



TÉCNICAS DE ROTEAMENTO

MODELOS DE ROTEAMENTO

Autor: Me. Gustavo Lins e Horta

Revisor: Rafael Rehm

INICIAR



introdução

Introdução

Os protocolos que utilizam o algoritmo de vetor de distância são o RIPv1, RIPv2, o IGRP e o EIGRP. Com exceção do EIGRP, os demais protocolos de roteamento que utilizam vetor de distâncias possuem convergência lenta, baixa escalabilidade, baixos recursos e implementação e manutenção simples. O EIGRP por sua vez é um protocolo mais moderno e robusto que possui convergência rápida, grande escalabilidade, mais recursos e sua implementação e manutenção é mais complexa.

O nome vetor distância vem do fato que as rotas são como vetores (distância e direção), a distância é a métrica do algoritmo e a direção o salto até o próximo roteador.

Protocolos que Utilizam Vetor de Distâncias

Os protocolos de roteamento do vetor de distância (DV) geralmente implantam uma técnica conhecida como *split horizon*. O *split horizon* impede o envio das informações pela mesma interface da qual foram recebidas, evitando assim os loops de roteamento. Os protocolos de vetor de distância são o RIP, IGRP e EIGRP (CISCO, 2003, p. 44).

RIP

A primeira versão do RIP (*Routing Information Protocol*), o RIPv1 criada em 1988, ainda é utilizada atualmente, é implementada como sendo um protocolo de roteamento classful, isso significa que ele não manda a máscara de rede das rotas que ele divulga em suas atualizações (TANENBAUM, 2011, p. 232).

Conforme Cisco (2003, p. 331), o RIPv1 foi desenvolvido para trabalhar com redes baseadas nas classes padrão A, B e C, ou seja, pelo número IP da rota, reduzida a respectiva classe.

Ainda segundo Cisco (2003, p. 331) o RIPv2 surgiu em 1993, já é um protocolo

de roteamento classless, ou seja, envia a máscara das redes divulgadas em suas atualizações. Já permitindo trabalhar com redes de tamanho de máscara variado.

Os anúncios de atualização do protocolo RIPv2 são baseados em tráfego multicast e não mais broadcast como no caso do protocolo RIPv1. O protocolo RIPv2 utiliza o endereço de multicast 224.0.0.9. Com isso os roteadores habilitados ao RIPv2 atuam como um grupo multicast, registrado para "escutar" os anúncios do protocolo (CISCO, 2003, p. 331)

O protocolo RIP é baseado em uma troca de mensagens entre os roteadores. Cada mensagem do RIP contém uma série de informações sobre as rotas que o roteador conhece (com base na sua tabela de roteamento atual) e a distância do roteador para cada uma das rotas (Tanenbaum, 2011, p. 283).

Conforme Cisco (2003), o RIP envia sua tabela de roteamento completa para todas as interfaces configuradas. A tabela é enviada periodicamente como uma transmissão (255.255.255.255) para todos os hosts. O cronômetro de atualização especifica a frequência das transmissões periódicas. Por padrão, o timer de atualização está definido para 30 segundos.

Ainda segundo Cisco (2003), cada rota tem um valor de tempo limite associado a ela. O tempo limite é redefinido toda vez que o roteador recebe uma atualização de roteamento contendo a rota. Quando o valor do tempo limite expirar, a rota será marcada como inacessível e depois marcada como inválida. A rota é marcada como inválida definindo a métrica para 16. A rota é mantida na tabela de roteamento. Por padrão, o cronômetro inválido é de 180 segundos ou seis períodos de atualização ($30 \times 6 = 180$).

Segundo Tanenbaum (2011), cada mensagem do protocolo RIP comporta, no máximo, informações de até 25 sub-redes de destino dentro do AS, além das distâncias entre a origem e cada uma delas.

IGRP

O protocolo IGRP (*Interior Gateway Routing Protocol*) foi desenvolvido pela Cisco em 1980 como uma resposta às limitações do RIP, das quais as mais importantes são a métrica de contagem de saltos e o tamanho da rede de 15 saltos. O IGRP calcula uma métrica composta a partir de uma variedade de variáveis de rota e fornece "pesos" para ponderar as variáveis para refletir as características e necessidades específicas da rede. Embora a contagem de saltos não seja uma dessas variáveis, o IGRP rastreia a contagem de saltos e pode ser implementado em internets de até 255 saltos.

Outras vantagens do IGRP sobre o RIP são o compartilhamento de carga de custo desigual, um período de atualização três vezes maior que o do RIP e um formato de pacote de atualização mais eficiente. A principal desvantagem do IGRP é que ele é proprietário da Cisco e, portanto, limitado aos produtos da Cisco, enquanto o RIP faz parte de qualquer processo de roteamento IP em qualquer plataforma (CISCO, 2019).

De acordo com Cisco (2003), o IGRP compartilha muitas características operacionais com o RIP. É um protocolo de vetor de distância de classe que transmite periodicamente toda a sua tabela de roteamento - com exceção das rotas suprimidas pelo horizonte dividido - a todos os seus vizinhos. Como o RIP, o IGRP transmite um pacote de solicitação para todas as interfaces ativadas pelo IGRP na inicialização e executa uma verificação de integridade nas atualizações recebidas para verificar se o endereço de origem do pacote pertence à mesma sub-rede na qual a atualização foi recebida. Novas entradas de atualização com métricas alcançáveis são colocadas na tabela de roteamento e uma entrada substitui uma entrada mais antiga no mesmo destino apenas se a métrica for menor. O IGRP também utiliza o conceito de sistemas autônomos.

Dentro de suas atualizações, o IGRP classifica as entradas de rota em uma de três categorias:

- Rotas internas;
- Sistema rotas;
- Rotas externas.

Rotas Internas

Uma rota interna é um caminho para uma sub-rede do endereço de rede do enlace de dados no qual a atualização está sendo transmitida. Em outras palavras, uma sub-rede anunciada como uma rota interna é "local" para a rede principal à qual o roteador de publicidade e o roteador de recebimento são comumente conectados.

Sistema Rotas

Uma rota do sistema é um caminho para um endereço de rede, que foi resumido por um roteador de limite de rede.

Rotas Externas

Uma rota externa é um caminho para uma rede que foi sinalizada como uma rede padrão. Uma rede padrão é um endereço para o qual um roteador enviará qualquer pacote que não possa ser correspondido a um destino mais específico.

Recursos de Estabilidade e Temporização

O período de atualização do IGRP é de 90 segundos. Uma variável de *jitter* aleatória de até 20% é subtraída de cada tempo de atualização para impedir a sincronização do cronômetro de atualização; portanto, o tempo decorrido entre as atualizações individuais varia de 72 a 90 segundos (CISCO, 2003, p. 339).

Quando uma rota é aprendida pela primeira vez, o timer inválido para essa rota é definido em 270 segundos ou três vezes o período de atualização. O cronômetro de liberação está definido para 630 segundos - sete vezes o período de atualização. Sempre que uma atualização é recebida para a rota, esses cronômetros são reinicializados. Se o cronômetro inválido expirar antes de uma atualização ser ouvida, a rota será marcada como inacessível. Ele será mantido na tabela de roteamento e anunciado como inacessível até que o temporizador de liberação expire, quando a rota será excluída da tabela (CISCO, 2003, p. 339).

O timer de 90 segundos usado pelo IGRP, em comparação com o timer de 30 segundos usado pelo RIP, significa que, comparado ao RIP, o IGRP usa menos largura de banda para atualizações periódicas. No entanto, o problema é que, em alguns casos, o IGRP pode ser mais lento do que o RIP. Por exemplo, se um roteador ficar offline, o IGRP leva três vezes mais que o RIP para detectar o vizinho inativo.

Métricas do IGRP

Conforme Cisco (2003), as características do *enlace* a partir das quais o IGRP calcula sua métrica composta são largura de banda, atraso, carga e confiabilidade. Por padrão, o IGRP escolhe uma rota com base na largura de banda e no atraso. Se um *enlace* de dados é considerado um canal, a largura de banda é a largura do canal e o atraso é o comprimento do canal. Em outras palavras, a largura de banda é uma medida da capacidade de carga e o atraso é uma medida do tempo de viagem de ponta a ponta.

EIGRP

O protocolo EIGRP (*Enhanced Interior Gateway Routing Protocol*) também é um protocolo de vetor de distâncias. Era um protocolo proprietário da Cisco, mas em 2016 foi colocado como um padrão aberto. O EIGRP é uma evolução do IGRP. O EIGRP é ocasionalmente descrito como um protocolo de vetor de distância que age como um protocolo de estado de enlace (CISCO, 2019).

Todos os protocolos de vetores de distância o algoritmo *Bellman-Ford* . Esses protocolos são propensos a rotear *loops* e contar até o infinito. Como resultado, eles devem implementar medidas de prevenção de *loop* , como horizonte dividido, envenenamento de rota e temporizadores de espera. Como cada roteador deve executar o algoritmo de roteamento nas rotas recebidas antes de transmiti-las aos seus vizinhos, redes maiores podem demorar a convergir. Mais importante, os protocolos vetoriais de distância anunciam rotas; a alteração de um enlace crítico pode significar o anúncio de muitas rotas alteradas.

Comparado aos protocolos de vetor de distância, os protocolos de estado de enlace são muito menos suscetíveis a *loops* de roteamento e informações incorretas de roteamento. O encaminhamento de pacotes de estado do enlace não depende da execução dos cálculos de rota primeiro, portanto grandes redes internas podem convergir mais rapidamente. E apenas os enlaces e seus estados são anunciados, não rotas, o que significa que a alteração de um enlace não causará o anúncio de todas as rotas usando esse enlace. No entanto, comparados aos algoritmos de vetores de distância, os complexos algoritmos *Dijkstra* e os bancos de dados associados impõem uma demanda maior de CPU e memória.

Funcionamento do EIGRP

O EIGRP usa a mesma fórmula que o IGRP para calcular sua métrica composta. No entanto, o EIGRP dimensiona os componentes métricos em 256 para obter uma granularidade métrica mais fina. Portanto, se a largura de banda mínima configurada no caminho para um destino for 512K e o atraso total configurado for 46000 microssegundos, o IGRP calculará uma métrica composta de 24.131. O EIGRP, no entanto, multiplicará a largura de banda e o atraso dos componentes por 256 para uma métrica de $256 \times 24131 = 6.177.536$ (PAQUET, 2003).

A tabela 2.1 apresenta os valores de padrão para largura de banda e atraso para o EIGRP.

Tipo de Conexão	Atraso	Largura de Banda
Satélite	5.120 (2 segundos)	5.120 (500 Mbps)
Ethernet	25,600 (1ms)	256,000 (10 Mbps)
T-1 (1.544 Mbps)	512.000 (20 ms)	1.657.856
64 kbps	512.000	40.000.000
56 kbps	512.000	45.714.176

Tabela 2.1 - valores de padrão para largura de banda e atraso

Fonte: Elaborado pelo autor

O EIGRP possui quatro componentes:

- Módulos dependentes de protocolo;
- Protocolo de transporte confiável (RTP - *Reliable Transport Protocol*);
- Descoberta / recuperação de vizinhos;
- Algoritmo de atualização difuso (DUAL);

Módulos Dependentes de Protocolo

O EIGRP implementa módulos para IP, IPX e AppleTalk, responsáveis pelas tarefas de roteamento específicas do protocolo. Por exemplo, o módulo IPX EIGRP é responsável por trocar informações de rota sobre redes IPX com outros processos IPX EIGRP e por transmitir as informações ao DUAL.

O EIGRP faz a redistribuição automática com outros protocolos em muitos casos:

- O IPX EIGRP será redistribuído automaticamente com o IPX RIP e o NLSP;
- O AppleTalk EIGRP será redistribuído automaticamente com o AppleTalk RTMP;

- O IP EIGRP redistribuirá automaticamente as rotas com o IGRP se o processo do IGRP estiver no mesmo sistema autônomo.

Protocolo de Transporte Confiável

O Protocolo de transporte confiável (RTP) gerencia a entrega e recepção de pacotes EIGRP. Entrega confiável significa que a entrega é garantida e que os pacotes serão entregues em ordem.

A entrega garantida é realizada por meio de um algoritmo de propriedade da Cisco conhecido como (*reliable multicast*) multicast confiável, usando o endereço de classe D reservado 224.0.0.10.

Descoberta / Recuperação de Vizinhos

Como as atualizações do EIGRP não são periódicas, é especialmente importante ter um processo pelo qual os vizinhos - roteadores que falam o EIGRP em redes diretamente conectadas - são descobertos e rastreados. Na maioria das redes, o *Hello* é multicast a cada 5 segundos, menos um pequeno tempo aleatório para impedir a sincronização.

Quando um roteador recebe um pacote *Hello* de um vizinho, o pacote inclui um tempo de espera. O tempo de espera informa ao roteador o tempo máximo que deve esperar para receber o *Hello* subsequente. Se o temporizador de espera expirar antes do recebimento de um *Hello*, o vizinho será declarado inacessível e o DUAL será informado da perda de um vizinho. Por padrão, o tempo de espera é três vezes o intervalo *Hello* - 180 segundos para redes de acesso múltiplo de baixa velocidade e sem broadcast e 15 segundos para todas as outras redes. A capacidade de detectar um vizinho perdido em 15 segundos, em oposição a 180 segundos para o RIP e 270 segundos para o IGRP, é um fator que contribui para a rápida convergência do EIGRP.

Algoritmo de Atualização Difuso (DUAL)

A filosofia de design por trás do DUAL é que mesmo os loops de roteamento temporários são prejudiciais ao desempenho de uma internetwork. O DUAL

usa cálculos difusos, propostos pela primeira vez por *Dijkstra* para executar o roteamento de caminho mais curto distribuído, mantendo a liberdade de loops a cada instante.

Para que o DUAL opere corretamente, um protocolo de nível inferior deve garantir que as seguintes condições sejam atendidas:

- Um nó detecta dentro de um tempo finito a existência de um novo vizinho ou a perda de conectividade com um vizinho;
- Todas as mensagens transmitidas através de um enlace operacional são recebidas corretamente e na seqüência correta dentro de um tempo finito;
- Todas as mensagens, alterações no custo de um enlace, falhas de enlace e notificações de novos vizinhos são processadas uma de cada vez, em um tempo finito e na ordem em que são detectadas.

Resumindo as características o EIGRP é protocolo de roteamento híbrido (vetor de distância que possui características de protocolo de estado de enlace), é um protocolo sem classe (suporta VLSMs), utiliza métrica composta padrão de largura de banda e atraso, tanto a carga e quanto a confiabilidade podem ser levadas em consideração na métrica, envia atualizações parciais da rota somente quando ocorrem alterações, possui suporte para autenticação, usa DUAL para prevenção de loop, por padrão utiliza balanceamento de carga de custo igual ou balanceamento de carga de custo desigual com o comando `variance` e a distância administrativa é 90 para rotas internas do EIGRP, 170 para rotas externas do EIGRP e 5 para rotas resumidas do EIGRP.

praticar
Vamos Praticar

O protocolo EIGRP (*Enhanced Interior Gateway Routing Protocol*) também é um protocolo de vetor de distâncias desenvolvido pela Cisco que se tornou um padrão aberto em 2013. O EIGRP é uma versão aprimorada do protocolo IGRP.

A respeito do EIGRP, assinale a alternativa que apresenta as características deste protocolo.

- ☐ **a)** Contagem de saltos máxima igual a 25.
- ☐ **b)** Não consegue diferenciar rotas internas e rotas externas.
- ☐ **c)** Mantêm apenas uma tabela de roteamento.
- ☐ **d)** Usa uma métrica composta.
- ☐ **e)** Precisa que todas as redes usem a mesma máscara de sub-rede.

Opções de Roteamento

O encaminhamento IP, ou roteamento IP, é simplesmente o processo de recebimento de um pacote IP, a decisão de onde enviar o pacote a seguir e o encaminhamento. O processo de encaminhamento precisa ser relativamente simples, ou pelo menos simplificado, para um roteador encaminhar grandes volumes de pacotes.

Duas formas básicas de encaminhamento são realizadas por um roteador, o encaminhamento direto ou indireto.

Encaminhamento Direto

O encaminhamento direto ocorre onde o endereço IP de destino está em uma rede conectada ao roteador.

Encaminhamento Indireto

O encaminhamento indireto ocorre onde o endereço IP de destino não está

em uma rede conectada ao roteador e, portanto, o datagrama deve ser encaminhado para um roteador mais adiante no caminho através da rede. Onde um roteador está conectado a várias redes, o encaminhamento é mais complicado do que no caso de hosts, que normalmente são conectados a uma única rede.

praticar

Vamos Praticar

Analise o trecho a seguir:

O encaminhamento de pacotes é um importante processo no roteamento de uma rede de computadores. É um processo relativamente simples, no qual o roteador recebe o pacote de dados e define para onde enviar esse pacote. No encaminhamento _____ o pacote IP e o roteador de destino devem estar na mesma rede.

Assinale a alternativa que completa corretamente a lacuna é:

- ☐ **a)** Indireto.
- ☐ **b)** Rede desconectada..
- ☐ **c)** de várias redes.
- ☐ **d)** Direto.
- ☐ **e)** Por saltos.

Roteamento Orientado por Tabela

Uma tabela de roteamento é um conjunto de regras, geralmente exibidas em formato de tabela, que é usado para determinar para onde os pacotes de dados que trafegam por uma rede IP (Internet Protocol) serão direcionados. Todos os dispositivos habilitados para IP, incluindo roteadores e comutadores, usam tabelas de roteamento.

Uma tabela de roteamento contém as informações necessárias para encaminhar um pacote ao longo do melhor caminho em direção ao seu destino. Cada pacote contém informações sobre sua origem e destino. A tabela de roteamento fornece ao dispositivo instruções para enviar o pacote para o próximo salto em sua rota pela rede.

Cada entrada na tabela de roteamento consiste nas seguintes entradas:

- ID de rede: O ID ou destino da rede correspondente à rota.
- Máscara de sub-rede: A máscara usada para corresponder um endereço IP de destino ao ID da rede.
- Próximo salto: O endereço IP para o qual o pacote é encaminhado
- Interface de saída: Interface de saída, o pacote deve sair para

alcançar a rede de destino.

- Métrica: Um uso comum da métrica é indicar o número mínimo de saltos (roteadores cruzados) para o ID da rede.

As entradas da tabela de roteamento podem ser usadas para armazenar os seguintes tipos de rotas:

- IDs de rede conectadas diretamente;
- IDs de rede remota;
- Rotas de host;
- Rota Padrão;
- Destino.

Quando um roteador recebe um pacote, ele examina o endereço IP de destino e consulta sua tabela de roteamento para descobrir qual pacote de interface será enviado.

Rotas Padrão

Outro conceito de roteamento é a rota padrão da rede. Essa rota se torna o gateway de último recurso para pacotes com endereços IP de destino que não estão na tabela de roteamento. Geralmente, são utilizados para acessar a Internet. Como as redes externas geralmente não são anunciadas na rede do usuário, a rota padrão é utilizada para rotear esses pacotes ligados à Internet para um roteador, firewall ou gateway padrão.

Os protocolos de roteamento lidam com a configuração de rota padrão de maneira diferente. A rota padrão geralmente é configurada usando um comando de rota estática, como o seguinte:

ip route 0.0.0.0 0.0.0.0 x.x.x.x

Onde x.x.x.x é o endereço IP do próximo salto.

O Processo de Pesquisa de Rota

Sabemos que a tabela de roteamento contém todas as informações necessárias para encaminhar um pacote ao destino correto. Precisamos saber como o roteador usa o conteúdo da tabela de roteamento.

A tabela de roteamento é uma lista de rotas e, para cada uma, temos a sub-rede de destino, sua máscara de sub-rede e a interface next-hop / exit. Para isso, podemos adicionar alguns dados sofisticados, como métrica, fonte de roteamento e muito mais (KUROSE, 2014).

Quando o roteador recebe um pacote IP, ele faz a correspondência ao cabeçalho do pacote na sua tabela de roteamento. Especificamente, o campo a ser correspondido é o endereço IP de destino. Para cada rota na tabela de roteamento, o roteador executa uma operação AND bit a bit entre o endereço IP de destino e a máscara de sub-rede contida na rota. Se o resultado da operação AND bit a bit for exatamente a rede alvo da rota, teremos uma correspondência.

Na tabela de roteamento, cada rota é única. Isso significa que a combinação da rede de destino e da máscara de sub-rede é única. Como resultado, não encontraremos várias rotas com exatamente a mesma rede de destino e máscara de sub-rede. No entanto, uma rota pode conter vários endereços do próximo salto para equilibrar o tráfego entre eles.

No entanto, podemos ter rotas sobrepostas. Com isso, uma rota aponta para uma rede de destino que já é alcançável usando a outra rota. De qualquer forma, nesses casos, a máscara de sub-rede entre as duas rotas é diferente. Quando duas (ou mais) rotas correspondem a um endereço de destino de pacote IP, a rota mais específica é usada. A rota mais específica é aquela com a máscara de sub-rede mais longa.

Vamos Praticar

Leia a situação a seguir:

Você é o gestor de TI da empresa XYZ e realizou a configuração de um roteador da empresa com uma rota padrão. Uma rota padrão é geralmente configurada por meio de um comando de configuração de rota estática do tipo ***ip route 0.0.0.0 0.0.0.0 x.x.x.x***, onde ***x.x.x.x*** é o endereço IP do próximo salto ou o destino pode ser uma interface de saída ***ip route 0.0.0.0 0.0.0.0 serial 0***.

Assinale a alternativa que apresenta qual é o objetivo de uma rota padrão.

- ☐ **a)** É uma rota a ser utilizada quando o protocolo de roteamento falhar.
- ☐ **b)** É uma rota configurada por um ISP que envia tráfego para a rede corporativa.
- ☐ **c)** É uma rota configurada manualmente para uma rede remota específica para a qual o roteador não está configurado.
- ☐ **d)** É uma rota utilizada quando o pacote é destinado a uma rota remota que não está na tabela de roteamento do roteador.
- ☐ **e)** É utilizada para enviar tráfego para um rede de stub.

Roteamento I

O protocolo IP possui duas versões, a versão 4 e a versão 6 e está na camada de rede do modelo OSI. Os três componentes principais dessa camada são o protocolo IP, o componente de roteamento e um dispositivo para comunicação de erros. Os protocolos de roteamento IP tem como objetivo determinar o caminho que um pacote deve seguir entre a origem e o destino.

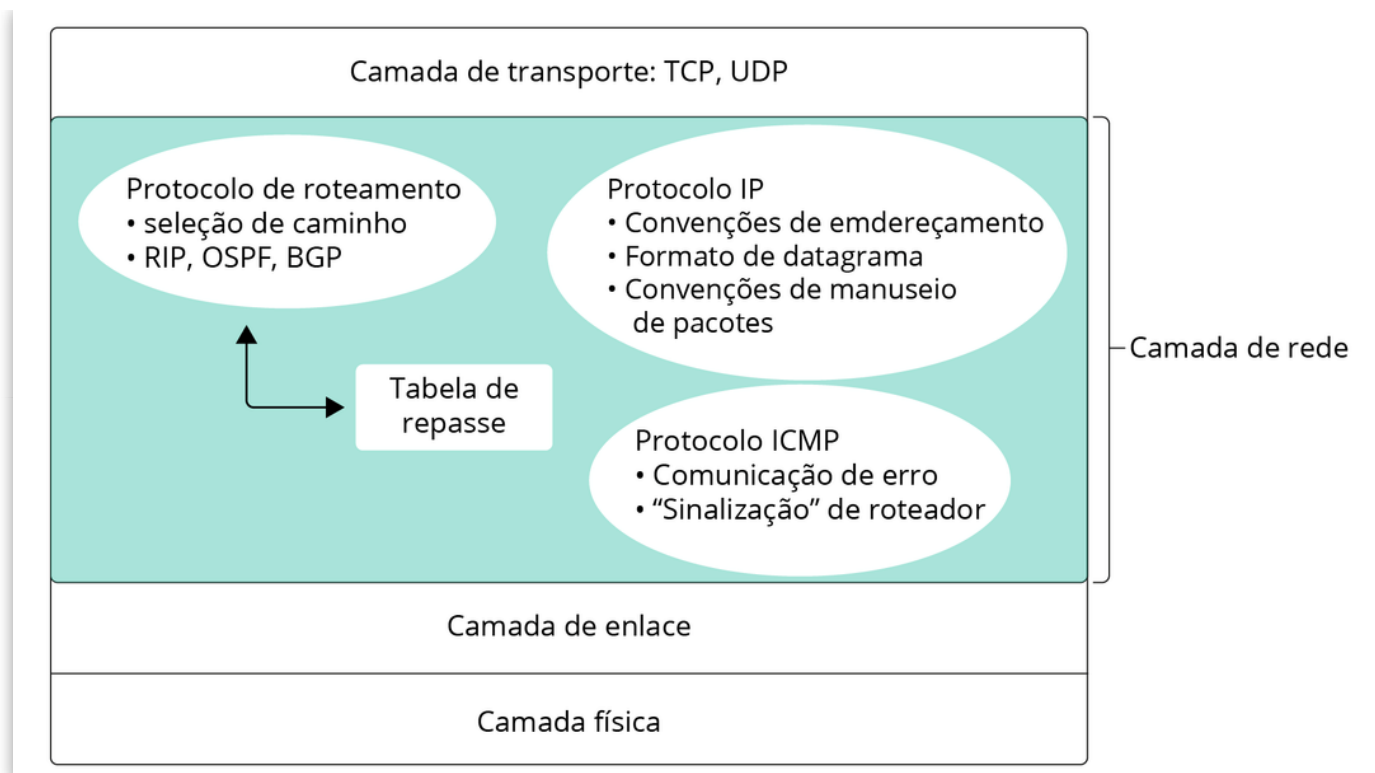


Figura 2.1 - Camada de rede

Fonte: Kurose (2014, p. 245).

Na camada de rede o pacote é chamado de *datagrama*. Os principais campos do *datagrama* IPv4 são (Kurose, 2014):

- Número da versão: 4 bits que especificam a versão do protocolo IP;
- Comprimento do cabeçalho: 4 bits determinam onde os dados iniciam no *datagrama* IP. Em um *datagrama* IP típico um cabeçalho possui 20 bytes;
- Tipo de serviço: identificam os diferentes tipos de *datagrama* IP;
- Comprimento do *datagrama*: Comprimento total do *datagrama* IP (dados + cabeçalho), geralmente possuem 1.500 bytes;
- Tempo de vida (TTL): campo incluído para que o *datagrama* não circule infinitamente na rede. Quando o campo TTL chega a zero o pacote é descartado;
- Identificador, flags e deslocamento de fragmentação: permite a fragmentação do IP;
- Protocolo: indica o protocolo da camada de transporte específico para passar o *datagrama* IP;
- Soma de verificação de cabeçalho: auxilia o roteador na detecção de erros de bits em um *datagrama*;

- Endereços IP de origem e destino: contêm os endereços IP de origem e destino;
- Opções: permite estender o cabeçalho IP;
- Dados: contêm os dados que serão transmitidos.

A Figura 2.2 apresenta o *datagrama* do IPv4.

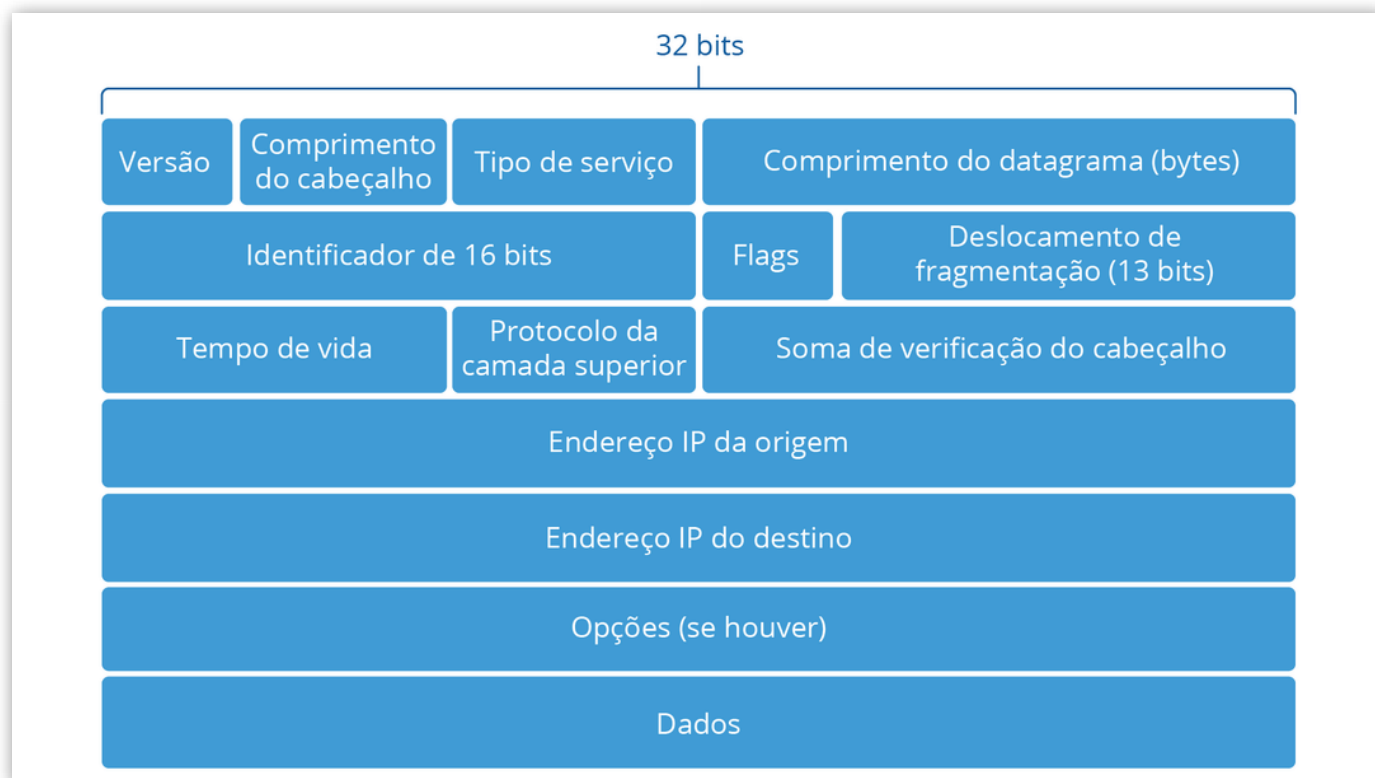


Figura 2.2 - Datagrama do IPv4
Fonte: Kurose (2014, p. 246).

Endereçamento IPv4

O endereço IPv4 possui 32 bits (4 bytes), logo é possível ter 2^{32} endereços IP possíveis, que são aproximadamente 4 bilhões de endereços IP possíveis.

reflita

Reflita

O protocolo IPv4 permite conectar os dispositivos à internet. Sempre que um dispositivo acessa a internet ele recebe um endereço IP único. A questão é que o número de dispositivos conectados à internet cresce a uma velocidade impressionante. A capacidade de endereçamento do protocolo IPv4 já se esgotou e por esse motivo foi criado o protocolo IPv6 que permite aproximadamente 4,29 bilhões de endereços IP únicos. Com um número cada vez maior de dispositivos conectados à internet (computadores, celulares, TV's, geladeiras, sensores, veículos, entre outros) e novas aplicações surgindo a cada dia será que esse limite de 4,29 bilhões de endereços IP será atingido algum dia, pensando em quantidade de endereços IP por pessoa (seu celular, seu computador, sua TV), uma pessoa pode utilizar mais de um endereço IPv6 só para si. Como será o futuro com bilhões de dispositivos conectados à internet?.

Fonte: <http://bit.ly/2SmqfSw>

Um exemplo de endereço IP é 193.32.216.9. Transformando esse endereço IP em notação binária temos: 11000001 00100000 11011000 00001001 (KUROSE, 2014).

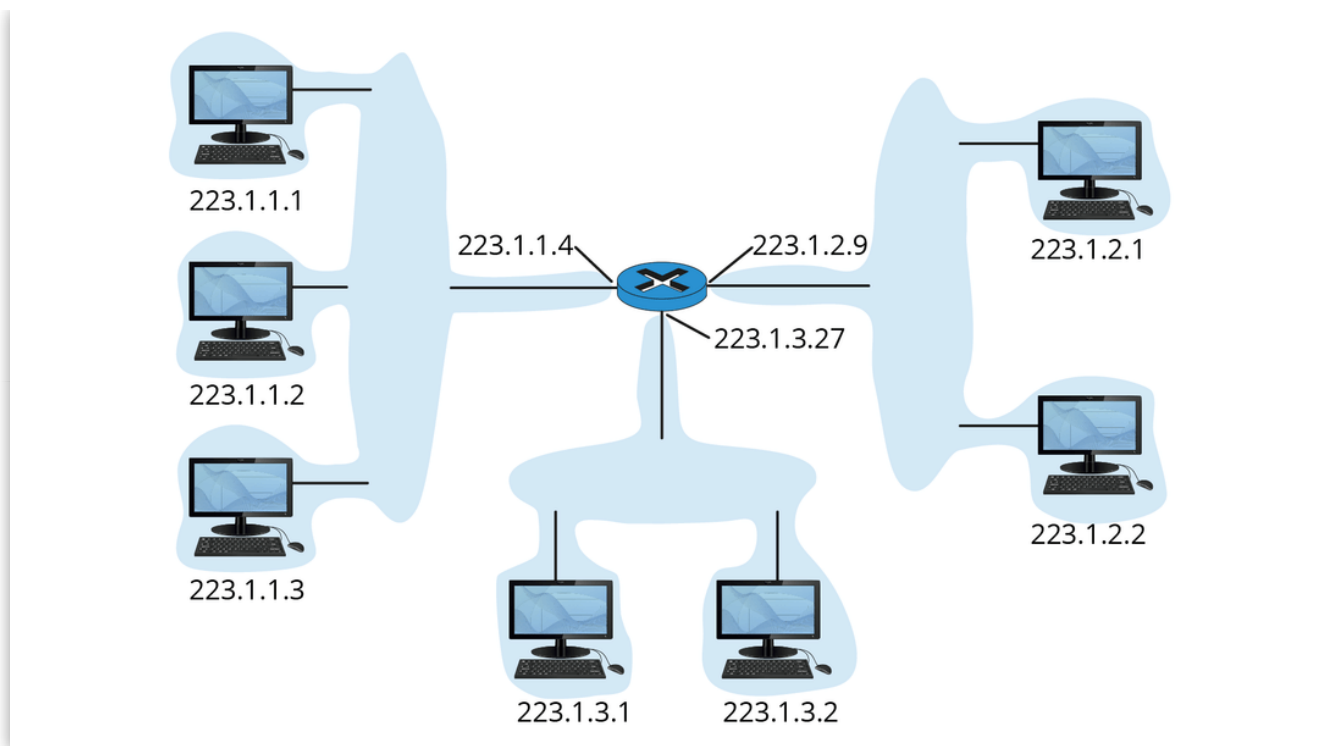


Figura 2.3 - Endereçamento IP de interfaces e sub-redes

Fonte: Kurose (2014, p. 251).

O roteador da Figura 2.3 interliga os computadores, o endereço IP está na forma 223.1.1.xxx, logo existem três sub-redes nessa rede, as sub-redes 223.1.1.0/24, 223.1.2.0/24 e 223.1.3.0/24.

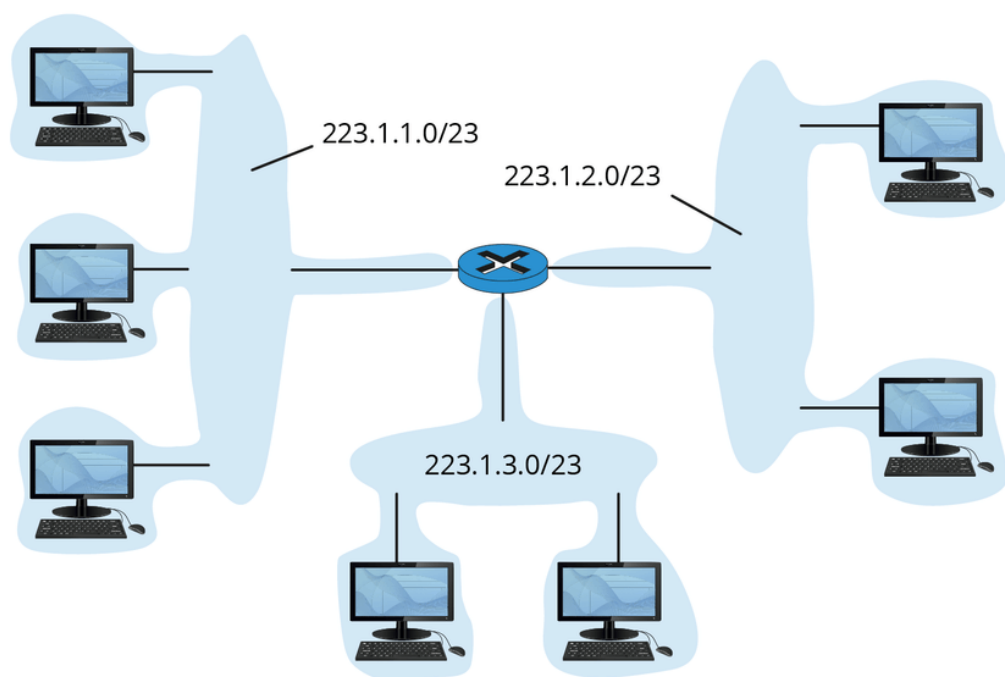


Figura 2.4 - Endereços de sub-redes

Fonte: Kurose (2014, p. 252).

O endereçamento IP é fundamental para o roteamento e o tráfego de informações na internet. O IPv4 vem sendo substituído pelo IPv6.

Endereçamento IPv6

O IPv6, foi desenvolvido devido a necessidade de se aumentar a quantidade de endereços IP, devido à limitação do IPv4 em 4 bilhões de endereços IPs disponíveis. O IPv6 fornece 128 bits para endereçamento - um aumento significativo em relação a 32 bits do IPv4.

saiba mais

Saiba mais

Você já está preparado para o IPv6? Seus dispositivos (PC, notebook, celular) já estão funcionando com o IPv6? E o seu provedor de internet, já fornece um endereço IPv6 para você? E os sites de internet já funcionam com o IPv6? Saiba mais sobre o IPv6 no Brasil e realize um teste para saber se determinado site já é acessível via IPv6.

Para conhecer mais sobre as estatísticas do IPv6 no Brasil e realizar um teste do IPv6, acesse o site:

[ACESSAR](#)

Os endereços IPv6 têm 128 bits. Os endereços IPv6 são representados em hexadecimal, divididos em oito partes de 16 bits. Este formulário é representado da seguinte maneira:

X:X:X:X:X:X:X

Cada X representa os dígitos hexadecimais. Um exemplo de um endereço IPv6 completo é: FE1A:4CB9:001B:0000:0000:12D0:005B:06B0.

Quando os endereços estão em um ambiente misto de IPv4 e IPv6, eles podem ser representados por seis partes hexadecimais de 16 bits que são concatenadas com o formato decimal com pontos. Este formulário é representado da seguinte maneira:

X: X: X: X: X: X :.d.d.d.d

Cada X representa os dígitos hexadecimais e d.d.d.d é a representação decimal com pontos.

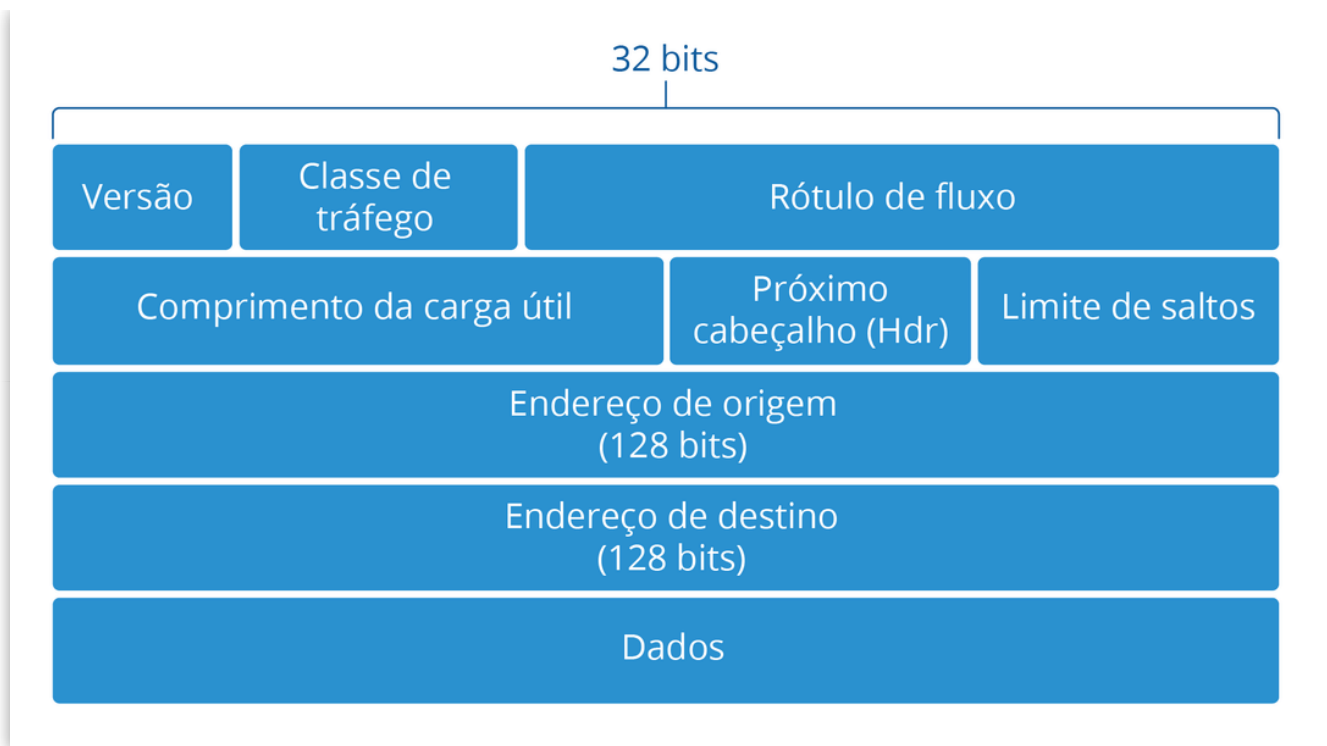


Figura 2.5 - Datagrama do IPv6

Fonte: Kurose (2014, p. 264).

Segundo Cisco (2003), um dos principais aprimoramentos de design do IPv6 sobre IPv4 é o cabeçalho simplificado do IPv6. O cabeçalho simplificado do IPv6 oferece várias vantagens sobre o IPv4:

- Melhor eficiência de roteamento para desempenho e escalabilidade da taxa de encaminhamento;
- Nenhum requisito para processar somas de verificação;
- Mecanismos de cabeçalho de extensão simplificados e mais eficientes (em oposição ao campo Opções do IPv4);
- Um campo Flow Label para processamento por fluxo sem necessidade de abrir o pacote interno de transporte para identificar os vários fluxos de tráfego.

Tabelas de Roteamento

Uma tabela de roteamento também conhecida como RIB (*Routing Information Base*) é uma tabela internas dos roteadores que listam as redes que eles conhecem e o caminho a ser seguido para os pacotes alcançarem estas redes. As tabelas informam a associação destination/next hop para preferência do

caminho que varia dependendo do protocolo de roteamento (KUROSE, 2014).

A tarefa de cada roteador é clara: enviar o tráfego para o destino correto. Para fazer isso, os roteadores aproveitam sua tabela de roteamento. A tabela de roteamento é exatamente o que o nome diz: uma tabela. Essa tabela, na realidade, é uma lista de rotas. Cada rota indica uma sub-rede de destino e também como alcançá-la. Especificamente, existem apenas duas informações que informam ao roteador como chegar a um destino que são o próximo salto e a interface de saída.

Os roteadores têm interfaces que se conectam com outros dispositivos de rede. Quando um pacote chega a uma interface, o roteador precisa encontrar a interface certa para enviar o pacote. O campo IP de destino do pacote é verificado em relação às informações armazenadas no roteador. Se houver uma correspondência, o pacote é enviado através da interface apropriada. esse processo é repetido ao longo do caminho em cada roteador.

praticar

Vamos Praticar

A empresa XYZ está realizando a transição do protocolo IPV4 para o protocolo IPV6. O roteador da empresa está configurado para executar o IPV4 e o IPV6 simultaneamente. Assinale a alternativa que apresenta como é conhecida essa técnica:

- ☐ a) Roteamento binário.
- ☐ b) Roteamento 6 para 4.
- ☐ c) Roteamento próxima geração.
- ☐ d) Roteamento de pilha dupla

- ☐ **e)** Roteamento de conversão IPv6 para IPv4..
-

indicações Material Complementar

WEB

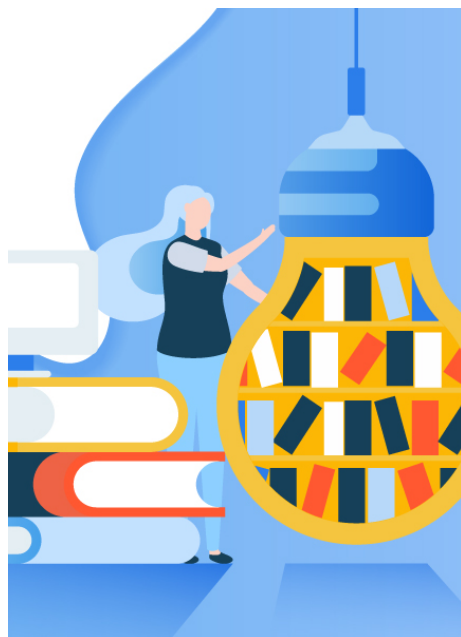
O que é o IPv6

Ano: 2014

Tipo: Vídeo

Comentário: O IPv6 já é uma necessidade e uma realidade em nossas vidas. Sem o IPv6 a expansão e o crescimento da internet, das redes de computadores e o desenvolvimento de novos serviços e aplicações de internet não seria possível. Neste vídeo é apresentado de forma simples e direta a necessidade e funcionamento do protocolo IPv6.

ACESSAR



LIVRO

Configurando Switches e Roteadores Cisco - para certificação CCENT/CCNA

Silva, César Felipe Gonçalves

Editora: Brasport

ISBN: 9788574526096

Comentário: Este livro aborda os principais conceitos e comandos para configuração de roteadores Cisco. O livro contempla os principais protocolos de roteamento como RIP, OSPF, BGP e outros. Apresenta ao final de cada capítulo questões no modelo das provas de certificação CCENT e CCNA da Cisco.

conclusão

Conclusão

Os protocolos de vetor de distância (DV) são muito utilizados no roteamento. Você percebeu que é necessário que o roteador informe a seus vizinhos sobre alterações topológicas periodicamente. Vimos os protocolos de vetor de distância RIP, IGRP e EIGRP. Entendemos que a principal vantagem desse tipo de protocolo é a simplicidade de configuração e manutenção. Também vimos que entre as desvantagens ele possui convergência mais lenta que o protocolo de estado de enlace, as atualizações nas tabelas de roteamento ocorrem periodicamente, mesmo que não ocorra alteração na topologia da rede e não se adapta bem a rede maiores já que resulta em tabelas muito grandes gerando um elevado consumo de CPU, memória e banda.

referências

Referências Bibliográficas

CISCO, **Diagnosticando Redes: Cisco Internetwork Troubleshooting** . São Paulo: Pearson, 2002.

CISCO, **Guia de Certificação do CCIE Roteamento e Comutação Exame** . Cisco Press, 2003.

CISCO, Networking Academy. **Cisco Packet Tracer** . Disponível em: < <https://www.netacad.com/pt-br/courses/packet-tracer> > Acesso em: 03 de dez. de 2019.

KUROSE, J. F. ROSS, K. W. **Redes de Computadores e a Internet - Uma Abordagem Top-Down** . 6a edição. São Paulo: Pearson. 2014.

TANENBAUM, A. S. WETHERALL, D. **Redes de Computadores** . 5a edição. São Paulo: Pearson. 2011.

PAQUET, C. **Construindo Redes Cisco de Acesso Remoto** . São Paulo: Pearson Education do Brasil. 2003.