

SERVIÇOS INTERNET

UNIDADE 2 – CAMADA DE REDE

Autora: Fernanda Rosa da Silva

Revisor: Rafael de Jesus Rehm

INICIAR

Introdução

Olá, estudante!

Um protocolo de rede é um conjunto de regras que permite que dois ou mais computadores conectados à internet se comuniquem entre si. Ele pode ser definido como uma linguagem universal utilizada pelos dispositivos de rede para interpretar as informações enviadas entre os computadores.

Após entender o funcionamento do modelo OSI e a forma como cada uma das camadas interage entre si, é importante entendermos melhor a estrutura dos protocolos e suas características que permitem a transmissão de dados.

Não somente de uma rede local dependem os serviços e aplicações, por isso, os protocolos também são o principal fator para que a comunicação seja possível na internet.

Tendo isso em vista, vamos analisar os tipos de roteamento utilizados em uma rede de computadores, os principais protocolos de roteamento e a diferença na operação de cada um deles.

Bons estudos!

2.1 Protocolos da camada de rede

A principal função da camada de rede do modelo OSI é transmitir pacotes de dados entre os sistemas finais da rede, por meio de três principais funções:

- Determinar o caminho pelo qual os pacotes devem ser enviados por meio de algoritmos e protocolos de roteamento, selecionando a melhor rota entre a origem e o destino;
- Comutar pacotes utilizando portas de entrada e saída para que os roteadores possam movimentar pacotes por meio da rede;
- Estabelecer conexões antes que seja possível a transmissão dos pacotes por meio do endereçamento lógico dos dispositivos.

Para que todas essas funções sejam possíveis, o uso de protocolos é necessário.

Os primeiros protocolos a surgirem na camada de rede estavam diretamente relacionados à estrutura de uma rede local (LAN), para atender às necessidades de compartilhamento de informações e recursos entre dispositivos. Esses protocolos foram essenciais para definir as funcionalidades de sistemas operacionais e as aplicações suportadas por eles.

O protocolo IP é o principal utilizado em redes de computadores, sendo responsável por realizar operações na camada de rede para identificar as necessidades de dispositivos que compartilham informações na rede local, se comunicando via internet ou possibilitando a interação entre qualquer dispositivo (conectado) que possa ser alcançado, mesmo que esteja no mesmo domínio ou em outra rede, podendo ser alcançado por meio de um provedor de serviços de internet.

Para o nível de endereçamento que ocorre na camada de rede é necessário que cada dispositivo seja endereçado por meio de uma identificação de 32 bits de comprimento que, de acordo com Forouzan (2010, p. 550), permite um máximo de 2^{32} (4.294.967.296 endereços).

Por muito tempo, o IPv4 foi utilizado como principal protocolo de comunicação da camada de rede para que os computadores fossem capazes de se comunicar na internet. Todavia, com o crescimento exacerbado da internet, das redes e de todas as tecnologias que foram surgindo no mercado, a identificação por IPV4 se tornou escassa e foi necessário buscar uma solução mais eficiente para estender a possibilidade de endereçamento e inserção de novos dispositivos na rede.

Consequentemente, surgiu o IPv6, aumentando o número de computadores e dispositivos tecnológicos que poderiam ser suportados diante da comunicação e transmissão por meio da internet, se tornando uma extensão do seu antecessor e suportando uma quantidade de 340 undecilhões de endereços possíveis com um endereçamento de 128 bits.

O endereço IP foi atribuído à interface de rede do computador, geralmente a uma placa de rede. Segundo Tanenbaum (2003, p. 550), “é importante notar que o endereço IP se refere a uma interface ativa na rede e não ao computador em si”. Portanto, se um computador estiver em duas redes, duas interfaces de rede são necessárias para que se possa atribuir um IP para cada uma delas. Esse IP pode ser utilizado por outro

equipamento quando esse não estiver mais disponível na rede.

2.1.1 Protocolo IPv4

Como sendo a primeira versão criada, protocolo IPv4 (Protocol version 4) prevê que uma identificação única seja atribuída a qualquer dispositivo na rede. Por isso, Forouzan (2010, p. 549) aponta que não é possível atribuir um mesmo endereço para dois dispositivos ao mesmo tempo. Ele também aponta que um endereço IPv4 pode ser representado por meio de duas notações: binária ou decimal.

» Clique nas setas ou arraste para visualizar as imagens

NOTAÇÃO BINÁRIA

Na notação binária, 32 bits são exibidos e a divisão do endereço é feita em quatro grupos de 8 bits, do seguinte modo:



11000000 10101000 00000010 00011101

Figura 1 – Formato de endereço IP com notação binária.

Fonte: Elaborada pela autora.

#PraCegoVer : a imagem ilustra a divisão dos octetos representados em notação binária, para representar o endereçamento IPv4. A sequência exemplificada é: um, um, zero, zero, zero, zero, zero, zero, espaço, um, zero, um, zero, um, zero, zero, zero, espaço, zero, zero, zero, zero, zero, zero, zero, um, zero, espaço, zero, zero, zero, um, um, um, zero, um.

NOTAÇÃO DECIMAL

De compreensão mais simples, por representar o modo como os números são lidos em atividades cotidianas, a notação decimal representa um intervalo de valores mais compacto, separando os bytes por meio de um ponto decimal, denominado dot, do seguinte modo:



192.168.2.29

Figura 2 – Formato de endereço IP com notação decimal.

Fonte: Elaborada pela autora.

#PraCegoVer : a imagem ilustra a divisão dos octetos representados em notação decimal, para representar o endereçamento IPv4. A sequência exemplificada é: cento e noventa e dois, ponto, cento e sessenta e oito, ponto, dois, ponto, vinte e nove.

A mesma identificação está representada em ambas as notações. Para entendê-las melhor, basta saber que

cada posição na notação binária tem os seguintes valores atribuídos e que eles apenas são somados para formar a notação decimal.



Figura 3 – Bits do endereçamento IPv4.

Fonte: Elaborada pela autora.

#PraCegoVer : a imagem ilustra os valores estabelecidos para facilitar a soma de cada octeto de um endereço IP na rede. Cada unidade está dentro de um círculo com fundo branco. Da esquerda para a direita, os valores são: cento e vinte e oito; sessenta e quatro; trinta e dois; dezesseis; oito; quatro; dois; e um.

Além do seu formato padrão, o endereçamento IPv4 é definido por classes, nas quais cada uma delas especifica quantos endereços uma rede pode ter. Essa técnica evita desperdício de endereços e adequa cada rede de acordo com sua necessidade técnica.

Nesse ponto, podemos considerar que existem IPs privados (não roteáveis) e públicos (roteáveis), em que os privados são endereços utilizados dentro de uma rede local para comunicação entre os dispositivos que compõem essa estrutura e os públicos, utilizados na internet e, geralmente, providos por provedores de internet.

Para qualquer rede, o IP é dividido em três classes, conforme ilustrado na Figura 4:

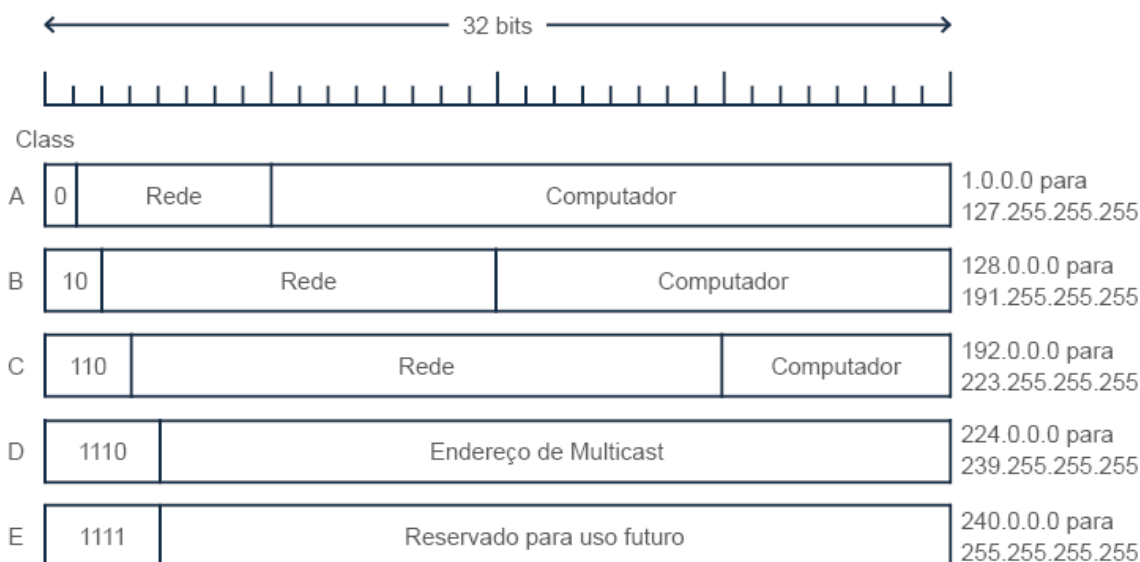


Figura 4 – Formato do endereçamento IP.

Fonte: TANENBAUM, 2003, p. 337. (Adaptada).

#PraCegoVer : a imagem ilustra as classes definidas no endereçamento IPv4, ilustrando que cada uma das classes é composta por 32 bits. A imagem apresenta uma tabela com cinco linhas e cada uma delas com duas colunas para definir os octetos utilizados pela rede e pelo host. A primeira linha ilustra a classe A, onde um octeto representa a rede e três representam os hosts. Do lado o range ilustrado para rede é representado da

seguinte forma: 1.0.0.0 para 127.255.255.255. A segunda linha ilustra a classe B, onde dois octetos representam a rede e dois representam os hosts. Do lado o range ilustrado para rede é representado da seguinte forma: 128.0.0.0 para 191.255.255.2. A terceira linha ilustra a classe B, onde dois octetos representam a rede e três representam os hosts. Do lado o range ilustrado para rede é representado da seguinte forma: 192.0.0.0 para 223.255.255.255. A quarta linha ilustra o range de endereços utilizados para comunicação multicast. Do lado o range ilustrado para rede é representado da seguinte forma: 224.0.0.0 para 239.255.255.255. A quinta linha ilustra o range reservado para o uso de redes futuras da seguinte forma: 240.0.0.0 para 255.255.255.255.

Os endereços IPs pertencentes à classe A são utilizados em redes que precisam suportar um grande número de computadores. Portanto o primeiro octeto é usado como identificador da rede e os demais octetos são todos liberados para garantir a identificação dos computadores configurados na rede.

Os endereços IP pertencentes à classe B atribuem os dois primeiros octetos do endereçamento IP para rede e a outra metade para os computadores. Uma rede de tamanho intermediário é ideal para ser coberta por esse tipo de classe.

Os endereços IPs de classe C são utilizados em redes de organizações que possuam um grande número de redes, mas poucos computadores alocados para cada uma delas. Portanto, os três primeiros octetos são usados para identificar a rede e somente o último octeto é usado para identificar os dispositivos.

2.1.2 Protocolo IPv6

Assim como qualquer recurso computacional, as necessidades foram evoluindo junto às tecnologias. Um exemplo disso foi em relação às tecnologias de armazenamento que foram evoluindo de acordo com a necessidade das organizações. Primeiro, os disquetes sendo substituídos pelos DVDs com capacidade maior, partindo para as mídias removíveis, que ofereciam ainda mais espaço; depois os Storages e até mesmo as soluções propostas pela computação em nuvem.

Isso não foi diferente com o protocolo IP. Por isso, o IPv6 se tornou uma boa solução para a limitação que o IPv4 vem trazendo às redes. Isso não significa que deixará de ser utilizado. Atualmente, diversas redes já utilizam as duas versões do protocolo. A estrutura de um IPv6 pode ser analisada na Figura 5.

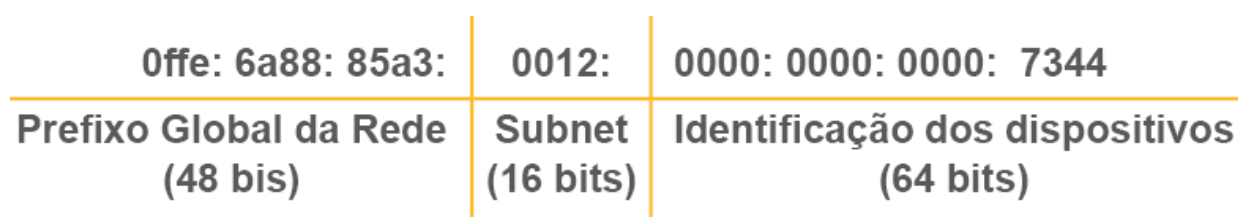


Figura 5 – Estrutura do endereço IPv6.

Fonte: FILIPETTI, 2014. (Adaptado).

#PraCegoVer : a imagem ilustra a divisão hexadecimal que representa a estrutura do IPv6. Uma linha horizontal separa o tamanho de 128 bits para um endereço, dividido em

uma estrutura em três partes. A primeira é representada por 48 bits identificando o prefixo da rede (0ffe:6:88:85:3:). É possível analisar que cada espaço é representado por 'xxxxx', ou seja, 16 bits para cada quadro (hexadecimal). A segunda parte é representada por 16 bits (0012:) e identifica a subnet e a terceira parte com 64 bits, é identificação dos dispositivos (0000:0000:0000:7344).

Ainda existe desvantagem em relação à estrutura do protocolo IPv6. Sua escrita é mais complexa e longa, dificultando sua representação. Nesse ponto, entra a atuação do protocolo DNS para resolver e facilitar a tarefa de entendimento desses protocolos.

2.1.3 Outros protocolos

Apesar do endereço IP ser o principal utilizado na camada de rede, existem outros protocolos que são utilizados em conjunto com ele e que muitas vezes representam uma extensão de sua estrutura, complementando sua funcionalidade.

O **ICMP (Internet Control Message Protocol)** é uma parte indispensável do protocolo IP e tem a função de fornecer funções de diagnóstico para problemas que ocorram na rede. De acordo com Forouzan e Mosharraf (2013), problemas que ocorrem durante o roteamento de pacotes podem ser identificados com a sua utilização.

As mensagens ICMP servem para que o comportamento de um determinado dispositivo, quando alterado, possa ser detectado, permitindo que erros e falhas de comunicação e transmissão na rede sejam resolvidos, restabelecendo o encaminhamento dos pacotes.

Geralmente, um roteador com a função de gateway (nó principal da rede, responsável por estabelecer interface com a internet e outras redes por meio do uso de diferentes protocolos) é utilizado para enviar as mensagens ICMP, após receber informações sobre o datagrama que causou o erro.

Uso do ICMP no diagnóstico da rede

- Uma mensagem ICMP é enviada sempre que um pacote de dados não é capaz de alcançar a interface de rede do dispositivo de destino por alguma falha no meio, na aplicação ou pelo tempo de resposta especificado pelo roteador ter esgotado;
- Se o gateway estiver congestionado devido ao recebimento de um número de solicitações maior do que o que é capaz de atender, o ICMP envia uma mensagem, informando que não é possível atender as requisições sem que existam perda de informações e problemas no fluxo de transmissão;
- Em alguns casos, o gateway pode sugerir uma nova rota e ela precisa ser redefinida para que a transmissão de pacotes possa continuar. Sendo assim, o ICMP alerta o administrador sobre a alteração antes que ela seja realizada.

CASO

Um exemplo prático do uso do ICMP é a ferramenta tracert. Quando ela é executada em um terminal do Windows, permitindo que a rota completa da rede seja analisada desde a origem até o destino, permitindo que se possa analisar todos os saltos pelos quais o pacote passa. Observe:



Rastreando a rota para dns.google [8.8.8.8] com no máximo 30 saltos:

```

1  8 ms  4 ms  4 ms  ARCHER_C5 [192.168.0.1]
2  7 ms  5 ms  6 ms  10.255.5.6
3  5 ms  5 ms  6 ms  172.30.0.13
4  9 ms  5 ms  5 ms  237.106.186.200.sta.impsat.net.br [200.186.106.237]
5  21 ms  22 ms  22 ms  64.209.11.190
6  21 ms  22 ms  20 ms  72.14.212.213
7  20 ms  21 ms  30 ms  216.239.46.205
8  22 ms  19 ms  18 ms  209.85.248.151
9  21 ms  19 ms  34 ms  dns.google [8.8.8.8]
```

Outro exemplo é o comando ping, que pode ser utilizado com a seguinte sintaxe: **ping [endereço de destino]** é utilizado para examinar atividades dos dispositivos de rede, enviando mensagens e confirmando suas atividades. Resumindo, sua função é enviar pacotes de dados ao dispositivo de destino e “ouvir” a resposta. Se o dispositivo de destino estiver ativo, a resposta será retornada ao computador solicitante. O procedimento pode ser visto na Figura 6.

```

Microsoft Windows [versão 10.0.18363.1198]
(c) 2019 Microsoft Corporation. Todos os direitos reservados.

C:\Users\Fernanda>ping www.terra.com.br

Disparando a1799.dscb.akamai.net [95.100.84.98] com 32 bytes de dados:
Resposta de 95.100.84.98: bytes=32 tempo=8ms TTL=60
Resposta de 95.100.84.98: bytes=32 tempo=5ms TTL=60
Resposta de 95.100.84.98: bytes=32 tempo=5ms TTL=60
Resposta de 95.100.84.98: bytes=32 tempo=3ms TTL=60

Estatísticas do Ping para 95.100.84.98:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 3ms, Máximo = 8ms, Média = 5ms
```

Figura 6 – Execução do comando ping com ICMP.

Fonte: Elaborado pela autora.

#PraCegoVer : a imagem ilustra o comando ping disparando uma mensagem para o site <www.terra.com.br>, através do seguinte comando: ping www.terra.com.br.

Quando o comando é executado, o sistema operacional responde com a seguinte mensagem: Disparando a1799.dscb.akamai.net [95.100.84.98] com 32 bytes de dados:

Alertando sobre o pedido de conexão para o IP 95.100.84.98, com tempo de resposta de 32 bytes, oscilando entre 8 ms na primeira linha, 5 ms na terceira e segunda linha e 3 ms na quarta linha. O TTL representa o número de 60 saltos. Mais abaixo, o comando informa que quatro pacotes foram enviados e recebidos sem nenhuma perda na transmissão, tendo alcançado um tempo mínimo de 3ms e máximo de 8ms e média de 5ms.



VOCÊ QUER LER?

Outro protocolo da camada de rede é o IGMP (Internet Group Management Protocol). Você pode entender sobre sua funcionalidade, lendo o artigo "O que é o IGMP e como ele funciona? - Dica técnica – 132521 ", disponível em: < <https://www.dell.com/support/article/pt-br/sln68773/o-que-%C3%A9-o-igmp-e-como-ele-funciona-dica-t%C3%A9cnica-132521> >.

O **DHCP (Dynamic Host Configuration Protocol)** , também denominado protocolo de configuração dinâmica de host, esse protocolo auxilia o administrador na obtenção do endereço IP de um computador por meio da camada de rede.



VOCÊ SABIA?

Para facilitar as tarefas administrativas em uma rede de computadores, o administrador de rede pode utilizar o DHCP para atribuir endereços de modo automático aos dispositivos, de acordo com sua disponibilidade. Desse modo, não é necessário adicionar os endereços IPs de modo manual, o que poupa tempo e evita problemas que possam causar conflito na identificação dos dispositivos.

O **DNS (Domain Name System)** ou sistema de nomes de domínio é usado por outros protocolos para localizar o endereço da camada de rede do computador e gerenciar os nomes de qualquer dispositivo na rede, convertendo-os de IPs para nomes, o que define o modo como o usuário, por exemplo, busca os sites e acessa a URL de modo facilitado.

A mesma Figura 5 que ilustra o comando ping, demonstra como o DNS funciona em um sistema operacional. Quando o ping foi realizado para o site <www.terra.com.br>, o ICMP retornou com a resposta da requisição e, ao mesmo tempo, informou sua identificação em forma de IP: 96.17.164.122, identificando um dos endereços que responde pelo servidor web. Isso ocorre geralmente transformando o IP em nome. Por isso, nesse caso, a técnica utilizada foi o DNS reverso.



VAMOS PRATICAR?

Experimente fazer um pequeno teste para entender melhor como o protocolo ICMP e a ferramenta traceroute funcionam. Utilize a ferramenta Wireshark para executar o laboratório: < <https://www.wireshark.org/#download> >.

- Abra o prompt de comando do Windows e execute o comando: `tracert 8.8.8.8` para analisar as rotas do seu equipamento até o site < www.google.com > para capturar os pacotes;
- Prepare Wireshark para capturar pacotes de dados usando filtros ICMP ou UDP;
- Tente determinar o funcionamento do traceroute analisando os datagramas IP enviados (ttl = 1, 2, 3, ...) e mensagens ICMP, de modo a analisar o tempo de vida do pacote;
- Observe que o traceroute usa o protocolo UDP para enviar datagramas comuns;
- Escreva um pequeno resumo sobre o funcionamento do traceroute.

2.2 Conceitos de roteamento

O roteamento é um processo que ocorre na camada da rede e é projetado para enviar mensagens ponta a ponta, usando o endereçamento de rede para operar na identificação de dispositivos e estabelecer comunicação entre redes de computadores e computadores que operam em sua infraestrutura.

De acordo com Moraes (2010), o roteamento é o processo que determina a rota que um pacote de dados e o modo como ele seguirá através do meio de transmissão.

Antes mesmo de iniciar o roteamento de pacotes, a rede define o caminho (rota) pelo qual os dados passarão, formando uma tabela de roteamento de todos os pontos da rede pelos quais o pacote de dados pode transitar.

Portanto, antes de sair da LAN e seguir para outra rede utilizando a internet, vários dispositivos (roteadores) podem ser acessados até que o “salto” final seja alcançado.

O roteamento de pacotes ainda pode descrever o modo como a transmissão de dados entre o remetente e o destinatário ocorre. Mesmo antes de os dados serem transmitidos, essa rota (caminho) pode ser selecionada pela rede (via roteador), ou pode ser selecionada passo a passo considerando vários aspectos, com o objetivo de definir o melhor caminho na rede. Desse modo, dois tipos de roteamento podem ser definidos: estático ou dinâmico.

2.2.1 Roteamento estático

O roteamento estático é um processo manual, em que as rotas que serão seguidas na rede são configuradas pelo administrador por meio do gateway, normalmente representado por um roteador. Sendo assim, o administrador precisa conhecer todas as redes para onde deseja transmitir dados e conhecer a estrutura entre elas, para que seja possível estabelecer os caminhos do melhor modo.

A vantagem em escolher o roteamento estático é em relação à segurança obtida, já que a divulgação das rotas se torna mais confiável, principalmente em redes nas quais poucos caminhos devem ser estabelecidos.

Quando as rotas são configuradas manualmente, é mais fácil evitar que dispositivos ou invasores não autorizados causem problemas na rede.

Não é uma boa estratégia usar uma tabela de roteamento estática, a não ser que isso envolva uma rede de pequeno porte, com poucos equipamentos, como uma rede LAN. Por isso, em uma rede WAN, essa técnica, de modo geral, não é adotada pelos provedores de internet (FOROUZAN, 2010).

A desvantagem de usar esse tipo de roteamento é que, como todas as entradas da tabela são configuradas manualmente, elas não serão ajustadas pelas alterações que ocorrem na rede, a menos que sejam feitas manualmente.

Nesse caso, se algum dos equipamentos envolvido no processo de roteamento apresentar defeito, isso causará danos e interromperá a transmissão dos dados, o que vale também para a adição de novos equipamentos ou alteração da topologia.

Para redes muito grandes, o administrador ainda precisa dispor de muito tempo até finalizar todas as configurações necessárias.

2.2.2 Roteamento dinâmico

O roteamento dinâmico é um método pelo qual os roteadores determinam, automaticamente, a melhor rota (caminho), sem intervenção manual. Para cada processo, o caminho deve ser o mais relevante na visão do gateway, que intermedia todas as comunicações que passam por ele de uma rede a outra.

O roteador faz isso por meio de uma tabela de roteamento que é construída e atualizada de acordo com as informações trocadas entre os protocolos de roteamento utilizados na rede. Esses protocolos são desenvolvidos principalmente para distribuir informações e ajustar as rotas de modo dinâmico, refletindo alterações sempre que uma condição da rede for alterada.

O roteador avalia diversas condições para tomar essa decisão, baseando-se em aspectos da rede e em qual será a rota mais rápida, até que os dados cheguem ao endereço de destino, sem envolver o administrador nesse processo, podendo resolver situações complexas de modo simplificado.

Os principais e mais utilizados protocolos de roteamento são o Routing Information Protocol (RIP) e o Open

Shortest Path First (OSPF).



VOCÊ SABIA?

Existem outros protocolos que ainda são utilizados em situações específicas, como Border Gateway Protocol (BGP), Intermediate System to Intermediate System Protocol (IS-IS), e o EIGRP(). Cada um desses protocolos possui características e funcionalidades diferentes.

Em redes que mudam constantemente, utilizar o roteamento dinâmico é o modo mais adequado de manter uma conexão possível entre os pontos. Periodicamente, tabelas dinâmicas de roteamento são atualizadas com o uso dos protocolos de roteamento dinâmico.

Forouzan (2010) aponta que o roteamento estático é utilizado na internet, pela necessidade de constante atualização na tabela de roteamento e a complexidade de sua estrutura, que não permite gerenciamento manual e acompanhamento por meio de intervenção humana. Portanto, quando houver alguma alteração na internet (como falha técnica no roteador ou em um link de internet), esses problemas podem ser resolvidos quase que imediatamente.

O Quadro 1 demonstra um modelo simples de tabela dinâmica.

Quadro 1 – Tabela de roteamento dinâmico

MÁSCARA	ENDEREÇO DE REDE	ENDEREÇO DO PRÓXIMO SALTO (HOP)	INTERFACE DE REDE	FLAGS	CONTAGEM DE SALTOS	USO
-----	8.8.4.4	192.168.2.1	-----	-----	55	2

Fonte: FOROUZAN, 2010. (Adaptado).

Conforme visto no roteamento estático, o roteador precisa ter conhecimento das informações necessárias para encaminhar corretamente os pacotes de dados na rede. No entanto, ao contrário, no roteamento dinâmico, o roteador pode descobrir e compartilhar automaticamente essas informações, armazenadas posteriormente na tabela de roteamento.

Nos cards a seguir, podemos entender o que cada um dos campos apresentados no Quadro 1 representa para a tabela de roteamento dinâmico.

Campos utilizados na tabela de roteamento dinâmico

» Clique nas abas para saber mais sobre o assunto

Máscara	Endereço da rede	Endereço do próximo salto	
Interface	Flags	Contagem de referência	Uso

Esse campo fornece o número de usuários atualmente conectados na rede, fazendo uso da rota estabelecida;

Todos os protocolos de roteamento executam as mesmas funções básicas e facilitam o roteamento na rede, tornando o processo mais eficiente e confiável do que ocorre na atualização estática de rotas.

Eles determinam a melhor rota para cada destino e distribuem as informações de roteamento entre os sistemas da rede, sempre visando a otimizar o processo.

O modo como eles decidem qual é a melhor rota é o que determina a diferença entre os pacotes roteados existentes, que podem ser internos ou externos, conforme abordaremos mais adiante.

2.2.3 Métricas e algoritmos de roteamento

Os protocolos de roteamento dinâmico usam algoritmos específicos para que possam funcionar corretamente. Entre eles, podemos citar o *link state routing* (LSR) e o *distance vector routing* (DVR) que serão apresentados a seguir.

» Roteamento por estado do link (LSR)

O princípio de consideração de roteamento por estado de link ou LSR é definido pelo modo como ele usa um algoritmo que considera se cada nó no domínio representa uma topologia inteira (lista de nós, conexão entre eles, métrica, custo e condições de link – estejam eles ativos ou não) que deve ser compartilhada com os demais. Ou seja, de acordo com Filipetti (2014), cada roteador enviará informações sobre seus vizinhos para todos os roteadores por meio de inundação de rede (broadcast).

O LSR usa o algoritmo de Dijkstra para construir a tabela de roteamento, sempre considerando o caminho mais curto e compartilhando informações quando ocorrem atualizações.

O algoritmo de Dijkstra foi concebido para resolver o problema das rotas seguidas na rede, trabalhando sempre com o caminho mais curto.

Em cada etapa do algoritmo, ele procura aquele vértice com menor distância e o adiciona na tabela de roteamento, repetindo essas etapas até que todos os vértices possam alcançar o destino.

Após a definição do custo, o valor dos vizinhos do nó inicial é analisado pelo algoritmo. Caso o ponto final seja

um vizinho, o custo do link até o destino é o valor entre os nós; caso contrário, o custo do link é considerado infinito.

Quando o valor do custo é definido como infinito, o vizinho de menor valor é considerado o ponto de partida, e seus vizinhos são analisados iniciando um loop que verificará todos os vértices até que o caminho de menor custo seja proposto.

» Roteamento por vetorial de caminho (DVR)

Os algoritmos de roteamento com vetor de distância, também denominados roteamento distribuído de Bellman-Ford, operam mantendo uma tabela em cada roteador, utilizadas como instrumento para fornecer a melhor distância conhecida para cada destino e determinar qual linha deve ser usada para chegar a esse destino. Essas tabelas são atualizadas trocando informações com os vizinhos.

As características do roteamento vetorial de distância e do roteamento por estado de link podem ser comparadas por meio do Quadro 2.

Quadro 2 – Comparação entre os roteamentos LSR e DVR

ROTEAMENTO POR ESTADO DO LINK	ROTEAMENTO POR VETORIAL DE CAMINHO
A largura de banda exigida é maior, por trabalhar inundando a rede e enviando um grande número de pacotes.	A largura de banda é menor devido ao compartilhamento local e envio de pacotes menores sem o uso de inundação.
Possui conhecimento sobre toda a rede e as tabelas não são mantidas por si só, mas por todos os roteadores que estão ao seu alcance.	Funciona com base no conhecimento local atualizando a tabela somente com base em informações recebidas dos vizinhos imediatos.
Faz uso do Dijkstra.	Faz uso do Bellman.
O tráfego é maior.	O tráfego é menor.
Implementação do protocolo OSPF.	Implementação do protocolo RIP.

Fonte: FILIPPETI, 2014. (Adaptado).

Tanto o roteamento estático quanto o dinâmico apresentam características únicas, porém, para permitir um melhor gerenciamento da rede, o protocolo dinâmico apresenta mais recursos e utiliza algoritmos, tabelas e outros fatores, a fim de garantir que seu processo, por ser mais complexo, ocorra corretamente. No entanto, sua complexidade não influencia diretamente em atividades que precisem ser realizadas pelo administrador, tornando mais fácil manter uma rede de grande proporção, operando adequadamente e minimizando os riscos

de indisponibilidade, falhas de segurança e problemas de conectividade.

Teste seus conhecimentos

Atividade não pontuada.

2.3 Protocolos de roteamento

Diversos protocolos de roteamento estão disponíveis no mercado, oferecendo abordagens diferentes e sendo ideais para situações específicas. Nessa seção, iremos abordar especificamente as características dos protocolos RIP e OSPF, analisando as diferenças entre eles e os recursos, algoritmos e métricas que cada um utiliza para possibilitar a transmissão de dados entre as redes.

2.3.1 RIP

O RIP é um protocolo muito simples, baseado no roteamento do vetor de distância. Forouzan (2010) aponta algumas considerações sobre esse algoritmo e seu funcionamento:

- Em um sistema autônomo, estamos lidando com roteadores e redes (links). O roteador tem uma tabela de roteamento, a rede não;
- O destino na tabela de roteamento é a rede, o que significa que a primeira coluna define seu endereço.



VOCÊ SABIA?

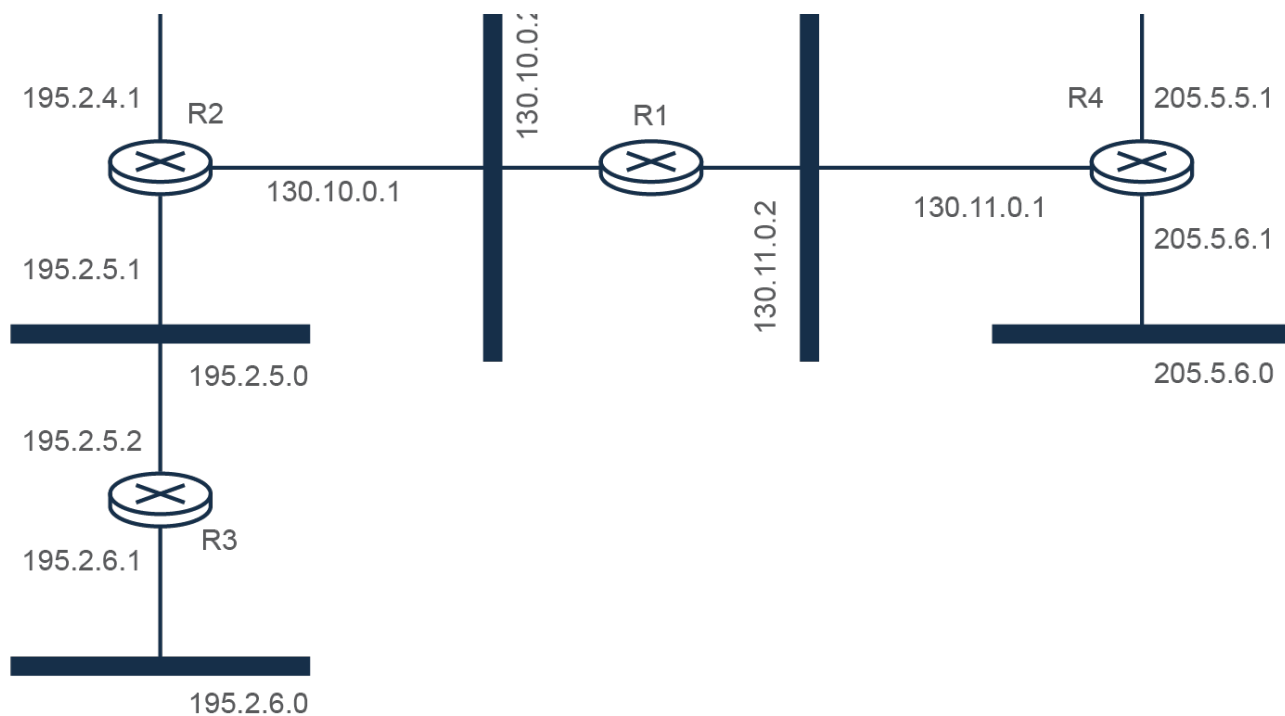
Na internet, um sistema autônomo (AS) é uma coleção de prefixos de roteamento conectados por meio do protocolo de internet (IP), sob o controle de um ou mais operadores de rede.

Além disso, a métrica utilizada pelo protocolo RIP também funciona de modo simples:

- A distância é definida em relação ao número de links (redes) que podem ser utilizados para chegar ao destino, denominado número de saltos;
- O número máximo de saltos definido pelo RIP é 15 (o valor começa em zero e finaliza quando chega em 15). Portanto, o roteamento em AS não pode ultrapassar 15. Caso isso aconteça, o pacote será descartado;
- A próxima coluna de nós define o endereço do roteador que o pacote deve alcançar ao chegar no final da sua rota.

Uma topologia que funciona considerando as etapas descritas e utilizando o protocolo RIP pode ser vista na Figura 7.





Dest.	Hop	Próximo
130.10.0.0	1	–
130.11.0.0	1	–
195.2.4.0	2	130.10.0.1
195.2.5.0	2	130.10.0.1
192.2.6.0	3	130.10.0.1
205.5.5.0	2	130.11.0.1
205.5.6.0	2	130.11.0.1

Tabela R1

Dest.	Hop	Próximo
130.10.0.0	1	–
130.11.0.0	2	130.10.0.2
195.2.4.0	1	–
195.2.5.0	1	–
192.2.6.0	2	195.2.5.2
205.5.5.0	3	130.10.0.2
205.5.6.0	3	130.10.0.2

Tabela R2

Dest.	Hop	Próximo
130.10.0.0	2	195.2.5.1
130.11.0.0	3	195.2.5.1
195.2.4.0	2	195.2.5.1
195.2.5.0	1	–
192.2.6.0	1	–
205.5.5.0	4	195.2.5.1
205.5.6.0	4	195.2.5.1

Tabela R3

Dest.	Hop	Próximo
130.10.0.0	1	130.11.0.2
130.11.0.0	1	–
195.2.4.0	2	130.11.0.2
195.2.5.0	2	130.11.0.2
192.2.6.0	3	130.11.0.2
205.5.5.0	2	–
205.5.6.0	2	–

Tabela R4

Figura 7 – Exemplo de uma rede WAN com o uso de protocolo RIP.

Fonte: FOROUZAN, 2010, p. 393. (Adaptada).

#PraCegoVer : a imagem ilustra uma topologia de rede utilizando o protocolo RIP para

estabelecer a comunicação entre os roteadores de diversas redes LAN que se conectam uns aos outros através do sistema de rotas definido. A direita a rede WAN 130.11.0.0 está conectada diretamente com a rede local 205.5.5 através de um roteador que também estabelece uma segunda conexão com a rede 205.5.6.0. No centro temos a mesma rede conectada através e um roteador central à outra rede de IP 130.10.0.0 e que está conectada diretamente a rede 195.2.5.0 e a rede 195.2.4.0. Cada rede alcança as demais através de um roteador. Abaixo da representação da rede, existem quatro tabelas representando as redes de destino que podem ser alcançadas, o número de saltos necessários e qualquer será o salto seguinte para que a rota seja iniciada.

Nesse exemplo, as redes estão interconectadas por roteamento e conectadas via internet, pelo fato de representarem redes locais geograficamente distantes. Quando um host na rede 130.11.0.0 deseja se comunicar com um host na rede 205.5.5.0, ele deve acessar o host de destino por meio da entrada diretamente conectada à sua interface.

Ao tentar se comunicar com o host 195.2.5.1, atribuído na rede 195.2.5.0, ele deve primeiro sair do roteador do gateway de rede (195.2.4.0) e, em seguida, encaminhar o pacote para o próximo salto, antes de chegar ao destino (rede e host). As mensagens enviadas pelo protocolo RIP respeitam um padrão específico, conforme ilustra a Figura 8.



Figura 8 – Campos de uma mensagem enviada pelo protocolo RIP.

Fonte: FOROUZAN, 2010, p. 394. (Adaptada).

#PraCegoVer : a imagem ilustra os campos que compõe uma mensagem enviada pelo protocolo RIP: contendo três colunas e seis linhas. A primeira linha é dividida em três colunas: Comando | Versão | Reservado. A segunda linha é dividida em duas colunas: Família | Tudo 0 representa o protocolo utilizado como o IP por exemplo. A terceira linha representa o endereço IP da rede. A quarta e a quinta linha representam um campo somente com 0 e o último campo representa a distância entre os pontos que estão trocando informações na rede.

O RIP divide a rede em que atua em máquinas ativas, representadas pelos roteadores que anunciam suas rotas para outras pessoas e máquinas passivas que não anunciam e atualizam suas rotas com base no anúncio.

Além disso, entende-se que as mensagens em RIP podem ser divididas em dois tipos, como exemplificado nos Cards a seguir.

Mensagens de RIP

» Clique nas abas para saber mais sobre o assunto

Pedido

Resposta (ou atualização de pacote)

Essa mensagem é enviada apenas de acordo com um pedido enviado anteriormente. Ela contém informações sobre o destino especificado no pedido correspondente. Por outro lado, é enviada, periodicamente, a cada 30 segundos, ou quando há uma alteração na tabela de roteamento, para manter os dados em conformidade com a tabela mantida pela rede;

Assim como qualquer cabeçalho, uma mensagem enviada pelo protocolo RIP também especifica as informações por meio de campos, em que cada um é utilizado para identificar dados específicos e necessários para a transmissão de pacotes.

- **Comando** : composto por 8 bits, para especificar qual tipo da mensagem está sendo emitida – pedido (1) ou resposta (2);
- **Versão** : composto de 8 bits, para definir qual a versão do protocolo (RIP ou RIP2) está sendo utilizada;
- **Família** : composto de 16 bits, define a família do protocolo usado – para TCP/IP, por exemplo, o valor é 2;
- **Endereço de rede** : define o endereço da rede de destino;
- **Distância** : composto por 32 bits, para definir a contagem de saltos desde o roteador origem até o roteador de destino.

2.3.2 OSPF

Além de ser definido como um protocolo de roteamento intradomínio, o protocolo OSPF também é um protocolo aberto, baseado no roteamento, no estado do link (algoritmo que tem como princípio o fato de que cada roteador tem informações sobre a rede à qual está conectado e as atualizações são realizadas periodicamente para determinar se cada link está ativo). O principal objetivo do OSPF é resolver problemas de roteamento de modo oportuno e eficaz, operando independentemente do fabricante, assim como o protocolo RIP.

Segundo Filippetti (2014), o protocolo OSPF utiliza o algoritmo de Dijkstra para calcular o roteamento e considera qual métrica selecionar para a largura de banda, o que difere da limitação que aparece no protocolo do vetor de distância. A exposição do protocolo pode causar problemas altamente complexos para a rede, por exemplo, quando ele é implementado (como é o caso de quando a rede recebe e propaga atualizações de roteamento).

O OSPF não causará *flood* (inundações) na rede, porque envia atualizações via multicast, ou seja, apenas roteadores com protocolos ativos processarão esses pacotes. Além disso, é usado junto às atualizações incrementais para enviar apenas as informações que foram alteradas desde o último processamento ocorrido em cada atualização.

Sendo assim, o OSPF é capaz de:

- Reduzir o tempo de convergência da rede;
- Economizar largura de banda;
- Hierarquizar uma rede, segmentando-a em diversos domínios de roteamento, também chamados de áreas, utilizadas para controlar as informações de roteamento compartilhadas na rede.

» Áreas OSPF

Ainda de acordo com Filippetti (2014), quando se fala em áreas no OSPF, a área principal é chamada de área zero, área de backbone ou área de tráfego e deve sempre existir na rede OSPF.

Todas as demais áreas criadas na rede OSPF devem estar conectadas à área zero diretamente ou por meio de um recurso denominado link virtual para operar normalmente, ou seja, o túnel é criado na rede na área zero para enganar o protocolo, o que não pode ser feito do modo tradicional.

Apesar dessa divisão, os roteadores ainda podem pertencer a várias áreas diferentes.

A estrutura é baseada nos seguintes componentes (Figura 9):

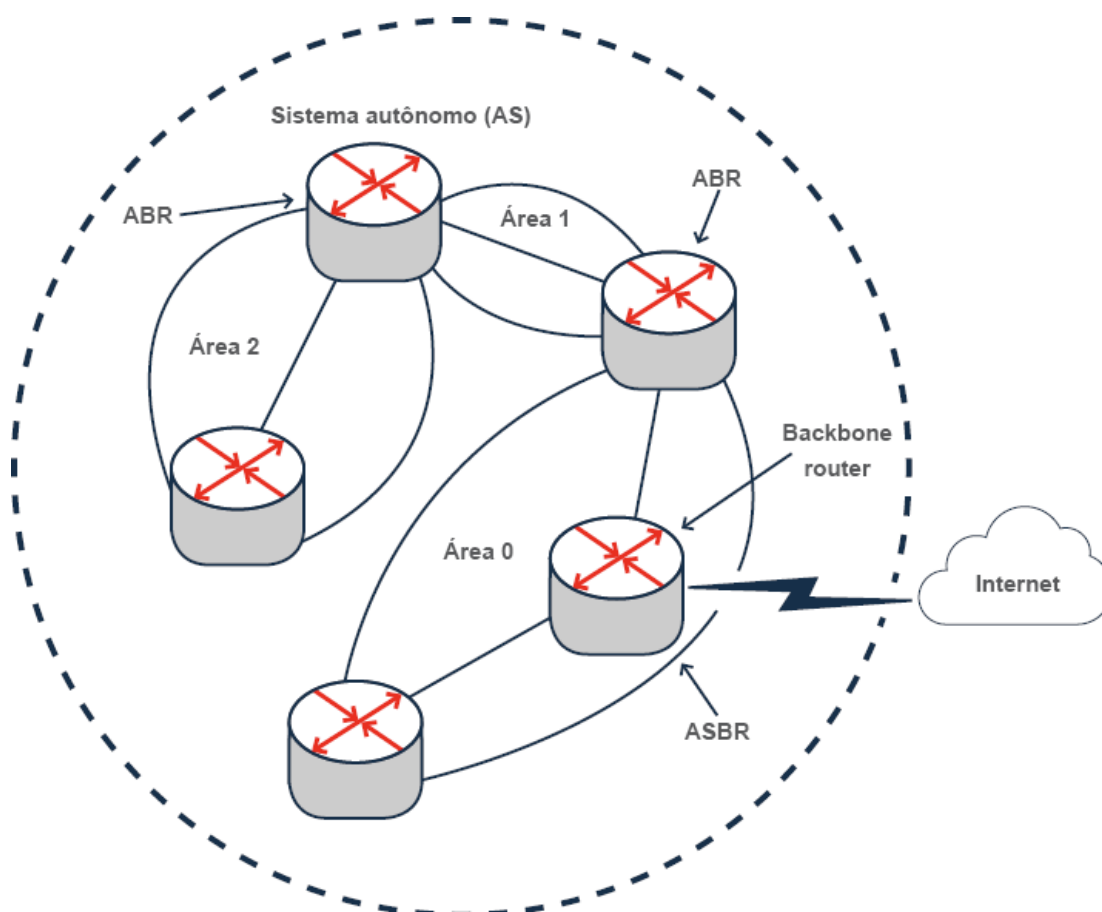


Figura 9 – Estrutura OSPF.
Fonte: FILIPPETTI, 2014, p. 269.

#PraCegoVer : a imagem ilustra a Área 0 dentro de um círculo representada por um roteador ASBR conectado a outros dois roteadores, sendo um deles um ABR com mais duas interfaces (uma para se conectar a área 1 e outra à área 2) e o outro conectado somente à área 0. O roteador ASBR também é conectado a uma nuvem denominada internet, através de um raio que representa a conexão WAN (rede de longa distância). Outro círculo envolve a área 1 e o ABR está conectado a outro roteador ABR dentro da Área 2, envolvida por outro círculo.

A descrição de cada elemento pode ser vista abaixo:

- **Internal Router** : roteador interno que possui todas as suas interfaces na mesma área (não precisa ser necessariamente na área zero);
- **Backbone Router** : especifica um roteador interno contido somente na área zero;
- **Area Border Router (ABR)** : mesmo se outras interfaces estiverem em outras áreas, o roteador tem pelo menos uma de suas interfaces na área zero;
- **Autonomous System Border Router (ASBR)** : define qualquer roteador que realize distribuição de rota de outras fontes (como roteamento estático, BGP e RIP) para a rede OSPF;
- **External Router (roteador externo)** : qualquer roteador fora da rede OSPF utilizando o protocolo RIP, por exemplo, e que em algum momento se comunique por meio da rede.

» Tabelas de roteamento OSPF

Geralmente, as tabelas utilizadas no roteamento OSPF são Neighbor table, Link State Database (LSDB) e Routing Information Base (RIB), que são definidas por Filipetti (2014), conforme apresentado nos Cards a seguir.

Campos da tabela OSPF

» Clique nas setas ou arraste para visualizar o conteúdo

Neighbor Table

Mantém as informações sobre os respectivos vizinhos, ou seja, os roteadores que estão diretamente conectados dentro de uma área OSPF;

LSDB

Mapeia a relação entre todos os roteadores da rede OSPF e o modo como eles se comunicam, as redes conhecidas e os custos envolvidos entre as rotas;

RIB

Tabela de roteamento. Todas as rotas são enviadas para RIB. O protocolo OSPF também suporta o balanceamento de carga, suportando até seis rotas de mesmo custo para a mesma rede remota.

Além dos campos que compõem a tabela OSPF e definem a sua funcionalidade, o custo (também denominado métrica) é o padrão usado pelo protocolo OSPF para selecionar rotas na rede. O menor custo define o melhor caminho de escolha. Quanto maior a largura de banda do link, menor o custo, pois a capacidade de atender a demanda torna-se maior. O OSPF soma o custo de todas as interfaces envolvidas no caminho adotado.

Sendo assim, podemos considerar que o custo de uma rota é a soma dos custos de todas as interfaces de saída para um destino. Por padrão, o roteador calcula o custo OSPF de acordo com a seguinte fórmula:

$$\text{Custo} = \text{valor da largura de banda de referência} / \text{largura de banda do link.}$$

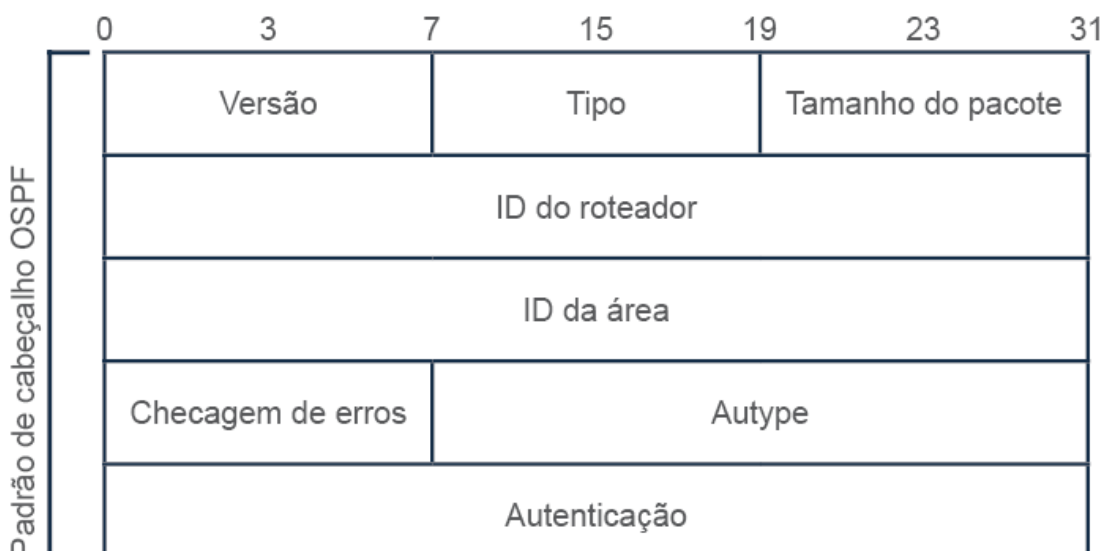
CASO



Se o valor de “largura de banda de referência” não for configurado, o roteador usará um valor padrão de 100 Mb para o cálculo. Nesse caso, se a interface tiver uma largura de 10 Mb, o cálculo será: 100 Mb dividido por 10 Mb, então o custo da interface é 10. O valor da fração foi arredondado para o valor inteiro mais próximo e qualquer velocidade maior que 100 Mb será alocada como um custo de 1.

» Cabeçalho do protocolo OSPF

Todos os pacotes OSPF enviam, junto aos pacotes, um cabeçalho contendo informações sobre a mensagem e as informações contidas neles. Os campos de um cabeçalho OSPF podem ser vistos na Figura 10.



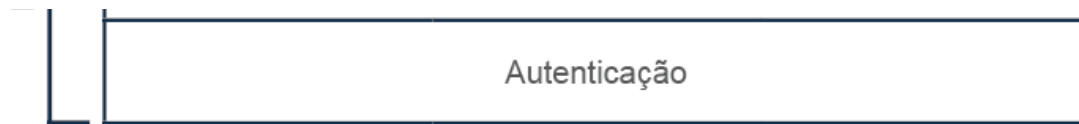


Figura 10 – Cabeçalho OSPF.
Fonte: TADIMETY, 2015, p. 43. (Adaptado).

#PraCegoVer : a imagem ilustra os campos de um cabeçalho OSPF, demonstrando uma tabela formada por seis linhas e três colunas, onde na primeira linha, as colunas são formadas pelas informações: versão, tipo e tamanho do pacote. Na segunda linha, um campo único representa a identificação do roteador, na terceira linha um campo inteiro representa a identificação da área, na quarta linha duas colunas representam um campo de checagem de erro e outro para o tipo de autenticação utilizada. Os dois últimos campos representam uma linha inteira cada um, utilizados para autenticação do pacote.

Cada um dos campos representa as funções a seguir:

- **Versão** : composto de 8 bits, que define a versão do protocolo OSPF. Atualmente, o protocolo OSPF está na versão 2, assim como o RIP;
- **Tipos** : composto de 8 bits, que define o tipo de pacote de dados;
- **Tamanho da mensagem** : possui 16 bits e representa o comprimento total da mensagem, incluindo o conteúdo do título;
- **Identificação do roteador** : composto de 32 bits, utilizado para definir o endereço IP do roteador de origem do pacote;
- **Identificador da área** : composto de 32 bits, para definir a área em que o roteamento irá ocorrer dentro da rede;
- **Soma de verificação** : campo usado para detecção de erros no pacote, excluindo os campos de autenticação;
- **Tipo de autenticação** : composto de 16 bits, para definir o protocolo de autenticação utilizado em uma área específica. Atualmente, dois tipos de autenticação são definidos: 0 significa nenhuma e a autenticação através de senha é representada pelo número 1;
- **Autenticação** : contém 64 bits e define o valor real dos dados de autenticação. Se for 0, é preenchido com 0; se for 1, irá possuir uma senha com tamanho de 8 bits.

» Pacotes OSPF

O OSPF usa cinco diferentes tipos de pacotes, descritos de acordo com Filippetti (2014), como:

Pacotes OSPF

» Clique nas setas ou arraste para visualizar o conteúdo

Hello	Database Descriptor (DBD)	Link State Request (LSR)
-------	---------------------------	--------------------------

Quando o pacote receber a mensagem DBD, ele verificará se as informações de roteamento estão corretas. Caso contrário, ele enviará pacotes LSR para verificar informações detalhadas sobre essas rotas com os vizinhos;

Link State Update (LSU):

LSAck

Esse pacote é enviado ao vizinho com as informações, após um pacote LSR ser recebido;

O principal objetivo do OSPF é dividir sua topologia em várias partes (área) e categorizar o roteamento para melhorar o processamento do roteador.

Sendo assim, a camada de rede e os protocolos de roteamento especificam o método de comunicação e a distribuição de informações entre os roteadores, permitindo que a melhor rota seja selecionada entre os nós da rede.

Do mesmo modo, os algoritmos de roteamento determinam opções de roteamento específicas. Cada roteador possui apenas um conhecimento prévio da rede diretamente conectada a ele, mas o protocolo de roteamento permite compartilhar informações entre seus vizinhos diretos. Compartilhando-as na rede, sua principal finalidade é chegar a um destino específico, de modo que o pacote seja transmitido por meio de toda a topologia da rede.

Teste seus conhecimentos

Atividade não pontuada.

Síntese

Nesta unidade, foram abordados os tipos de roteamento, suas características e vantagens e desvantagens de cada um deles. Além disso, conhecemos os principais protocolos que atuam na camada de rede entendendo de que forma a interconexão entre dispositivos que se encontram em redes diferentes pode ser possível através da internet. Abordamos conceitos importantes que definem as funções da camada de rede, além dos componentes, protocolos, mensagens e cabeçalhos inseridos aos pacotes que permitem a transmissão de dados da melhor forma, comunicando os serviços entre si e garantindo confiabilidade, segurança e agilidade em torno do processo. Por fim, foi possível entender como os protocolos de roteamento se diferenciam entre si e em relação aos algoritmos utilizados por eles em cenários específicos, comparando seus prós e contras. Foi possível entender a importância da camada de rede e sua relação com as demais camadas do Modelo OSI.

SAIBA MAIS



Título: Controle de congestionamento – Camada de transporte

Autor: Oficinadanet

Ano: 2008

Comentário: O conteúdo aborda os conceitos sobre a camada de transporte e o cabeçalho de cada um deles, apresentando o conceito de controle de congestionamento.

Onde encontrar: < https://www.oficinadanet.com.br/artigo/968/controle_de_congestionamento >



Título: Camada de transporte – Multiplexação e Demultiplexação

Autor: Silva

Ano: 2008

Comentário: O vídeo traz uma explicação sobre multiplexação e demultiplexação, mostrando qual a funcionalidade dos processos na camada de transporte.

Onde encontrar: < <https://www.youtube.com/watch?v=56GZ-9XtzYk> >.



Título: Redes de Computadores.

Autor: Andrew Stuart Tanenbaum

Ano: 2003

Comentário: Este livro aborda diversos conceitos de redes de computadores, apresentando noções básicas sobre o funcionamento dos protocolos, principalmente na camada de rede e em suas estruturas.

Onde encontrar: Biblioteca Virtual da Laureate.

Referências bibliográficas

FILIPPETTI, M. A. **CCNA 5.0** : guia completo de estudo. Florianópolis: Visual Books, 2014.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores** . Porto Alegre: AMGH, 2010.

FOROUZAN, B. A.; MOSHARRAF, F. **Redes de computadores** : uma abordagem top-down. Porto Alegre: AMGH, 2013.

MORAES, A. F. **Redes de computadores** : fundamentos. São Paulo: Saraiva, 2010.

TADEMETY, P. R. **OSPF** : A Networking Routing Protocol. New York: Apress, 2015.

TANENBAUM, A. **Redes de computadores** . Rio de Janeiro: Campus, 2003.
