funcionalidades, conforme representa a figura 5 (CCNA Discovery, 2010).

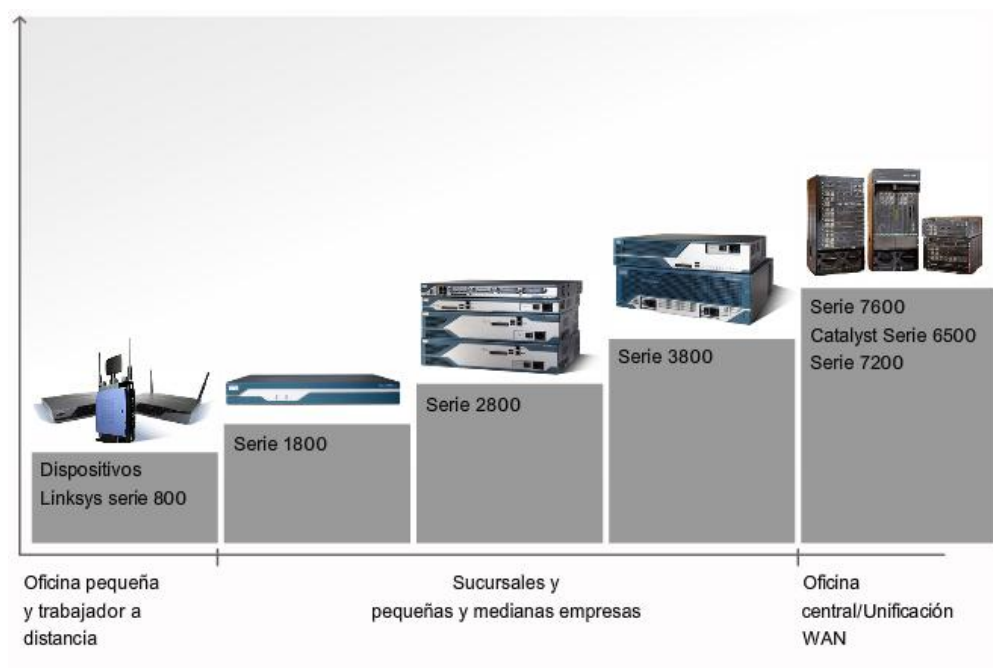


Figura 5: Diversidade de roteadores. Fonte: (CCNA Discovery, 2010).

Um roteador tem os mesmos componentes básicos de um PC desktop padrão como: CPU, memória, barramento do sistema e diversas interfaces de entrada/saída. Entretanto, os roteadores são projetados para realizar algumas funções muito específicas, que geralmente não são realizadas pelos computadores desktop. Por exemplo, os roteadores conectam e permitem a comunicação entre duas redes e determinam o melhor caminho para que os dados viajem através dessas redes conectadas.

Assim como os computadores precisam de sistemas operacionais para executar aplicativos de software, os roteadores precisam do IOS (*Internetwork Operating System – Sistema Operacional de Interconexão de Redes*) para executar as funções definidas nos arquivos de configuração. Esses arquivos de configuração contêm as instruções e os parâmetros que controlam o fluxo de tráfego que entra e sai dos roteadores.

Especificamente, usando protocolos de roteamento, os roteadores tomam decisões com relação ao melhor caminho para os pacotes. E os arquivos de configuração especificam todas as informações para uma configuração e uma utilização corretas dos protocolos roteados e de roteamento, selecionados ou ativados, no roteador (CHAPPELL, 2007).

3 PROTOCOLOS DE ROTEAMENTO

Os protocolos são usados para facilitar a troca de informações de roteamento entre roteadores. Eles permitem que os roteadores compartilhem informações dinamicamente sobre redes remotas e adicionam essas informações automaticamente às suas próprias tabelas.

Esses protocolos determinam o melhor caminho para cada rede adicionada à tabela de roteamento. Um dos principais benefícios do uso de um protocolo de roteamento dinâmico é que os roteadores trocam informações sempre que há uma alteração de topologia. Essa troca permite que os roteadores aprendam novas redes automaticamente e também localizem caminhos alternativos quando houver uma falha do link atual para uma rede (ODOM, 2003).

3.1 ROTEAMENTO ESTÁTICO E DINÂMICO

Comparados ao roteamento estático, os protocolos de roteamento dinâmico requerem uma sobrecarga administrativa menor. No entanto, para usar este tipo de protocolo é necessário dedicar parte dos recursos de um roteador à operação de protocolos, incluindo tempo de CPU e largura de banda de link de rede. Apesar dos benefícios do roteamento dinâmico, o estático ainda é usado. Há situações em que ele é mais apropriado e outras em que o roteamento dinâmico é a melhor escolha.

Um protocolo de roteamento é um conjunto de processos, algoritmos e mensagens usados para trocar informações de roteamento e preencher as tabela de roteamento com os melhores caminhos escolhidos pelo protocolo. Dentre suas finalidades estão:

- A detecção de redes remotas.
- A manutenção de informações de roteamento atualizadas.
- A escolha do melhor caminho para as redes de destino.
- A capacidade de localizar um novo melhor caminho, se o caminho atual não estiver mais disponível.

Assim, a detecção de rede é a capacidade que tem um protocolo de roteamento de compartilhar informações sobre as redes aprendidas com outros roteadores que também estão usando o mesmo tipo de protocolo. Em vez de configurar rotas estáticas para redes remotas em todos os roteadores, um protocolo de roteamento dinâmico permite aos roteadores aprender automaticamente essas redes com outros roteadores. Essas redes – e o melhor

caminho— são adicionadas à tabela de roteamento do roteador e denotadas como uma rede aprendida por um protocolo de roteamento dinâmico específico. Após a detecção de rede inicial, os protocolos atualizam e mantêm as redes em suas tabelas de roteamento. Eles não apenas criam uma determinação de melhor caminho para várias redes, mas também determina um novo melhor caminho caso o caminho inicial fique inutilizável ou caso a topologia seja alterada (ODOM, 2003).

Por essas razões, eles possuem vantagens em relação a rotas estáticas, conforme compara a figura 06. Os roteadores que usam protocolos dinâmicos compartilham automaticamente informações de roteamento com outros roteadores e compensam qualquer alteração feita na topologia sem envolver o administrador de rede.

	Roteamento dinâmico	Roteamento estático
Complexidade de configuração	Geralmente independente do tamanho da rede	Aumenta com o tamanho da rede
Conhecimento administrativo necessário	Conhecimentos avançados necessários	Nenhum conhecimento adicional necessário
Mudanças na topologia	Adaptáveis automaticamente às mudanças na topologia	Intervenção do administrador necessária
Dimensionando	Adequado para topologias simples e complexas	Adequado para topologias simples
Segurança	Menos seguro	Mais seguro
Uso de recursos	Utiliza CPU, memória e largura de banda de link	Nenhum recurso adicional necessário
Previsibilidade	A rota depende da topologia atual	A rota para o destino é sempre a mesma

Figura 6: Comparação entre roteamento estático e dinâmico. Fonte: (CCNA Exploration, 2010).

Todos os protocolos de roteamento têm a mesma finalidade: aprender redes remotas e adaptar-se rapidamente sempre que houver uma alteração na topologia. O método usado pelo protocolo, o algoritmo utilizado e as características operacionais desse protocolo é que variam.

Suas operações variam de acordo com o tipo de protocolo de roteamento e o próprio protocolo de roteamento. Em geral, as operações de um protocolo de roteamento dinâmico podem ser descritas da seguinte forma: O roteador envia e recebe mensagens de roteamento em suas interfaces. Compartilha mensagens e informações de roteamento com outros roteadores que estão usando o mesmo protocolo de roteamento. Trocam informações de roteamento para aprender redes remotas. E quando um roteador detecta uma alteração de topologia, o protocolo pode anunciar essa alteração a outros roteadores.

Há vários protocolos de roteamento dinâmico para IP. Aqui são lembrados alguns dentre os mais comuns:

- Protocolo de informações de roteamento (*RIP, Routing Information Protocol*)
- Protocolo de Roteamento de Gateway Interior (*IGRP, Interior Gateway Routing Protocol*)
- Protocolo de Roteamento de Gateway Interior Aprimorado (*EIGRP, Enhanced Interior Gateway Routing Protocol*)
- Abrir caminho mais curto primeiro (*OSPF, Open Shortest Path First*)
- Sistema Intermediário para Sistema Intermediário (*IS-IS, Intermediate System-to-Intermediate System*)
- Protocolo de Roteamento de Borda (*BGP, Border Gateway Protocol*)

	Protocolos de roteamento do vetor de distância	Protocolos de roteamento Link-state	Vetor de caminho
Classful	RIP	IGRP	EGP
Classless	RIPv2	EIGRP	OSPFv2
IPv6	RIPng	EIGRP para IPv6	OSPFv3
			IS-IS para IPv6
			BGPv4 para IPv6

Figura 7: Protocolos de Roteamento Comuns. Fonte: (CCNA Exploration, 2010).

Como a Internet é baseada no conceito de sistema autônomo (administração comum), os protocolos de roteamento são classificados em: protocolos de roteamento interior e exterior.

Protocolos de gateway interior (IGP, *Interior Gateway Protocol*) são usados para roteamento de sistema intra-autônomo - roteamento dentro de um sistema autônomo.

Protocolos EGP (*Exterior Gateway Protocol*) são usados para roteamento de sistema inter-autônomo - roteamento entre sistemas autônomos.

Os IGPs são usados para roteamento dentro de um domínio de roteamento, redes sob controle de uma única organização. Geralmente, um sistema autônomo é formado por muitas redes individuais que pertencem a empresas, escolas e outras instituições e incluem RIP, IGRP, EIGRP, OSPF e IS-IS.

Por outro lado, os EGPs foram projetados para o uso entre sistemas autônomos diferentes que estejam sob o controle de administrações diferentes.

O BGP é o único EGP atualmente viável e é o protocolo de roteamento usado pela Internet. O BGP é um protocolo de vetor de caminho que pode usar muitos atributos diferentes para medir rotas, normalmente usado entre *ISPs*.

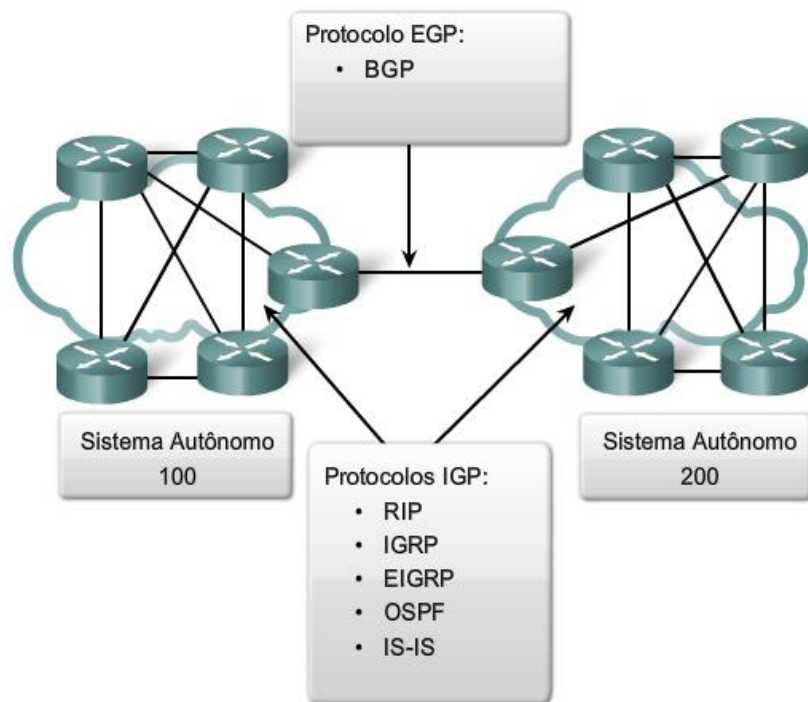


Figura 8: Tipos de Protocolos de Roteamento. Fonte: (CCNA, 2008).

3.2 CLASSIFICAÇÃO DOS PROTOCOLOS DE ROTEAMENTO DINÂMICO

Os Protocolos de Gateway Interior (*IGP, Interior Gateway Protocol*) são os mais comumente estudados e podem ser classificados em dois tipos:

- Protocolos de roteamento do vetor de distância
- Protocolos de roteamento Link-state ou Estado de Link

Vetor de distância significa que as rotas são anunciadas como vetores de distância e direção. A distância é definida em termos de uma métrica como contagem de saltos e a direção é dada simplesmente pelo roteador do próximo salto ou pela interface de saída. Esse tipo de protocolo normalmente usa o algoritmo *Bellman-Ford* para determinar a melhor rota.

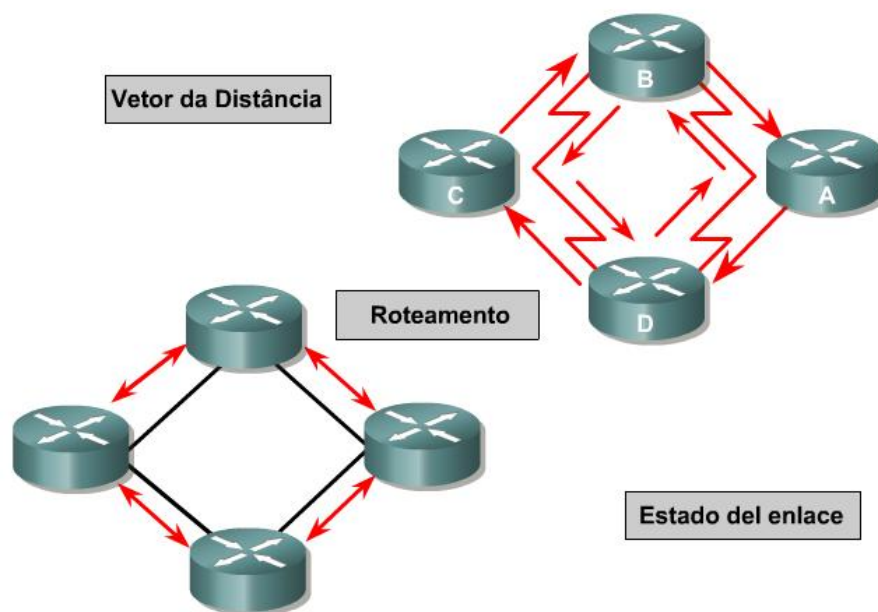


Figura 9: Comparação do modo de funcionamento entre Vetor de Distância e Link State. Fonte: (CCNA, 2008).

Alguns protocolos do vetor de distância enviam periodicamente tabelas de roteamento completas a todos os vizinhos conectados. Em redes grandes, essas atualizações de roteamento podem ficar enormes, causando tráfego significativo nos links.

Embora esse algoritmo acabe acumulando conhecimentos suficientes para manter um banco de dados de redes alcançáveis, ele não permite que um roteador aprenda a topologia exata de redes interconectadas. O roteador só conhece as informações de roteamento recebidas de seus vizinhos. Eles usam os roteadores como postagens de sinal ao longo do caminho para o destino final. As únicas informações que um roteador conhece sobre uma rede remota são a distância ou a métrica para alcançar essa rede e o caminho ou a interface que devem ser usados para isso. Eles não têm um mapa real da topologia da rede. Mas podem funcionar melhor em situações nas quais:

- A rede seja simples ou fixa e não requeira um design hierárquico especial.
- Os administradores não tenham conhecimentos suficientes para configurar e solucionar os problemas dos protocolos link-state.
- Ou os tempos de convergência inesperadas em uma rede não sejam uma preocupação.

Em comparação com a operação do protocolo de roteamento vetor de distância, um roteador configurado com um protocolo link-state pode criar uma “exibição completa” ou topologia da rede coletando informações de todos os outros roteadores (LEINWANT, 2002).

Para continuar na analogia de postagens de sinal, usar um protocolo de roteamento link-state é como ter um mapa completo da topologia da rede. As postagens de sinal ao longo do caminho, da origem ao destino, não são necessárias, pois todos os roteadores link-state estão usando um "mapa" idêntico da rede. Um roteador link-state usa essas informações para criar um mapa de topologia e selecionar o melhor caminho para todas as redes de destino da topologia.

Diferente dos protocolos de roteamento do vetor de distância, que enviam atualizações periódicas de suas informações de roteamento aos seus vizinhos. Os protocolos de roteamento link-state não usam atualizações periódicas. Depois que a rede converge, a atualização de link-state só será enviada quando houver uma alteração na topologia. Logo, eles funcionam melhor em situações nas quais:

- O design de rede é hierárquico, o que normalmente ocorre em grandes redes.
- Os administradores têm um bom conhecimento do protocolo de roteamento implementado.
- A convergência rápida da rede é crucial.

A convergência ocorre quando as tabelas de roteamento de todos os roteadores estão em um estado de consistência. Haverá convergência na rede quando todos os roteadores tiverem informações completas e precisas sobre ela. O tempo de convergência é o tempo que os roteadores levam para compartilhar informações, calcular os melhores caminhos e atualizar suas tabelas de roteamento. Para que uma rede seja completamente operável, é necessário que haja convergência nela. Portanto, a maioria das redes requer pouco tempo de convergência (LEINWANT, 2002).

As propriedades da convergência incluem a velocidade de propagação das informações de roteamento e o cálculo de caminhos ideais. Os protocolos de roteamento podem ser classificados com base na velocidade de convergência; quanto mais rápida for a convergência, melhor será o protocolo de roteamento. Geralmente, o RIP e o IGRP são lentos para convergir, enquanto o EIGRP e o OSPF são mais rápidos.

Roteadores que executam um protocolo de roteamento link-state enviam informações sobre o estado dos links desse protocolo para outros roteadores no domínio de roteamento. O

estado desses links refere-se a suas redes diretamente conectadas e inclui informações sobre o tipo de rede e todos os roteadores vizinhos nessas redes – daí o nome protocolo.

O objetivo final é que cada roteador receba todas as informações sobre todos os outros roteadores na área de roteamento. Com essas informações cada roteador pode criar seu próprio mapa topológico da rede e calcular de maneira independente o caminho mais curto para toda rede. Por isso, eles são conhecidos como protocolos de caminho mais curto e são criados a partir do algoritmo (SPF) de *Edsger Dijkstra*. Eles têm a reputação de serem muito mais complexos que seus correlatos vetores de distância. Entretanto, a funcionalidade básica e a configuração de protocolos de roteamento link-state não são nada complexas. Até mesmo o próprio algoritmo pode ser entendido facilmente além de proporcionam diversas vantagens, comparados a protocolos vetor de distância.

Eles criam um mapa topológico ou uma árvore SPF da topologia de rede. Protocolos de roteamento do vetor de distância não têm um mapa topológico da rede. Roteadores que implementam um protocolo de roteamento do vetor de distância têm apenas uma lista de redes que inclui o custo (distância) e roteadores do próximo salto (direção) para essas redes. Como protocolos link-state trocam estados de link, o algoritmo SPF pode criar uma árvore SPF da rede. Usando a árvore SPF, cada roteador pode determinar de maneira independente o caminho mais curto para cada rede.

Ao receberem um pacote link-state, protocolos link-state imediatamente inundam o LSP em todas as interfaces com exceção da interface da qual o LSP foi recebido. Depois da inundação inicial dos LSPs, os protocolos de roteamento link-state só enviam um LSP quando há uma mudança na topologia. O LSP contém apenas as informações relativas ao link afetado.

E usam o conceito de áreas. Áreas múltiplas criam um design hierárquico para redes, possibilitando melhor agregação de rota (sumarização) e o isolamento de problemas de roteamento dentro de uma área. Os mais modernos são criados para minimizar os efeitos sobre memória, CPU e largura de banda (LEINWANT, 2002).

No entanto, a decisão sobre que tipo de protocolo de roteamento usar em determinada situação é influenciada por vários fatores como:

- O tamanho da rede
- Compatibilidade entre modelos de roteadores
- Conhecimento administrativo necessário

Na camada de Internet do conjunto de protocolos TCP/IP, um roteador pode usar um protocolo de roteamento IP para realizar roteamento através da implementação de um algoritmo de roteamento específico. Exemplos de protocolos de roteamento IP:

O RIP (*Routing Information Protocol*) foi especificado originalmente na RFC 1058. Suas principais características são as seguintes:

- É um protocolo de roteamento por vetor da distância.
- A contagem de saltos é usada como métrica para seleção do caminho.
- Se a contagem de saltos for maior que 15, o pacote é descartado.
- Por padrão, as atualizações de roteamento são enviadas por broadcast a cada 30 segundos.

O IGRP (*Interior Gateway Routing Protocol*) é um protocolo proprietário desenvolvido pela Cisco. Algumas das principais características do projeto do IGRP enfatizam o seguinte:

- É um protocolo de roteamento por vetor da distância.
- A largura de banda, carga, atraso e confiabilidade são usados para criar uma métrica composta.
- Por padrão, as atualizações de roteamento são enviadas por broadcast a cada 90 segundos.

O OSPF (*Open Shortest Path First*) é um protocolo de roteamento por estado dos links não-proprietário. As principais características do OSPF são:

- Protocolo de roteamento por estado dos links.
- Protocolo de roteamento de padrão aberto, descrito na RFC 2328.
- Usa o algoritmo SPF para calcular o menor custo até um destino.
- Quando ocorrem alterações na topologia, há uma enxurrada de atualizações de roteamento.

O EIGRP (*Enhanced Interior Gateway Routing Protocol*) é um protocolo avançado de roteamento por vetor da distância proprietário da Cisco. As principais características do EIGRP são:

- É um protocolo avançado de roteamento por vetor da distância.
- Usa balanceamento de carga com custos desiguais.

- Usa características combinadas de vetor da distância e estado dos links.
- Usa o DUAL (*Diffusing Update Algorithm* – Algoritmo de Atualização Difusa) para calcular o caminho mais curto.
- As atualizações de roteamento são enviadas por multicast usando 224.0.0.10 e são disparadas por alterações da topologia.

O BGP (Border Gateway Protocol) é um protocolo de roteamento exterior. As principais características do BGP são:

- É um protocolo de roteamento exterior por vetor da distância.
- É usado entre os provedores de serviço de Internet ou entre estes e os clientes.
- É usado para rotear o tráfego de Internet entre sistemas autônomos.

3.3 METRICA E DISTÂNCIA ADMINISTRATIVA

Há casos em que um protocolo de roteamento aprende mais de uma rota para o mesmo destino. Para selecionar o melhor caminho, o protocolo de roteamento deve poder avaliar e diferenciar os caminhos disponíveis. A métrica é usada para essa finalidade. Métrica é um valor usado por protocolos de roteamento para atribuir custos com a finalidade de alcançar redes remotas. A métrica é usada para determinar o melhor caminho quando houver vários caminhos para a mesma rede remota.

A métrica usada em protocolos de roteamento IP inclui:

- Contagem de saltos - Uma métrica simples que conta o número de roteadores que um pacote deve atravessar.
- Largura de banda - Influencia a seleção do caminho ao escolher o caminho com a maior largura de banda.
- Carga - Considera a utilização de tráfego de determinado link.
- Atraso - Considera o tempo que um pacote leva para atravessar um caminho.
- Confiabilidade - Avalia a probabilidade de uma falha de link, calculada a partir da contagem de erros de interface ou de falhas de link anteriores
- Custo - Um valor determinado pelo IOS ou pelo administrador de rede para indicar sua preferência por uma rota. O custo pode representar uma métrica, uma combinação de métricas ou uma política.

Cada protocolo de roteamento usa sua própria métrica. Por exemplo, o RIP usa a contagem de saltos, o EIGRP usa uma combinação de largura de banda e atraso e a implantação do OSPF feita pela Cisco usa a largura de banda. A contagem de saltos é a métrica mais fácil de visualizar. A contagem de saltos se refere ao número de roteadores que um pacote deve atravessar para alcançar a rede de destino.

Embora menos comum, mais de um protocolo de roteamento dinâmico pode ser implantado na mesma rede. Em algumas situações, pode ser necessário rotear o mesmo endereço de rede que usa vários protocolos de roteamento como RIP e OSPF. Como protocolos de roteamento diferentes usam métricas diferentes, o RIP utiliza a contagem de saltos e o OSPF utiliza a largura de banda, não é possível comparar as métricas para determinar o melhor caminho.

A distância administrativa define a preferência de uma origem de roteamento. Cada origem de roteamento, incluindo protocolos de roteamento específicos, rotas estáticas e até mesmo redes diretamente conectadas, é priorizada na ordem da mais para a menos preferível usando um valor de distância administrativa. Ela é representado por um valor inteiro de 0 a 255. Quanto menor o valor, melhor será a origem de rota. A melhor distância é a de 0. Somente uma rede diretamente conectada tem uma distância administrativa de 0. Essa distância não pode ser alterada. Uma distância de 255 significa que o roteador não acreditará na origem dessa rota e não será instalado na tabela de roteamento. Logo, quanto menor o valor da distância administrativa, maior será a confiabilidade da rota (LEINWANT, 2002).

Origem da rota	Distância administrativa
Conectado	0
Estática	1
Rota sumarizada EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

Figura 10: Distância Administrativa dos Protocolos de Roteamento. Fonte: (CCNA Exploration, 2010).

3.4 PROTOCOLOS DE ROTEAMENTO VETOR DISTÂNCIA

Como o próprio nome diz, vetor de distância significa que as rotas são anunciadas como vetores de distância e direção. A distância é definida em termos de uma métrica como contagem de saltos, e a direção é dada simplesmente pelo roteador do próximo salto ou pela interface de saída.

Um roteador que usa um protocolo de roteamento do vetor de distância não tem o conhecimento do caminho inteiro para uma rede de destino. O roteador só conhece:

- A direção ou a interface para a qual os pacotes devem ser encaminhados.
- A distância até a rede de destino.

Alguns protocolos vetor de distância pedem que o roteador difunda periodicamente a tabela de roteamento inteira para cada um de seus vizinhos. Esse método é ineficiente, pois as atualizações consomem largura de banda e recursos de CPU dos roteadores para processar as atualizações.

Assim, os protocolos de roteamento do vetor de distância compartilham determinadas características.

As atualizações periódicas são enviadas em intervalos regulares (30 segundos para o RIP e 90 segundos para o IGRP). Mesmo que a topologia não tenha sido alterada nos últimos dias, as atualizações periódicas continuarão sendo enviadas a todos os vizinhos.

Vizinhos são roteadores que compartilham um link e são configurados para usar o mesmo protocolo de roteamento. O roteador só conhece os endereços de rede de suas próprias interfaces e os endereços de rede remota que pode alcançar através de seus vizinhos. Ele não tem nenhum conhecimento mais amplo da topologia da rede.

As atualizações de broadcast são enviadas para a 255.255.255.255. Os roteadores vizinhos que estiverem configurados com o mesmo protocolo de roteamento processarão as atualizações. Todos os outros dispositivos processarão a atualização até a Camada 3 e depois a descartarão. Alguns usam endereços *multicast* em vez de endereços de broadcast.

As atualizações da tabela de roteamento inteira são enviadas periodicamente a todos os vizinhos. Os vizinhos que recebem essas atualizações devem processar a atualização inteira para localizar as informações pertinentes e descartar o restante. Alguns protocolos vetor de distância, como o EIGRP, não enviam atualizações periódicas da tabela de roteamento.

No centro do protocolo do vetor de distância está o algoritmo. O algoritmo é utilizado para calcular os melhores caminhos e enviar essas informações aos vizinhos. Um algoritmo é um procedimento para realizar determinada tarefa, iniciando em determinado estado inicial e finalizando em um estado de término definido. O algoritmo usado para os protocolos de roteamento define os seguintes processos:

- Mecanismo para enviar e receber informações de roteamento.
- Mecanismo para calcular os melhores caminhos e instalar rotas na tabela de roteamento.
- Mecanismo para detectar e reagir a alterações de topologia.

Por sua vez, os protocolos de roteamento podem ser comparados com base nas seguintes características:

- Tempo de convergência: O tempo de convergência define a rapidez com que os roteadores da topologia de rede compartilham informações de roteamento e alcançam um estado de conhecimento consistente. Quanto mais rápida for a convergência, melhor será o protocolo. Os loops de roteamento podem ocorrer quando as tabelas de roteamento inconsistentes não são atualizadas devido a uma convergência lenta em uma rede variável.
- Escalabilidade: ela define o tamanho máximo que uma rede pode ter com base no protocolo de roteamento implantado. Quanto maior for a rede, mais escalável deverá ser o protocolo de roteamento.
- *Classless* (uso de VLSM) ou *classful* - Os protocolos de roteamento *classless* incluem a máscara de sub-rede nas atualizações. Esse recurso suporta o uso de Máscara de sub-rede de tamanho variável (VLSM) e melhor sumarização de rota. Os protocolos de roteamento *classful* não incluem a máscara de sub-rede e não podem suportar VLSMs.
- Uso de recursos - O uso de recursos inclui os requisitos de um protocolo de roteamento como espaço de memória, utilização de CPU e utilização de largura de banda de link. Os requisitos de recursos mais altos precisam de hardware mais avançado para suportar a operação do protocolo de roteamento, além dos processos de encaminhamento de pacotes.

- **Implantação e manutenção** - Implantação e manutenção descreve o nível de conhecimento necessário para que um administrador de rede implante e mantenha a rede com base no protocolo de roteamento implantado.

As vantagens e as desvantagens dos protocolos de roteamento do vetor de distância são mostradas na figura 11 a seguir.

Vantagens:	Desvantagens:
Implementação e manutenção simples. O nível de conhecimento exigido para implementar e manter uma rede com o protocolo do vetor de distância não é alto.	Convergência lenta. O uso de atualizações periódicas pode causar uma convergência mais lenta. Mesmo se algumas técnicas avançadas forem usadas, como atualizações disparadas, que serão discutidas posteriormente, a convergência geral ainda será mais lenta em comparação com os protocolos de roteamento link-state.
Requisitos de recursos baixos. Os protocolos do vetor de distância normalmente não precisam de grandes quantidades de memória para armazenar as informações. Eles também não precisam de uma CPU avançada. Dependendo do tamanho da rede e o endereçamento IP implementado, geralmente eles também não precisam de um alto nível de largura de banda de link para enviar atualizações de roteamento. No entanto, isso poderá se tornar um problema se você implementar um protocolo do vetor de distância em uma rede grande.	Escalabilidade limitada. A convergência lenta pode limitar o tamanho da rede porque redes maiores requerem mais tempo para propagar informações de roteamento.
	Loops de roteamento. Os loops de roteamento podem ocorrer quando as tabelas de roteamento inconsistentes não são atualizadas devido a uma convergência lenta em uma rede variável.

Figura 11: Vantagens e Desvantagens dos Protocolos Vetor Distância. Fonte: (CCNA Discovery, 2010).

Dentre os protocolos de roteamento do vetor de distância incluem RIP, IGRP e EIGRP. Suas principais características são:

3.4.1 RIP

O RIP impede a continuação indefinida de *loops* de roteamento, implementando um limite sobre o número de saltos permitidos em um caminho da origem até o destino. O número máximo de saltos em um caminho é de 15. Quando um roteador recebe uma atualização de roteamento que contém uma entrada nova ou alterada, o valor da métrica é aumentado em 1, para incluir-se como um salto nesse caminho. Se isso fizer com que a métrica seja incrementada além de 15, então ele será considerado como infinito e esse destino de rede será considerado inalcançável.

O RIP inclui diversos recursos comuns em outros protocolos de roteamento. Por exemplo, o RIP implementa o mecanismo de *split horizon* e de retenção para impedir a propagação de informações de roteamento incorretas. A métrica usada para a seleção de caminhos é a contagem de saltos. Se a contagem de saltos de uma rede for maior do que 15, o RIP não poderá fornecer uma rota a essa rede. Por padrão, as atualizações de roteamento são broadcast ou *multicast* a cada 30 segundos (LEINWANT, 2002).

Suporta *split horizon* e *split horizon com poison reverse* para impedir loops. É capaz de fazer o balanceamento de carga de até seis caminhos de custo iguais. O padrão é quatro caminhos de custo iguais.

Ao longo dos anos, o RIP evoluiu de um protocolo de roteamento classful (RIPv1) para um protocolo de roteamento classless (RIPv2). O RIPv2 é um protocolo de roteamento padronizado que funciona em um ambiente misto de roteadores e fornecedores. Os roteadores feitos por empresas diferentes podem comunicar-se usando o RIP. Ele é um dos protocolos de roteamento mais fáceis de configurar. Por isso, é uma boa opção para redes pequenas. No entanto, o RIPv2 ainda possui limitações. O RIPv1 e o RIPv2 têm uma métrica de rota baseada somente na contagem de saltos e limitada a 15 saltos (LEINWANT, 2002).

O RIPv2 introduziu seguintes melhorias no RIPv1:

- Inclui a máscara de sub-rede nas atualizações de roteamento, tornando-o um protocolo de roteamento classless.
- Tem mecanismo de autenticação para proteger atualizações da tabela de roteamento.
- Suporta a máscara de sub-rede de tamanho variável (VLSM).
- Utiliza endereços de multicast em vez de broadcast.
- Suporta a sumarização manual de rota.

Além de agregar:

- Capacidade de transportar informações adicionais sobre roteamento de pacotes.
- Mecanismo de autenticação para garantir as atualizações da tabela.
- Suporte a VLSM (máscaras de sub-rede com tamanho variável).

RIP v1	RIP v2
É fácil de se configurar	É fácil de se configurar
Suporta apenas protocolo de roteamento classful	Suporta a utilização de roteamento classless
Não inclui informações de sub-redes na atualização de roteamento	Envia informações de máscara de sub-rede com as atualizações de roteamento
Não suporta o roteamento baseado em prefixos e assim todos os dispositivos na mesma rede precisam utilizar a mesma máscara de sub-rede	Suporta roteamento de prefixos com VLSM e assim as sub-redes diferentes dentro da mesma rede podem ter máscaras de sub-rede diferentes.
Não suporta autenticação nas atualizações	Proporciona autenticação nas suas atualizações
Broadcasts utilizando 255.255.255.255	Envia atualizações de roteamento em multicast através do endereço Classe D 224.0.0.9, o que o torna mais eficiente

Figura 12: Comparação entre as versões do RIP. Fonte: (CCNA, 2008).

3.4.2 IGRP

O IGRP é um protocolo de roteamento de vetor da distância desenvolvido pela Cisco. O IGRP envia atualizações de roteamento a intervalos de 90 segundos, anunciando redes para um sistema autônomo específico. As principais características de projeto do IGRP são:

- Versatilidade para manipular automaticamente topologias complexas.
- Flexibilidade necessária para segmentação com diferentes características de largura de banda e de atraso.
- Escalabilidade para funcionamento em redes muito grandes .

Por padrão, o protocolo de roteamento IGRP usa largura de banda e atraso como métricas. Além disso, o IGRP pode ser configurado para usar uma combinação de variáveis para determinar uma métrica composta. Essas variáveis incluem:

- Largura de banda – O menor valor de largura de banda do caminho
- Atraso – O atraso cumulativo de interfaces na rede
- Confiabilidade – A confiabilidade no link em direção ao destino, conforme determinado pela troca de keepalives
- Carga – A carga em um link em direção ao destino, em base de bits por segundo

Ele tem diversos recursos criados para aumentar sua estabilidade, tais como:

As retenções usadas para impedir que mensagens de atualização regulares incorretamente reapliquem uma rota que talvez não esteja ativa. Quanto um roteador não

funciona, isso é detectado pelos vizinhos através da falta de mensagens de atualização programadas regularmente.

Os *split horizons* partem do princípio segundo o qual, normalmente, não é útil enviar de volta informações sobre uma rede na direção de onde vieram. A regra de split horizon ajuda a impedir loops de roteamento.

As atualizações de *poison reverse* são usadas para impedir *loops* de roteamento maiores. Em termos gerais, aumentos nas métricas de roteamento indicam *loops* de roteamento. As atualizações de poison reverse são, então, enviadas para remover a rota e colocá-la em modo de retenção (LEINWANT, 2002).

O IGRP também mantém diversos temporizadores e variáveis que contêm intervalos de tempo. Eles incluem um temporizador de atualização, um temporizador de invalidação, um temporizador de retenção e um temporizador de limpeza.

O temporizador de atualização especifica a frequência do envio de mensagens de atualização de roteamento. O padrão do IGRP para essa variável é de 90 segundos.

O temporizador de invalidação especifica o tempo que um roteador deve esperar, na ausência de mensagens de atualização de roteamento relativas a uma rota específica, antes de declará-la inválida. O padrão do IGRP para essa variável é de três vezes o período de atualização.

O temporizador de retenção especifica o tempo durante o qual informações sobre rotas mais deficientes são ignoradas. O padrão do IGRP para essa variável é de três vezes o período de atualização mais 10 segundos.

Finalmente, o temporizador de limpeza indica o tempo para que uma rota seja eliminada da tabela de roteamento. O padrão do IGRP é de sete vezes o temporizador de atualização de roteamento.

Hoje, o IGRP dá sinais de envelhecimento, pois não oferece suporte a VLSM (máscaras de sub-rede com tamanho variável). Em vez de desenvolver uma versão 2 do IGRP para corrigir esse problema, a Cisco utilizou o legado de sucesso do IGRP no *Enhanced* IGRP, ou seja, um IGRP Melhorado (LEINWANT, 2002).

3.4.3 EIGRP

O EIGRP é um protocolo de roteamento proprietário da Cisco que é baseado no IGRP. O EIGRP suporta CIDR e VLSM, o que permite que os projetistas de redes maximizem o espaço de endereçamento.

Comparado ao IGRP, que é um protocolo de roteamento *classful*, o EIGRP oferece tempos de convergência mais rápidos, melhor escalabilidade e um melhor gerenciamento de loops de roteamento. Além do mais, o EIGRP pode substituir o Novell RIP e o *AppleTalk Routing Table Maintenance Protocol* (RTMP). O EIGRP serve tanto em redes IPX e *AppleTalk* com possante eficiência. O EIGRP é freqüentemente descrito como um protocolo de roteamento híbrido que oferece o melhor dos algoritmos vetor de distância e *link-state* (LEINWANT, 2002).

O EIGRP é um protocolo de roteamento avançado que se vale de recursos geralmente associados aos protocolos *link-state*. Alguns dos melhores recursos do OSPF, tais como atualizações parciais e descoberta de vizinhos, são igualmente utilizados pelo EIGRP. No entanto, o EIGRP é mais fácil de configurar que o OSPF.

O EIGRP é uma escolha ideal para redes grandes com vários protocolos baseadas principalmente em roteadores Cisco. A ênfase desse protocolo está na maneira em que o EIGRP estabelece relações com roteadores adjacentes, calcula rotas primárias e de backup e responde a falhas nas rotas conhecidas para um determinado destino.

O EIGRP possui propriedades de convergência melhoradas e opera com mais eficiência do que o IGRP. Isso permite que uma rede tenha uma arquitetura melhorada, mantendo o investimento já feito no IGRP.

As comparações entre o EIGRP e o IGRP cabem dentro das seguintes categorias principais:

- Modo de compatibilidade
- Cálculo da métrica
- Contagem de saltos
- Redistribuição automática de protocolos
- *Route tagging*

Eles são compatíveis um com o outro. Esta compatibilidade proporciona uma interoperabilidade transparente de roteadores que utilizam IGRP. Isto é importante porque os usuários podem valer-se das vantagens de ambos os protocolos. O EIGRP oferece suporte de vários protocolos, mas o IGRP não.

Eles calculam suas métricas de forma um pouco diferente. O EIGRP multiplica a métrica do IGRP por um fator de 256. Isso é porque o EIGRP utiliza uma métrica de 32 bits e

o IGRP utiliza uma métrica de 24 bits. O EIGRP pode multiplicar ou dividir por 256 para facilmente trocar informações com o IGRP.

O IGRP possui uma contagem máxima de saltos de 255. O EIGRP tem um limite máximo de contagem de saltos de 224. Isso é mais que suficiente para suportar redes de grande porte apropriadamente projetadas (LEINWANT, 2002).

Os roteadores que utilizam o EIGRP mantêm informações sobre rotas e topologia prontamente disponíveis em RAM. Como o OSPF, o EIGRP guarda essas informações em três tabelas. A tabela de vizinhos enumera os roteadores adjacentes, a tabela de topologia, que consiste em todas as tabelas de roteamento do EIGRP no sistema autônomo, e a tabela de roteamento que contém as melhores rotas até um destino.

O DUAL (o algoritmo de vetor de distância do EIGRP) utiliza as informações fornecidas na tabela de vizinhos e na tabela de topologia e calcula as rotas de menor custo para cada destino. A rota primária preferida é conhecida como *successor route* e a rota de reserva é conhecida como *feasible successor (FS)*.

O EIGRP é um protocolo de roteamento de vetor de distância avançado e age como protocolo link-state ao atualizar os vizinhos e ao manter informações de roteamento. Suas vantagens incluem convergência rápida, utilização eficiente de largura de banda, suporte para VLSM e CIDR, suporte para várias camadas de rede e independência de protocolos roteados.

O algoritmo DUAL realiza a convergência rápida do EIGRP. Cada roteador constrói uma tabela de topologia que contém informações sobre como rotar até cada destino. Cada tabela de topologia identifica o protocolo de roteamento ou o EIGRP, o custo mais baixo da rota, conhecido como *Feasible Distance (FD)* e o custo da rota conforme anunciado pelo roteador vizinho, conhecido como *Reported Distance (RD)*.

Ao contrário do que ocorre com outros protocolos de roteamento do vetor de distância, o EIGRP não envia atualizações periódicas. Em vez disso, o EIGRP enviará atualizações associadas sobre uma rota quando um caminho for alterado ou a métrica dessa rota for alterada. Quando uma nova rota fica disponível ou quando uma rota precisar ser removida, o EIGRP envia somente uma atualização sobre essa rede, e não sobre a tabela inteira. Essas informações são enviadas somente aos roteadores que precisam delas.

O termo atualizações associadas significa que o EIGRP usa menos largura de banda, principalmente em redes grandes com muitas rotas. O EIGRP suporta vários protocolos de camada de Rede através de módulos dependentes do protocolo, que incluem suporte a IP, IPX e AppleTalk (LEINWANT, 2002).

3.5 PROTOCOLOS DE ROTEAMENTO LINK STATE

Os protocolos de roteamento link-state coletam informações de rota de todos os outros roteadores da rede ou dentro de uma área definida da rede. Uma vez coletadas todas as informações, cada roteador calcula os melhores caminhos para todos os destinos da rede. Como cada roteador mantém sua própria visão da rede, tem menor probabilidade de propagar informações incorretas fornecidas por algum de seus roteadores vizinhos.

A seguir algumas funções do protocolo de roteamento link-state:

- Responder rapidamente a mudanças na rede;
- Enviar *triggered updates* apenas quando ocorrer uma alteração na rede;
- Enviar atualizações periódicas, conhecidas como atualizações link-state;
- Usar um mecanismo *hello* para determinar se os vizinhos podem ser alcançados.

Cada roteador envia pacotes *hello* em *multicast* para ficar informado sobre o estado dos roteadores vizinhos. Cada roteador usa LSAs para se manter informado sobre todos os roteadores em sua área da rede. Os pacotes *hello* contêm informações sobre as redes que estão conectadas ao roteador. Os LSAs fornecem atualizações sobre o estado dos enlaces (*links*) que são interfaces nos outros roteadores da rede (LEINWANT, 2002). Logo, os roteadores que usam protocolos de roteamento link-state têm as seguintes características:

- Usam as informações de hello e os LSAs recebidos de outros roteadores para criar um banco de dados sobre a rede;
- Usam o algoritmo SPF para calcular a rota mais curta para cada rede;
- Armazenam as informações da rota na tabela de roteamento.

Os protocolos de roteamento *link-state* foram criados para superar as limitações dos protocolos de roteamento distance vector. Por exemplo, os protocolos *distance vector* somente trocam atualizações de roteamento com vizinhos imediatos, enquanto os protocolos de roteamento *link-state* trocam informações de roteamento através de uma área muito maior.

Quando ocorre uma falha na rede, por exemplo um vizinho fica inalcançável, os protocolos *link-state* inundam LSAs com um endereço *multicast* especial para toda a área. *Flooding*, ou inundar é o processo de enviar informações por todas as portas, exceto aquela

em que as informações foram recebidas. Cada roteador obtém uma cópia do LSA e atualiza seu banco de dados topológico.

Em seguida, o roteador encaminha o LSA para todos os dispositivos vizinhos. Os LSAs fazem com que todos os roteadores dentro da área recalculuem as rotas. Por esse motivo, a quantidade de roteadores *link-state* dentro de uma área deve ser limitada.

Um link é o mesmo que uma interface em um roteador. O estado do link é uma descrição de uma interface e da relação com os roteadores vizinhos. O conjunto de *link-states* forma um banco de dados que às vezes é chamado de banco de dados topológico. O banco de dados é usado para calcular os melhores caminhos através da rede. Os roteadores aplicam o algoritmo Dijkstra do "caminho mais curto primeiro" (SPF – *Shortest Path First*) consultando o banco de dados. Isso cria a árvore SPF, tendo o roteador local como raiz. Em seguida, os melhores caminhos são selecionados a partir da árvore SPF e colocados na tabela de roteamento.

Cada roteador constrói um banco de dados topológico a partir dos LSAs que recebe. Em seguida, o algoritmo SPF é usado para computar a facilidade de alcance dos destinos. Essa informação é usada para atualizar a tabela de roteamento. Esse processo pode descobrir alterações na topologia da rede causadas por falha de componentes ou crescimento da rede.

Distance Vector	Link-State
• Visualiza a topologia da rede sob a perspectiva de um roteador vizinho • Acrescenta vetores de distância de um roteador a outro • Possui atualizações freqüentes e periódicas e convergência lenta • Passa cópias de tabelas de roteamentos a roteadores vizinhos	• Obtém uma visão geral de toda a topologia da rede • Calcula o caminho mais curto para outros roteadores • Possui atualizações acionadas por eventos com convergência mais rápida • Passa atualizações de roteamento link state a outros roteadores

Figura 13: Comparação entre protocolos Distância Vetor e Link State. Fonte: (CCNA, 2008).

3.5.1 OSPF

OSPF é um protocolo de roteamento *link-state* que se baseia em padrões abertos. O OSPF, quando comparado com o RIP v1 e v2, é o IGP preferido, visto que pode ser escalado.

O RIP é limitado a 15 saltos, converge lentamente e às vezes escolhe rotas lentas, pois ignora fatores críticos, tais como a largura de banda, na determinação das rotas.

O OSPF pode ser usado e configurado como uma única área para redes pequenas. Também pode ser usado para redes grandes, pois usa um projeto hierárquico.

Várias áreas se conectam a uma área de distribuição, ou área 0, que também é chamada de *backbone*. A abordagem do projeto permite extenso controle das atualizações de roteamento. A definição da área reduz a sobrecarga de roteamento, acelera a convergência, confina a instabilidade da rede a uma área e melhora o desempenho.

Os roteadores *link-state* mantêm uma imagem comum da rede e trocam informações sobre links após a descoberta inicial ou após mudanças na rede. Os roteadores *link-state* não enviam tabelas de roteamento em broadcasts periodicamente como os protocolos distancia vetor. Portanto, usam menos largura de banda para a manutenção da tabela de roteamento.

O RIP é apropriado para redes pequenas, e o melhor caminho se baseia no menor número de saltos. O OSPF é apropriado para redes grandes que podem ser escaladas, e o melhor caminho é determinado pela velocidade do link.

O RIP e outros protocolos distancia vetor usam algoritmos simples para computar os melhores caminhos. O algoritmo SPF é complexo. Os roteadores que implementam primeiro precisam de menos memória e de processadores menos poderosos do que os que implementam OSPF.

O OSPF seleciona as rotas com base no custo, que está relacionado à velocidade. Quanto maior a velocidade, menor o custo OSPF do link. Seleciona o caminho mais rápido sem loop a partir da árvore SPF como sendo o melhor caminho da rede. E garante um roteamento sem loops. Os protocolos distancia vetor não (LEINWANT, 2002).

Em grandes redes, a convergência do RIP pode levar vários minutos, já que a tabela de roteamento de cada roteador é copiada e compartilhada com os roteadores conectados diretamente. Após a convergência inicial do OSPF, manter um estado convergente é mais rápido, pois apenas as alterações da rede são despejadas para outros roteadores de uma área. Ele suporta VLSMs e, por isso, é chamado de protocolo *classless*. O RIP v1 não suporta, só a versão 2.

O OSPF seleciona um caminho usando custo, uma métrica baseada na largura de banda. Todos os seus roteadores precisam obter informações completas sobre as redes de cada roteador para calcular o caminho mais curto. Esse algoritmo é complexo. Portanto, requer roteadores mais poderosos e mais memória do que o RIP.

O RIP usa uma topologia linear. Os roteadores de uma região RIP trocam informações com todos os roteadores. O OSPF usa o conceito de áreas. Uma rede pode ser subdividida em grupos de roteadores. Dessa maneira, o OSPF pode limitar o tráfego a essas áreas. Alterações em uma área não afetam o desempenho em outras áreas. Essa abordagem hierárquica permite que uma rede aumente em escala de maneira eficiente.

4 CONSIDERAÇÕES FINAIS

Assim, pode-se perceber ao longo desse trabalho a importância do processo de roteamento, de suas regras ou protocolos, sejam eles estáticos ou dinâmicos e dos roteadores para a consolidação da comunicação através das redes, meio imprescindível ao cenário atual. Estruturado para atender e respaldar uma variedade de serviços, conectado a diferentes tecnologias da qual dependem cada vez mais as empresas e pessoas.

REFERÊNCIAS BIBLIOGRÁFICAS

_____ CCNA 2008. Site: <http://cisco.netacad.net/>

_____ CCNA Discovery 2010. Site: <http://cisco.netacad.net/>

_____ CCNA Exploration 2010. Site: <http://cisco.netacad.net/>

CHAPPELL, Laura; FARKAS, Dan. **Diagnosticando redes CISCO Internetwork Troubleshooting**. Ed. Pearson Education. Rio de Janeiro – RJ, 2007.

LEINWANT, Allan; PINSK, Bruce. **Como Configurar Roteadores Cisco**. (trad.)Ed. Ciência Moderna. São Paulo – SP, 2002.

ODOM, Wendell. **Cisco CCNA – Guia de Certificação do Exame**. Ed. Alta Books. 3ª edição. Rio de Janeiro – RJ, 2003.

XAVIER, Fabio Correa. **Roteadores Cisco – Guia Básico de Configuração e Operação**. Ed. Novatec. São Paulo – SP, 2004.