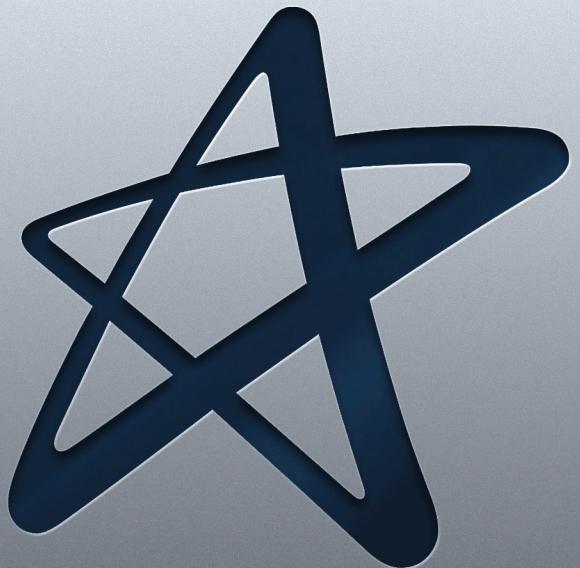


# Tecnologias de Roteamento



Cruzeiro do Sul Virtual  
Educação a distância



# Material Teórico



**Operação do Roteador e Decisão de Roteamento**

**Responsável pelo Conteúdo:**

Prof. Esp. Antonio Eduardo Marques da Silva

**Revisão Textual:**

Prof.<sup>a</sup> Dr.<sup>a</sup> Selma Aparecida Cesarin



# UNIDADE

## Operação do Roteador e Decisão de Roteamento



- [O Dispositivo Roteador;](#)
- [Gerenciamento do Roteador;](#)
- [Conectando a Interface Local \(LAN\);](#)
- [Conectando a Interface Remota \(WAN\);](#)
- [Decisão de Encaminhamento de Pacotes;](#)
- [Configurando Um Roteador Cisco;](#)
- [Examinando o Roteador;](#)
- [Configurando Interface Serial;](#)
- [Alterando Configurações.](#)



### OBJETIVO DE APRENDIZADO

- Compreender e abordar o que é e como funciona de fato um roteador dentro de uma Rede. Para isso, vamos entender como esse dispositivo é gerenciado, acessado e posicionado, tanto numa LAN quanto numa WAN, e algumas configurações básicas e importantes para colocá-lo em atividade.





# Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:

Determine um horário fixo para estudar.

Mantenha o foco! Evite se distrair com as redes sociais.

Procure manter contato com seus colegas e tutores para trocar ideias! Isso amplia a aprendizagem.

Seja original! Nunca plagie trabalhos.

Aproveite as indicações de Material Complementar.

Conserve seu material e local de estudos sempre organizados.

Não se esqueça de se alimentar e de se manter hidratado.

## Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu “momento do estudo”;
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

# O Dispositivo Roteador

O roteador é uma espécie de computador com funções específicas e, por esse motivo, ele tem os mesmos componentes básicos de um computador padrão, isto é, ele tem CPU, memórias, barramento do sistema e diversas interfaces de entrada/saída de Dados.

Entretanto, os roteadores são projetados para realizar algumas funções muito específicas, como foi dito, que, geralmente, não são realizadas pelos computadores *desktop* tradicionais, ou até podem ser executadas, mas, sem dúvida, de forma muito menos performática e confiável. Por exemplo, os roteadores conectam e permitem a comunicação entre duas ou mais Redes diferentes e determinam, por meio de vários cálculos, o melhor caminho para que os dados possam viajar através dessas Redes (TANENBAUM, 2011).

Assim como os computadores tradicionais, os roteadores precisam de Sistemas Operacionais de Rede (SOR) para executarem os softwares aplicativos e outros recursos de controle da máquina, no caso, os roteadores da Cisco precisam do SISTEMA OPERACIONAL IOS (*Internetwork Operating System* – Sistema Operacional de Interconexão de Redes) que é proprietário dessa empresa, para poder executar as funções definidas nos arquivos de configuração que foram pré-configuradas.

Esses arquivos de configuração contêm as instruções e os parâmetros que controlam o fluxo de tráfego de dados que entra e sai dos roteadores.

Especificamente, usando Protocolos de roteamento, os roteadores tomam decisões de encaminhamento em relação ao melhor caminho para que os pacotes cheguem ao destinatário sem maiores problemas.

O arquivo de configuração específica todas as informações e as configurações necessárias para utilização correta dos Protocolos roteados/roteáveis e de roteamento, selecionados ou ativados pelo roteador (CISCO NETACAD, 2017).



Por dentro das coisas – Roteadores. Acesse: <https://youtu.be/4bC4J6tFifQ>

Um dos principais componentes internos do roteador são a Memória de Acesso Aleatório (RAM), a memória de Acesso Aleatório Não Volátil (NVRAM), a memória flash, a Memória Somente de Leitura (ROM) e as interfaces que permitem a interconexão com o mundo externo.

A RAM, também chamada de RAM dinâmica (DRAM) e/ou memória de trabalho, tem as seguintes principais características e funções:

- Armazena Tabelas de roteamento, que foram calculadas pelos Protocolos de roteamento; nelas sempre estão as melhores rotas para seus destinos;
- Fornece memória ativa temporária para o arquivo de configuração do roteador enquanto ele estiver ligado (memória de trabalho);

- Mantém a cache do ARP, a fim de identificar endereços de enlace e outras informações importantes para comunicação interna;
- Mantém a cache do *fast-switching* (comutação rápida), que é uma das técnicas usadas para a comutação/chaveamento de pacotes;
- Armazena pacotes em *buffers* (RAM compartilhada) para uma execução seguinte;
- Mantém filas para armazenamento temporário de pacotes (*queues*), que podem ser utilizadas em priorização de tráfego;
- É um tipo de memória volátil, ou seja, perde todo o seu conteúdo quando o roteador é desligado ou reiniciado.

A NVRAM tem as seguintes características e funções:

- Armazena o arquivo de configuração que será utilizado somente no Processo de Inicialização (*startup-configuration*); também podemos chamar de arquivo de *backup* de configurações;
- Retém seu conteúdo quando o roteador é desligado ou reiniciado, pois a memória NVRAM, como o próprio nome indica, é uma memória não volátil, ou seja, armazena um conteúdo mesmo se não estiver energizada.

A memória *flash* tem as seguintes características e funções:

- Mantém a imagem do Sistema Operacional (IOS) que será usado no processo de *boot* do equipamento;
- Pode armazenar várias versões do *software* do IOS. Nesse caso, o administrador da rede pode escolher qual das versões do IOS o equipamento virá a utilizar;
- Permite que o *software* seja atualizado sem remover nem substituir *chips* do processador;
- Retém seu conteúdo quando o roteador é desligado ou reiniciado, pois também é uma memória não volátil;
- É um tipo de ROM programável, apagável eletronicamente (EEPROM).

A Memória Somente de Leitura (ROM) tem as seguintes características e funções:

- Mantém instruções que definem o autoteste realizado na inicialização do roteador, que conhecemos pelo nome POST (*Power-on self test*);
- Armazena o programa de *bootstrap* e softwares básicos do Sistema Operacional de Rede;
- Requer a substituição de *chips* plugáveis na placa mãe para as atualizações de *software*, pois eles, geralmente, são gravados em memória de acesso não tão fácil.

As interfaces físicas têm as seguintes características e funções:

- Conectam o roteador à Rede local ou remota para as funções de entrada e saída de pacotes de dados. Um exemplo de interfaces poderiam ser as conexões seriais e/ou *ethernet*;
- Podem ficar fixadas na placa mãe (*on-board*) ou num módulo separado e conectado ao barramento (*off-board*).

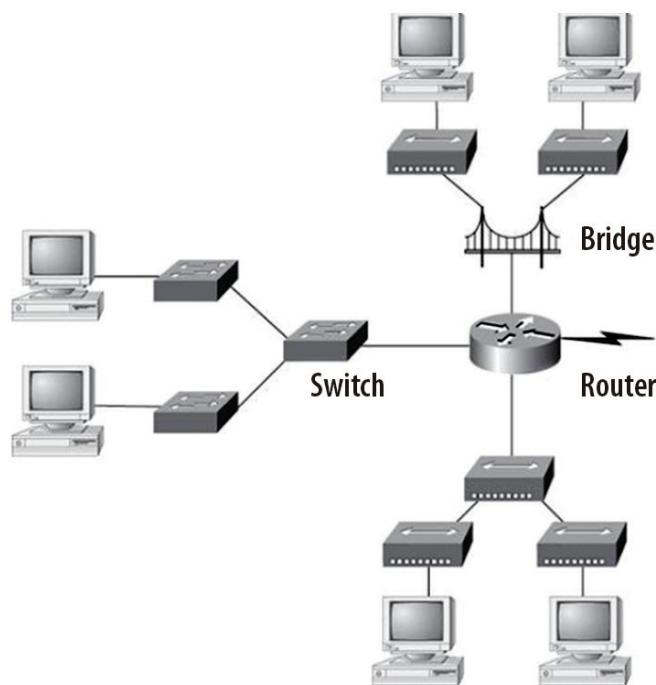


Figura 1 – Segmentação de Redes

Embora um roteador possa ser utilizado para segmentar Redes locais, sua principal utilização é como dispositivo de WAN. É importante nos lembarmos de que os roteadores possuem tanto interfaces de Rede local quanto de Rede remota em acesso a uma WAN.

As Tecnologias WAN, geralmente, são utilizadas para conectar roteadores, ou seja, os roteadores se comunicam entre si por meio de conexões WAN, como conexões Seriais, ISDN e outras.

Os roteadores são os equipamentos de rede que compõem o *backbone* das grandes Redes, como *Intranets*, e até mesmo da *Internet*.

Os roteadores são dispositivos de camada de Rede, pois operam na camada 3 do modelo OSI, tomando decisões de encaminhamento com base nos endereços de Rede destino, que foi previamente calculada por um algoritmo de roteamento, ou até mesmo por uma rota estaticamente configurada.

As duas principais funções de um roteador são a seleção do melhor caminho para e entrega de Dados a um destino e a comutação de pacotes para a interfaces apropriadas.

Os roteadores realizam essas funções criando Tabelas de roteamento e trocando informações de Rede com outros roteadores em uma topologia (TANENBAUM, 2011).

Um administrador de Rede pode manter Tabelas de roteamento por meio da configuração de rotas estáticas, mas, geralmente, as Tabelas de roteamento são mantidas dinamicamente por meio da utilização de um Protocolo de roteamento dinâmico, que trocam informações sobre toda a topologia (caminhos) da Rede (CISCO NETACAD, 2017).

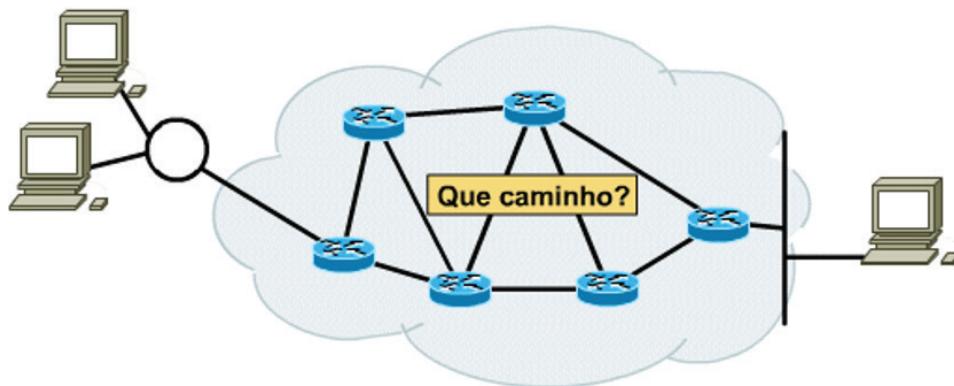


Figura 2 – Determinação de Caminho

Uma interconexão de Redes (*Internet work*) corretamente configurada oferece as seguintes funcionalidades:

- Endereçamento fim a fim consistente;
- Endereços que representam topologias de Rede;
- Seleção do melhor caminho;
- Roteamento dinâmico ou estático;
- Comutação.

Considera-se que uma Rede WAN opera na camada física (Camada 1) e na camada de enlace (Camada 2) do Modelo OSI; isso não significa que as outras cinco camadas desse modelo de referência não sejam encontradas em uma WAN.

Significa, apenas, que as características que diferenciam uma WAN de uma LAN (Rede local), normalmente, são encontradas na camada física e na camada de enlace, sendo que os padrões e os Protocolos utilizados nas camadas 1 e 2 das WANs são diferentes dos utilizados nas mesmas camadas das LANs (TANENBAUM, 2011).

A camada física da WAN descreve a interface entre o equipamento Terminal de Dados (DTE) e o equipamento de terminação do circuito de dados (DCE).

Tradicionalmente, o DCE é o provedor do serviço e o DTE é o dispositivo conectado à Rede de um determinado cliente. Nesse modelo, os serviços oferecidos para o DTE são disponibilizados por meio de um *modem* ou de um CSU/DSU, que é uma espécie de *modem* digital usado em grandes instalações (STALLINGS; ROSS, 2010).

Como já foi percebido e como o próprio nome indica, a principal função de um roteador é o roteamento, que ocorre na Camada de Rede (camada 3) do modelo OSI; mas, se uma WAN opera nas camadas 1 e 2, então, o roteador é um dispositivo de Rede local ou de WAN?

A resposta correta é que ele opera nos dois, como, geralmente, ocorre na área de Redes, pois ele possui interfaces tanto para conexão local quanto para a conexão remota.

Um roteador pode ser exclusivamente um dispositivo de Rede local, pode ser exclusivamente um dispositivo WAN ou pode estar na fronteira entre uma Rede local

e uma WAN, ou seja, pode ser um dispositivo de Rede local e de WAN ao mesmo tempo (STALLINGS; ROSS, 2010).

Tanto em LAN como em WAN, a função do roteador é rotear pacotes. Quando um roteador usa os padrões e os Protocolos das camadas física e de enlace que estão associados às WANs, ele opera como um dispositivo WAN.

As principais funções na WAN de um roteador, portanto, não são de roteamento, mas oferecer conexões entre os vários padrões físicos e de enlace de dados de uma WAN. Por exemplo, um roteador pode ter uma interface ISDN, que utiliza o encapsulamento PPP, e uma interface serial na terminação de uma linha T1, que usa encapsulamento *Frame Relay*.

O roteador deve ser capaz de mover um fluxo de *bits* de um tipo de serviço, como ISDN, para outro, como T1, e mudar o encapsulamento do enlace de dados de PPP para *Frame Relay*.

É por esse motivo que o roteador faz o papel de *gateway* da Rede, que é possibilitar a interconexão de Redes diferentes, encapsulando e desencapsulando seus Protocolos (CISCO NETACAD, 2017).

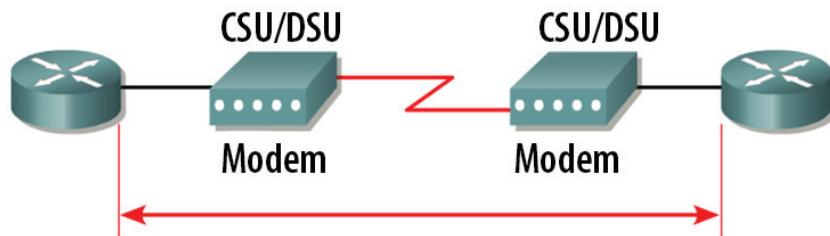


Figura 3 – Roteador e Modem

Podemos, então, listar alguns Protocolos e padrões da camada física da WAN que os roteadores podem suportar:

- EIA/TIA-232 (RS 232);
- EIA/TIA-449 (RS 449);
- V.24; V.35; X.21; G.703 e EIA-530;
- ISDN;
- T1, T3, E1 e E3;
- xDSL (ADSL, SDSL, HDSL etc.);
- SONET (OC-3, OC-12, OC-48, OC-192).

Exemplos de Protocolos e padrões da camada de enlace da WAN:

- *High-Level Data Link Control* (HDLC);
- *Frame Relay*;
- *Point to Point Protocol* (PPP);

- *Synchronous Data Link Control* (SDLC);
- *Serial Line Internet Protocol* (SLIP);
- X.25;
- ATM.

## Gerenciamento do Roteador

A Porta de Console (COM) e a Porta Auxiliar (AUX) que estão inseridas no roteador são portas de acesso para gerenciamento, ou seja, essas portas, apesar de parecidas, não foram concebidas como portas de Rede, como é o caso da Porta *ethernet*.

A Porta console é a primeira forma de configuração inicial num Roteador ou *Switch* da Cisco (modelos corporativos) e, para poder acessar a porta AUX, ela deverá ser antes pré-configurada. É importante lembrar que não são todos os modelos de roteadores que possuem a porta AUX (CISCO NETACAD, 2017).

Quando o roteador entra em operação pela primeira vez, nenhum parâmetro da Rede está devidamente configurado. Nesse caso, o roteador não pode comunicar-se com nenhuma Rede ou Dispositivo.

Para prepará-lo para a inicialização e o funcionamento, são necessárias configurações iniciais; para isso, conecte um terminal ASCII RS-232, ou um computador que emule um terminal ASCII, à porta de console do Sistema.

Assim, é possível inserir os comandos de configuração inicial para acesso o roteador (STALLINGS; ROSS, 2010).

Além da conectividade física através dessa porta ser assíncrona, é também necessária a utilização de uma aplicação de emulação de terminal, como, por exemplo, o *TeraTerm*, *Putty* e outros, que também possuem configurações próprias.

Uma vez acessado e inserida a configuração inicial do Roteador através da porta console e depois pela porta auxiliar (caso seja necessário), o roteador poderá ser conectado à Rede para fins de acesso, configuração e gerenciamento.

Uma vez aplicadas as configurações de acesso padrão (TTY, por exemplo), o roteador também pode ser configurado remotamente, por meio da aplicação *Telnet* em uma rede IP, ou discando para um *modem* conectado à porta auxiliar do roteador (que foi criada com essa finalidade).

Para a resolução de problemas, também é preferível e recomendado utilizar a porta de console, ao invés da porta auxiliar. Isso porque ela apresenta, de forma padrão (*default*), as mensagens de inicialização, depuração e de possíveis erros de hardware ou software do roteador no processo de boot.

Essa porta (console) também pode ser utilizada quando os serviços de Rede não tiverem sido inicializados ou tiverem alguma falha, o que é muito útil nos

procedimentos de recuperação de desastres e recuperação de senhas (processo de *password recovery*).

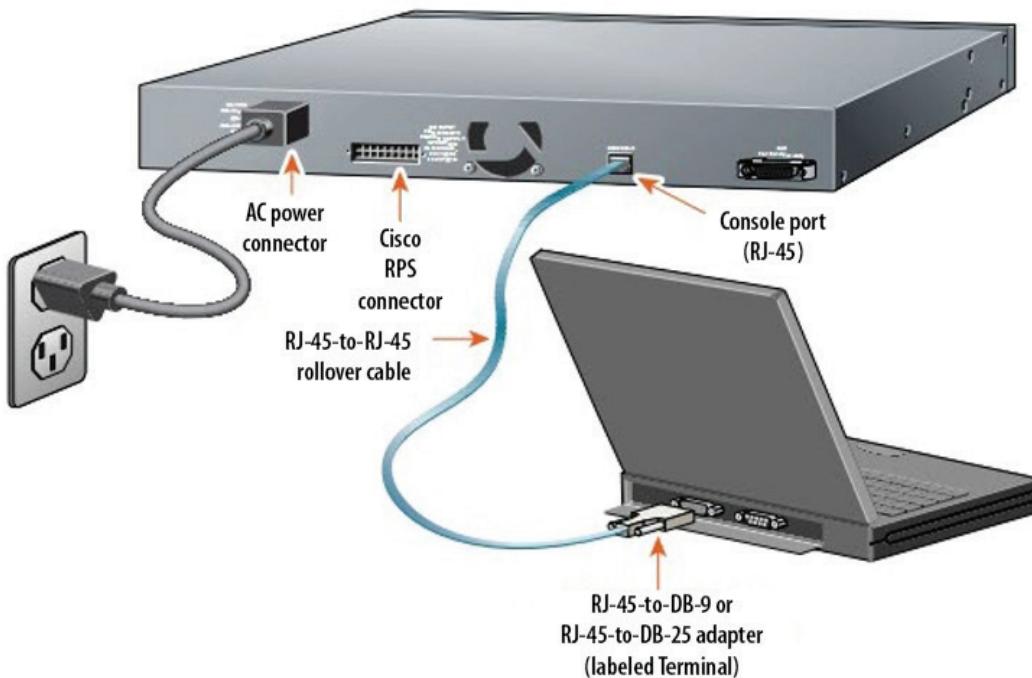


Figura 4 – Gerenciamento através de porta console

A porta de console é uma porta de gerenciamento utilizada para fornecimento de acesso fora de banda (*out-of-band* ou OOB) ao roteador, sendo utilizada, principalmente, na configuração inicial do roteador, no monitoramento do dispositivo e em procedimentos de recuperação de senhas e desastres (CISCO NETACAD, 2017).



Conectando um Cisco em porta console (em inglês). Acesse: <https://youtu.be/Z2-QHMQPqAU>

Um cabo de console, também conhecido como cabo *rollover* (ou cabo de configuração), e um adaptador RJ-45/DB-9 são utilizados para a conexão à porta de console a um computador.

Uma vez realizada a conexão física, o computador ou terminal de acesso precisa suportar a emulação de terminal VT100. Geralmente, são utilizados softwares de emulação de terminal, tais como o *Hyper Terminal* ou *Putty* (CISCO NETACAD, 2017).

Para conectar o computador a um roteador:

1. Conecte o conector RJ-45 do cabo *rollover* à porta de console do roteador;
2. Conecte a outra ponta do cabo *rollover* ao adaptador RJ-45/DB-9.  
Em alguns cabos de console, o adaptador DB-9 já vem adicionado, não necessitando de adaptadores;
3. Conecte o adaptador DB-9 fêmea a um computador, caso o cabo ainda não tenha esse adaptador acoplado;

4. Acesse o *software* de emulação de terminal do computador (*Putty*, *TeraTerminal* etc.), e configure:

- A porta COM correta;
- 9600 *baud*;
- 8 bits de Dados;
- Sem paridade;
- 1 bit de parada;
- Sem fluxo de controle.

## Conectando a Interface Local (LAN)

Na maioria dos ambientes de Rede de Área Local (LAN), o roteador é conectado à Rede local através de uma interface do tipo *Ethernet*, *Fast Ethernet* ou *Gigabit Ethernet*.

O roteador é um *host* que, geralmente, comunica-se com a rede LAN através de um *switch*. Para realizar essa conexão, utiliza-se um cabo direto (ou cabo reto) do tipo UTP (cabo de par trançado não blindado) de categoria 5 ou 6.

Caso deseje conectar um roteador a outro roteador através de um cabo UTP, seria necessária a utilização de um cabo cruzado (*crossover*) que, em uma ponta, tem um padrão de terminação T568A e no outro, um T568B; no caso do cabo reto, as duas pontas são T568A ou T568B (TANENBAUM, 2011).

Deve-se tomar muito cuidado, também, com possíveis erros de conexão em portas do tipo *Ethernet*, ISDN BRI, Console, AUX com CSU/DSU integrados e *Token Ring* (que não é mais muito utilizada), que utilizam o mesmo conector de oito pinos, como: RJ-45, RJ-48 ou RJ-49. Por exemplo, se conectar uma porta *Ethernet* em uma ISDN, pode ocorrer até mesmo danos físicos à conexão e ocorrer curto na respectiva porta.

A próxima Figura ilustra a conexão do roteador a uma Rede de área local:

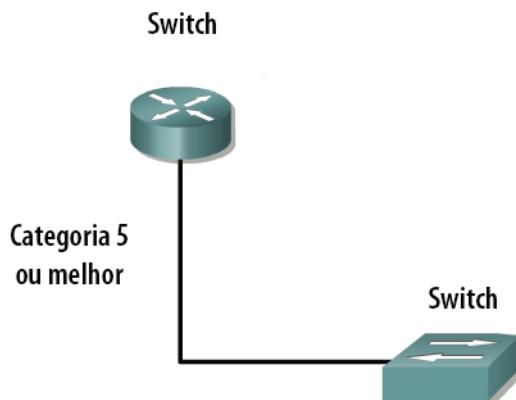


Figura 5 – Conectando uma LAN

# Conectando a Interface Remota (WAN)

As WANs estabelecem conexões de dados por meio de uma ampla área geográfica, utilizando muitos tipos de tecnologias diferentes. Esses serviços de WAN, geralmente, são alugados de provedores de serviços.

Dentre esses tipos de conexão de WAN estão: as linhas dedicadas, as linhas alugadas, as linhas comutadas por circuitos e as linhas comutadas por pacotes (TANENBAUM, 2011).

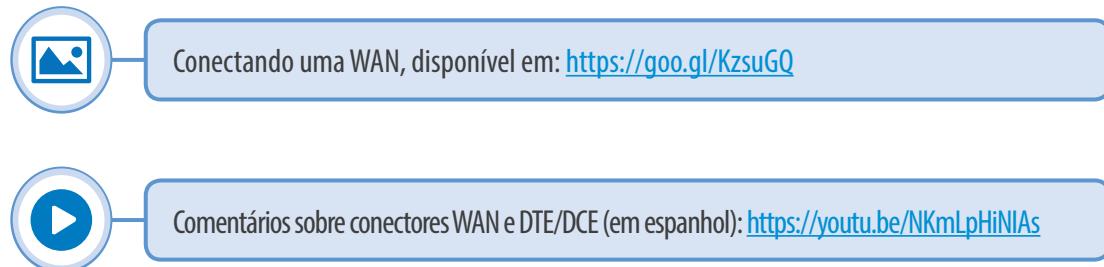
Para a utilização de serviços de WAN, o equipamento instalado no CPE (*Customer Premises Equipment*), que é geralmente um roteador, tem a função de DTE (*Data Terminal Equipment* – Equipamento Terminal de Dados).

Eles são conectados ao provedor de serviços utilizando um Dispositivo DCE (*Data Circuit –Terminating Equipment* – Equipamento de Terminação do Circuito de Dados) que, geralmente, é um *modem* ou um CSU/DSU (CISCO NETACAD, 2017).

Certamente, as interfaces do roteador mais utilizadas para a conectividade de serviços WAN são as interfaces seriais.

Para selecionar adequadamente o cabo serial, devemos observar as características de entrega de conexão realizada pelo provedor de serviços.

Na próxima Figura, observamos algumas interfaces seriais.



# Decisão de Encaminhamento de Pacotes

Um roteador tem como função conectar diversas Redes e, para isso, necessita de várias interfaces, que são identificadas com endereços IPs diferentes. Quando um roteador recebe um determinado pacote IP por uma interface serial, por exemplo, ele determina qual interface deve utilizar para encaminhar o pacote ao destino, corretamente.

A interface que o roteador utiliza para encaminhar o pacote de origem pode ser o destino final ou, então, pode ser uma Rede conectada a outro roteador, que será utilizada para alcançar essa determinada Rede destino (TANENBAUM, 2011).

É importante se lembrar de que para que um roteador possa rotear os pacotes IPs para suas Redes destino, é necessário que ele conecte Redes diferentes através de interfaces separadas e que identificam essas Redes, ou seja, as interfaces são utilizadas para conectar uma combinação de Redes Locais (LANs) e de Redes de Longa Distância (WANs).

Em grande maioria, as LANs são Redes baseadas no Protocolo do tipo *Ethernet* (que também é uma tecnologia de Rede) e que possui diversos dispositivos de Rede, como, por exemplo, *desktops*, *notebooks*, impressoras e servidores de Rede.

Já as Redes WANs são utilizadas para conectar Redes numa área geográfica ampla, como, por exemplo, uma conexão de interface WAN a um (ISP) ou Provedor de Serviços de *Internet*.

Podemos, certamente, afirmar que as principais funções de um roteador seriam:

- Determinar o melhor caminho/rota para enviar pacotes para uma Rede;
- Aprender e manter as várias rotas possíveis para seus destinos.

Para isso, o roteador utiliza a Tabela de roteamento, ou Tabela de rotas, para determinar a escolha do melhor caminho e com tal informação poder encaminhar um pacote para o meio correto.

Quando o roteador recebe um determinado pacote, ele examina o seu cabeçalho e identifica o endereço destino do pacote; após essa identificação, ele utiliza a Tabela de roteamento para identificar o melhor caminho para tal rede.

Na Tabela de roteamento, também é incluída a interface a ser usada para encaminhar pacotes para cada Rede conhecida. Quando uma correspondência de rota é devidamente encontrada, o roteador, então, encapsula o pacote IP no quadro/*frame* do *link* de dados de saída ou da interface de saída correto, o que faz o pacote ser corretamente encaminhado para o destino.

É possível que um roteador receba um tipo de encapsulamento de quadro de *link* de Dados e o encaminhe para outra interface que utilize outro tipo de encapsulamento. Por exemplo: um roteador pode receber um *frame* em uma interface local *Ethernet*, e depois deve encaminhá-lo para uma interface configurada com o Protocolo PPP ou Protocolo Ponto a Ponto.

Nesse caso o roteador deverá ter a capacidade de desencapsular o pacote IP num quadro e encapsular esse mesmo pacote em outro quadro (TANENBAUM, 2011).

Os roteadores podem ser configurados tanto para utilizar rotas estáticas (rotas manualmente configuradas pelo administrador de rede), como rotas dinâmicas (essas automáticas), para encontrar Redes destino remotamente descobertas e atualizar suas Tabelas de roteamento.

# Configurando Um Roteador Cisco

Todas as configurações e alterações em um roteador da Cisco são realizadas através da CLI ou interface de linha de comando e que são realizadas a partir do modo de configuração global (**config#**).

Existe a possibilidade de haver necessidade de entrar em outros modos e configurações mais específicos. Isso vai depender da alteração de configuração que for necessária; o importante é entender que todos esses modos específicos são subconjuntos do modo de configuração global (CISCO NETACAD, 2017).

Os comandos do modo de configuração global, como o nome propriamente indica, são utilizados num roteador para aplicar instruções de configuração que afetem o Sistema do Dispositivo como um todo.

O comando a seguir modifica o roteador para o modo de configuração global e permite que comandos possam ser inseridos a partir do terminal:

```
Router# configure terminal  
Router(config)#
```

Note que após o comando “conf t” ser realizado, o *prompt* indica que se está na configuração global. O modo de configuração global, muitas vezes chamado de config global, certamente, é o principal modo de configuração do equipamento em questão.

Podemos verificar apenas alguns modos em que se pode acessar a partir do modo de configuração global:

- Modo de Interface;
- Modo de Linha;
- Modo de Roteador;
- Modo de SubInterface;
- Modo de Controlador.

Quando entramos nesses modos mais específicos, o *prompt* do roteador se altera, indicando o modo de configuração atual para uma correta configuração.

Nesse caso, quaisquer alterações de configuração que forem realizadas aplicam-se somente aos processos ou às interfaces suportadas por esse modo específico (CISCO NETACAD, 2017).

Digitar o comando **exit** a partir de um desses modos de configuração mais específicos, geralmente, leva o roteador a retornar para um modo anterior do que está.

Pressionando as teclas **Ctrl-Z**, o roteador sai completamente dos modos de configuração anteriores e vai de volta para o modo execução privilegiado ou EXEC privilegiado.

- Modo EXEC Usuário
- Modo EXEC Privilegiado
- Modo de configuração global
- Modos de configuração específica

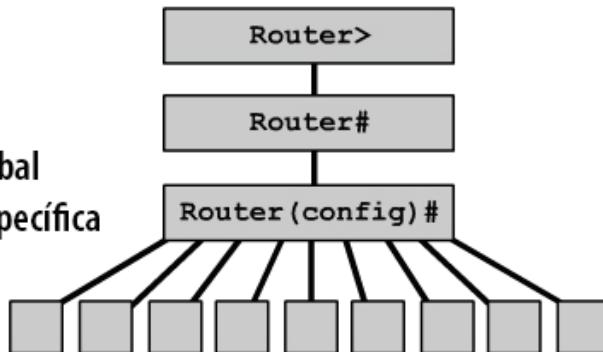


Figura 7 – Modos do Cisco IOS

## Configurando Nome no Roteador

---

Uma das primeiras tarefas de configuração básica, tanto num roteador, como num *switch*, certamente é a aplicação do nome desses Dispositivos, pois facilita o administrador a identificar em qual *device (host)* ele está operando.

Essa atividade é realizada, também, no modo de configuração global, com o seguinte comando:

```
Router(config)# hostname Unicsul
Unicsul(config)#
```

Note que, assim, o comando aplicado a *prompt* indica o nome do equipamento que acaba de receber sua identificação.

## Configurando Uma Senha

---

As senhas podem restringir o acesso aos roteadores e aos seus modos de configuração. Deve-se sempre configurar senhas para as linhas do Terminal Virtual (VTY) e para a linha do console (COM).

As senhas também são utilizadas para controlar o acesso ao modo EXEC privilegiado, fazendo com que apenas usuários devidamente autorizados possam realizar alterações no arquivo de configuração principal (*running-configuration*), que está armazenando em memória RAM (CISCO NETACAD, 2017).

Os comandos a seguir são utilizados para definir uma senha na linha do console:

```
Router(config)#line console 0
Router(config-line)#password <senha>
Router(config-line)#login
```

Podemos, também, definir uma senha em uma ou mais linhas de Terminal Virtual (VTY), para que os usuários possam ter acesso remoto ao roteador utilizando a aplicação *Telnet*.

Geralmente, os roteadores Cisco suportam várias linhas virtuais do tipo VTY. Em nosso exemplo, vamos definir cinco linhas VTY numeradas de 0 a 4. Frequentemente, utiliza-se a mesma senha para todas as linhas virtuais identificadas no comando.

São utilizados os seguintes comandos para definir a senha nas linhas virtuais do tipo VTY:

```
Router(config)# line vty 0 4  
Router(config-line)#password <senha>  
Router(config-line)#login
```

Uma vez aplicado esse conjunto de comando, é possível fazer uma conexão *Telnet*, mas é importante que seja aplicada uma senha no modo de configuração privilegiado.

A senha de ativação e o segredo de ativação são utilizados para restringir o acesso ao modo EXEC privilegiado, que, certamente, é o modo mais importante do roteador, pois dele se navega em quaisquer outros modos. A senha de ativação só é usada se o segredo de ativação não tiver sido definido.

Por esse motivo, é recomendável que o segredo de ativação esteja sempre ativado, para que possa ser sempre utilizado, já que é criptografado e a senha de ativação normalmente não é.

Vamos, então, conhecer os comandos utilizados para definir as senhas de ativação:

```
Router(config)# enable password <senha>  
Router(config)# enable secret <senha>
```

Lembre-se de que a senha de ativação secreta se sobrepõe à senha de ativação normal, pois essa última tem segurança fraca em função de ser uma senha em texto claro, isto é, caso você monitore o arquivo de configuração, você verá essa senha da forma como ela foi configurada, sem nenhum tipo de criptografia ou embaralhamento aplicado (CISCO NETACAD, 2017).

Mesmo aplicando uma senha de ativação normal, às vezes, não é desejável que essas senhas sejam apresentadas em texto claro na saída dos comandos **show running-config** ou **show startup-config**.

Para isso, foi criado um recurso de embaralhamento dessas senhas, por meio dos comandos:

```
Router(config)# servicepassword-encryption
```

É importante indicar que o comando **servicepassword-encryption** aplica um tipo de criptografia fraca em todas as senhas não criptografadas (texto claro).

Já o comando **enablesecret<senha>** utiliza um algoritmo de criptografia do tipo MD5; esse mais forte do que o anterior (CISCO NETACAD, 2017).

# Examinando o Roteador

Há muitos comandos de verificação, os conhecidos comando **show**, que podem ser usados para examinar o conteúdo de arquivos do roteador e para a realização na solução de problemas de rede.

Tanto no modo EXEC privilegiado quanto no modo EXEC usuário, o comando **show?** fornece uma lista dos comandos **show** disponíveis.

Por características de privilégio, certamente, a lista de opção do comando **show** é consideravelmente maior no modo EXEC privilegiado do que no modo EXEC usuário.

Vamos, então, conhecer alguns comandos **show** interessantes para uma boa observação do funcionamento dos dispositivos de Rede da Cisco, como, por exemplo, um roteador:

- **Show interfaces**: exibe todas as estatísticas de todas as interfaces do roteador que está sendo monitorado;
- **Show interface serial 0/0**: é o mesmo comando anterior; porém, agora, estamos observando uma interface em específico;
- **Show controllers <serial>**: exibe informações específicas da interface de *hardware* e características importantes como, por exemplo, se o cabo tem a função de DTE ou DCE numa conexão de Rede;
- **Show startup-config**: exibe o conteúdo do arquivo de configuração (também conhecido como arquivo de *backup* ou *startup-configuration*), que é devidamente armazenado em NVRAM e também exibe o arquivo de configuração apontado pela variável de ambiente *CONFIG\_FILE*;
- **Show running-config**: exibe o conteúdo do arquivo de configuração em execução naquele momento (executando na memória de trabalho, ou memória RAM);
- **Show flash**: exibe informações sobre a memória *flash* e os arquivos do IOS estão armazenados nela. Geralmente, na memória *flash*, é onde reside a imagem do Sistema Operacional da Cisco (IOS);
- **Show version**: exibe informações sobre a versão do *software* carregado no momento, além de informações de *hardware* e Dispositivo. Também apresenta a configuração de registro aplicada; por exemplo, 0x2102, 0x2142 e em diante;
- **Show ARP**: exibe a Tabela ARP que o roteador apreendeu dos equipamentos que estão conectados em sua Rede local;
- **Show protocol**: exibe o *status* global e o *status* específico da interface de quaisquer Protocolos de camada 3 configurados. É um comando muito usado para sabermos quais Protocolos o roteador tem habilitados;

- **Show clock:** mostra o horário definido no roteador;
- **Show hosts:** mostra uma lista em cache dos nomes e dos endereços dos *hosts* que foram configurados;
- **Show users:** exibe todos os usuários que estão conectados ao roteador naquele momento;
- **Show history:** exibe um histórico dos comandos que foram inseridos anteriormente. É um comando muito útil para uma rápida configuração, pois com teclas em seta, podemos repetir um determinado comando dado.

## Configurando Interface Serial

Uma interface serial pode ser configurada a partir da porta console ou através de uma Linha de Terminal Virtual (VTY) acessada por *Telnet*, por exemplo.

Para configurar uma interface serial, siga as seguintes etapas:

1. Entre no modo de configuração global;
2. Entre no modo de interface;
3. Especifique o endereço da interface e a máscara de sub-rede;
4. Se houver um cabo DCE conectado, defina a taxa do *clock*. Se o cabo for DTE, pode pular essa etapa;
5. Ligue a interface, ou seja, tire-a de *shutdown*;

Cada interface serial conectada precisa ter um endereço IP e uma máscara de sub-rede se for esperado que a interface roteie pacotes IP.

Configure, então, um endereço IP utilizando os seguintes comandos:

```
Router(config)# interface serial 0/0
Router(config-if)#ipaddress<endereço IP><máscara de rede>
```

A máscara de Rede no comando indicado é aplicada no formato também decimal pontuado, como é o caso da formatação do endereço IP, ou seja, 255.255.255.0, por exemplo.

Em algumas versões de Sistemas Operacionais da Cisco se aceita a formatação binária de representação de uma máscara de Rede, como, por exemplo, um /24 (CISCO NETACAD, 2017).

As interfaces seriais necessitam de um sinal de *clock* para controlar a temporização das Comunicações. Na maioria dos ambientes, um dispositivo DCE (por exemplo, um *modem* ou um CSU/DSU) fornece o *clock* automaticamente.

Por padrão, os roteadores Cisco são dispositivos DTE, ou seja, são dispositivos de terminal, mas, em configurações ponto a ponto, podem ser configurados como dispositivos DCE.

Nesse caso, a própria interface DCE gera o sincronismo e **clock**. Para identificarmos os *clocks* suportados por uma interface do comando **clock?** e conseguiram verificar uma dezena de *clocks* disponíveis (CISCO NETACAD, 2017).

Por **default** (padrão), as interfaces seriais, por exemplo, ficam desligadas ou desativadas. Para ligar ou ativar uma interface de Rede, utilize o comando **no shutdown**.

Se uma interface precisar ser desativada administrativamente para manutenção ou solução de problemas, use o comando **shutdown** para desligá-la.

Note que o indicador **no** nega o comando realizado, ou seja, quando você aplica um **no shutdown** em uma interface, você a está liberando.

Vamos, então, verificar um exemplo com o comando:

```
Router(config)# interface serial 0/0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

## Alterando Configurações

Um dos comandos mais utilizados para que possamos observar o estado de configuração realizado no roteador, sem dúvida alguma, é o comando **show running-config**, que exibe a configuração atual rodando em memória RAM.

Caso se deseje eliminar ou desativar um comando aplicado, usa-se o qualificador “no” na frente do comando, como, por exemplo, o **no shutdown** ou o **no ip address** (CISCO NETACAD, 2017).

Caso deseje copiar o arquivo de configuração que está rodando em memória de trabalho (memória RAM) e protegê-lo num eventual *boot*, podemos fazer a cópia desse arquivo na memória **NVRAM** com o seguinte comando:

```
Router# copy running-config startup-config
```

Caso deseje apagar o arquivo de configuração criado em NVRAM, você pode usar o seguinte comando:

```
Router# erase startup-config
```

# Material Complementar

## Indicações para saber mais sobre os assuntos abordados nesta Unidade:



Sites

### CISCO NETACAD

**Módulo de Roteamento e Switching** – Conceitos Essenciais. Capítulo 4 – Sessão 4.0: Conceitos de Roteamento, Versão 6.0

<https://goo.gl/lNdwR>

### CISCO NETACAD

**Módulo de Roteamento e Switching** – Conceitos Essenciais. Capítulo 4 – Sessão 4.1: configuração inicial do Roteador, Versão 6.0

<https://goo.gl/lNdwR>

### CISCO NETACAD

**Módulo de Roteamento e Switching** – Conceitos Essenciais. Capítulo 4 – Sessão 4.2: decisões de Roteamento, Versão 6.0. EUA

<https://goo.gl/lNdwR>



Livros

### Redes de Computadores e a Internet

STALLINGS, W. e ROSS K. **Redes de Computadores e a Internet**. 5<sup>a</sup> Ed. São Paulo: Editora Pearson, 2010.

### Redes de Computadores

TANENBAUM, A. S; WETHERALL, D. **Redes de Computadores**. 5<sup>a</sup> Ed. Rio de Janeiro: Editora Campus, 2011.

# Referências

CISCO NETACAD. **Módulo de Roteamento e Switching: Conceitos Essenciais (CCNA2)**. 6<sup>a</sup> versão, Cisco Systems, 2017 (Material *on-line*). Disponível em [www.netacad.com](http://www.netacad.com).

STALLINGS, W. e ROSS K. **Redes de Computadores e a Internet**. 5<sup>a</sup> Ed. São Paulo: Editora Pearson, 2010.

TANENBAUM, A. S; WETHERALL, D. **Redes de Computadores**. 5<sup>a</sup> Ed. Rio de Janeiro: Editora Campus, 2011.



**Cruzeiro do Sul**  
Educacional

# Tecnologias de Roteamento



Cruzeiro do Sul Virtual  
Educação a distância



# Material Teórico



**Roteamento Estático X Roteamento Dinâmico**

**Responsável pelo Conteúdo:**

Prof. Esp. Antonio Eduardo Marques da Silva

**Revisão Textual:**

Prof.<sup>a</sup> Dr.<sup>a</sup> Selma Aparecida Cesarin



# UNIDADE

## Roteamento Estático X Roteamento Dinâmico



- Roteamento;
- Rota Padrão/Rota *Default*;
- Protocolos de Roteamento Dinâmico;
- Protocolos de Roteamento Dinâmico;
- Sistemas Autônomos e Protocolos IGP e EGP.



### OBJETIVO DE APRENDIZADO

- Compreender e abordar como é o funcionamento do Processo de Roteamento de Pacotes, apresentar as características e as diferenças entre Roteamento Estático e Roteamento Dinâmico, identificar o uso de rotas padrão/*default* e conhecer as principais características de Protocolos de Roteamento Dinâmico do tipo vetor distância e estado de *link*.



# Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:



## Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu “momento do estudo”;
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

# Contextualização

Para que os equipamentos intermediários de Rede possam funcionar corretamente e realizar suas atividades com segurança, é necessário que nós, administradores de Redes, tenhamos o conhecimento necessário para a configuração deles.

Para isso, vamos conhecer aqui alguns comandos utilizados na configuração de alguns recursos, como, por exemplo, definição de rotas estáticas e aplicação do Processo de Roteamento Dinâmico e outras definições importantes para conhecer melhor esses temas tratados nesta Unidade.

# Roteamento

O Processo de Roteamento é realizado por roteador, com o intuito de encaminhar pacotes para uma Rede de destino.

Esse roteador toma decisões de encaminhamento com base no endereço IP de destino de um determinado pacote. Todos os Dispositivos e Rede ao longo de um caminho utilizam o endereço IP de destino para orientar o pacote na direção correta e sem erros, até o seu destino.

Para que os roteadores possam tomar as decisões corretas, eles precisam aprender, através de um algoritmo de Roteamento e/ou através da configuração de um administrador de Rede, como podem alcançar essas Redes remotamente.

Caso estejam utilizando um Processo de Roteamento Dinâmico, essa informação é obtida de outros roteadores da topologia. No entanto, se estiverem utilizando o Roteamento Estático, essas informações sobre as Redes remotas são configuradas manualmente, por um administrador de Rede.

Nesse caso, qualquer alteração na topologia da Rede requer que esse operador adicione e exclua rotas estáticas manualmente a fim de refletir essas alterações, ou seja, uma eventual mudança da Rede também precisa ser configurada manualmente o que às vezes pode acarretar um retrabalho e um Processo de configuração cansativo.

Em uma Rede grande, essa manutenção das Tabelas de Roteamento pode exigir grande quantidade de tempo na administração da Rede. Já em Redes pequenas e com poucas alterações, as rotas estáticas acabam exigindo pouquíssima manutenção e por esse motivo é uma técnica mais utilizada, pois não usa tantos recursos de CPU e de consumo de banda nos roteadores (TANENBAUM, 2011).



Introdução a Roteamento de pacotes. Acesse: <https://youtu.be/y9Vx5I-th9Y>

Outra característica é que, no Roteamento Estático, a escalabilidade é praticamente nula se comparada ao Processo de Roteamento Dinâmico; porém, mesmo em Redes grandes e complexas, as rotas estáticas podem ter objetivos de atender a uma finalidade específica e, por esse motivo, são geralmente configuradas em conjunto com um Protocolo de Roteamento Dinâmico (TANENBAUM, 2011).

## Roteamento Estático

Como já verificamos, as rotas estáticas são configuradas manualmente pelo administrador da Rede, as mudanças também são manuais, consomem pouca ou nenhuma CPU e praticamente não consome largura de banda em vão, pois não necessita fazer *updates* (atualizações) de Roteamento.

Operações com rotas estáticas podem ser divididas em três partes:

- O administrador da Rede configura a rota manualmente;
- O roteador aplica a rota configurada na Tabela de Roteamento;
- Os pacotes são roteados usando a rota estática; caso ela tenha a menor métrica ou a menor distância administrativa que, geralmente, é o caso.

Como uma rota estática é configurada manualmente, o administrador de Rede deve configurá-la no roteador usando o comando IOS **ip route**, como veremos no exemplo de configuração a seguir (*CISCO NETACAD*, 2017).

Na próxima figura, o administrador de Rede responsável pelo roteador *Hoboken* precisa configurar rotas estáticas apontando para as Redes 172.16.1.0/24 e 172.16.5.0/24 nos outros roteadores vizinhos.

Para isso, ele precisa configurar as rotas estáticas com os seguintes comandos:

```
Hoboken(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.1  
Hoboken(config)# ip route 172.16.5.0 255.255.255.0 172.16.4.1
```

Nesse caso, estamos utilizando para alcançar as rotas destino o endereço IP do próximo salto (*next-hop*) para o roteador *Hoboken* ou, também, podemos usar os comandos a seguir:

```
Hoboken(config)# iproute 172.16.1.0 255.255.255.0 Serial 1  
Hoboken(config)# ip route 172.16.5.0 255.255.255.0 Serial 0
```

Já nesse exemplo, estamos utilizando as interfaces de saída do roteador *Hoboken* em relação às Redes destino.

Qualquer um dos comandos configurados instalará uma rota estática na Tabela de Roteamento de *Hoboken*. A única diferença entre os dois comandos está na identificação da distância administrativa atribuída à rota pelo roteador quando ela é colocada na Tabela de Roteamento.

A Distância Administrativa (DA) é um parâmetro opcional, que fornece uma medida de confiabilidade da rota aplicada. Quanto menor for o valor da distância administrativa, mais confiável a rota definida. Nesse caso, uma rota com distância administrativa menor será instalada antes de uma rota idêntica para o mesmo destino, usando uma distância administrativa maior. A distância administrativa padrão para as rotas estáticas é o valor um (1).

Já quando uma interface de saída é configurada como o *gateway* de uma rota estática, essa rota será apresentada na Tabela de Roteamento como sendo uma rota diretamente conectada e nesse caso terá o valor de distância administrativa igual a zero (0).

E, como podemos verificar, uma rota diretamente conectada tem distância administrativa menor do que qualquer rota possivelmente aplicada (rotas estáticas e/ou rotas aprendidas dinamicamente por um Processo de Roteamento) (CISCO NETACAD, 2017).

Para que possamos verificar a distância administrativa de uma rota em particular (tanto estática quanto aprendida dinamicamente), utilize o comando **show ip route <address>**, em que o endereço IP da rota em questão é inserido para a opção de endereço; caso ele não seja aplicado, veremos todas as melhores rotas aprendidas pelo roteador.

Se for desejável a configuração de uma distância administrativa diferente do padrão, o administrador pode-se inserir um valor entre 0 e 255 após a especificação do próximo salto (*next-hop*) ou da interface de saída em relação à Rede destino, da seguinte maneira:

```
Hoboken(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.1 130
```

Nesse exemplo, aplicamos para essa rota estática a distância administrativa como valor 130, pois o administrador desejou influenciar nos valores padrões e DA.

Em alguns casos, as rotas estáticas podem ser utilizadas para fins de *backup* de rotas. Nesse, uma rota estática pode ser configurada num roteador para ser usada somente quando a rota obtida dinamicamente falhar. Para que possamos utilizar uma rota estática com essa finalidade, basta definir sua distância administrativa com valor mais alto (maior) do que a distância administrativa do Protocolo de Roteamento Dinâmico, utilizado naquela topologia (CISCO NETACAD, 2017).



*Introduction to Static Routing* (Inglês). Acesse: <https://youtu.be/Sa5Xu09H29M>

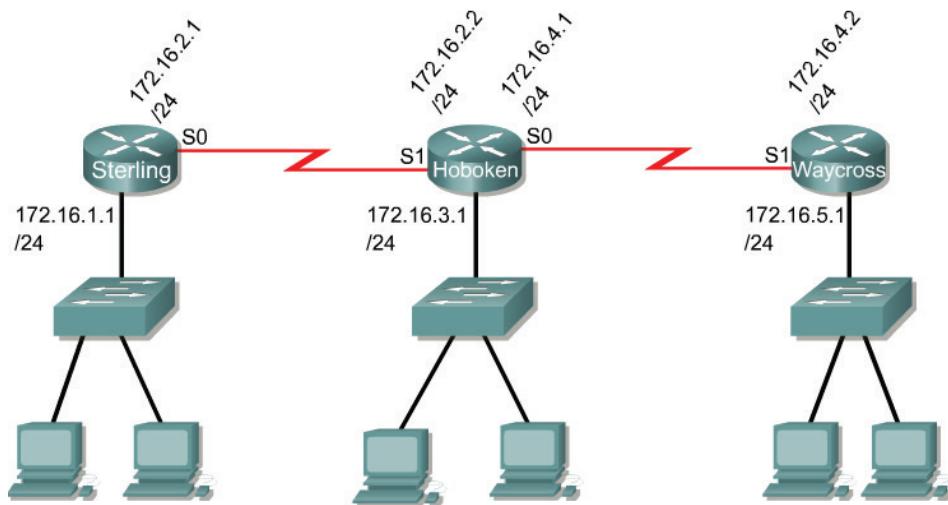


Figura 1 – Roteamento Estático

### Configurando Rotas Estáticas

Vamos, então, verificar a lista as etapas referentes à configuração de rotas estáticas e/ou dinâmicas de forma simples, fornecendo exemplo de configuração bem prático.

Siga as seguintes etapas, a seguir para configurar rotas estáticas:

1. Determine todos os prefixos, máscaras e endereços desejados e que serão configurados nas rotas estáticas. O endereço pode ser tanto uma interface local quanto um endereço do próximo salto (*next-hop*), que pode levar ao destino desejado;
2. Entre no modo de configuração global no equipamento;
3. Digite o comando *ip route* indicando um endereço de Rede destino e uma máscara de sub-Rede destino e o caminho a ser seguido para encontrar a Rede destino. Esse caminho pode ser a interface de saída ou o endereço IP de próximo salto. A inclusão de uma distância administrativa é opcional, como, por exemplo, se você desejar aplicar duas rotas estáticas e indicar uma preferência e outro *backup*;
4. Repita a etapa 3 para todas as Redes de destino definidas conforme a etapa 1;
5. Saia do modo de configuração global;
6. Salve a configuração ativa que está na RAM para a NVRAM, utilizando o comando ***copy running-config startup-config*** ou apenas ***wr***.

A Rede do próximo exemplo é uma configuração bem simples com três roteadores aplicados. O *Hoboken* precisa ser configurado para que possa alcançar a Rede destino 172.16.1.0 e a Rede 172.16.5.0.

Essas duas Redes têm como máscara de sub-Rede o valor de 255.255.255.0. Os pacotes que têm como Rede de destino 172.16.1.0 precisam ser roteados para o roteador *Sterling* e os pacotes que têm como endereço de destino 172.16.5.0 precisam ser roteados para o roteador *Waycross* (CISCO NETACAD, 2017).

As duas rotas estáticas serão configuradas, inicialmente, para usar uma interface local como *gateway* para as Redes de destino. Como a distância administrativa não foi especificada, o padrão de rotas estáticas será “1” quando a rota for instalada na Tabela de Roteamento.

Observe que uma distância administrativa de uma rota diretamente conectada tem valor “0”, ou seja, esse tipo de rota se sobrepõe a todas as outras técnicas de Roteamento utilizadas. Essas mesmas duas rotas estáticas também podem ser configuradas utilizando um endereço do próximo salto como *gateway*.

A primeira rota configurada, para a Rede 172.16.1.0, tem um *gateway* 172.16.2.1. A segunda rota configurada, para a Rede 172.16.5.0, tem um *gateway* 172.16.4.2. Como a distância administrativa não foi especificada, então, o padrão aplicado pelo roteador será 1 (CISCO NETACAD, 2017).

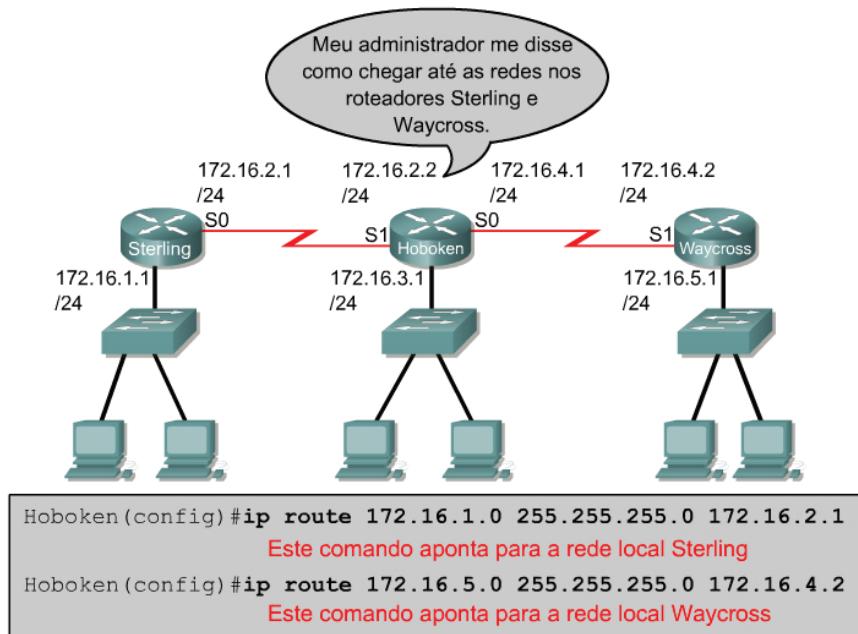


Figura 2 – Configurando Roteamento Estático

## Rota Padrão/Rota Default

As rotas padrão ou rotas default são utilizadas para rotear pacotes com destinos que não correspondem a nenhuma das entradas de rotas na Tabela de Roteamento, aprendidas por rotas estaticamente configuradas ou por meio de algoritmos de Roteamento Dinâmicos.

É comum configurarmos uma rota padrão nos roteadores, para dirigir o tráfego para à Internet, já que é impraticável, trabalhoso e/ou desnecessário manter rotas específicas para todas as Redes na Internet.

Uma rota padrão, na verdade, é uma rota estática especial, que utiliza o seguinte formato de comando:

```
Unicsul(config)#ip route 0.0.0.0 0.0.0.0 (endereço-de-próximo-salto|interface-de-saída)
```

Note que o comando de configuração **ip route** é o mesmo utilizado para a configuração de uma rota estática; porém, os primeiros quatro octetos 0.0.0.0 indicam a Rede destino e os outros próximos quatro octetos 0.0.0.0 definem a máscara dessa Rede.

Se calcularmos esses dois valores com a operação lógica AND, o resultante será sempre a Rede 0.0.0.0 que indica a Internet, ou seja, para que se chegue à Rede 0.0.0.0 (Internet) saia para uma interface de saída e/ou um endereço IP de próximo salto, endereço esse que, geralmente, está aplicado no provedor de serviços que oferta essa conexão para sua Empresa (CISCO NETACAD, 2017).

Depois, devemos seguir as etapas para configuração de rotas padrão:

1. Entre no modo de configuração global;
2. Digite o comando *ip route* com 0.0.0.0 para o prefixo de Rede e 0.0.0.0 para a máscara de Rede. A opção endereço para a rota *default* pode ser tanto a interface do roteador local que se conecta às Redes externas quanto o endereço IP do roteador do próximo salto que, geralmente, está posicionado no provedor de acesso. Na maioria dos casos, é preferível especificar o endereço IP do roteador do próximo salto, pois garantem uma confiabilidade maior que as interfaces de saída que podem ser alteradas localmente com frequência;
3. Saia do modo de configuração global;
4. Salve a configuração ativa na RAM na memória NVRAM, utilizando o comando **copy running-config startup-config**.

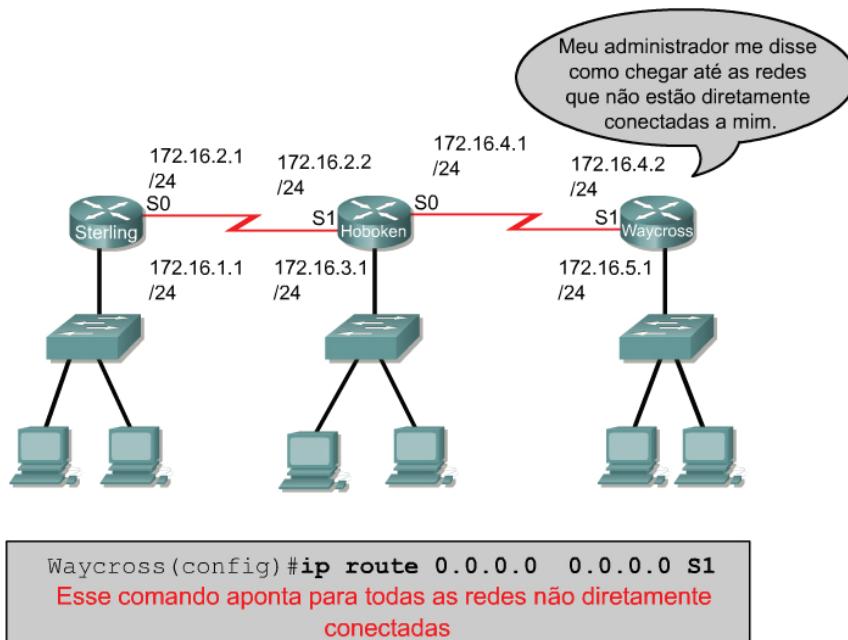


Figura 3 – Rota Padrão/Default

## Verificando Rotas Estáticas e Rotas Padrão

Uma vez configuradas as rotas estáticas como rotas padrão, é importante verificar-las no roteador para identificar suas entradas na Tabela de Roteamento e, por consequência, checar se elas estão funcionando corretamente.

O comando do IOS da Cisco ***show running-config*** é utilizado para a visualização da configuração ativa na memória RAM (memória de trabalho), bem como a verificação se a rota estática ou default foram adicionadas corretamente (CISCO NETACAD, 2017).

Outro comando muito utilizado é o ***show ip route*** que tem como objetivo verificar a Tabela de Roteamento que inclui as melhores rotas escolhidas de um Protocolo de Roteamento Dinâmico e/ou de rotas estáticas/padrão, configuradas manualmente.

Verifique as seguintes etapas para verificação da configuração das rotas estáticas ou padrão:

- No modo privilegiado do IOS, digite o comando ***show running-config*** para visualização da configuração ativa em RAM;
- Verifique se a rota estática e as rotas padrão foram inseridas corretamente na configuração ativa. Caso a rota tenha sido configurada erradamente, será necessário o administrador voltar ao modo de configuração global e remover a rota estática ou rota padrão incorreta e inseri-la novamente;
- Digite o comando ***show ip route*** para a verificação da Tabela de Roteamento e identifique as rotas padrão ou estáticas configuradas manualmente.

# Protocolos de Roteamento Dinâmico

Como foi dito no início deste módulo, temos duas formas de aplicar as rotas em uma Tabela de Roteamento, por meio da configuração estática (manual) ou por meio de um Processo de Roteamento Dinâmico (automático).

Esses Protocolos de Roteamento são diferentes dos Protocolos roteados/roteáveis, tanto em termos de tarefa quanto de função (TANENBAUM, 2011).

Um Protocolo de Roteamento é encarregado da comunicação entre os roteadores da Rede e possuem o objetivo de manter de forma automática as entradas da Tabela de Roteamento.

Esse Protocolo de Roteamento permite que um roteador possa compartilhar informações com outros roteadores da sua topologia.

Essas informações de Roteamento (ou atualizações de Roteamento) são trocadas entre esses roteadores da Rede, a fim de manter sincronismo e manter as Tabelas de Roteamento íntegras e atuais, identificando sempre as melhores rotas para um determinado destino (STALLINGS; ROSS, 2010).

Alguns exemplos de Protocolos de Roteamento Dinâmico são:

- RIPv1 e RIPv2 (*Routing Information Protocol*);
- OSPF (*Open Shortest Path First*);
- IS-IS (*Intermediate System to Intermediate System*);
- IGRP (*Interior Gateway Routing Protocol*);
- EIGRP (*Enhanced Interior Gateway Routing Protocol*).

Já um Protocolo roteado/roteável é utilizado para direcionar o tráfego dos Dados dos usuários em uma Rede, ou seja, ele fornece informações suficientes no endereço de sua camada de Rede para permitir que um determinado pacote seja encaminhado e entregue de um *host* origem para outro *host* destino.

Exemplos de Protocolos roteados/roteáveis:

- IPv4 (*Internet Protocol v4*);
- IPv6 (*Internet Protocol v6*);
- IPX (*Internetwork Packet Exchange*);
- AppleTalk e outros.

# Sistemas Autônomos (AS)

Um Sistema Autônomo (AS) nada mais é do que uma coleção de Redes sob uma administração comum, e que compartilha estratégias próprias de Roteamento.

Para o mundo exterior, um AS é visto como uma única entidade de Rede e pode ser controlado por um ou mais operadores, apresentando uma visão consistente de Roteamento para o mundo exterior. A maioria dos provedores de acesso para operarem na grande Rede (Internet) necessitam de um AS.

E as trocas de informações de Roteamento são realizadas por um Protocolo de Roteamento específico, com tal finalidade, de interligação de AS externamente (CISCO NETACAD, 2017).

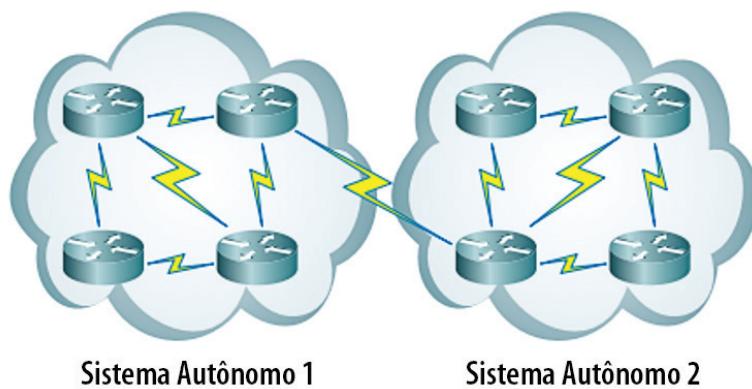


Figura 4 – Sistemas Autônomos

O ARIN (*American Registry of Internet Numbers*) ou o Órgão de Administração da Internet local do país, como é o caso do CGIbr – Comitê Gestor da Internet Brasil (no Brasil), tem como finalidade atribuir um AS (número de identificação de cada AS) aos provedores de serviços da sua região.

Esse número de identificação de AS tem o tamanho de 16 bits. Alguns Protocolos de Roteamento Dinâmico como, por exemplo, o IGRP e o EIGRP da Cisco, requerem a atribuição desse número de Sistema Autônomo único de forma mandatória em sua configuração (CISCO NETACAD, 2017).

Como já comentamos, os objetivos de um Protocolo de Roteamento é construir, manter e atualizar a Tabela de Roteamento para que as rotas destino sejam alcançadas da melhor forma possível.

Na Tabela de Rotas ou Tabela de Roteamento, estão armazenadas as melhores Redes conhecidas e as portas/interfaces associadas a essas Redes de destino.

Os roteadores utilizam Protocolos de Roteamento para gerenciar e manter as informações (atualizações) recebidas de outros roteadores, que são obtidas da configuração manual de rotas estáticas ou automáticas, caso seja utilizado um Protocolo de Roteamento Dinâmico.

É importante lembrar que a finalidade principal do Protocolo de Roteamento é identificar as rotas possíveis para os destinos de Rede e escolher, entre essas várias rotas identificadas, as melhores. Além disso, o roteador pode atualizar ou remover as rotas que não são mais válidas.

Uma vez que as melhores rotas estejam implementadas na Tabela de Roteamento, o roteador envia ao destino os Protocolos roteadores, como o IP, por exemplo, que carrega os Dados de uma aplicação de Rede (STALLINGS; ROSS, 2010).

O algoritmo de Roteamento é fundamental para o Roteamento Dinâmico, pois, sempre que houver alteração na topologia de Rede devido à sua expansão, reconfiguração de rotas ou falha na Rede, essa base de conhecimento também deve ser atualizada, que reflete visão precisa e consistente da topologia da Rede.

Quando todos os roteadores de uma determinada Rede interconectada (*internetwork*) estiverem operando com as mesmas informações sobre uma determinada topologia da Rede, diz-se que esse grupo de Redes interconectadas convergiu, ou seja, possui o mesmo conhecimento para as Redes destino da respectiva topologia.

Certamente, é desejável uma convergência rápida de Rede, pois isso reduz o período de tempo ao qual os roteadores poderiam continuar a tomar decisões de Roteamento incorretas (TANENBAUM, 2011).

Os Sistemas Autônomos (AS) propiciam a divisão do grupo de Redes interconectadas (*internetwork*) globalmente em Redes menores e mais fáceis de administrar e gerenciar.

Cada AS tem seu próprio conjunto de regras, padrões, diretrizes e um número de identificação do AS que o distingue de maneira exclusiva dos outros ASs no resto do globo terrestre

## Classes de Protocolo de Roteamento

Os Protocolos de Roteamento Dinâmico fazem parte de pelo três classes, se forem considerados Protocolos Interiores (IGPs), ou seja, Protocolos de atuam dentro de um Sistema Autônomo (AS).

A maioria dos algoritmos de Roteamento podem, então, ser classificados numa destas três categorias:

- Vetor de distância (*distance vector*);
- Estado do enlace (*link state*);

- Híbrido (proprietário da Cisco).

A abordagem de Roteamento pelo vetor da distância determina uma direção (vetor) e uma distância para qualquer link dentro de um grupo de Redes interconectadas (*internetwork*).

Já a abordagem dada ao estado dos links (*link state*), também chamada de *shortest path first* (caminho mais curto primeiro, em português), recria uma topologia exata de todo o grupo de Redes interconectadas (*internetwork*) dentro de um Sistema Autônomo.

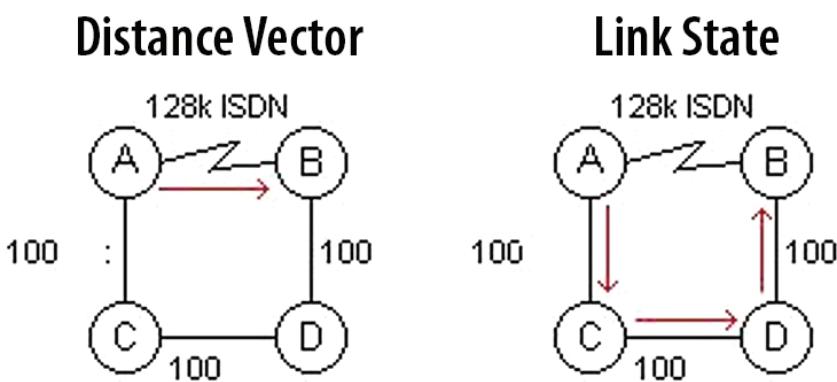


Figura 5 – Classes de Protocolo de Roteamento

### Protocolos de Vetor Distância

Os algoritmos de Roteamento por vetor da distância ou, do inglês, distance vector, passam cópias periódicas de uma Tabela de Roteamento (Tabela completa) de um roteador para o seu vizinho diretamente conectado através de atualizações (*updates*) periódicas.

Os algoritmos de Roteamento Dinâmico baseados no vetor da distância também são conhecidos como algoritmos de *Bellman-Ford*.

Como exemplo, um roteador B recebe atualizações de um roteador A vizinho. O roteador B adiciona um número ao vetor da distância (como uma quantidade de saltos, por exemplo), que aumenta o vetor da distância.

Logo em seguida, o roteador B passa essa nova Tabela de Roteamento acrescida ao seu outro vizinho, o roteador C, que executa esse mesmo Processo ao seu vizinho, ou seja, é um Processo que ocorre em todas as direções entre os roteadores vizinhos dentro de uma *internetworking*, até que todos os dispositivos possam convergir com a Rede. Esse Protocolo também é conhecido como Protocolo por rumor ou Protocolo fofoqueiro (CISCO NETACAD, 2017).

Esse algoritmo acumula distâncias de Rede para poder manter um Banco de Dados de Informações sobre toda a topologia da Rede em cada roteador; porém, os algoritmos de vetor da distância não acabam permitindo que um roteador co-

nheça a topologia exata de um grupo de Redes interconectadas (*internetwork*), já que cada roteador somente identifica os roteadores que são seus vizinhos (TANENBAUM, 2011).



Introdução ao Roteamento de pacotes IP. Acesse: <https://youtu.be/y9Vx5l-th9Y>

No início do Processo de divulgação e atualização de rotas, cada roteador que utiliza Roteamento de vetor da distância começa identificando seus próprios vizinhos. A interface que conduz a cada Rede diretamente conectada é apresentada como tendo distância 0 (que é a menor distância possível dentro do algoritmo).

Conforme o Processo de descoberta do vetor de distância avança, os roteadores descobrem os melhores caminhos para as Redes de destino, com base nas informações que receberam de cada vizinho da Rede (CISCO NETACAD, 2017).

Em função disso, quando a topologia de Rede muda, a Tabela de Roteamento também muda e é atualizada com as novas informações aprendidas.

Dessa forma, as atualizações das alterações da topologia de Rede avançam de um roteador para o outro, pois os algoritmos de vetor de distância pedem que cada roteador envie toda a sua Tabela de Roteamento (Tabela completa) para cada um de seus vizinhos adjacentes.

As Tabelas de Roteamento contêm informações sobre o custo total do determinado caminho a ser seguido, conforme definido pela sua métrica calculada.

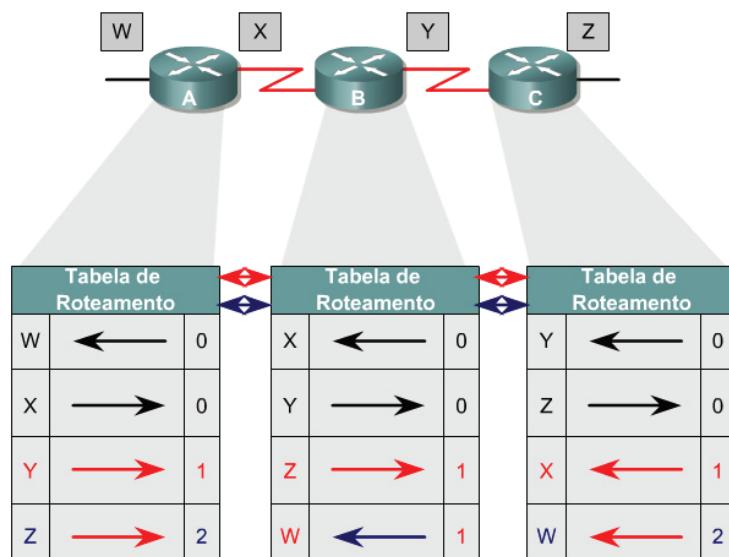


Figura 6 – Troca de Rotas com Vetor Distância

## Protocolo de Estado de *Link*

O outro algoritmo básico utilizado para Roteamento é o *Link state* (Estado de *Link*). Esses algoritmos também são conhecidos como algoritmos SPF (*Shortest Path First* – o caminho mais curto primeiro) ou *Dijkstra*, que é um nome de um matemático famoso que desenvolveu tal algoritmo.

Os algoritmos de Roteamento de estado de *link* mantêm um RDB ou Banco de Dados complexo com as informações da topologia de Rede.

Como já verificamos, o algoritmo de vetor distância tem informações não específicas sobre as Redes de destino distantes, mas no algoritmo de estado de *link* se tem conhecimento completo sobre os roteadores distantes e de toda a Rede.

O Roteamento de *Link State* utiliza:

- **Anúncios do Estado dos Links (LSAs – *Link-State Advertisements*)**: são anúncios dos estados dos *links* (LSA), que nada mais são do que um pequeno pacote de informações de Roteamento que são enviados entre os roteadores;
- **Banco de Dados Topológico** – É um Banco de Dados da topologia de Rede, que é uma coleção de informações reunidas aprendidas pelos LSAs;
- **Algoritmo SPF** – O algoritmo SPF (o caminho mais curto primeiro) é uma estrutura matemática realizada no Banco de Dados e que resulta na árvore SPF de topologia completa;
- **Tabelas de Roteamento** – Uma lista das interfaces e dos melhores caminhos conhecidos por meio da árvore topológica.

### Processo de Descoberta do Protocolo de Estado de *Link*

Os pacotes LSAs são trocados entre os roteadores da topologia, começando pelas Redes diretamente conectadas. Cada roteador, em paralelo com os outros, constrói um Banco de Dados topológico completo, que consiste em todos os LSAs trocados entre os roteadores da topologia.

Depois disso, o algoritmo SPF calcula a alcançabilidade da Rede e o roteador constrói essa topologia lógica em árvore, tendo a si mesmo como o dispositivo raiz (*root*), que consiste em todos os possíveis caminhos para cada Rede no grupo de Redes interconectadas (*internetwork*), em que está sendo usado o Protocolo por link state. Em seguida, ele ordena esses caminhos, colocando os caminhos mais curtos primeiro (SPF) na Tabela de Roteamento ou Tabela de melhores rotas.

Note que os rotadores de estado de link possuem esse Banco de Dados de elementos da topologia em paralelo à Tabela de Roteamento, o que agiliza a mudança de rotas modificadas (atualizadas, novas entradas e rotas que foram desligadas (STALLINGS; ROSS, 2010).

Porém, primeiro o roteador toma conhecimento de uma alteração na topologia pelos estados dos *links* e encaminha essa informação para que os outros roteadores possam aprender e fazer as atualizações necessárias.

Para que se alcance a convergência de Rede, cada roteador rastreia seus vizinhos quanto ao nome do roteador, o status da interface e o custo do *link* até esse determinado vizinho.

O roteador constrói um pacote LSA, que lista essas informações, juntamente com os novos vizinhos, as mudanças nos custos dos *links* e os *links* que não são mais válidos e, em seguida, o respectivo pacote LSA é distribuído para que todos os outros roteadores o recebam e possam dar continuidade no Processo de convergência.

Quando o roteador recebe um determinado LSA, o Banco de Dados, então, é atualizado com as informações mais recentes; após isso, ele calcula um mapa do grupo de Redes interconectadas utilizando todos os Dados acumulados e determina o caminho mais curto para outras Redes, utilizando o algoritmo SPF.

Por esse motivo, cada vez que um LSA causa uma alteração dentro do Banco de Dados de estado dos *links*, o algoritmo recalcula os melhores caminhos e após isso atualiza a Tabela de Roteamento.

Preocupações relacionadas ao uso de Protocolos por estado de enlace:

- Sobrecarga do Processador;
- Exigência de Memória;
- Consumo de Largura de Banda.

Por características de funcionamento do algoritmo de SPF, os roteadores requerem mais memória e realizam mais processamento de CPU do que os que utilizam Protocolos de vetor da distância, pois eles precisam ter memória suficiente para armazenar todas as informações recebidas no Bancos de Dados. É claro que, por questões óbvias, a enxurrada inicial de pacotes LSA consome largura de banda, pois, nesse momento, são disparados de uma única vez e com alta intensidade.

Ocorrida a convergência da Rede, os Protocolos de estado de *link*, geralmente, exigem uma largura de banda mínima para enviar pacotes LSA que não são muito frequentes ou que são disparados por eventos (*Event Triggered LSA*), que podem refletir na alteração da topologia (TANENBAUM, 2011).

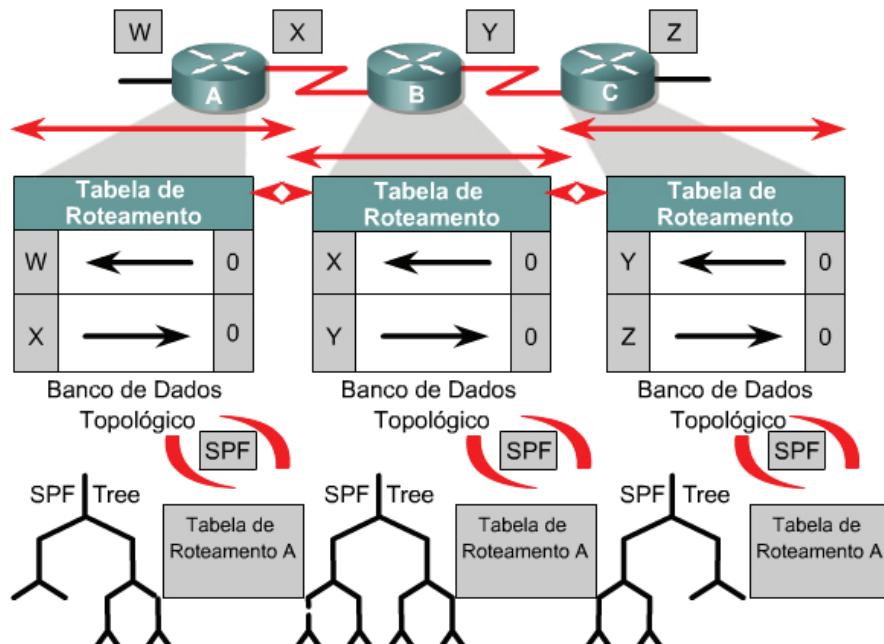


Figura 7 – Troca de Rotas com Estado de *Link*

## Definição de Caminho de Rota

Um roteador determina o caminho de um pacote, de um link de Dados para outro, utilizando duas funções principais:

- Uma função de determinação do caminho;
- Uma função de comutação (*switching*).

A função de determinação do caminho ocorre na camada de Rede (Camada 3), que possibilita que um roteador avalie os caminhos até um destino e que estabeleça um tratamento preferencial de um pacote.

Nesse caso, o roteador utiliza então a Tabela de Roteamento para determinar o melhor caminho que o pacote deverá fazer e o encaminha utilizando a função de comutação.

Por esse motivo, a função de comutação (*Switching*) é o Processo interno utilizado pelo roteador para poder aceitar um pacote numa interface de entrada e depois encaminhá-la para uma segunda interface de saída do mesmo roteador.

Uma responsabilidade essencial da função de comutação que o roteador executa é o encapsulamento dos pacotes apropriados para o próximo *link* de Dados.

# Protocolos de Roteamento Dinâmico

Baseado no conjunto de Protocolos do TCP/IP que estão na camada de Internet desse Protocolo, um roteador pode utilizar um Protocolo de Roteamento IP, a fim de realizar o Roteamento de pacotes por meio das implementações de um algoritmo de Roteamento específico utilizado.

Exemplos de Protocolos de Roteamento IP seriam:

- RIPv1 e v2 – Protocolo de Roteamento interior de vetor da distância;
- OSPF – Protocolo de Roteamento interior de estado de link;
- IGRP – Protocolo de Roteamento interior de vetor da distância da Cisco;
- EIGRP – Protocolo de Roteamento interior de vetor da distância da Cisco, mas avançado se comparado com o IGRP;
- BGP – Protocolo de Roteamento exterior por vetor da caminhos.

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

- É um Protocolo de Roteamento de vetor da distância;
- A contagem de saltos é utilizada como métrica para a seleção de caminhos;
- Se a contagem de saltos for maior que 15, o pacote de atualização, então, é descartado;
- Por padrão, as atualizações de Roteamento são enviadas através de *broadcast*, a cada 30 segundos, mesmo que o roteador tenha enviado tal informação anteriormente.

O **IGRP (Interior Gateway Routing Protocol)** é um Protocolo devolvido e proprietário da Cisco.

Algumas das principais características do IGRP são:

- É um Protocolo de Roteamento de vetor da distância;
- Largura de banda, carga, atraso, confiabilidade e MTU são utilizados para criar uma métrica composta calculada;
- Por padrão, as atualizações de Roteamento são enviadas através de broadcast, a cada 90 segundos, mesmo que o roteador tenha enviado tal informação anteriormente.

O **OSPF (Open Shortest Path First)** é um Protocolo de Roteamento de estado de *link* aberto (não proprietário).

As principais características do OSPF são:

- Protocolo de Roteamento de estado de *link*;
- Protocolo de Roteamento de padrão aberto, descrito pela RFC 2328;

- Usa o algoritmo SPF para calcular o menor custo até um destino, usando como métrica a velocidade do *link*;
- Quando ocorrem alterações na topologia, há uma enxurrada de atualizações de Roteamento, que ocorrem quando tais eventos são executados.

**EIGRP (Enhanced Interior Gateway Routing Protocol)** é um Protocolo avançado de Roteamento de vetor da distância desenvolvido e de propriedade da Cisco.

As suas principais características são:

- É um Protocolo avançado de Roteamento de vetor da distância; porém, a Cisco o chama de Protocolo de Roteamento híbrido;
- Usa balanceamento de carga com custos desiguais;
- Usa características combinadas de vetor da distância e estado dos *links*. Por isso é chamado de Protocolo de Roteamento híbrido;
- Usa o algoritmo DUAL (*Diffusing Update Algorithm* – Algoritmo de Atualização Difusa) para calcular o caminho mais curto, baseando-se nas métricas de Roteamento (K1, K2, K3, K4 e K5);
- As atualizações de Roteamento são enviadas através de *multicast* utilizando o endereço IPv4 224.0.0.10, que são disparadas por alterações da topologia, por meio de eventos;

**BGP (Border Gateway Protocol)** é um Protocolo de Roteamento exterior (que interliga vários Sistemas Autônomos).

Suas principais características são:

- É um Protocolo de Roteamento exterior de vetor de caminhos (uma espécie de vetor distância);
- É usado entre os provedores de serviço de Internet ou entre Redes de clientes (ASs). Esse Protocolo também é conhecido como Protocolo da Internet;
- É utilizado para rotear o tráfego de Internet entre Sistemas Autônomos (ASs).

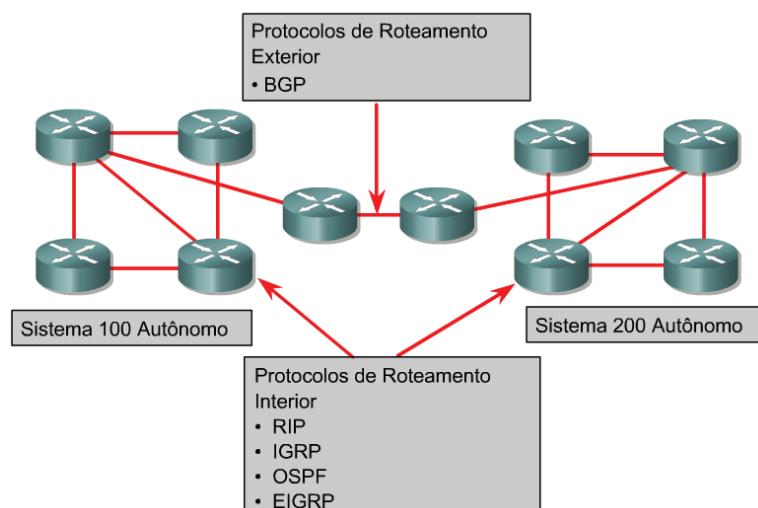


Figura 8 – Protocolos de Roteamento

# Sistemas Autônomos e Protocolos IGP e EGP

Os Protocolos de Roteamento Interior (IGPs) foram criados para utilização numa Rede cujas partes estejam sob controle de uma única organização.

Os critérios de Projeto para um Protocolo de Roteamento interior exigem que ele encontre o melhor caminho por meio da Rede interior, ou seja, a métrica e a maneira como essa métrica é utilizada são os elementos mais importantes num Protocolo de Roteamento Interior (CISCO NETACAD, 2017).

Já um Protocolo de Roteamento Exterior (EGPs) são concebidos para a utilização entre duas ou mais Redes diferentes, que estejam sob controle de diferentes organizações.

Geralmente, esses Protocolos de Roteamento são utilizados entre provedores de serviço de Internet ou entre a interligação de grandes Redes de uma mesma Empresa.

Os Protocolos de Gateway IP Exteriores requerem três conjuntos básicos de informações antes de iniciar o Roteamento.

São eles:

- Uma lista de roteadores vizinhos com os quais possam trocar informações de Roteamento entre si;
- Uma lista de Redes para poder anunciar como diretamente alcançáveis;
- O número que identifica um sistema autônomo do roteador local.

Um Protocolo de Roteamento exterior deve, então, isolar os Sistemas Autônomos, que são gerenciados por diferentes administrações.

Esses Sistemas Autônomos (ASs) possuem um número de identificação, atribuído pelo ARIN (*American Registry of Internet Numbers*) ou por um provedor de serviços de Internet.

Esse número de identificação possui 16 bits de tamanho.

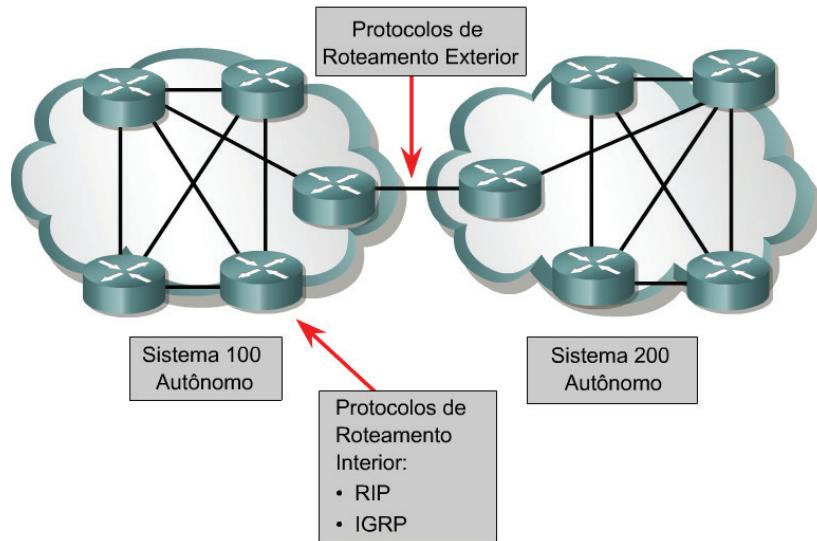


Figura 9 – Protocolos de Roteamento IGP e EGP

# Material Complementar

## Indicações para saber mais sobre os assuntos abordados nesta Unidade:



Livros

### Redes de Computadores e a Internet

STALLINGS, W. e ROSS K. **Redes de Computadores e a Internet.** 5<sup>a</sup> Ed. São Paulo: Editora Pearson, 2010.

### Redes de Computadores

TANENBAUM, A. S; WETHERALL, D. **Redes de Computadores.** 5<sup>a</sup> Ed. Rio de Janeiro: Editora Campus, 2011.

### Módulo de Roteamento e Switching

CISCO NETACAD – **Módulo de Roteamento e Switching** – Conceitos Essenciais – Capítulo 6 – Roteamento Estático, Versão 6.0, EUA, 2017.

## Referências

CISCO NETACAD. **Módulo de Roteamento e Switching:** Conceitos Essenciais (CCNA2). 6<sup>a</sup> versão, Cisco Systems, 2017 (Material *on-line*). Disponível em [www.netacad.com](http://www.netacad.com). Acesso em: 27/09/2018.

STALLINGS, W. e ROSS K. **Redes de Computadores e a Internet.** 5<sup>a</sup> Ed. São Paulo: Editora Pearson, 2010.

TANENBAUM, A. S; WETHERALL, D. **Redes de Computadores.** 5<sup>a</sup> Ed. Rio de Janeiro: Editora Campus, 2011.





**Cruzeiro do Sul**  
Educacional

# Tecnologias de Roteamento



Cruzeiro do Sul Virtual  
Educação a distância



# Material Teórico



**Protocolos de Roteamento Dinâmico IGP**

**Responsável pelo Conteúdo:**

Prof. Esp. Antonio Eduardo Marques da Silva

**Revisão Textual:**

Prof.<sup>a</sup> Dr.<sup>a</sup> Selma Aparecida Cesarin



# UNIDADE

## Protocolos de Roteamento Dinâmico IGP



- **Introdução;**
- **Roteamento de Vetor Distância;**
- **RIP v2;**
- **Roteamento de Estado de *Link*;**
- **Protocolo OSPF.**



### OBJETIVO DE APRENDIZADO

- Esta Unidade tem como principal objetivo compreender e abordar os Protocolos de Roteamento Internos (IGPs), que são classificados em vetores de distância e estado de link e alguns Protocolos de Roteamento Dinâmicos, como o RIP e o OSPF e as configurações simples de ambos esses Protocolos.





# Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:



## Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu “momento do estudo”;
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

# Introdução

Como já vimos, para que os roteadores possam comutar os pacotes através de uma ou várias Redes, surge a necessidade de conhecê-los melhor e também de configurá-los corretamente.

Nesta Unidade, vamos tratar um pouco dos aspectos dos Protocolos do tipo IGP, que rodam dentro de um Sistema Autônomo e também vamos conhecer alguns desses Protocolos e como eles funcionam dentro de uma Rede de Comunicação.

## Roteamento de Vetor Distância

Os Protocolos de Roteamento Dinâmico de Vetor Distância exigem rotas para encaminhar a Tabela de Roteamento completa ao repassar as atualizações entre os roteadores vizinhos e continuam a fazer isso durante toda a atividade desse processo, o que é um contraste em relação aos Protocolos de Roteamento de Estado de Enlace, que encaminham suas atualizações de Roteamento a todos os roteadores da Área e esses, depois de calculados pelo algoritmo de Roteamento, extraem as melhores rotas e as armazenam na Tabela de Roteamento.

Essas Tabelas de Roteamento incluem informações sobre o custo total de uma rota até seu destino e o endereço lógico do primeiro roteador no caminho para cada Rede contida na Tabela de rotas (TANENBAUM, 2011).

Os roteadores precisam atualizar as informações das respectivas Tabelas de Roteamento para tomar boas decisões relacionadas à determinação de melhores caminhos.

Periodicamente, as alterações numa Rede podem afetar as decisões tomadas por um roteador na *internetworking*. Por exemplo, um roteador pode ser desativado para atualizações ou reparos ou, então, uma interface de um roteador pode ficar inoperante por algum desligamento.

Normalmente, os Protocolos de Roteamento de Vetor Distância transmitem atualizações em certos intervalos de tempo; por exemplo, no caso do RIPVv1, a cada 30 segundos, e no IGRP, a cada 90 segundos (CISCO NETACAD, 2017).

As atualizações da Tabela de Roteamento podem ocorrer periodicamente ou quando é realizada alguma alteração na topologia numa Rede com Protocolos de Vetor da Distância. É importante que um Protocolo de Roteamento seja eficiente na atualização das Tabelas de Roteamento para que a Rede possa convergir satisfatoriamente.

Os algoritmos de Vetor da Distância solicitam que cada roteador envie toda a sua Tabela de Roteamento (Tabela completa) a cada roteador vizinho adjacente.

Essas Tabelas de Roteamento incluem informações sobre o custo total do caminho, conforme definido pelas métricas de Roteamento (por exemplo, quantidade de saltos, velocidade de *link* ou algum custo calculado) e pelo endereço lógico do primeiro roteador do caminho para cada Rede contida na Tabela de rotas (STALLINGS; ROSS, 2010).



*Distance Vector and Link State Protocols* (Inglês). Acesse: <https://youtu.be/ygxBBMztT4U>

## Problemas de Loops de Roteamento

Em função dessa atualização de Tabelas completas para seus vizinhos, a convergência de Rede se torna lenta e isso pode provocar entradas inconsistentes de Roteamento e até mesmo *loops* de Roteamento.

Se uma Rede ficar inoperante, talvez essas informações não sejam propagadas na Rede com a rapidez necessária e, por esse motivo, um roteador pode desenvolver uma visão incorreta da Rede, transmitindo informações incorretas para seus vizinhos, que teriam também uma posição errada da topologia.

A convergência ocorre quando todos os roteadores possuem as mesmas informações sobre a Rede, ou seja, ela é um subproduto das atualizações de Roteamento transmitidas com base no Protocolo de Roteamento escolhido e utilizado num roteador.

Se informações atualizadas não podem chegar a todos os roteadores de uma Rede rapidamente, informações incorretas de atualizações de Roteamento podem ser transmitidas para toda a topologia.

Os Protocolos de Vetor Distância possuem técnicas para evitar possíveis loops de Roteamento como:

- Determinação de contagem máxima;
- *Split Horizon*;
- Inviabilidade de rota;
- Atualizações acionadas;
- Temporizadores de *Holddown*.

## Protocolo de Roteamento RIP

O Protocolo de Roteamento RIP (*Routing Information Protocol*), às vezes chamado de IP RIP, está detalhado formalmente em dois documentos separadamente.

O primeiro é conhecido como RFC (*Request for Comments*), sob o registro número 1058, e outro como STD (*Internet Standard*), sob a identificação número 56.

O Protocolo RIP evoluiu de um *Classful Routing Protocol* (Protocolo de Roteamento com classes), o RIP Versão 1 (RIP v1), e para um *Classless Routing Protocol* (Protocolo de Roteamento sem classes), o RIP Versão 2 (RIP v2).

As evoluções do RIP v2 incluem:

- Capacidade de transportar informações adicionais sobre Roteamento de pacotes de Dados;
- Mecanismo de autenticação para garantir as atualizações da Tabela de rotas;
- Suporte à VLSM (máscaras de Sub-rede com tamanho variável) ou FLSM (máscara de Sub-rede com tamanho fixo).

O RIP impede a continuação indefinida de loops de Roteamento, implementando limite sobre o número de saltos permitidos num caminho, da origem até uma determinada Rede destino.

O número de limite máximo de saltos num caminho usando o RIP é 15. Quando um roteador recebe uma atualização de Roteamento que contém uma entrada nova ou alterada, o valor da métrica é aumentado em 1, que identifica um salto nesse caminho.

Caso o número de saltos exceda 15, então, essa rota será considerada infinita e esse destino de Rede será considerado inalcançável.

O RIP inclui diversos recursos comuns em outros Protocolos de Roteamento, como a implementação dos mecanismos de *split horizon* e de retenção para impedir a propagação de informações de Roteamento incorretas (STALLINGS; ROSS, 2010).

## Configuração do RIP

---

O comando **router rip** habilita o Protocolo de Roteamento RIP no dispositivo configurado, e o comando **network** é usado em seguida, para informar ao roteador em que interfaces executar o Protocolo RIP.

Esse Processo de Roteamento dinâmico associa interfaces específicas aos endereços de Rede e começa a enviar e receber atualizações do RIP através dessas interfaces.

O RIP, então, acaba enviando mensagens de atualização em intervalos regulares. Quando um roteador recebe uma atualização de Roteamento que inclui alterações numa entrada, ele atualiza sua Tabela de Roteamento para que possa refletir a nova rota.

O valor da métrica recebida para o caminho é aumentado em 1 e a interface de origem da atualização é indicada como o próximo salto na Tabela de Roteamento. Os roteadores RIP mantêm, então, apenas a melhor rota para um determinado destino (CISCO NETACAD, 2017).

Os Protocolos como o RIP e o IGRP enviam atualizações dentro de tempos pré-determinados; porém, foram criados gatilhos que quando ocorrem uma eventual mudança de topologia são devidamente acionados, bem como temporizadores que auxiliam na montagem e na manutenção das Tabelas de Roteamento desses Protocolos.

Essas atualizações, chamadas de atualizações de Roteamento acionadas, são enviadas independentemente daquelas programadas regularmente pelos Protocolos como no caso do RIP (CISCO NETACAD, 2017).

Vamos dar uma olhada na implementação dos rotadores utilizando o Protocolo RIP e entender algumas particularidades.

Vamos aos comandos:

- **Router(config)# router rip** – Seleciona o Protocolo RIP como o Protocolo de Roteamento a ser utilizado;
- **Router(config-router)#network 10.0.0.0** – Especifica uma Rede diretamente conectada;
- **Router(config-router)#network 192.168.13.0** – Especifica uma Rede conectada diretamente.

As interfaces dos roteadores Cisco que estão conectadas às Redes 10.0.0.0 e 192.168.13.0 enviam e recebem atualizações do RIP.

Essas atualizações de Roteamento permitem que o roteador aprenda a Tabela de Roteamento do roteador vizinho e monte, baseado nisso, na sua Tabela de Roteamento; por consequência, tem sua topologia de Rede.

O RIP deve ser ativado em todos os rotadores da topologia e as Redes diretamente conectadas devidamente especificadas. As tarefas restantes são opcionais.

Entre elas estão:

- Aplicação de deslocamentos a métricas de Roteamento;
- Ajuste de temporizadores;
- Verificação do resumo da rota IP;
- Ativação ou desativação do *split horizon* (técnica de evitar loops);
- Desativação do resumo automático da rota;
- Execução simultânea do IGRP e do RIP;
- Especificação de uma versão do RIP;
- Conexão do RIP a uma WAN;
- Ativação da autenticação do RIP (caso a versão possua);
- Configuração do resumo da rota em uma interface;
- Desativação da validação de endereços IP de origem.

Para ativar o Protocolo RIP, utilize, então, os seguintes comandos, começando no modo de configuração global do IOS:

- **Router(config)# router rip** – Ativa o processo de Roteamento dinâmico do RIP;
- **Router(config-router)#network network-number** – Associa uma Rede ao processo de Roteamento do RIP.

Configuração Básica do RIP:

```
Sydney(config)# router rip
```

```
Sydney(config-router)# network 172.16.0.0
```

```
Sydney(config-router)# network 12.168.100.0
```

## IP Classless

---

Às vezes, um roteador recebe pacotes destinados a uma Sub-rede desconhecida de uma Rede que possui Sub-redes conectadas diretamente em sua *internetworking*.

Para que o software Cisco IOS encaminhe esses pacotes a melhor rota de Super Rede possível, use o comando de configuração global **IP classless**.

Uma rota de Super Rede cobre um intervalo de Sub-redes com uma única entrada. Por exemplo, uma Empresa usa toda a Sub-rede 10.10.0.0 /16; nesse caso, uma rota de Sub-rede para 10.10.10.0 /24 seria 10.10.0.0 /16.

O comando **IP classless** é ativado por padrão no Sistema Operacional Cisco IOS Versão 11.3 e próximos. Para desativar esse recurso, use o comando forma no **IP classless** (CISCO NETACAD, 2017).

Quando o recurso for devidamente desativado, qualquer pacote recebido e destinado a uma Sub-rede, cuja numeração esteja contida no esquema de endereçamento do roteador serão descartados, ou seja, ele retorna a divulgar Redes no formato de máscara padrão.

O IP sem classes afeta apenas a operação dos Processos de encaminhamento no Sistema Operacional da Cisco, ou seja, ele não afeta o modo de construção da Tabela de Roteamento do Dispositivo.

Essa é a essência do Roteamento com classes, pois, se uma parte de uma Rede principal for conhecida, mas a Sub-rede à qual o pacote se destina nessa Rede principal for desconhecido, o pacote será descartado pelo roteador (TANENBAUM, 2011).

O aspecto mais confuso dessa regra é que o roteador utiliza a rota padrão/*default* somente se o destino de Rede principal não existir na Tabela de Roteamento, pois um roteador assume, por padrão, que todas as Sub-redes de uma Rede conectada diretamente devem estar presentes na Tabela de Roteamento.

Se um pacote for recebido com endereço de destino desconhecido em uma Sub-rede desconhecida de uma Rede diretamente conectada, o roteador corrente presumirá que a Sub-rede não existe e, por esse motivo, irá descartar esse pacote.

Por esse motivo, a função de configuração de **IP classless** no roteador solucionará esse problema, ao permitir que o roteador ignore os endereços com classes das Redes em sua Tabela de Roteamento e, simplesmente, utilize a rota padrão como rota de destino.

## Problemas Comuns do RIP

---

Os roteadores configurados com o Protocolo RIP devem basear-se na vizinhança para obter informações de Rede não conhecidas em primeira mão. Um termo comum utilizado para descrever essa funcionalidade é Roteamento por Rumor (ou fofoqueiro).

O Protocolo RIP utiliza um algoritmo de Roteamento de Vetor Distância que possui problemas criados, principalmente, pela demorada convergência.

Entre esses problemas, estão os loops de Roteamento e a contagem até o infinito (é claro que, matematicamente, não se tem contagem do infinito, isso é apenas um número que limita o Protocolo propagar suas atualizações de uma forma descontrolada e infinita).

Eles resultam em inconsistências causadas por mensagens de atualização de Roteamento com rotas desatualizadas que se propagam na Rede (STALLINGS; ROSS, 2010).

Para reduzir problemas desses Protocolos, principalmente, os loops de Roteamento e a contagem até o infinito, o RIP utiliza as seguintes técnicas:

- Contagem até o infinito;
- *Split horizon*;
- Contadores de retenção;
- Inviabilização de rotas;
- Atualizações acionadas.

## Verificação do RIP

---

Existem dezenas de comandos que podem ser utilizados para verificar se o RIP está configurado corretamente nos roteadores. Os comandos mais comuns são o **show ip route** e **show ip protocols** (CISCO NETACAD, 2017).

O comando do IOS show ip protocols apresenta quais Protocolos de Roteamento foram configurados e estão transportando o tráfego IP no roteador.

Esse resultado pode ser utilizado para verificar a maior parte, se não a totalidade, da configuração do RIP.

Algumas das informações de configuração mais comuns a serem verificadas são:

- Se o Roteamento do RIP está configurado corretamente;
- Se as interfaces configuradas e ativas estão enviando e recebendo atualizações do Processo de Roteamento do RIP;
- Se o roteador está anunciando e divulgando as atualizações das Redes corretamente.

Já o comando do IOS **show ip route** pode ser utilizado para verificar se as rotas recebidas pelos vizinhos do RIP estão instaladas na Tabela de Roteamento.

Uma vez aplicado esse comando, é possível examinar o resultado para a identificação das rotas aprendidas via Protocolo RIP que, na Tabela de Roteamento, é indicado pela letra “R”.

Lembre-se de que a Rede levará algum tempo para convergir em função da forma como o Protocolo RIP faz seus anúncios de rotas por meio dos vizinhos e, assim, as rotas poderão não aparecer imediatamente na Tabela de Roteamento (CISCO NETACAD, 2017).

Alguns outros comandos adicionais de auxílio para a verificação da configuração do Protocolo RIP são, como podemos ver:

- **show running-config;**
- **show interface;**
- **show ip interface.**

## RIP v2

O RIPv2 é irmão do RIPv1 e proporciona Roteamento de prefixo, o que permite que ele envie informações sobre máscaras de Sub-rede junto com a atualização de rotas (*Classless*).

E, por isso, o RIPv2 suporta a utilização de Roteamento *classless* no qual diferentes Sub-redes dentro da mesma Rede podem usar diferentes máscaras de Sub-rede, como é o caso do VLSM e o FLSM.

Ambas as versões RIPv1 e RIPv2 possuem as seguintes características:

- Um Protocolo de Vetor Distância usa uma métrica de contagem de saltos;
- Utiliza temporizadores do tipo holddown para evitar loops de Roteamento, sendo que o padrão é de 180 segundos;
- Utiliza a técnica de *split-horizon* para evitar loops de Roteamento;
- Utiliza 16 saltos como limite para distância infinita, que evita que o processo entre também em loop infinito.

Outra funcionalidade do RIPv2 é a acomodação de autenticação nas suas atualizações, ou seja, um conjunto de chaves pode ser utilizado numa interface como verificação de autenticação.

Essa configuração permite uma escolha do tipo de autenticação a ser usada nos pacotes de RIPv2. A escolha será entre texto claro e criptografia *Message-Digest 5* (MD5).

Texto claro, também conhecido como texto puro, é a propriedade padrão no Protocolo; porém, o MD5 pode ser utilizado para autenticar a origem de uma atualização de Roteamento.

O MD5 é tipicamente usado para criptografar senhas ***enable secret*** que são usadas na aplicação de senha para o acesso ao modo privilegiado e não existe nenhum tipo reversão de senha conhecida (CISCO NETACAD, 2017).

Outra diferença entre as versões 1 e 2 do RIP é em relação aos *updates* de Roteamento, pois o RIPv2 envia atualizações de Roteamento em *multicast* usando o endereço de Classe D 224.0.0.9, que permite melhor eficiência, se comparado ao RIPv1, que faz esse envio em broadcast (CISCO NETACAD, 2017).

## Configuração do RIPv2

A combinação dos comandos ***router rip*** e ***version 2*** especificam a aplicação do Protocolo de Roteamento RIPv2, enquanto o comando ***network*** identifica uma Rede conectada diretamente e que será indicada da Tabela de Roteamento caso ela seja a de melhor escolha e está aplicada na Tabela de Roteamento, que depois é divulgada entre os vizinhos da *internetworking* (CISCO NETACAD, 2017).

Podemos, então, resumir a configuração do RIP nos seguintes itens:

- ***router rip*** – Ativa o RIP como Protocolo de Roteamento;
- ***version 2*** – Identifica a versão 2 como a versão do RIP sendo utilizada;
- ***network 172.16.0.0*** – Especifica uma Rede diretamente conectada;
- ***network 10.0.0.0*** – Especifica outra Rede diretamente conectada.

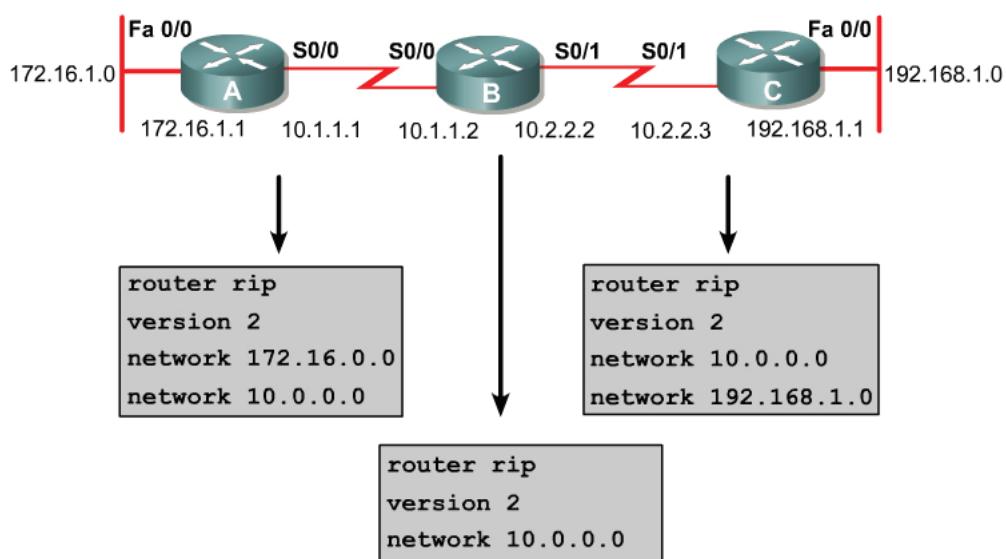


Figura 1 – Configuração do RIPv2

# Roteamento de Estado de Link

Os Protocolos de Roteamento de *Link State* funcionam de maneira diferente dos Protocolos de *Distance Vector*. Uma diferença essencial é que os Protocolos de *Distance Vector* utilizam um método bem mais simples para trocar informações de Roteamento (troca de Tabelas completas entre vizinhos).

Os algoritmos de Roteamento de *Link State* mantêm um Banco de Dados complexo com as informações de topologia de Rede. Enquanto o algoritmo *Distance Vector* tem informações não específicas sobre Redes distantes e nenhum conhecimento sobre roteadores distantes, um algoritmo de Roteamento de *Link State* mantém conhecimento completo sobre roteadores distantes e sobre como eles estão interconectados entre si, dando uma visão global da Rede como um todo.

## Características do Protocolo de Estado de Link

---

Os Protocolos de Roteamento de *Link State* coletam informações de rota de todos os outros roteadores da Rede ou dentro de uma área definida dela. Uma vez coletadas todas essas informações, cada roteador calcula os melhores caminhos para todos os destinos da Rede.

Nesse caso, cada roteador mantém sua própria visão da Rede como um todo e, por isso, tem menor probabilidade de propagar informações incorretas fornecidas por algum de seus roteadores vizinhos (TANENBAUM, 2011).

Algumas funções do Protocolo de Roteamento Dinâmico de *Link State*:

- Responder rapidamente a mudanças na Rede;
- Enviar *triggered updates* ou gatilhos apenas quando ocorrer uma alteração das rotas na Rede;
- Enviar atualizações periódicas, conhecidas como atualizações *Link State* ou também LSAs;
- Usar um mecanismo *hello* para determinar se os vizinhos podem ou não ser alcançados.

Cada roteador envia pacotes *hello* em *multicast* para informar sobre o estado dos roteadores vizinhos. Eles utilizam 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.

Então, podemos citar:

- Os LSAs fornecem atualizações sobre o estado dos enlaces (*links*) que são interfaces nos outros roteadores da Rede;

- Os roteadores que usam Protocolos de Roteamento *Link State* usam as informações de hello e os LSAs recebidos de outros roteadores para criar um Banco de Dados completo sobre a Rede;
- Utilizam o algoritmo SPF para calcular a rota mais curta para cada Rede;
- Armazenam as informações da rota na Tabela de Roteamento, que foram extraídas do Banco de Dados e das rotas diretamente conectadas (vizinhos).

Assim, podemos resumir os recursos dos Protocolos *Link State*:

- Os LSAs;
- Um Banco de Dados topológico;
- O algoritmo SPF e a árvore SPF;
- Uma Tabela de Roteamento de caminhos e indicação de interfaces para determinação do melhor caminho para os pacotes.

Quando ocorre uma eventual falha na Rede, por exemplo, um vizinho fica inalcançável. Nesse caso, os Protocolos *Link State* inundam (*flood*) LSAs com um endereço *multicast* especial para toda a área em que estão.

A sigla *Flooding*, ou inundação, é o processo de enviar informações para todas as portas, exceto para aquela em que as informações foram recebidas.

Cada roteador *Link State* toma uma cópia do LSA e atualiza seu Banco de Dados *Link State*, ou Banco de Dados topológico.

Em seguida, o roteador *Link State* encaminha o LSA para todos os dispositivos vizinhos, fazendo com que todos os roteadores dentro da área recalculem 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 num roteador. Por esse motivo, 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 de *Link States* que, às vezes, é chamado de Banco de Dados topológico. Esse Banco de Dados de *Link States* é utilizado para calcular os melhores caminhos através da Rede.

Os roteadores da topologia de *Link States* aplicam o algoritmo *Dijkstra* ou caminho mais curto primeiro (SPF – *Shortest Path First*) consultando o Banco de Dados de *Link States*.

Isso cria a árvore SPF topológica, tendo o roteador local como raiz desse processo. Em seguida, os melhores caminhos são selecionados a partir da árvore SPF e colocados na Tabela de Roteamento (TANENBAUM, 2011).

## Algoritmos de Roteamento do Estado de Link

Os algoritmos de Roteamento *Link State* mantêm um Banco de Dados complexo e completo da topologia da Rede trocando anúncios de *Link State* (LSAs) com outros roteadores dessa topologia.

Resumindo, os algoritmos de Roteamento de *Link State* têm as seguintes características principais:

- São conhecidos coletivamente como Protocolos SPF;
- Mantêm um Banco de Dados complexo sobre a topologia da Rede;
- São baseados no algoritmo *Dijkstra*.

Cada roteador constrói um Banco de Dados topológico a partir dos LSAs que recebe, como centro da topologia. Em seguida, o algoritmo SPF é utilizado para computar a facilidade de alcance aos destinos e essa informação é utilizada para atualizar a Tabela de Roteamento.

Esse processo pode descobrir alterações na topologia da Rede causadas por falha de componentes ou crescimento da Rede.

Uma troca de LSAs é acionada por um novo evento de Rede, e não por atualizações periódicas, como é o caso do funcionamento dos Protocolos de *Distance Vector*. Isso acelera o processo de convergência, pois não há necessidade de esperar até que uma série de temporizadores expire.

## Protocolo OSPF

O Protocolo de Roteamento OSPF é um Protocolo de *Link State* que se baseia em padrões abertos, pois está descrito em diversos padrões da IETF (*Internet Engineering Task Force*).

A letra inicial O de OSPF vem de open e significa que é um padrão aberto ao público e não proprietário de uma Instituição privada e/ou governamental.

O OSPF, quando comparado ao RIP v1 e v2, é o IGP (Protocolo Interior) preferido, haja vista sua distância administrativa menor e com a funcionalidade de poder ser mais bem escalado.

Como já vimos, o RIP é limitado a 15 saltos (16 seria a contagem do infinito), converge lentamente e, às vezes, escolhe rotas lentas, pois ignora fatores críticos, tais como a largura de banda, na determinação das rotas.

Uma desvantagem da utilização do Protocolo OSPF é que ele só suporta Protocolos baseados em TCP/IP.

O Protocolo de Roteamento OSPF pode ser utilizado e configurado como uma única área para Redes pequenas, mas também pode ser utilizado em grandes Re-

des; porém, de uma forma mais hierarquizada, pois várias áreas se conectam a uma área de distribuição, ou área 0, que também é chamada de área de *backbone*. A abordagem desse projeto permite extenso controle das atualizações de Roteamento.

A definição de áreas reduz a sobrecarga de Roteamento, acelera a convergência, confina a instabilidade da Rede a uma área e melhora significativamente o desempenho da Rede.

Essa forma de configuração de grandes Redes usando o OSPF é conhecida como OSPF em Múltiplas Áreas.

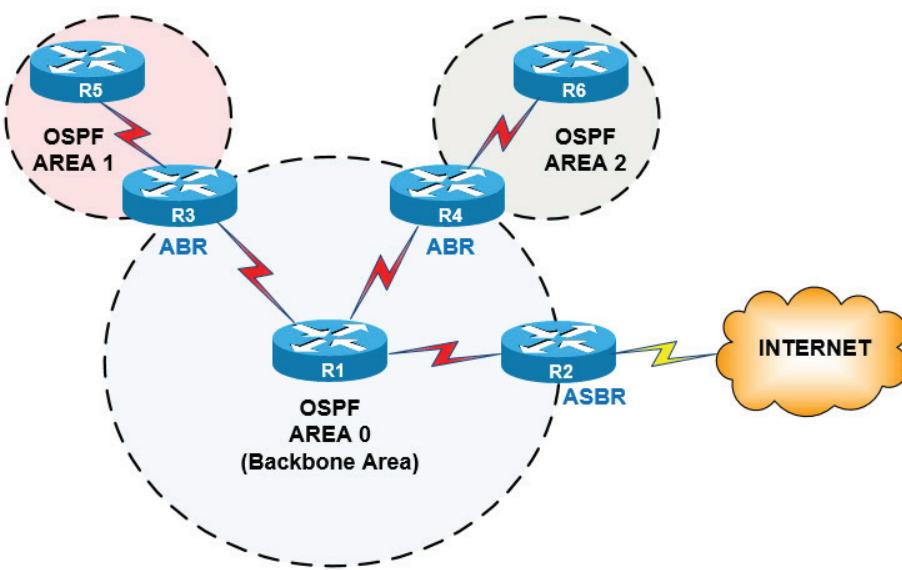


Figura 2 – Protocolo OSPF

## Terminologia OSPF

Os roteadores *Link State* identificam os roteadores vizinhos e, então, comunicam-se com eles, reunindo informações deles. Essa informação é despejada para todos os seus vizinhos, ou seja, um roteador OSPF anuncia os estados de seus próprios links e repassa os estados de links recebidos.

Os roteadores processam as informações sobre os *Link States* e criam um Banco de Dados de *Link States*.

Assim, cada roteador da área OSPF tem o mesmo Banco de Dados de *Link States* e, por esse motivo, cada roteador tem as mesmas informações sobre o estado dos links e dos vizinhos de todos os outros roteadores da topologia (TANENBAUM, 2011).

Em seguida, cada roteador aplica o algoritmo SPF em sua própria cópia do Banco de Dados. Esse cálculo pode determinar a melhor rota até um determinado destino. O algoritmo SPF aumenta o custo, que, geralmente, é um valor baseado na largura de banda.

O caminho de menor custo é adicionado à Tabela de Roteamento, pois o menor valor é a melhor métrica e também é conhecido como Banco de Dados de encaminhamento (*forwarding database*).

Cada roteador mantém uma lista dos vizinhos adjacentes, chamada de Banco de Dados de adjacências, que nada mais é do que uma lista de todos os roteadores vizinhos com os quais um roteador estabeleceu comunicação bidirecional. Ele é exclusivo de cada roteador (CISCO NETACAD, 2017).

Em caso de grandes topologias de Rede, para reduzir a quantidade de trocas de informações de Roteamento entre vários vizinhos na mesma Rede, os roteadores OSPF elegem um roteador designado, ou *Designated Router* (DR), e um roteador designado de backup, ou backup *Designated Router* (BDR), que atuam como pontos focais (ponto de encontro) para a troca de informações de Roteamento (CISCO NETACAD, 2017).

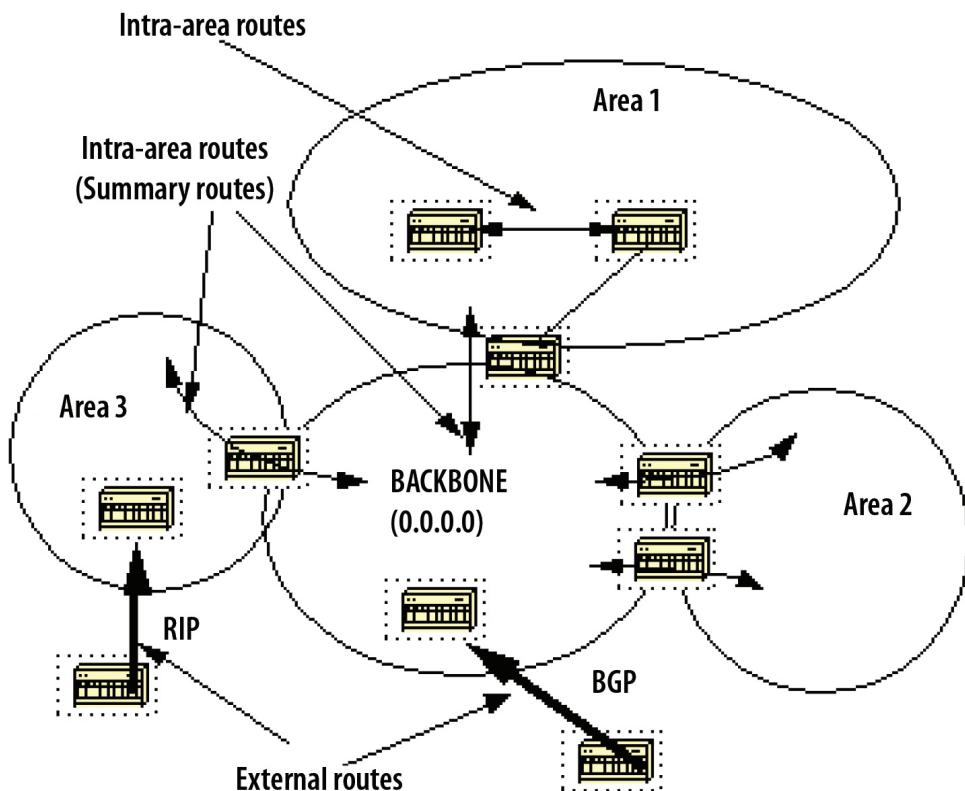


Figura 3 – Terminologia do OSPF

## Tipos de Rede OSPF

É necessária uma relação de vizinhança para que os roteadores OSPF compartilhem informações de Roteamento. Um roteador tentará se tornar vizinho, ou adjacente, de pelo menos outro roteador em cada Rede IP à qual estiver interconectado.

Os roteadores OSPF determinam os roteadores que se tornam adjacentes com base no tipo de Rede à qual estão conectados e, uma vez formada uma adjacência entre vizinhos, são trocadas informações de *Link States*.

As interfaces OSPF reconhecem automaticamente (3) três tipos de Redes:

- Multiacesso com broadcast, como a Rede Ethernet;

- Multiacesso sem *broadcast* (NBMA), como a Rede *Frame Relay*;
- Redes ponto a ponto;
- Redes ponto a multiponto (configurada manualmente por um administrador).

Em uma Rede multiacesso, não se sabe antecipadamente quantos roteadores serão conectados dentro da área; já nas Redes ponto a ponto, somente dois roteadores podem ser conectados.

Em um segmento de Rede multiacesso com broadcast, muitos roteadores podem ser conectados. Se cada roteador estabelecesse a adjacência completa com todos os outros roteadores e trocasse informações de *Link State* com todos os vizinhos, haveria uma grande sobrecarga.

A solução para essa sobrecarga é eleger um Roteador Designado (DR), que ficará adjacente a todos os outros roteadores no segmento de *broadcast*.

Todos os outros roteadores do segmento enviam suas informações de *Link State* para o DR que, por sua vez, age como porta-voz ou ponto de encontro do segmento. E a função do DR é enviar informações de *Link State* para todos os outros roteadores do segmento usando o endereço de *multicast* 224.0.0.5 (CISCO NETACAD, 2017).

Apesar do ganho de eficiência fornecido pela eleição de um DR, há uma desvantagem. O DR representa um único ponto de falha. Elege-se, então, um segundo roteador como roteador designado de backup (BDR), para assumir as funções do DR caso ele venha a falhar. Para garantir que tanto o DR quanto o BDR verão os *Link States* enviados por todos os roteadores do segmento, usa-se o endereço de *multicast* de todos os roteadores designados, 224.0.0.6.

Já em Redes ponto a ponto, existem apenas dois nós, e não há motivo para a eleição de um DR e nem de um BDR, pois, em Redes ponto a ponto, ambos os roteadores se tornam completamente adjacentes um do outro (CISCO NETACAD, 2017).

## Configuração do OSPF

---

O Roteamento OSPF é um Protocolo hierárquico e utiliza o conceito de áreas. Cada roteador contém um Banco de Dados de *Link States* de uma área específica.

Uma área da Rede OSPF pode receber qualquer número de identificação de 0 a 65.535. Entretanto, uma única área recebe o número 0 e é conhecida como área 0 ou área de *backbone*. Em Redes OSPF com mais de uma área, todas as áreas precisam obrigatoriamente se conectar à área 0.

A configuração do OSPF requer que o Processo de Roteamento OSPF esteja ativado no roteador com os endereços de Rede e as Informações da Área especificados.

Os endereços de Rede são configurados com uma máscara curinga e não com uma máscara de Sub-rede. A máscara curinga representa os links ou endereços de

host que podem estar presentes nesse segmento. O ID da área pode ser escrito como um número inteiro ou em notação decimal com pontos (CISCO NETACAD, 2017).

Para ativar o Roteamento OSPF, use a sintaxe do comando de configuração global:

```
Router(config)# router ospf id-do-processo
```

O ID do Processo é um número utilizado para identificar um Processo de Roteamento OSPF no roteador.

Vários Processos OSPF podem ser iniciados no mesmo roteador e este número pode ser qualquer valor entre 1 e 65.535.

A maioria dos administradores de Rede mantém o mesmo ID de processo em todo um Sistema Autônomo, mas isso não é obrigatório.

Raramente, é necessário executar mais do que um processo OSPF em um roteador.

As Redes IP são anunciadas da seguinte forma no OSPF:

```
Router(config-router)#network endereço máscara-curinga área id-da-área
```

Cada Rede deve ser identificada com a área à qual pertence. O endereço de Rede pode ser uma Rede inteira, uma Sub-rede ou o endereço da interface.

A máscara curinga representa o conjunto de endereços de host que o segmento poderia suportar. Ela é diferente da máscara de Sub-rede, que é usada ao configurar endereços IP em interfaces (CISCO NETACAD, 2017).

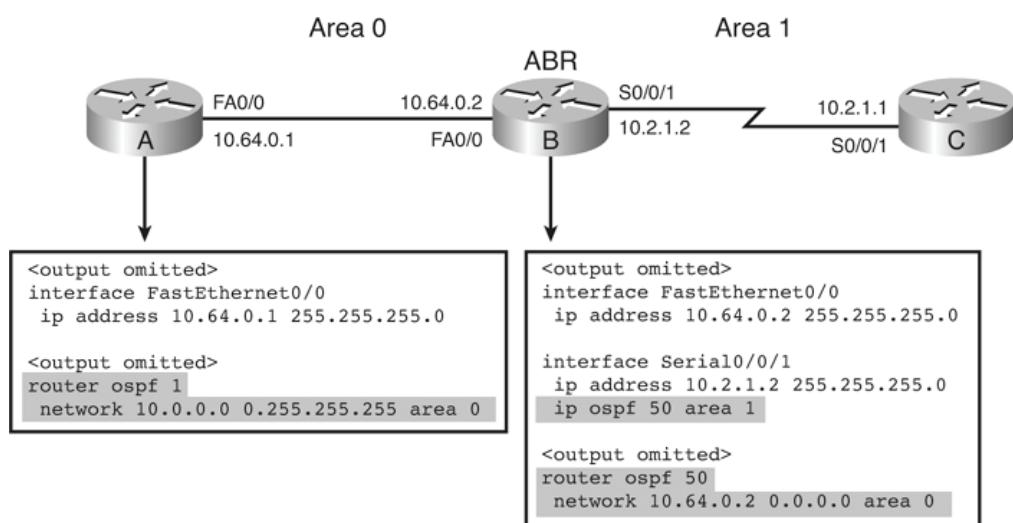


Figura 4 – Configuração do OSPF

## Identificação do OSPF

Quando o processo OSPF se inicia, o Sistema Operacional Cisco IOS utiliza o maior endereço IP local que esteja ativo como o ID base do roteador no processo OSPF.

Se não houver uma interface ativa, o processo OSPF não será inicializado; se a interface ativa ficar inoperante, o processo OSPF não tem um ID do roteador e, portanto, pára de funcionar até que a interface fique operante novamente.

Para garantir a estabilidade do Protocolo OSPF, deve haver uma interface ativa para o processo OSPF, o tempo todo. Uma interface de **loopback**, que é uma interface lógica, pode ser configurada para essa finalidade.

Quando se configura uma interface de **loopback**, o OSPF utiliza esse endereço como ID do roteador, independentemente do valor. Num roteador com mais de uma interface de **loopback**, o OSPF toma o maior endereço IP de loopback como o ID do roteador (CISCO NETACAD, 2017).

Para criar e atribuir um endereço IP a uma interface de loopback, use os seguintes comandos:

```
Router(config)# interface Loopback número
```

```
Router(config-if)#ip address endereço-IP máscara-de-Sub-rede
```

É considerada prática recomendável utilizar interfaces de loopback para todas as rotas que executem OSPF; elas devem ser configuradas com um endereço usando uma máscara de Sub-rede de 32 bits igual a 255.255.255.255.

Uma máscara de Sub-rede de 32 bits é chamada de máscara de host, pois a máscara de Sub-rede especifica uma Rede de um *host*.

Quando o OSPF recebe uma solicitação para anunciar uma Rede de *loopback*, ele sempre anuncia o *loopback* como uma rota de host com uma máscara de 32 bits (CISCO NETACAD, 2017).

Em Redes multiacesso com *broadcast*, pode haver mais de dois roteadores. O OSPF elege um Roteador Designado (DR) para ser o foco de todas as atualizações de *Link States* e de todos os anúncios de *Link States*. Como o papel do DR é crucial, elege-se um roteador designado de *backup* (BDR) para assumir se o DR falhar.

Se o tipo de Rede de uma interface for broadcast, a prioridade padrão do OSPF é 1. Quando as prioridades OSPF são iguais, a eleição do DR é decidida pelo ID do roteador; nesse caso, o roteador de maior ID é selecionado.

Outra forma de fazer com que o roteador se torne principal é em relação ao comando de prioridade. A interface que relata a maior prioridade para um roteador garante que ele se torne o DR. Essas prioridades podem ser definidas com qualquer valor entre 0 e 255.

Um valor 0 impede que um roteador seja eleito como DR e o contrário escolhe tal roteador como prioritário.

Um roteador com a prioridade OSPF mais alta será escolhido como DR e o roteador com a segunda prioridade OSPF mais alta será o nomeado como BDR.

Após o processo de eleição, o DR e o BDR retêm suas funções, mesmo se forem adicionados à Rede de roteadores com valores mais altos de prioridade OSPF.

Para modificar a prioridade OSPF, digite o comando de configuração da interface global “**ip ospf priority** número” em uma interface que esteja participando do **OSPF**.

O comando “**show ip ospf interface** tipo número” exibe o valor de prioridade da interface, assim como outras informações importantes.

Vamos, então, entender sua sintaxe.

## Propagação de Rota Default no OSPF

O Roteamento OSPF garante caminhos sem *loops* para todas as Redes do domínio. Para alcançar Redes fora do domínio, o OSPF precisa saber sobre a Rede ou precisa ter uma rota padrão/*default*.

Ter uma entrada para cada Rede do mundo exigiria enormes recursos de cada roteador. Uma alternativa prática é adicionar uma rota padrão até o roteador OSPF conectado à Rede externa. Essa rota pode ser redistribuída para cada roteador do AS por meio de atualizações OSPF normais.

Uma rota padrão configurada é utilizada por um roteador para gerar um *gateway* de último recurso. A sintaxe de configuração da rota padrão estática usa o endereço de Rede 0.0.0.0 e uma máscara de Sub-rede 0.0.0.0:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 (interface| próximo-salto endereço)
```

Essa rota é denominada “rota quad-zero” ou “rota de quatro zeros”, e qualquer endereço de Rede se encaixa na regra a seguir. O *gateway* da Rede é determinado pela operação AND entre o destino do pacote e a máscara de Sub-rede.

Para facilitar a propagação dessa rota padrão determinada, temos outro comando com tal finalidade, que seria:

```
Router(config-router)#default-information originate
```

Todos os roteadores da área aprenderão uma rota padrão após a aplicação desse comando, desde que a interface do roteador de borda até o *gateway* padrão esteja ativa (CISCO NETACAD, 2017).

## Verificação do OSPF

Todos os Protocolos de Roteamento possuem vários comandos de verificação, alguns deles, inclusive, parecidos.

Vamos, então, conhecer alguns comandos de verificação do OSPF:

- **show ip ospf interface;**
- **show ip ospf;**
- **show ip ospf neighbor detail;**
- **show ip ospf database.**

# Material Complementar

## Indicações para saber mais sobre os assuntos abordados nesta Unidade:



Livros

### Redes de Computadores e a Internet

STALLINGS, W. e ROSS K. **Redes de Computadores e a Internet.** 5<sup>a</sup> Ed. São Paulo: Editora Pearson, 2010.

### Redes de Computadores

ANENBAUM, A. S; WETHERALL, D. **Redes de Computadores.** 5<sup>a</sup> Ed. Rio de Janeiro: Editora Campus, 2011.



Leitura

### Curso WEB – Módulo de Roteamento e Switching

CISCO NETACAD – **Módulo de Roteamento e Switching** – Conceitos Essenciais – Capítulo 6 – Roteamento Estático, Versão 6.0, EUA, 2017.

<https://goo.gl/DAWJF1>

### Curso WEB – Módulo de Roteamento e Switching

CISCO NETACAD – **Módulo de Roteamento e Switching** – Conceitos Essenciais – Roteamento Dinâmico, Versão 6.0, EUA, 2017.

<https://goo.gl/DAWJF1>

## Referências

CISCO NETACAD. **Módulo de Roteamento e Switching: Conceitos Essenciais (CCNA2)**. 6<sup>a</sup> versão, Cisco Systems, 2017 (Material on-line). Disponível em [www.netacad.com](http://www.netacad.com). Acesso em: 27/09/2018.

STALLINGS, W. e ROSS K. **Redes de Computadores e a Internet**. 5<sup>a</sup> Ed. São Paulo: Editora Pearson, 2010.

TANENBAUM, A. S; WETHERALL, D. **Redes de Computadores**. 5<sup>a</sup> Ed. Rio de Janeiro: Editora Campus, 2011.





**Cruzeiro do Sul**  
Educacional

# Tecnologias de Roteamento



Cruzeiro do Sul Virtual  
Educação a distância



# Material Teórico



Protocolos de Roteamento Dinâmico Híbrido e EGP

**Responsável pelo Conteúdo:**

Prof. Esp. Antonio Eduardo Marques da Silva

**Revisão Textual:**

Prof.<sup>a</sup> Dr.<sup>a</sup> Selma Aparecida Cesarin



# UNIDADE

## Protocolos de Roteamento Dinâmico Híbrido e EGP



- Introdução;
- Comparando Protocolos Proprietários da Cisco: IGRP e EIGRP;
- BGP.



### OBJETIVO DE APRENDIZADO

- Compreender e abordar os Protocolos de Roteamento Internos (IGPs) da Cisco, como o IGRP e o EIGRP, suas principais características e diferenças, conceitos e configuração do Protocolo EIGRP e conhecimento dos Protocolos de Roteamento externos (EGP), como o BGP, que é considerado o Protocolo de Roteamento da Internet.





# Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:

Determine um horário fixo para estudar.

Mantenha o foco! Evite se distrair com as redes sociais.

Procure manter contato com seus colegas e tutores para trocar ideias! Isso amplia a aprendizagem.

Seja original! Nunca plágie trabalhos.

Aproveite as indicações de Material Complementar.

Conserve seu material e local de estudos sempre organizados.

Não se esqueça de se alimentar e de se manter hidratado.

## Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu “momento do estudo”;
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

# Introdução

Nesta Unidade, vamos tratar de um Protocolo proprietário da Cisco, que é aplicado como um Protocolo do tipo IGP; depois, trataremos da comparação entre os IGPs e os EGPs e, por fim, uma base teórica do Protocolo EGP, mais conhecido como BGP.

## Comparando Protocolos Proprietários da Cisco: IGRP e EIGRP

A Cisco lançou o Protocolo de Roteamento EIGRP, em 1994, como uma versão melhorada e escalável do seu Protocolo de Roteamento de Vetor de Distância antecessor, o IGRP.

Apesar de o EIGRP ser considerado um Protocolo de Roteamento Híbrido, a Tecnologia de Vetor Distância e as informações de distâncias utilizadas pelo IGRP são usadas, também, pelo EIGRP (CISCO NETACAD, 2017).

O EIGRP tem propriedades de convergência bem melhoradas e opera com mais eficiência se comparado ao IGRP. As comparações entre o EIGRP e o IGRP podem ser apresentadas nas seguintes categorias principais:

- Modo de compatibilidade;
- Contagem de saltos;
- Cálculo da métrica;
- Redistribuição automática de Protocolos.

Além de irmãos criados por um mesmo fabricante, o IGRP e o EIGRP são compatíveis um com o outro, o que proporciona interoperabilidade transparente entre roteadores que utilizam IGRP.

Isso se torna importante porque os usuários podem valer-se das vantagens de ambos os Protocolos; porém, o EIGRP oferece suporte de vários Protocolos de Rede, mas o IGRP não.

Tanto o EIGRP como o IGRP calculam suas métricas de forma semelhante. O EIGRP multiplica a métrica do IGRP por um fator de 256, isso ocorre porque o EIGRP utiliza uma métrica de 32 bits e o IGRP utiliza uma métrica de 24 bits de tamanho.

Nesse caso, o EIGRP pode multiplicar ou dividir por 256 para, facilmente, trocar informações com o IGRP e obter métricas compatíveis com ambos os Protocolos (CISCO NETACAD, 2017).

O IGRP é um Protocolo de Vetor Distância clássico e tem contagem máxima de saltos de 255. Já o EIGRP tem limite máximo de contagem de saltos de 224. Apesar de menor, é mais do que suficiente para suportar Redes de grande porte projetadas (CISCO NETACAD, 2017).

Para permitir que Protocolos de Roteamento Dinâmico tão diferentes como o OSPF e o RIP compartilhem informações, é necessário que se faça uma configuração avançada, conhecida como redistribuição de rotas.

A redistribuição ou o compartilhamento de rotas é um Processo automático depois de configurado nos roteadores entre o IGRP e o EIGRP, contanto que ambos os Processos usem o mesmo número de Sistema Autônomo (AS).

O EIGRP marca como externas as rotas aprendidas por IGRP ou vindas de qualquer outra fonte de Roteamento externa porque essas rotas não são oriundas de roteadores que utilizam o EIGRP.

Já o IGRP é mais antigo e não pode diferenciar rotas internas e externas. Uma vez aplicado o comando *show ip route* para os roteadores, as rotas EIGRP são marcadas com D e as rotas externas são identificadas por EX (CISCO NETACAD, 2017).

## Conceitos do EIGRP

---

Os roteadores que utilizam o EIGRP mantêm informações sobre rotas e topologia de Rede prontamente disponíveis em RAM para que possam reagir rapidamente às eventuais mudanças. Como o OSPF, o EIGRP guarda essas informações em várias outras Tabelas de Apoio, como uma Tabela de Bancos de Dados.

O EIGRP guarda rotas aprendidas de maneira específica. Essas rotas recebem um determinado *status* e podem ser marcadas para fornecer outras informações úteis.

Podemos identificar as seguintes três Tabelas mantidas pelo EIGRP:

- Tabela de Vizinhos/Vizinhança;
- Tabela de Topologia;
- Tabela de Roteamento.

A Tabela de Vizinhança é uma das Tabelas mais importantes do EIGRP, pois cada roteador EIGRP mantém uma lista os roteadores adjacentemente aprendidos.

Essa Tabela é comparável ao Banco de Dados de adjacências utilizado pelo OSPF, sendo que existe uma Tabela de Vizinhos para cada Protocolo suportado pelo EIGRP.

Quando novos vizinhos são descobertos, o endereço e a interface do vizinho são registrados nessa Tabela; tais informações são armazenadas na estrutura de dados referente ao vizinho.

Quando um vizinho envia um pacote de *hello*, ele anuncia um *hold time* (tempo de retenção), que é o período de tempo em que um roteador trata um vizinho como operacionalmente alcançável.

Se um pacote de *hello* não for recebido dentro do *hold time* limite, esse *hold time* se expirará. Ao acontecer isso, o algoritmo DUAL – *Diffusing Update Algorithm*, que é o algoritmo de Vetor de Distância do EIGRP, recebe notificações da mudança na topologia e precisa recalcular essa nova topologia de Rede.

A Tabela de topologia consiste em todas as Tabelas de rotas do EIGRP dentro de um Sistema autônomo. O DUAL utiliza essas informações fornecidas pela Tabela de Vizinhos e pela Tabela de Topologia e calcula as rotas de menor custo para cada destino.

O EIGRP mantém essas informações de modo que os roteadores que utilizam esse Protocolo possam identificar e realizar comutação de rotas mais rapidamente.

As informações que o roteador aprende do DUAL são utilizadas para determinar a rota sucessora (*successor route*), que é o termo utilizado para identificar a rota primária ou a melhor rota definida. Essas informações também são inseridas na Tabela de Topologia, ou seja, todas as rotas aprendidas para cada destino no EIGRP são mantidas na Tabela de Topologia (CISCO NETACAD, 2017).

Os campos da Tabela de Topologia são os seguintes:

- **Feasible Distance (FD)** – É a menor métrica calculada pelo algoritmo para cada Rede destino;
- **RouteSource (RS)** – Número de identificação do roteador que originalmente anunciou essa rota. Esse campo só está preenchido em rotas externas à Rede EIGRP. O *route tagging* (etiqueta do roteador) pode ser útil quando for utilizando Roteamento baseado em diretivas;
- **Reported Distance (RD)** – Distância relatada por um vizinho adjacente para um determinado destino específico;
- **Interface Information** – Interface através da qual o destino pode ser alcançado dentro da *internetworking*;
- **Route Status** – Status de uma rota. As rotas são identificadas como passivas – significa que a rota é estável e pronta para ser utilizada, ou ativa – significa que a rota está em Processo de ser recomputada pelo algoritmo DUAL;
- **RouteTable** – A Tabela de Roteamento do EIGRP contém as melhores rotas até cada destino de Rede. Essas informações são geradas a partir da Tabela de Topologia e da Tabela de Vizinhança. Os roteadores que utilizam o EIGRP mantêm uma Tabela de Roteamento para cada Protocolo de Rede devidamente configurado;
- **Successor Route (SR)** – É uma rota selecionada como rota primária para alcançar um destino de Rede. O algoritmo DUAL identifica essa rota a partir das informações contidas nas Tabelas de vizinhos e de topologia e as coloca na

Tabela de Roteamento. Podem existir até quatro *successor routes* para qualquer destino determinado. Elas podem ser de custo igual ou desigual e são identificadas como os melhores caminhos livres de *loops* até uma Rede de destino;

- **Feasible Successor (FS)** – É uma rota de reserva, identificada ao mesmo tempo em que as *successor routes*; porém, essas rotas só ficam armazenadas na Tabela de Topologia, na qual podem ser retidas várias *feasible successors* para um determinado destino; porém, isso não é mandatório.

Nesse caso, um roteador enxerga as *feasible successors* como rotas de próximos vizinhos, ou seja, mais perto do destino do que dele mesmo. O custo de uma *feasible successor* é computado de acordo com o custo anunciado pelo roteador vizinho até a sua Rede destino.

Se uma *successor route* se tornar inativa, o roteador procurará uma *feasible successor* já identificada pelo algoritmo e essa rota será promovida ao *status* de *successor route*.

Uma *feasible successor* precisa ter um custo anunciado inferior ao custo atual da *successor route* até a determinada Rede destino.

Se uma *feasible successor* não for identificada a partir das informações atuais, o roteador colocará a rota com o *status* ativo e enviará pacotes de solicitação para todos os vizinhos, a fim de computar a topologia atualmente descrita.

O roteador pode identificar qualquer nova *successor route* ou *feasible successor* dentre os novos dados recebidos nos pacotes de resposta (*Reply*) relativos às solicitações realizadas pelo Processo de Roteamento. O roteador, então, irá colocar um *status* passivo na rota.

A Tabela de Topologia pode registrar informações adicionais sobre cada rota. Com isso, o EIGRP classifica as rotas como internas ou externas e, nesse caso, acrescenta um *routetag* (etiqueta) em cada rota para identificar sua classificação.

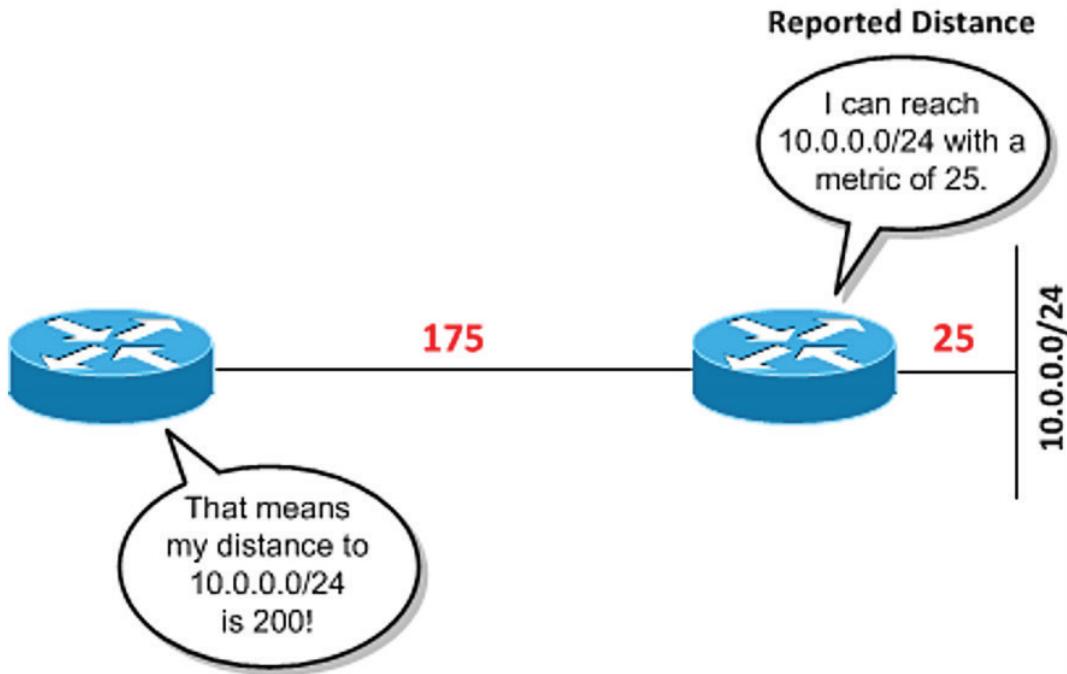
As rotas internas se originam dentro do Sistema Autônomo definido no EIGRP. Já as rotas externas se originam externamente ao Sistema Autônomo do EIGRP.

As rotas aprendidas ou redistribuídas de outros Protocolos de Roteamento tais como o RIPv1, o RIPv2, o OSPF e o IGRP, são definidas como externas.

As rotas estáticas que se originam fora do Sistema Autônomo do EIGRP são também consideradas rotas externas. O *routetag* (etiqueta do roteador) pode ser configurado como número entre 0 e 255 (CISCO NETACAD, 2017).



Funcionamiento del Protocolo EIGRP (Espanhol). Acesse: <https://youtu.be/LfzllLq7hK8>.

Figura 1 – *Feasible Successor (FS)* do EIGRP

Fonte: packetlife.net

## Características do EIGRP

O Protocolo de Roteamento EIGRP opera de forma diferente do Protocolo de Roteamento IGRP.

O EIGRP é um Protocolo avançado de Vetor de Distância, mas também age como Protocolo *Link State* na maneira como atualiza os vizinhos e também como mantém informações de Roteamento em Tabela Topológica.

Essa mesclagem de funcionalidade o fez ser conhecido como Protocolo híbrido; porém, essa classificação é mais utilizada pela Cisco.

A seguir, são apresentadas algumas vantagens do EIGRP sobre os Protocolos de Vetor Distância mais simples, como o RIP e o IGRP:

- Suporte para VLSM e CIDR;
- Convergência rápida;
- Utilização eficiente da largura de banda;
- Não depende dos Protocolos roteados;
- Suporte para várias camadas de Rede.

Os PDMs – *Protocol-Dependent Modules*, protegem o Protocolo EIGRP contra revisões muito longas. A evolução de Protocolos roteados, como o IPv4, poderão exigir um novo módulo de Protocolo, mas não necessariamente uma revisão do EIGRP será necessária.

Os roteadores que utilizam o Protocolo de Roteamento Dinâmico EIGRP têm convergência rápida porque se valem do algoritmo DUAL, que garante uma operação livre de *loops* durante uma computação de rota que permita que todos os roteadores envolvidos numa mudança de topologia façam a sincronização, simultaneamente.

O EIGRP envia atualizações parciais e limitadas, utilizando eficientemente a largura de banda da Rede, pois os roteadores que utilizam esse Protocolo de Roteamento não enviam as Tabelas inteiras (como o RIP), mas sim, enviam atualizações parciais e incrementais.

Essa operação é semelhante à forma de atualização do OSPF, exceto que os roteadores que utilizam o EIGRP enviam essas atualizações parciais somente aos roteadores que precisam de fato das informações, e não a todos os roteadores dentro de uma área.

Por esse motivo, são denominadas atualizações limitadas, em lugar de atualizações de Roteamento temporizadas.

Os roteadores que utilizam o EIGRP utilizam pequenos pacotes de *hello* para manter o contato entre si e é importante lembrar-se de que, apesar de trocados regularmente, os pacotes de *hello* não ocupam grande quantidade de largura de banda nas interfaces ativas interconectadas (CISCO NETACAD, 2017).

Como dito, o EIGRP suporta vários Protocolos roteados, como, por exemplo o IP, IPX e o AppleTalk através das PDMs.

O EIGRP pode redistribuir informações IPX/RIP e IPX/SAP e outras, de forma a melhorar o desempenho geral da Rede.

## Terminologias do EIGRP

---

Algumas das novas tecnologias foram introduzidas no EIGRP e representam melhoria significativa na eficiência de operação, na velocidade de convergência e na funcionalidade do EIGRP se comparado ao IGRP ou outros Protocolos de Roteamento existentes.

Essas tecnologias se enquadram em uma das seguintes quatro categorias:

- Descoberta e recuperação de vizinhos;
- Módulos dependentes do Protocolo;
- Algoritmo DUAL que usa uma máquina de estado finito;
- Protocolo de Transporte Confiável.

Os roteadores que utilizam os Protocolos de Vetor Distância simples não estabelecem relacionamento com seus roteadores vizinhos; já os roteadores que utilizam o EIGRP ativamente estabelecem relações de vizinhança, de maneira muito parecida com os roteadores que utilizam o Protocolo OSPF.

Os pacotes de *hello* no EIGRP são enviados por padrão em tempos de cinco em cinco segundos, que indicam viabilidade (estado ativo) ou inviabilidade (estado passivo) entre vizinhos, a fim de formar adjacências.

Quando os roteadores que utilizam o EIGRP formam adjacências, é possível:

- Aprender dinamicamente novas rotas que se juntam à Rede;
- Descobrir novamente roteadores que antes eram inalcançáveis;
- Identificar roteadores que se tornam inalcançáveis ou inoperantes.

O RTP – *Reliable Transport Protocol* é um Protocolo da camada 4 do modelo OSI (camada de transporte), que garante a entrega de pacotes EIGRP para todos os seus vizinhos.

Em uma Rede IP, os *hosts* usam TCP para numerar e sequenciar os pacotes, assegurando sua pronta entrega aos destinatários. No entanto, o EIGRP é independente de Protocolo, ou seja, isso significa que ele não depende do suíte de Protocolos do TCP/IP para trocar informações de Roteamento, como é o caso do RIPv1, RIPv2, IGRP e do OSPF.

Para manter essa independência do TCP, o EIGRP utiliza o RTP como seu Protocolo proprietário de camada de transporte, a fim de garantir a entrega de informações de Roteamento confiáveis.

O EIGRP pode valer-se do RTP para providenciar serviços confiáveis ou não confiáveis, conforme as exigências da situação em que está contido. Com o RTP, o EIGRP pode enviar *multicast* ou *unicast* simultaneamente para diferentes pares de roteadores.

Isso permite eficiência máxima do Protocolo. Outro ponto forte a citar sobre o EIGRP é o seu algoritmo DUAL, que é um mecanismo de cálculo de rotas eficiente. O nome completo dessa tecnologia é *DUAL Finite State Machine (FSM)*. Uma FSM é uma máquina de estados finitos e definem um conjunto de possíveis estados, pelos quais algo pode passar.

A FSM do DUAL contém toda a lógica matemática utilizada para calcular e comparar rotas numa Rede EIGRP e também garante que cada caminho esteja livre de *loops*.

As informações de rotas na Tabela de Vizinhos e na Tabela de Topologia fornecem ao DUAL informações abrangentes sobre rotas por ocasião de algum distúrbio da Rede. Ele utiliza essas informações para que rapidamente possa selecionar rotas alternativas, caso um *link* seja desativado (CISCO NETACAD, 2017).

Uma das melhores características do EIGRP é seu Projeto modular ou em camadas, pois são comprovadamente mais escaláveis e adaptáveis que outros métodos singulares.

O suporte para Protocolos roteados, tais como IP, IPX e *AppleTalk* é incluído no EIGRP através de PDMs, a fim de se ter fácil adaptação a novos Protocolos, como é o caso do surgimento do IPv6.

Cada PDM é responsável por todas as funções relacionadas ao seu Protocolo roteado específico. O módulo IP-EIGRP é responsável pelas seguintes funções:

- Enviar e receber pacotes EIGRP que contêm dados IP;
- Notificar o DUAL sobre novas informações de Roteamento recebidas;
- Manter os resultados de decisões de Roteamento do DUAL na Tabela de Roteamento IP;
- Redistribuir informações de Roteamento que foram aprendidas por outros Protocolos de Roteamento compatíveis com IP.

## Estrutura do EIGRP

---

Como o Protocolo OSPF, o EIGRP se vale de diferentes tipos de pacotes para manter suas Tabelas de apoio e estabelecimento e relações com roteadores vizinhos.

São cinco os tipos de pacotes utilizados pelo EIGRP:

- *Hello*;
- *Update*;
- *Query*;
- *Reply*;
- *Acknowledgment*.

O EIGRP depende dos pacotes de *hello* para descobrir, verificar e redescobrir roteadores vizinhos. Esses pacotes de *hello* têm intervalo fixo, mas possivelmente configurável pelo administrador de Rede, denominado intervalo de *hello*.

O intervalo de *hello* padrão depende da largura de banda da interface utilizada para a definição de um alcance de rota. Nas Redes IP, os roteadores que utilizam o EIGRP enviam pacotes de *hello* ao endereço IP de multicast 224.0.0.10.

Essas informações de pacotes *hello* são armazenadas na Tabela de vizinhos, que inclui o campo *Sequence Number* (*Seq No*) para registrar o número do último pacote EIGRP recebido de cada vizinho.

A Tabela de vizinhos também inclui um campo *Hold Time* que registra a hora em que foi recebido o último pacote por uma determinada interface. Os pacotes devem ser recebidos dentro do intervalo de *Hold Time* para manter um estado passivo. O estado passivo representa um *status* de alcançável e operacional.

Se o EIGRP não receber um pacote de *hello* de um vizinho dentro do *hold time*, ele considerará aquele vizinho inativo. O algoritmo DUAL, então, entra em cena para reavaliar a forma como a Tabela de Roteamento está construída. Por *default*, o tempo de *hold time* é três vezes o intervalo de *hello*.

No Protocolo OSPF, há uma exigência de que os roteadores vizinhos tenham os mesmos intervalos de *hello* e *dead interval* para se comunicarem.

No caso do EIGRP, essa tal restrição é ignorada, ou seja, os roteadores vizinhos aprendem sobre cada um por meio da troca de pacotes de *hello*; em seguida, utilizam essas informações para formar uma relação estável, independentemente dos temporizadores desiguais. Os pacotes de *hello* são sempre enviados como não confiáveis, o que significa que nenhuma confirmação é transmitida (CISCO NETACAD, 2017).

Para isso, os roteadores que utilizam o EIGRP usam pacotes de confirmação (*Acknowledgment*) para indicar o recebimento de qualquer pacote EIGRP durante uma troca confiável.

O RTP, por exemplo, provê a comunicação confiável entre *hosts* do EIGRP. E, nesse caos, uma mensagem recebida de um *host* de origem precisa ser confirmada pelo destino para que possa ser considerada confiável.

Os pacotes de confirmação (*Acknowledgment*), que são um tipo de pacotes de *hello* sem informações, são utilizados para tal finalidade.

Diferentemente dos *hellos multicast*, os pacotes de confirmação (*Acknowledgment*) são do tipo *unicast* (de *host* para *host*). Confirmações podem ser anexadas a outros tipos de pacotes EIGRP, tais como pacotes de resposta (*Reply*).

Os pacotes de atualização (*Update*) são utilizados quando um roteador descobre um novo vizinho. Esses tipos de pacotes também são enviados em *unicast* a aquele novo vizinho para que ele possa ser adicionado à sua Tabela Topológica. No entanto, poderá ser necessário enviar mais de um pacote de atualização (*Update*) para comunicar todas as informações de topologia ao vizinho recém-descoberto.

Os pacotes de atualização (*Update*) também são utilizados quando um roteador detecta uma eventual mudança na topologia de Rede. Quando isso acontece, o roteador EIGRP envia um pacote de atualização (*Update*) em *multicast* a todos os seus vizinhos, alertando-os sobre a eventual mudança de estado. Esses pacotes de atualização (*Update*) são enviados como pacotes confiáveis (CISCO NETACAD, 2017).

Um roteador EIGRP utiliza pacotes de consulta (*Query*) sempre que necessite de alguma informação específica de um ou de todos os seus roteadores vizinhos. Já os pacotes de resposta (*Reply*) são utilizados para responder uma consulta.

Caso um roteador de uma topologia EIGRP perca o seu sucessor e não puder encontrar um *feasible successor* para uma rota de Rede, o algoritmo DUAL coloca essa rota no estado ativo.

Depois disso é enviada em *multicast* uma consulta a todos os vizinhos, na tentativa de localizar uma rota sucessora até a Rede de destino calculada.

Os vizinhos precisam enviar, então, respostas que proporcionem informações sobre sucessores ou que indiquem indisponibilidade de informações sobre as rotas.

As consultas podem ser em *multicast* ou *unicast*, mas as respostas sempre são em *unicast* nesse Processo de Roteamento.

## Configurando o EIGRP

Apesar da complexidade do Protocolo EIGRP e seu algoritmo DUAL, sua configuração pode ser relativamente simples. Os comandos de configuração do EIGRP variam conforme o Protocolo roteado a ser utilizado na topologia.

Respeite as seguintes etapas para configurar o EIGRP usando o Protocolo Roteado IP do suíte de Protocolos do TCP/IP:

1. Use o seguinte comando para ativar o Processo de Roteamento EIGRP e definir o Sistema Autônomo (AS):

```
router(config)# router eigrp autonomous-system-number
```

O *autonomous-system-number* é utilizado para identificar todos os roteadores dentro dessa grande área chamada de AS. Esse valor precisa ser igual para todos os roteadores pertencentes a uma determinada Rede, ou seja, a um determinado AS;

2. Indique quais Redes pertencem ao Sistema Autônomo do EIGRP no roteador local através do seguinte comando:

```
router(config-router)#network network-number
```

O *network-number* é o número da Rede que determina quais interfaces do roteador estão participando do Processo de Roteamento EIGRP e quais Redes são anunciadas por esse roteador. Já o comando *network* configura somente as Redes diretamente conectadas;

3. Ao configurar *links* seriais usando o EIGRP, é importante configurar o parâmetro de largura de Banda (*Bandwidth*) na interface. Se a largura de Banda para essas interfaces não for modificada, o EIGRP assume a largura de Banda padrão no *link*, ao invés da largura de Banda verdadeira. É possível fazer isso com o comando:

```
router(config-if)#bandwidth kbps
```

O comando *bandwidth* é utilizado somente pelo Processo de Roteamento e deve ser definido para corresponder à velocidade da linha da interface realmente utilizada. O Processo de Roteamento não tem essa capacidade de identificação de BW automaticamente;

4. Também é recomendado adicionar o seguinte comando a todas as configurações do EIGRP:

```
router(config-if)#eigrp log-neighbor-changes
```

Esse comando possibilita a criação de um registro de mudanças de adjacências para monitorar a estabilidade do Sistema de Roteamento e, assim, auxiliar na detecção de eventuais correções de problemas.

## Sumarização no EIGRP

O Processo de Roteamento EIGRP faz automaticamente a summarização das rotas no limite *classful*, ou seja, ele anunciará as rotas aprendidas (mesmo que subnetadas) de forma original.

Na maioria dos casos, a summarização automática é vantajosa porque mantém as Tabelas de Roteamento compactas, o que faz com que o processamento de CPU do roteador seja minimizado.

No entanto, a summarização automática poderá não ser uma opção preferida em alguns casos. Por exemplo, caso haja sub-Redes não contíguas, a summarização automática precisa ser desativada para que a operação de Roteamento seja realizada com sucesso.

Para desativar a summarização automática, utilize o seguinte comando do IOS:

```
router(config-router)#no auto-summary
```

Caso seja necessário, um endereço para summarização pode ser manualmente configurado pela configuração de uma Rede de prefixo.

Rotas summarizadas manualmente são configuradas em cada interface e não globalmente, de modo que a interface que irá propagar a summarização das rotas necessita ser selecionada primeiro, com o comando de interface para poder acessá-la.

Depois, o endereço para summarização poderá ser definido com o comando:

```
router(config-if)#ip summary-address eigrp autonomous-system-number ip-address mask administrative-distance
```

As rotas de sumarização EIGRP têm distância administrativa de peso 5 por padrão. Opcionalmente, podem ser configuradas à vontade do administrador de Rede, com um valor entre 1 e 255.

## Verificando o EIGRP

---

Como todos os Protocolos de Roteamento Dinâmico, o EIGRP possui vários comandos de verificação.

Alguns deles são:

- *router# show ip eigrp neighbors;*
- *router# show ip eigrp interfaces;*
- *router# show ip eigrp topology;*
- *router# show ip eigrp topology all links;*
- *router# show ip eigrp traffic.*

E há muitos outros, inclusive, alguns que utilizam qualificadores diferentes.

Sugerimos que você aplique tais comandos após uma configuração modelo, que pode ser realizada pelo simulador *packet tracer* da Cisco.

## BGP

O BGP (*Border Gateway Protocol*) é um Protocolo que gerencia como os Pacotes de DADOS são roteados pela *Internet* por meio da troca de informações de Roteamento e alcançabilidade entre os roteadores de borda.

O BGP dirige pacotes entre Sistemas Autônomos (AS) – Redes gerenciadas por uma única empresa ou provedor de serviços.

O tráfego que é roteado dentro de uma única Rede é chamado de BGP interno ou iBGP. Mais frequentemente, o BGP é usado para conectar um AS a outros Sistemas Autônomos e é, então, referido como um BGP externo, ou eBGP (TANENBAUM, 2011).

## Para Que Serve o BGP?

---

O BGP oferece estabilidade de Rede que garante que os roteadores possam se adaptar rapidamente para enviar pacotes por meio de outra reconexão se um dos caminhos da *Internet* cair.

O BGP toma decisões de Roteamento com base em caminhos, regras ou políticas de Rede configuradas por um administrador de Rede.

Cada roteador BGP mantém uma Tabela de Roteamento padrão utilizada para direcionar pacotes em trânsito. Essa Tabela é usada em conjunto com uma Tabela de Roteamento separada, conhecida como base de Informações de Roteamento (*RIB*), que é uma Tabela de dados armazenada no roteador que roda o BGP.

A Tabela RIB contém informações de rota de pares externos conectados diretamente, bem como de pares internos, e atualiza continuamente a Tabela de Roteamento à medida que ocorrem alterações de topologia (STALLINGS; ROSS, 2010).



Como funciona a *Internet*? Parte 1 – O Protocolo IP. Acesse: <https://youtu.be/HNQD0qJOTC4>.

## Noções Básicas de Roteamento do BGP

O BGP envia informações atualizadas da Tabela do roteador apenas quando algo se altera; mesmo assim, envia apenas as informações afetadas.

Esse Protocolo não possui mecanismo de detecção automática, o que significa que as conexões entre os pares precisam ser configuradas manualmente, com endereços de pares programados em ambas as extremidades.

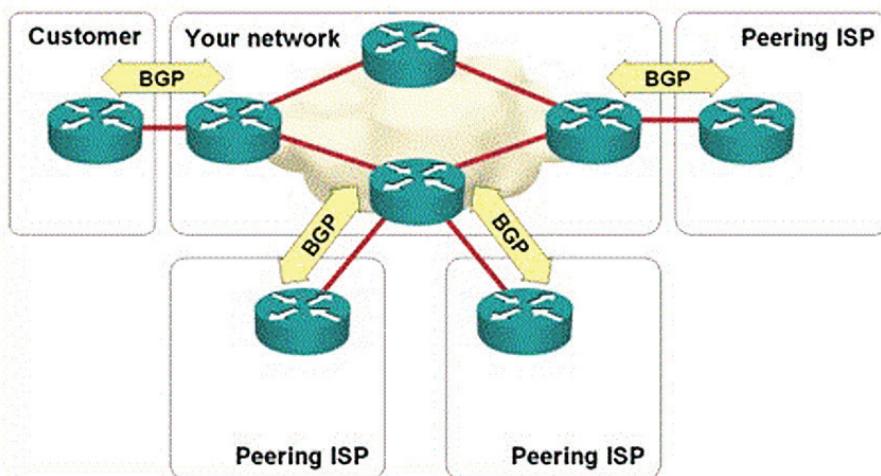


Figura 2 – Utilização de BGP

Fonte: searchtelecom.techtarget.com

O BGP toma, então, decisões sobre o melhor caminho, com base na acessibilidade atual, na contagem de saltos e em outras características do caminho.

Em situações em que vários caminhos estão disponíveis, o BGP pode ser utilizado para comunicar as próprias preferências de uma organização em termos de qual caminho o tráfego deve seguir para dentro e para fora de suas Redes.

O BGP tem até um mecanismo para definir tags arbitrárias, chamadas comunidades, que podem ser utilizadas para controlar o comportamento de propagação de rotas por acordo mútuo entre pares (TANENBAUM, 2011).

Ratificado em 2006, o BGP-4, a versão atual do BGP, suporta o IPv6 e o Roteamento interdomínio sem classe (CIDR), que permite a viabilidade contínua do IPv4.

O uso do CIDR é uma maneira de ter mais endereços dentro da Rede do que com o esquema de atribuição de endereço IP atual (sumarização de rotas).

## Introdução do BGP

A melhor definição que poderíamos ter em relação ao BGP é exatamente considerá-lo o Protocolo de Roteamento que faz a *Internet* funcionar corretamente.

Como a alocação de endereços na *Internet* não é nem de longe tão hierárquica se comparada ao Plano de Discagem por Telefone (DDD), a maioria dos roteadores nas Redes centralizadas dos provedores de serviços precisam trocar informações sobre várias centenas de milhares de prefixos IP.

O BGP é capaz de realizar essa tarefa, apresentando sua competência como sendo um Protocolo de Roteamento Dinâmico altamente escalável.

As informações de Roteamento do *Border Gateway Protocol* geralmente são trocadas entre entidades comerciais concorrentes, como ISPs – *Internet Service Providers* (Provedores de Serviços de *Internet*) num ambiente aberto e hostil (*Internet* pública).

Por esse motivo o BGP, é muito focado em segurança (por exemplo, todos os roteadores adjacentes precisam ser configurados manualmente) e as implementações do BGP fornecem um rico conjunto de filtros de rotas para permitir que os ISPs defendam suas Redes e controlem os seus anúncios de rotas (STALLINGS; ROSS, 2010).



Como funciona a *Internet*? Parte 2 – Sistemas Autônomos, BGP, PTTs.  
Acesse: [https://youtu.be/C5qNAT\\_j63M](https://youtu.be/C5qNAT_j63M).

Na terminologia do BGP, um domínio de Roteamento independente (que quase sempre significa um ISP) é chamado de Sistema Autônomo, que possui uma administração comum.

O BGP é sempre utilizado como o Protocolo de Roteamento escolhido entre os ISPs (BGP externos), mas também, como o principal Protocolo de Roteamento dentro de grandes Redes ISP (BGP interno), ou seja, alguns Protocols do tipo IGP utilizam o BGP também como meio de transporte de rotas.

Todos os outros Protocols de Roteamento estão preocupados apenas em encontrar o caminho ideal para todos os destinos conhecidos. O BGP não pode adotar essa abordagem simplista porque os acordos de *peering* entre ISPs quase sempre resultam em políticas complexas de Roteamento. Por esse motivo, para

ajudar os operadores de Rede a implementar essas Políticas, o BGP carrega um grande número de atributos com cada prefixo de IP, por exemplo:

- **AS path** – Caminho completo que documenta quais Sistemas Autônomos um pacote teria de percorrer para chegar ao destino;
- **Local preference** – “Custo interno” de um destino, usado para garantir a consistência em todo o AS;
- **Multi-exitdiscriminator** – Esse atributo dá aos ISPs adjacentes a capacidade de preferir um ponto de *peering* em detrimento de outro;
- **Communities** – Um conjunto de *tags* genéricas que podem ser usadas para sinalizar várias políticas administrativas entre roteadores BGP.

Como o foco do *design* e implementação do BGP sempre foi a segurança e a escalabilidade, é mais difícil configurar do que outros Protocolos de Roteamento, por causa da sua complexidade (mas, quando você começa a configurar várias políticas de Roteamento).

Como apoio, um Protocolo de Roteamento interno (na maioria das vezes, OSPF ou IS-IS) é usado para obter convergência rápida para rotas internas (incluindo endereços IP de roteadores BGP).

Devido à complexidade inherente do BGP, os clientes e pequenos ISPs implantariam o BGP somente onde é necessário, por exemplo, em pontos de *peering* e um subconjunto mínimo de roteadores principais (aqueles entre os pontos de *peering*), conforme apresentado na Figura a seguir.

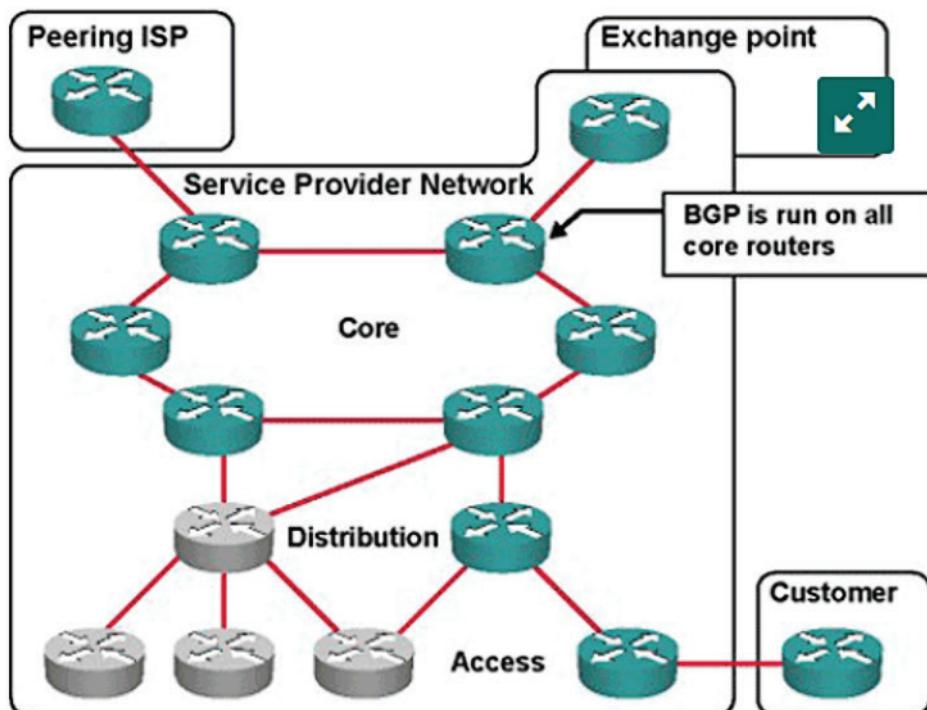


Figura 3 – Complexidade do BGP

Fonte: [searchtelecom.techtarget.com](http://searchtelecom.techtarget.com)

O BGP requer uma malha completa de sessões BGP internas (sessões entre roteadores no mesmo Sistema Autônomo). Você pode usar refletores de rota BGP ou confederações BGP para tornar sua Rede escalável.

Há também outra excelente razão pela qual se deseja implantar o BGP numa grande Rede: é um serviço de Rede inovador, pois é muito utilizado em Rede Privadas Virtuais (VPNs) baseadas em MPLS (que é um Protocolo de comutação em camada 2 que usa *tags* e muito rápido), implantações de qualidade de serviço em grande escala e outros recursos escaláveis (TANENBAUM, 2011).

# Material Complementar

## Indicações para saber mais sobre os assuntos abordados nesta Unidade:



Livros

### **Redes de Computadores e a Internet**

STALLINGS, W. e ROSS K. **Redes de Computadores e a Internet.** 5<sup>a</sup> Ed. São Paulo: Editora Pearson, 2010.

### **Redes de Computadores**

TANENBAUM, A. S; WETHERALL, D. **Redes de Computadores.** 5<sup>a</sup> Ed. Rio de Janeiro: Editora Campus, 2011.

### **Módulo de Roteamento e Switching**

CISCO NETACAD – **Módulo de Roteamento e Switching** – Conceitos Essenciais – Capítulo 6– Roteamento Estático, Versão 6.0, EUA, 2017;

### **Módulo de Roteamento e Switching**

CISCO NETACAD – **Módulo de Roteamento e Switching** – Conceitos Essenciais – Roteamento Dinâmico, Versão 6.0, EUA, 2017.

# Referências

CISCO NETACAD. **Módulo de Roteamento e Switching**: Conceitos Essenciais (CCNA2). 6<sup>a</sup> versão, Cisco Systems, 2017 (Material *on-line*). Disponível em: [www.netacad.com](http://www.netacad.com). Acesso em: 30/09/2018.

STALLINGS, W. e ROSS K. **Redes de Computadores e a Internet**. 5<sup>a</sup> Ed. São Paulo: Editora Pearson, 2010.

TANENBAUM, A. S; WETHERALL, D. **Redes de Computadores**. 5<sup>a</sup> Ed. Rio de Janeiro: Editora Campus, 2011.



**Cruzeiro do Sul**  
Educacional

# Tecnologias de Roteamento



Cruzeiro do Sul Virtual  
Educação a distância



# Material Teórico



Definindo a Técnica de VLSM e *Supernet*

**Responsável pelo Conteúdo:**

Prof. Esp. Antonio Eduardo Marques da Silva

**Revisão Textual:**

Prof.<sup>a</sup> Dr.<sup>a</sup> Selma Aparecida Cesarin



# UNIDADE

## Definindo a Técnica de VLSM e *Supernet*



- Introdução;
- Desperdício de Endereço;
- Quando Utilizar VLSM;
- Cálculo de Sub-Redes com VLSM;
- Sumarização de Rotas;
- Configurando VLSM.



### OBJETIVO DE APRENDIZADO

- Compreender e abordar as Técnicas de VLSM e *SuperNet*;
- Entender a necessidade de utilização, esgotamento de endereços e aumento de entradas em tabelas de roteamento, sumarização de rota;
- Aprender como calcular uma Rede usando a técnica de VLSM.





# Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:



## Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu “momento do estudo”;
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

# Introdução

Um dos maiores problemas da Internet rodando o IPv4 é, certamente, o limite de capacidade de endereçamento que esse Protocolo pode ter (cerca de 4 bilhões de endereços) e, por causa do crescimento exponencial da Internet, tornou-se quase impossível a utilização de endereços públicos para dentro de um ambiente de Rede local.

Para isso, foram criadas várias técnicas a fim de minimizar desperdícios de endereços. Outro problema não muito falado na comunidade é em relação ao aumento de rotas nas Tabelas de roteamento dos roteadores em função também do crescimento da Internet.

Essa manipulação de muitas rotas num equipamento de Rede pode, certamente, afetar a *performance* dessa máquina em função da utilização dos recursos de máquina (como CPU, memórias etc.).

Nesta Unidade, vamos discutir um pouco sobre algumas dessas técnicas, como o uso de VLSM e a agregação de rotas.

## Desperdício de Endereço

Num passado próximo, não era aconselhável usar a primeira e a última Sub-redes calculadas. A utilização da primeira Sub-rede, conhecida como Sub-rede zero, era desencorajada em função da confusão que poderia ocorrer se uma Rede e uma Sub-rede tivessem o mesmo endereço, em virtude de as Redes genéricas sempre acabarem em zero (0) nos endereços dedicados a *host*.

Isso também se aplicava na utilização da última Sub-rede, conhecida como Sub-rede *all-ones* (totalmente de uns), que se pode confundir com o *broadcast* de uma Rede genérica, já que um endereço de *broadcast* em uma Rede padrão/*default* é a ligação de números um (1) no campo dedicado à *host* de um endereço.

Com a evolução das tecnologias de Redes e com o esgotamento dos endereços IPv4, a utilização da primeira e da última Sub-rede se tornou uma prática aceitável, em conjunto com as técnicas de máscara de Rede de tamanho variável, também conhecida como VLSM.

Na próxima Figura, temos um exemplo da utilização de três *bits* da porção *host* de um endereço Classe C que foram emprestados para a criação de novas Redes menores.

Se uma determinada equipe optar por utilizar a Sub-rede zero, haverá oito Sub-redes utilizáveis. Cada Sub-rede pode suportar 30 *hosts* ativos. É importante lembrar que *hosts* ativos dizem respeito ao endereçamento dos dispositivos, ou seja, não aplicamos endereço de Rede, de Sub-rede e de broadcast nos *hosts*, e sim, endereços que estão dentro desses intervalos calculados (TANENBAUM, 2011).

Se uma Equipe optar por utilizar o comando *no ipsubnet-zero* aplicado no roteador, haverá sete Sub-redes utilizáveis com 30 *hosts* em cada uma.

Os roteadores da Cisco com o Sistema Operacional iOS versão 12.0 ou posterior setam a Rede Sub-rede zero por *default* (CISCO NETACAD, 2017).

Quadro 1 – Desperdício de Endereços

Número da Sub-rede	Endereço de Sub-rede	
Sub-rede 0	192.168.187.0	/27
Sub-rede 1	192.168.187.32	/27
Sub-rede 2	192.168.187.64	/27
Sub-rede 3	192.168.187.96	/27
Sub-rede 4	192.168.187.128	/27
Sub-rede 5	192.168.187.160	/27
Sub-rede 6	192.168.187.192	/27
Sub.redes 7	192.168.187.224	/27

Fonte: ebah.com.br

Na próxima Figura, note que os escritórios remotos Sydney, Brisbane, Perth e Melbourne podem ter 30 *hosts* cada um, pois estamos utilizando endereços dentro dos intervalos anteriormente criados (/27 ou máscara de Rede/Sub-rede 255.255.255.224).

Uma equipe reconhece que será necessário endereçar os três *links* WAN ponto a ponto que interligam Sydney, Brisbane, Perth e Melbourne.

Se essa Equipe utilizar as últimas três Sub-redes criadas para os *links* de WAN ponto a ponto, teremos um desperdício de 28 endereços de *host* de cada Sub-rede, pois, necessariamente, vamos precisar apenas de dois endereços em cada Rede ponto a ponto.

Esse esquema de endereçamento clássico de criação de Sub-redes desperdiça um terço do espaço de endereços em potencial nesse caso. Tal esquema de endereços é aceitável para uma Rede de ambiente local pequena. No entanto, ele gera muito desperdício se forem utilizados para conexões ponto a ponto, como podemos verificar (CISCO NETACAD, 2017).

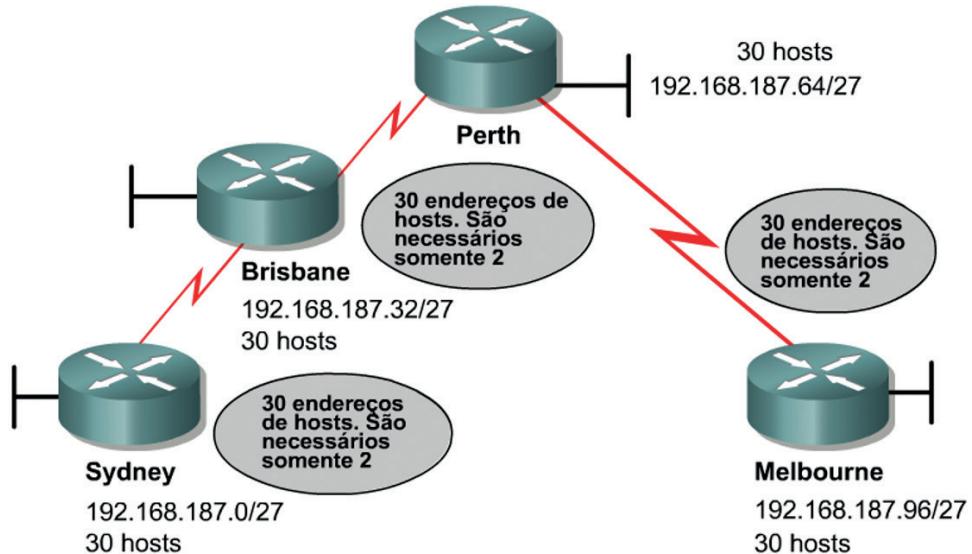


Figura 1 – Exemplo de VLSM

Fonte: ebah.com.br

## Quando Utilizar VLSM

É muito importante projetar um esquema de endereçamento de Rede que permita crescimento e que não desperdice endereços de forma desnecessária.

Com essa finalidade, foram criadas algumas novas técnicas de criação e mapeamento de endereços, como, por exemplo, o VLSM, que pode ser utilizado em *links* ponto a ponto, sem, necessariamente, desperdiçar endereços de uma eventual Sub-rede calculada.

Como exemplo, na próxima Figura, podemos identificar que uma a Equipe de Administração da Rede decidiu evitar o desperdício da utilização da máscara /27 criada, inicialmente, nos *links* ponto a ponto. Como eventual solução, essa equipe aplicou a técnica de VLSM para resolver o eventual desperdício.

A sigla VLSM é o significado de máscara de Sub-rede de tamanho variável, ou seja, estamos criando Sub-redes menores ainda, extraídas de uma Sub-rede calculada inicialmente e, por esse motivo, às vezes são chamadas de Sub-sub-rede (STALLINGS; ROSS, 2010).

Quadro 2 – Esquema de uso do VLSM

Número da Sub-rede	Endereço de Sub-rede	
Sub-rede 0	192.168.187.0	/27
Sub-rede 1	192.168.187.32	/27
Sub-rede 2	192.168.187.64	/27
Sub-rede 3	192.168.187.96	/27
Sub-rede 4	192.168.187.128	/27
Sub-rede 5	192.168.187.160	/27
Sub-rede 6	192.168.187.192	/27
Sub-rede 7	192.168.187.224	/27

Número da Sub-rede	Endereço de Sub-rede	
sub-sub-rede 0	192.168.187.192	/30
sub-sub-rede 1	192.168.187.196	/30
sub-sub-rede 2	192.168.187.200	/30
sub-sub-rede 3	192.168.187.204	/30
sub-sub-rede 4	192.168.187.208	/30
sub-sub-rede 5	192.168.187.212	/30
sub-sub-rede 6	192.168.187.216	/30
sub-sub-rede 7	192.168.187.220	/30

Fonte: ebah.com.br

No exemplo, para aplicar a técnica de VLSM, a Equipe de Rede escolhe um endereço de Classe C em Sub-redes de vários ou de um único tamanho, no caso, uma /27.

As Sub-redes grandes são criadas para serem aplicadas nas Redes locais. Após essa aplicação, escolhe-se uma Rede desse pool para a criação de Redes menores e que serão usadas para as conexões de WAN ponto a ponto.

Uma máscara de 30 bits (/30) ou 255.255.255.252 é utilizada para criar essas novas Sub-sub-redes com apenas dois endereços de host válidos, suficientes para o endereçamento de duas interfaces ponto a ponto, o que acaba se tornando a melhor solução para essa conectrização (CISCO NETACAD, 2017).

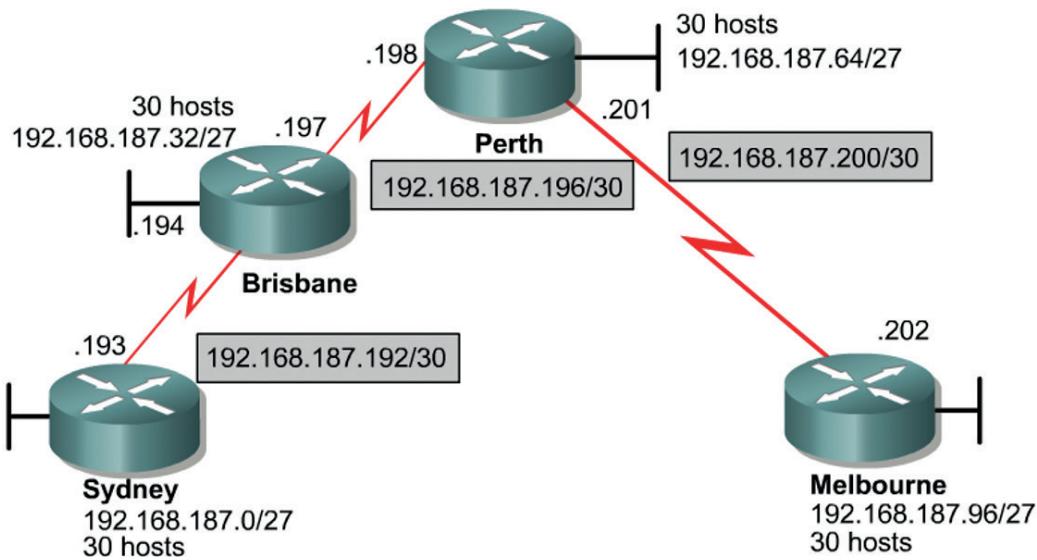


Figura 2 – Esquema de Mapa com VLSM

Fonte: ebah.com.br

## Cálculo de Sub-Redes com VLSM

A técnica de VLSM ajuda a gerenciar endereços IPv4 para definir máscaras de Sub-rede que atendam aos requisitos de um *link* ou segmento de Rede.

Uma máscara de Sub-rede deve satisfazer aos requisitos de endereçamento de uma Rede local, como os requisitos de uma conexão WAN ponto a ponto (TANENBAUM, 2011).

No próximo exemplo, a Figura apresenta uma Rede que necessita de um esquema de endereçamento; um endereço Classe B 172.16.0.0 e duas Redes locais que exigem um mínimo de 250 hosts ativos cada uma.

Se os roteadores utilizarem um Protocolo de Roteamento do tipo *classless*, o *link* WAN precisará ser uma Sub-rede da mesma Rede de Classe B.

Já os Protocolos de Roteamento *classful*, tais como RIP v1, IGRP e EGP, não suportam VLSM e CIDR e, nesse caso, mesmo que criadas técnicas de Sub-redes ou de VLSM o roteador retornaria tais endereços como endereços originais (padrão).

Um *link* WAN precisará apenas de dois endereços válidos, um para cada roteador dessa conectorização e isso resulta em 252 endereços desperdiçados desnecessariamente.

Se a técnica de VLSM for utilizada, uma máscara de 24 bits ainda seria aplicada nos segmentos LAN para os 250 hosts; porém, uma máscara de 30 bits poderia ser utilizada para o endereçamento de *link* WAN ponto a ponto (CISCO NETACAD, 2017).

O endereço de sub-rede é 172.16.32.0/20  
 A forma binária é 10101100.00010000.00100000.00000000

O endereço de VLSM é 172.16.32.0/26  
 A forma binária é 10101100.00010000.0010|0000.00|000000

	Rede	Sub-rede	Sub-rede	VLSM	Host
<b>sub-rede 1:</b>	172 • 16	.0010	0000.00	000000 = 172.16.32.0/26	
<b>sub-rede 2:</b>	172 • 16	.0010	0000.01	000000 = 172.16.32.64/26	
<b>sub-rede 3:</b>	172 • 16	.0010	0000.10	000000 = 172.16.32.128/26	
<b>sub-rede 4:</b>	172 • 16	.0010	0000.11	000000 = 172.16.32.192/26	
<b>sub-rede 5:</b>	172 • 16	.0010	0001.00	000000 = 172.16.33.0/26	

Figura 3 – Cálculo de VLSM

Fonte: ebah.com.br

Na próxima Figura, os endereços de Sub-rede utilizados nesse Mapeamento serão gerados quando a Sub-rede 172.16.32.0/20 for dividida em Sub-redes /26 ou marcadas no formato decimal 255.255.255.224.

Já para calcular os endereços de Sub-rede que serão utilizados nos *links WAN*, pegaremos uma dessas Sub-redes /26 criadas e vamos novamente subdividi-la em Redes de tamanho que atendam nossas necessidades.

No exemplo, a Sub-rede 172.16.33.0/26 é subdividida em novas Sub-redes com um prefixo /30. Esse cálculo pode fornecer mais quatro bits de Sub-rede e, portanto, 16 ( $2^4$ ) Sub-redes para as conexões de WANs (CISCO NETA-CAD, 2017).

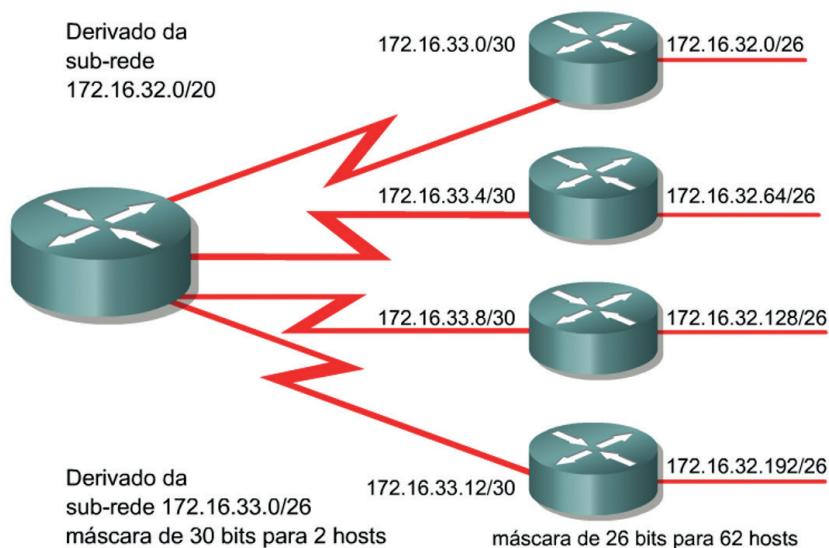


Figura 4 – Aplicação do VLSM

Fonte: ebah.com.br

A técnica de VLSM pode ser utilizada, então, para dividir em Sub-redes um endereço já dividido em Sub-redes. Considere, por exemplo, o endereço de Sub-rede 172.16.32.0/20 e uma Rede que precisa de dez (10) endereços de host válidos.

Com esse endereço de Sub-rede, existem  $2^{12} - 2$ , ou seja, teríamos 4094 endereços de host válidos, a maioria dos quais será desperdiçada certamente numa Rede que necessita de muito menos número de endereços.

Com VLSM, é possível dividir 172.16.32.0/20 em Sub-redes menores em quantidade de números de hosts válidos. Quando o endereço de Sub-rede 172.16.32.0/20 é dividido num endereço de Sub-rede 172.16.32.0/26, há um ganho de  $2^6$  Sub-rede, ou seja 64 Sub-redes novas.

Cada Sub-rede pode suportar  $2^6 - 2$ , ou seja, 62 hosts válidos em cada uma dessas Sub-redes criadas.

Utilize, então, as seguintes etapas para aplicar a técnica de VLSM à Rede 172.16.32.0/20:

- **Etapa 1:** escreva o endereço 172.16.32.0 em forma binária;
- **Etapa 2:** trace uma linha vertical entre o 20º e o 21º bits, conforme indicado no exemplo. O limite original da Sub-rede foi /20;
- **Etapa 3:** trace uma linha vertical entre o 26º e o 27º bits, conforme indicado no exemplo. O limite original da Sub-rede /20 é estendido mais seis bits à direita, o que resulta em /26;
- **Etapa 4:** calcule os 64 endereços de Sub-rede com os bits entre as duas linhas verticais, do menor para o maior valor de endereço. O exemplo demonstra as primeiras cinco Sub-redes disponíveis calculadas.

## Sumarização de Rotas

Quando a técnica de VLSM for utilizada, é importante manter os números de Sub-rede sequencialmente agrupados para que possamos permitir uma eventual agregação.

Por exemplo, Redes como os endereços 172.16.14.0 e 172.16.15.0 precisam estar perto uma da outra para que os roteadores possam transportar uma rota para um agrupamento único de endereço (CISCO NETACAD, 2017).

A utilização de CIDR – *Classless Interdomain Routing* e VLSM impedem o desperdício de endereços e promove a agregação ou resumo de rotas. Vale lembrar que dois problemas são principais em relação à utilização do IPv4, um deles e o mais famoso seria o limite de capacidade de endereçamento que vem se esgotando (ou que já se esgotou) com o crescimento escalável da Internet e o outro problema,

mas não muito divulgado, diz respeito ao excesso de criação de rotas na Internet que, certamente, consome muito recurso dos roteadores e dispositivos intermediários nessa grande Rede (TANENBAUM, 2011).

Por esse motivo, sem o resumo de rotas (sumarização), o roteamento do *backbone* da Internet, provavelmente, teria entrado em colapso antes de 1997.

A próxima Figura ilustra como o resumo de rotas reduz a carga ao longo do fluxo entre os roteadores de uma Rede.

Essa hierarquia complexa de Redes e Sub-redes de tamanhos variáveis é resumida em vários pontos com um endereço de prefixo, até que toda a Rede possa ser anunciada como uma única rota agregada ao endereço IPv4 200.199.48.0/20.

O resumo de rotas também é conhecido como Super-rede, por se tratar de uma técnica e, ao invés de criar novas Redes/Sub-redes, tem o objetivo de aumentar o número de *hosts* dentro de uma única Rede, a fim de divulgá-lo em menos rotas, diminuindo, assim, os recursos dos roteadores da Rede. Isso só será possível se os roteadores de uma determinada Rede utilizar um Protocolo de roteamento do tipo *classless*, como, por exemplo, o OSPF ou o EIGRP.

Os Protocolos de Roteamento do tipo *classless* transportam um prefixo que consiste em um endereço IP em uma máscara de *bits*; de 32 *bits* nas atualizações de Roteamento e que são usados para cálculos a fim de identificarem as Redes da topologia (CISCO NETACAD, 2017).

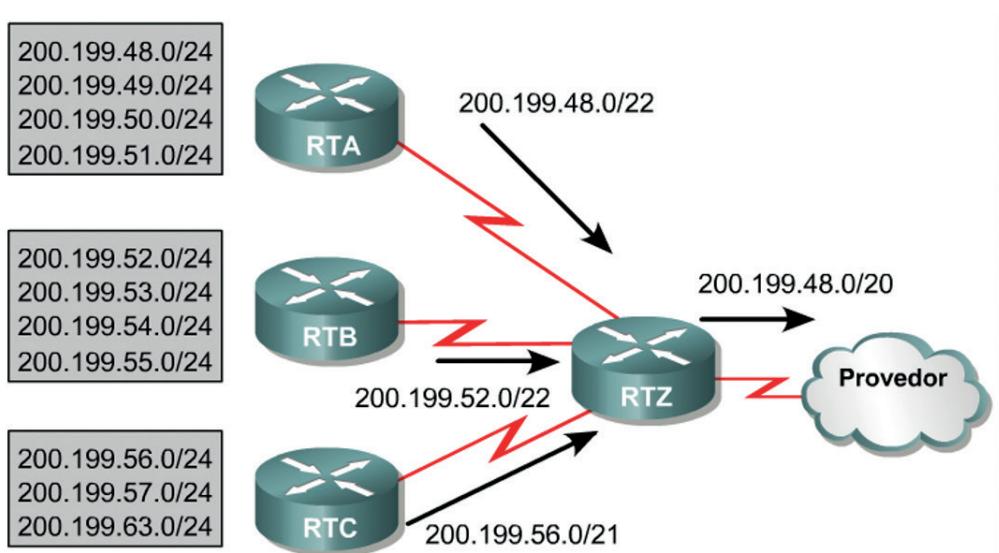


Figura 5 – Sumarização de Rotas  
 Fonte: ebah.com.br

A rota resumida que eventualmente chega ao provedor de serviços no exemplo proposto tem um prefixo de 20 *bits* (/20), comum a todos os endereços dentro da Organização que divulga essa rota.

Esse endereço de sumarização é o 200.199.48.0/20 na representação decimal pontuada usada pelo endereço IPv4, ou 11001000.11000111.0011 em número binário.

Para que o respectivo resumo funcione corretamente, os endereços precisam ser cuidadosamente designados de maneira hierárquica, de modo que os endereços resumidos compartilhem os *bits* de ordem superior.

A seguir, apresentaremos algumas regras importantes que devem ser lembradas:

- Um roteador precisa saber em detalhes os números de Sub-redes a ele conectadas;
- Um roteador não precisa informar a outros roteadores sobre cada Sub-rede que ele conhece, se o roteador puder enviar uma rota agregada para um conjunto de rotas;
- Um roteador que utiliza rotas agregadas tem um menor número de entradas na sua Tabela de Roteamento e, por consequência, utiliza menos recursos de máquina, como *CPU*, memória etc.

A próxima Figura mostra que os endereços compartilham os primeiros 20 *bits*, que estão representados em vermelho. O 21º *bit* não é o mesmo para todos os roteadores; portanto, o prefixo para a rota resumida terá 20 *bits* de comprimento, ou seja, é utilizado para o cálculo do número de Rede da rota resumida (CISCO NETACAD, 2017).

Quadro 3 – Rota Sumarizada

Endereços	Primeiro Octeto	Segundo Octeto	Terceiro Octeto	Quarto Octeto
192.168.98.0	11000000	10101000	01100010	00000000
192.168.99.0	11000000	10101000	01100011	00000000
192.168.100.0	11000000	10101000	01100100	00000000
192.168.101.0	11000000	10101000	01100101	00000000
192.168.102.0	11000000	10101000	01100110	00000000
192.168.105.0	11000000	10101000	01101001	00000000
<b>A rota sumarizada é 192.168.96.0/20</b>				
192.168.96.0	11000000	10101000	01100000	00000000

Fonte: ebah.com.br

E, na Figura a seguir, mostra-se que os endereços compartilham os primeiros 21 *bits* e esses *bits* estão representados na cor vermelha.

O 22º *bit* não é o mesmo para todos os roteadores; portanto, o prefixo para a rota resumida terá 21 *bits* de comprimento, utilizado para calcular o número de Rede da rota devidamente resumida (CISCO NETACAD, 2017).

Quadro 4 – Finalização do Processo de Sumarização

Endereços	Primeiro Octeto	Segundo Octeto	Terceiro Octeto	Quarto Octeto
172.16.0.0	10101100	00010000	00000000	00000000
172.16.2.0	10101100	00010000	00000010	00000000
172.16.3.128	10101100	00010000	00000011	10000000
172.16.4.0	10101100	00010000	00000100	00000000
172.16.4.128	10101100	00010000	00000100	10000000
<b>Resposta:</b>				
172.16.0.0/21	10101100	00010000	00000000	00000000

Fonte: ebah.com.br

## Configurando VLSM

Então, na próxima Figura, vamos colocar em prática o que foi comentado e entender melhor os cálculos da técnica de VLSM que foram aplicados:

- O Endereço de Rede que estamos trabalhando no exemplo é um endereço de Classe C: 192.168.10.0;
- O roteador de nome *Perth* precisa suportar 60 hosts válidos. Isso significa que serão necessários pelo menos seis (6) bits na porção dedicada ao *host* do endereço. Seis bits resultarão em  $2^6 - 2$ , ou seja, 62 endereços de hosts possíveis. A conexão de Rede Local do roteador *Perth* recebe a designação da Sub-rede 192.168.10.0/26;
- Os roteadores de nome *Sydney* e *Singapore* necessitam suportar 12 hosts cada um (número menor que o de *Perth*). E isso significa que serão necessários pelo menos quatro (4) bits na porção dedicada a *host* do endereço. Quatro bits resultarão em  $2^4 - 2$ , ou seja, 14 possíveis endereços de host válidos e suficientes para o mapeamento de endereços necessário. Por esse motivo, para a conexão de Rede Local do roteador *Sydney*, é designada a Sub-rede 192.168.10.96/28, e para a conexão da Rede Local do roteador *Singapore* é designada a Sub-rede 192.168.10.112/28, ambos os endereços poderiam suportar a necessidade de endereçamento proposta;
- O roteador *KL* (que está no topo da tipologia) precisa suportar 28 hosts válidos. Isso significa que serão necessários pelo menos cinco (5) bits na porção dedicada a *host* do endereço. Cinco bits resultarão em  $2^5 - 2$ , ou seja, 30 possíveis endereços de host válidos. A conexão de Rede local do roteador *KL* recebe, então, a designação de endereço de Sub-rede 192.168.10.64/27.

Note que, utilizando a técnica de VLSM, nós, Administradores de Rede, podemos calcular Redes distintas com tamanhos conforme nossa necessidade de Projeto e, nesse caso, atendendo aos requisitos do não desperdício de endereços IPv4, que era nossa principal preocupação.

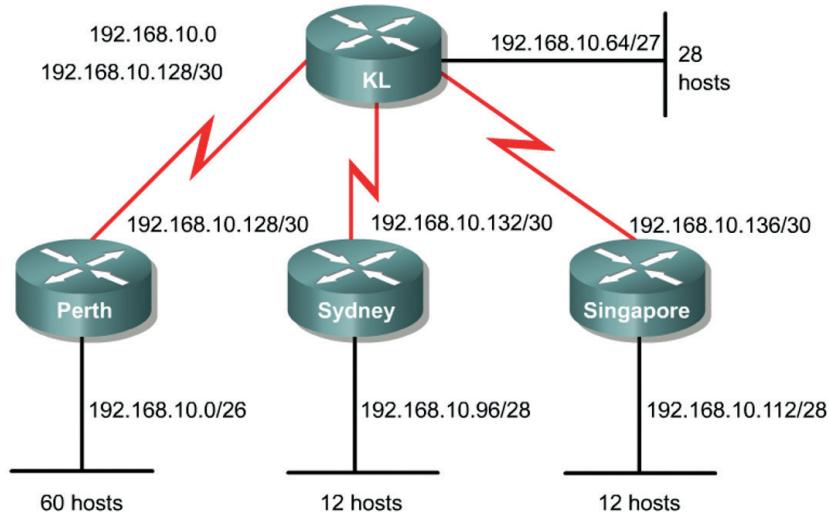


Figura 6 – Configurando o VLSM

Fonte: ebah.com.br

Vamos agora entender o processo de cálculos usando a Técnica de VLSM para as conexões ponto a ponto:

- A conexão entre os roteadores *Perth* e *KL* requerem apenas dois endereços de host válidos para suas conexões ponto a ponto. Isso significa que serão necessários pelo menos dois bits na porção host do endereço. A utilização de dois bits resultarão em  $2^2 - 2$ , ou seja, 2 possíveis endereços de host válidos. Nesse caso, a conexão entre os roteadores *Perth* e Kuala Lumpur recebem a designação da Sub-rede 192.168.10.128/30;
- E, da mesma forma, aplicada essa mesma técnica aos roteadores *Sidney* e *Singapura* em relação ao roteador *KL*, ou seja, ambos estão usando uma máscara de Sub-rede /30 ou 255.255.255.252, que permitem a utilização de dois (2) hosts válidos.

Podemos observar um exemplo de configuração de conexão ponto a ponto entre KL e *Singapure*, como segue:

```
KL(config)# interface serial 1
```

```
KL(config-if)# ip address 192.168.10.138 255.255.255.252
```

```
Singapore(config)# interface serial 0
```

```
Singapore(config-if)#ip address 192.168.10.137 255.255.255.252
```

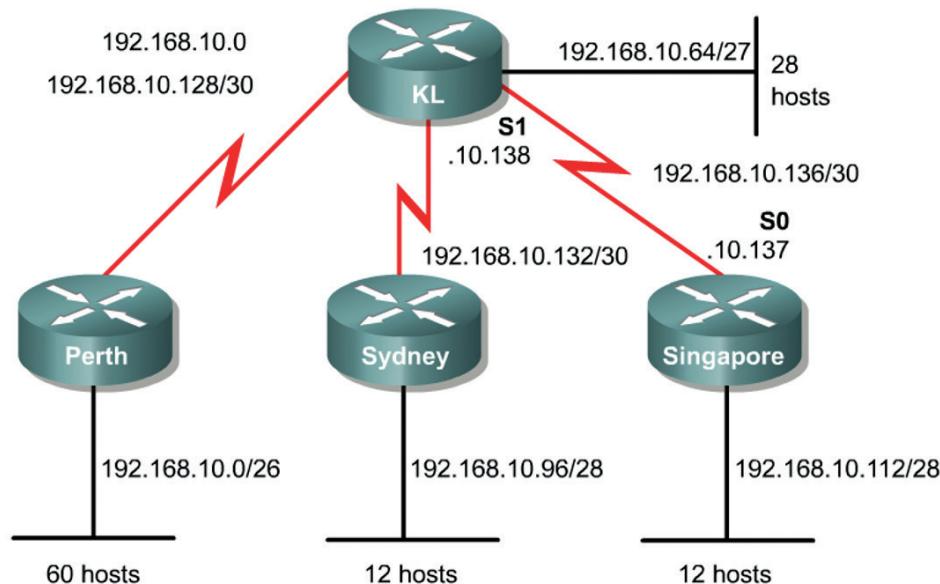


Figura 7 – Finalizando a Configuração do VLSM

Fonte: ebah.com.br

# Material Complementar

## Indicações para saber mais sobre os assuntos abordados nesta Unidade:



Livros

### Redes de Computadores e a Internet

STALLINGS, W. e ROSS K. 5.ed Pearson, 2010.

### Redes de Computadores

TANENBAUM, A. S. 5.ed. Pearson, 2011.



Leitura

### Cursos Web

CISCO NETACAD. **Módulo de Roteamento e Switching** – Conceitos Essenciais. Capítulo 6 – Sessão 6.3: Técnica de VLSM, Versão 6.0, EUA, 2017.

CISCO NETACAD. **Módulo de Roteamento e Switching** – Conceitos Essenciais. Capítulo 6 – Sessão 6.3: Técnica de CIDR, Versão 6.0, EUA, 2017.

# Referências

CISCO NETACAD. **Módulo de Roteamento e Switching:** Conceitos Essenciais (CCNA2) – 6<sup>a</sup> Versão, Cisco Systems, 2017 (Material *on-line*).

STALLINGS, W.; ROSS. **Redes de Computadores e a Internet.** 5.ed. Pearson, 2010.

TANENBAUM, A. S. **Redes de Computadores.** 5.ed. Pearson, 2011.



**Cruzeiro do Sul**  
Educacional

# Tecnologias de Roteamento



Cruzeiro do Sul Virtual  
Educação a distância



# Material Teórico



**Características e Gerência de Roteadores**

**Responsável pelo Conteúdo:**

Prof. Esp. Antonio Eduardo Marques da Silva

**Revisão Textual:**

Prof.<sup>a</sup> Dr.<sup>a</sup> Selma Aparecida Cesarin



# UNIDADE

## Características e Gerência de Roteadores



- **Introdução;**
- **Descoberta de Vizinhos (CDP);**
- **Criando Mapa de Rede;**
- **Conexão *TELNET*;**
- **Inicialização do Roteador Cisco;**
- **Visão Geral do Sistema de Arquivos do IOS;**
- **Nomenclatura do Nome do IOS da Cisco;**
- **Registrador de Configuração.**



### OBJETIVO DE APRENDIZADO

- Compreender e abordar a importância de gerenciamento de roteadores;
- Conhecer a ferramenta proprietária da Cisco, o *Cisco Discovery Protocol* (CDP);
- Realizar de testes de conectividade, usando o *ping* e *traceroute*. O processo de inicialização do roteador e a visão geral do Sistema de Arquivos da máquina de roteamento.



# Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:



## Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu “momento do estudo”;
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

# Introdução

Para que os equipamentos de Rede possam ser confiáveis, é muito importante a funcionalidade de gerenciamento desses dispositivos dentro de uma *internetworking*, sendo que algumas formas são clássicas e padronizadas.

Algumas proprietárias possuem um Protocolo, como é o caso da Cisco, que possui um Protocolo chamado CDP, cuja finalidade é a descoberta de equipamentos vizinhos.

Nesta Unidade, vamos explorar alguns desses recursos de gerência e, no final, entender um pouco mais sobre a sintaxe de nomes e locais nos quais o Sistema Operacional da Rede da Cisco é devidamente armazenado.

## Descoberta de Vizinhos (CDP)

A ferramenta *Cisco Discovery Protocol* (CDP) é um Protocolo de camada de enlace (camada 2) que faz a conexão de Protocolos inferiores de meio físico (camada 1) com os Protocolos superiores de camadas de Rede (camada 3), ou seja, a finalidade do CDP da Cisco é obter informações a respeito de dispositivos vizinhos, tais como: os tipos de dispositivos conectados (roteadores, switches etc.) às interfaces desses dispositivos às quais eles conectam e são conectados (*seriais, ethernet* etc.) e os números de modelos desses dispositivos (*Catalyst 2960, ISR 2800* etc.).

Esse Protocolo de descoberta é independente de meio físico e de Protocolo de Rede, pois funciona em todos os equipamentos da Cisco por meio do SNAP (*Subnetwork Access Protocol* – Protocolo de Acesso à Sub-Rede), para extrair essas informações de vizinhos (CISCO NETACAD, 2014).

Quando um dispositivo da Cisco é inicializado, o CDP é iniciado automaticamente, caso esteja habilitado, permitindo que esse dispositivo detecte os dispositivos vizinhos que também possuem o CDP em modo de execução.

Como dito, ele opera através da camada de enlace e permite que dois Sistemas aprendam um sobre o outro, mesmo que estejam usando diferentes Protocolos de camadas de Rede, como o IPv4, por exemplo (CISCO NETACAD, 2014).

Cada dispositivo configurado com o CDP envia mensagens periódicas, conhecidas como anúncios (*advertisements*), para os dispositivos diretamente conectados a esse dispositivo.

Cada dispositivo anuncia pelo menos um endereço no qual pode receber as mensagens de SNMP (*Simple Network Management Protocol* – Protocolo de Gerenciamento de Redes Simples). Esses anúncios possuem informações a respeito do “tempo de vida restante” (*time-to-live*), indicando o tempo de espera limite durante o qual tais dispositivos receptores devem armazenar as informações da CDP da Cisco antes de descartá-los.

Além disso, cada dispositivo também fica em alerta às mensagens periódicas do CDP enviadas por outros dispositivos, com o intuito de aprender informações desses vizinhos (CISCO NETACAD, 2014).

## Informações Obtidas Pelo CDP

A principal utilização do CDP, certamente, é identificar todos os dispositivos Cisco que estão conectados diretamente a um dispositivo local. Para isso, utilize o comando ***show cdpneighbors*** a fim de exibir as atualizações do CDP nesse dispositivo local.

A próxima figura apresenta um exemplo de como o Protocolo CDP fornece informações coletadas para que o administrador da Rede possa visualizar. Cada dispositivo de Rede Cisco que executa o CDP troca informações de Protocolo somente com seus vizinhos, numa topologia de Rede, e esse administrador da Rede poderá apresentar os resultados da troca de informações entre CDPs numa console conectada a um dispositivo de Rede Local que gerencia tal processo (CISCO NETACAD, 2014).

O Administrador da Rede pode, então, utilizar o comando Cisco IOS ***show cdpneighbors*** para exibir essas informações sobre as Redes conectadas diretamente ao dispositivo gerenciador escolhido, como um roteador ou um *switch*. Esse Protocolo, então, fornece informações sobre cada dispositivo CDP vizinho, transmitindo (TLVs) Valores de Comprimento de Tipo, que são blocos de informações embutidos em anúncios do Protocolo CDP (CISCO NETACAD, 2014).

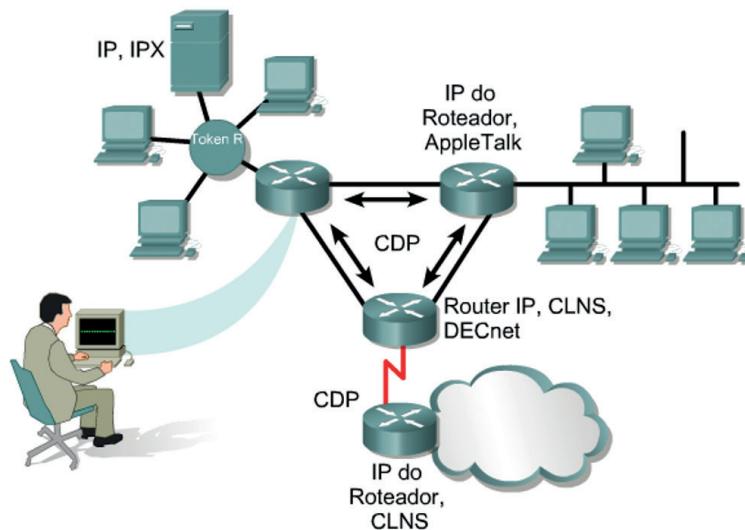


Figura 1 – Descobrindo Vizinhos com CDP

Fonte: Acervo do conteudista

Os TLVs dos dispositivos exibidos por meio do comando ***show cdpneighbors*** possuem as seguintes informações:

- ID do dispositivo;
- Interface local;
- Tempo de espera;

- Capacidade (o que o dispositivo está realizando);
- Plataforma/Modelo do equipamento;
- ID da porta de destino.

Os seguintes TLVs são incluídos somente no CDPv2:

- Nome de domínio de gerenciamento do VTP;
- VLAN nativa;
- Conexão *Full/Half duplex*.

## Monitorando as Informações do CDP

Para que possamos aproveitar ao máximo essa ferramenta de monitoramento da Cisco, vamos, aqui, apresentar alguns comandos que podem ser úteis para implementar, monitorar e manter as informações do Protocolo CDP:

- `cdprun`;
- `cdpenable`;
- `clearcdpcounters`;
- `show cdptraffic`;
- `show cdp`;
- `show cdp interface [número-do-tipo]`;
- `show cdpeighbors [número-do-tipo] [detalhe]`;
- `show cdpentry {*}|nome-do-dispositivo [*][Protocolo | versão]}`.

O comando do CDP **`cdprun`** é utilizado para ativar globalmente o processo do CDP no dispositivo de Rede. Por padrão, o CDP está globalmente ativado, ou seja, surte efeito em todas as interfaces do dispositivo de Rede.

Já o comando do CDP **`cdpenable`** é utilizado para ativar o CDP numa interface em específico, ou seja, podemos aplicar o Processo de monitoramento em apenas uma ou mais interfaces, ao interesse do administrador de Rede. Isso evita que mensagens do CDP possam ser trafegadas em *links* suspeitos ou passíveis de espionagem.

No Sistema Operacional Cisco IOS versão 10.3 ou superiores, o CDP é ativado por padrão/*default* em todas as interfaces suportadas [CISCO NETACAD, 2017].



Protocolo CDP – Cisco Systems – Introducción (Espanhol). Acesse: <https://youtu.be/i0lgY0EGtCo>

## Criando Mapa de Rede

Uma das atividades mais utilizadas com o uso do CDP é a capacidade que um administrador de Rede tem para criar um mapa de Redes completo (caso ele não o conheça ou esteja faltando um *layout* da Rede) de forma simples e com baixo custo.

Embora um frame CDP possa ser pequeno e simples, pode ser capaz de recuperar grande quantidade de informações úteis sobre os dispositivos vizinhos e conectados da Cisco. Com a extração dessas informações, pode-se criar um mapa de Rede dos dispositivos conectados e descobrir algumas funcionalidades desses equipamentos.

## Desativando o CDP num Dispositivo

---

Para desativar o CDP globalmente (em todas as interfaces que o equipamento de Rede possui), utilize o comando **no cdprun** no modo de configuração global.

Se o CDP estiver desativado globalmente, não será possível ativar interfaces individualmente para o CDP.

No Cisco IOS versão 10.3 ou superior, o CDP é ativado por *default* em todas as interfaces suportadas (globalmente), para enviar e receber informações de monitoramento dessa ferramenta. Entretanto, em algumas interfaces, como as interfaces assíncronas, o CDP está desativado por padrão.

Se o CDP estiver desativado, use o comando **cdpenable** no modo de configuração de interface, para que esse processo funcione pontualmente. Para desativá-lo em uma determinada interface, após seu ativamento, utilize o comando **no cdpenable**, também no modo de configuração de interface (CISCO NETACAD, 2014).

## Monitoramento do CDP

---

Além dos comandos apresentados anteriormente, temos, ainda, uma série de comandos que podem auxiliar o administrador a obter mais informações por meio desse Protocolo.

Vamos conhecer alguns:

- *show cdp;*
- *show cdptraffic;*
- *show debugging;*
- *debug cdpadjacency;*
- *debug cdpevents;*
- *debug cdppip;*
- *debug cdppackets;*
- *clearcdptable;*
- *clearcdpcounters;*
- *cdp timer;*
- *cdpholdtime.*

## Testes de Conectividade (*Ping* e *Traceroute*)

Uma das formas mais simples e econômicas de fazermos um diagnóstico de Rede e testar conectividade seria a utilização de Protocolos de eco, que são utilizados para testar se os pacotes de um determinado dispositivo de Rede estão sendo roteados e, respectivamente, enviados a um determinado destino.

O comando que realiza essa função na maioria dos Sistemas Operacionais existentes é o comando *ping*, que envia um pacote para o *host* de destino e espera um pacote de resposta desse *host*.

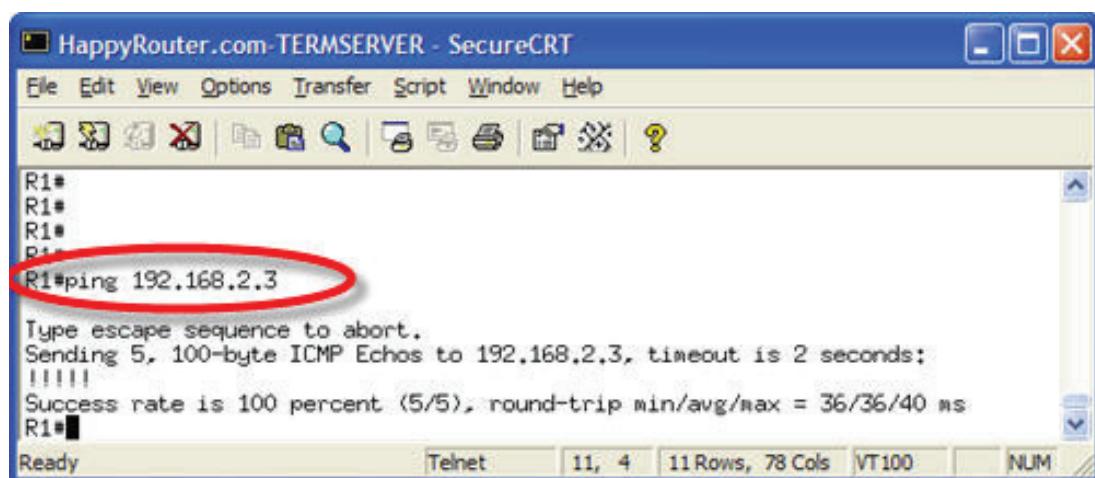
Os resultados desse Protocolo de eco podem ajudar a avaliar – e muito – a confiabilidade do caminho até o *host* destino, bem como os atrasos ao longo desse caminho, se o *host* pode ou não pode ser alcançado ou se está funcionando corretamente.

Para o Sistema Operacional da Cisco (IOS), esse é um mecanismo básico de teste e pode ser realizada tanto no modo EXEC do usuário quanto no modo EXEC privilegiado.

Na próxima figura, observamos um dispositivo de Rede realizando um *ping* no endereço IP de destino 192.168.2.3. Para isso, foram enviados cinco datagramas e o dispositivo destino os respondeu com êxito.

Os pontos de exclamação (!) indicam que cada eco foi bem sucedido, caso seja recebido um ou mais pontos (.) ao invés de exclamações, o aplicativo do dispositivo excedeu o tempo-limite esperando um determinado eco de pacote do destino do *ping* realizado.

O comando *ping* nada mais é do que uma espécie de “programinha” que utiliza como base o ICMP (*Internet Control Message Protocol* – Protocolo de Mensagens de Controle da *Internet*). No *ping* utilizado numa plataforma IPv4, os códigos do ICMP são 0 (Eco) e 8 (*Echo Replay*) (TANENBAUM, 2011).



```
HappyRouter.com-TERMSERVER - SecureCRT
File Edit View Options Transfer Script Window Help
R1#
R1#
R1#
R1# ping 192.168.2.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/36/40 ms
R1#
```

Figura 2 – Comando *Ping*

Fonte: Acervo do conteudista

Outro comando muito utilizado para testar conectividade é o **traceroute**, que nada mais é do que uma ferramenta ideal para se descobrir para onde e para qual o caminho estão sendo enviados os dados numa Rede.

O comando **traceroute** é semelhante ao comando *ping*, exceto que, ao invés de testar a conectividade ponto a ponto, ele também testa cada etapa ao longo do caminho, indicando ao administrador por onde os pacotes enviados para um destino passaram naquele momento (STALLINGS; ROSS, 2010).



O que é *Ping?* (Brasil). Acesse: <https://youtu.be/mIFthHD3NUs>

Essa operação no Sistema Operacional da Cisco (IOS) pode ser realizada tanto no modo EXEC do usuário quanto no modo EXEC privilegiado.

Da mesma forma que o *ping*, o **traceroute** é um “programinha ou comando” que executa o ICMP; porém, a cada salto que o pacote enviado a um destino realiza, esse Protocolo de Rede envia à máquina de teste o nome ou a identificação por onde chegou o pacote. Isso é realizado até que o pacote alcance seu destino final e o administrador obtenha informações por onde o ele passou naquele momento.

Se, por acaso, um desses dispositivos não puder ser alcançado, então, serão retornados três asteriscos (\*) em vez do nome de um dispositivo. O comando **traceroute** continuará tentando alcançar a próxima etapa, até que seja usada a sequência de escape **Ctrl-Shift-6**, utilizada para interromper esse processo (CISCO NETACAD, 2014).

## Conexão *Telnet*

A aplicação *Telnet* é um Protocolo de terminal virtual que faz parte do conjunto de Protocolos da família TCP/IP na camada de aplicação. Ele permite fazer remotamente conexões para *hosts*, oferecendo um recurso de terminal de Rede ou *login* remoto. Para que possamos utilizar essa aplicação tão conhecida, podemos executá-la com o comando *Telnet* no modo EXEC do IOS.

Esse recurso é muito utilizado para verificar o *software* da camada de aplicação entre os dispositivos origem e destino, tornando-se um dos mecanismos mais eficientes e baratos para essa finalidade.

Como vimos, o *Telnet* atua na camada de aplicação do modelo OSI e, por consequência, na camada de aplicação do TCP/IP; porém, depende do TCP para garantir a entrega correta e organizada dos dados entre as máquinas que fazem parte desse Processo (TANENBAUM, 2011).

Um dispositivo de Rede (como um roteador da Cisco) possui várias sessões *Telnet* simultâneas. Quando aplicamos na configuração o intervalo de 0 a 4, significa que estamos especificando um limite de cinco linhas *Telnet* ou VTY simultâneas.

Deve-se observar, também, que a verificação da conectividade da camada de aplicação é um subproduto da aplicação *Telnet*, pois sua principal função, certamente, é fornecer conectividade remota entre dispositivos de Rede, por meio de uma aplicação simples e universalmente conhecida.

## Estabelecendo Conexão *Telnet*

Como podemos observar, o comando *Telnet* permite que um usuário se conecte de um dispositivo de Rede a outro dispositivo de Rede.

O Sistema Operacional da Cisco permite que se faça o *Telnet* usando várias formas, desde a mais clássica que seria aplicar o comando *telnet* (endereço IP), como apenas indicar o nome de um dispositivo.

Vamos verificar algumas formas aceitas no IOS da Cisco, segue:

```
router>connect unicsul  
router>unicsul  
router>131.108.100.152  
router>telnet unicsul  
router>telnet 192.168.13.10
```

Para que o *Telnet* possa funcionar com um nome, deve haver uma tabela de nomes de hosts ou acesso à DNS criada. Caso contrário, é necessário inserir o endereço IP do dispositivo a ser remotamente conectado (STALLINGS; ROSS, 2010).

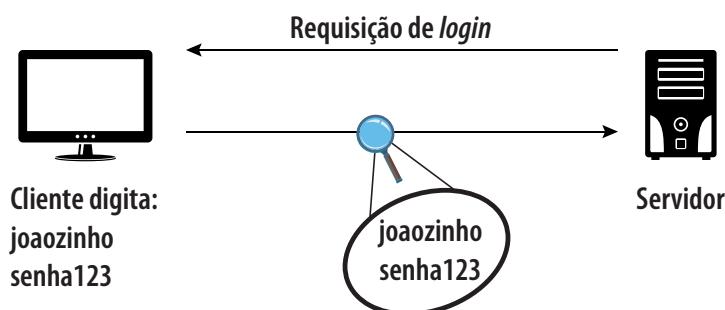


Figura 3 – Conexão *Telnet*

## Inicialização do Roteador Cisco

O objetivo das rotinas de inicialização do Sistema Operacional Cisco IOS é iniciar a operação do roteador (nesse caso). O roteador deve, então, proporcionar desempenho confiável e, principalmente, realizar seus trabalhos de comutação (Camada 3) de Rede.

Para isso, as rotinas de inicialização do dispositivo devem:

- Testar o *hardware* do roteador;
- Encontrar e carregar o Sistema Operacional Cisco IOS;

- Localizar e aplicar as instruções de configuração, inclusive as que determinam as funções dos Protocolos e os endereços das interfaces.

Na figura a seguir, podemos verificar uma ilustração dos locais em que estão armazenados os serviços utilizados para a inicialização do roteador.

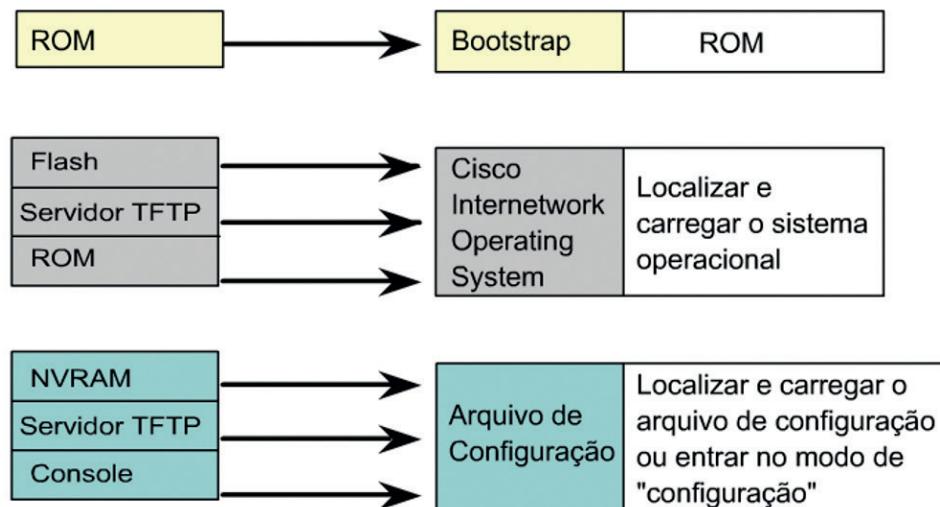


Figura 4 – Inicializando o Roteador

Fonte: Acervo do conteudista

## Carregando a Imagem do IOS

A origem padrão para o Sistema Operacional Cisco IOS depende da plataforma de *hardware* é a memória *Flash*; porém, o mais comum é que o roteador verifique os comandos ***boot system*** salvos na NVRAM para identificar esse local.

O Cisco IOS pode permitir a utilização de várias alternativas para esse comando, como, por exemplo, especificar que se busca o SOR ou usar a sua própria sequência (*fallback sequence*) para localizar e carregar o Sistema Operacional, caso não encontre um (CISCO NETACAD, 2014).

Os valores que podem ser utilizados no registro de configuração (*configuration register*) permitem as seguintes alternativas:

- Comandos *boot system* do modo configuração global: podem ser especificados para definir outras origens a serem utilizadas sequencialmente pelo roteador, no caso de não serem encontradas as anteriores;
- Se a NVRAM não tiver comandos do Sistema de inicialização que possam ser utilizados pelo roteador, o Sistema utiliza, por *default*, o Sistema Operacional Cisco IOS armazenado na memória *flash*;
- Se a memória *flash* estiver vazia, o dispositivo tenta utilizar o servidor TFTP para carregar uma imagem do IOS através da Rede. O roteador usa o valor do registro de configuração para formar um nome de arquivo que será inicializado a fim de carregar uma imagem padrão do Sistema Operacional IOS armazenada em um servidor de Rede;

- Se um servidor TFTP não estiver disponível, o roteador irá carregar uma versão limitada da imagem do Sistema Operacional Cisco IOS armazenada em ROM, conhecida como *Mini-IOS*.

## Comando *Boot System*

O exemplo a seguir apresenta a utilização de vários comandos do Sistema de inicialização a fim de especificar a sequência que será utilizada para carregar o Sistema Operacional Cisco IOS no dispositivo (CISCO NETACAD, 2014).

```
Router# configure terminal  
Router(config)# boot system flash unicsul-image  
[Ctrl+Z]  
Router# copy running-config startup-config
```

O comando **configure terminal** aplicado no modo EXEC do usuário acessa o modo de configuração global do equipamento. O comando **boot system flash unicsul-image** está indicando que o dispositivo no momento do *boot* vá até a memória *flash* e carregue a imagem *unicsul-image*.

O [Ctrl+Z] sai do modo de configuração (e de qualquer outro modo), e vai para a *prompt* no modo EXEC privilegiado. E o comando **copy running-config startup-config** copia o arquivo de configuração que está em RAM para uma cópia *backup* desse arquivo, que ficará armazenada em NVRAM e que, num eventual desligamento, possa carregar as configurações realizadas na última mudança (CISCO NETACAD, 2014).

Os três exemplos a seguir apresentam as entradas do *boot system* que especificam que uma imagem do Sistema Operacional Cisco IOS será carregado, primeiramente, de um servidor de Rede e, em último caso, da memória ROM:

- **Memória Flash** – Uma imagem do Sistema Operacional pode ser carregada da memória *flash* (geralmente, é por padrão). A vantagem é que essas informações armazenadas na memória *flash* não são vulneráveis às falhas da Rede que podem ocorrer ao carregar imagens de Sistema de servidores TFTP, pois são memórias de armazenamento instaladas dentro do dispositivo em questão;
- **Servidor de Rede** – Caso a memória *flash* seja corrompida, pode ser carregada uma imagem do Sistema de um servidor TFTP, externamente. Para que isso ocorra com sucesso, o administrador deverá preparar o servidor TFTP anteriormente (configurá-lo) e também confirmar conectividade desse servidores com o dispositivo de roteamento que está sendo configurado para buscar o IOS nesse componente;
- **Memória ROM** – Se a memória *flash* estiver corrompida e se houver uma falha no carregamento da imagem do servidor de Rede, a carga da imagem a partir da ROM será a opção final de inicialização (*bootstrap*). No entanto, a imagem do Sistema armazenada na ROM, provavelmente, será um subconjunto do

Sistema Operacional Cisco IOS, que não terá todos os recursos e configurações que podem ser encontrados na versão de SOR completa.

## Visão Geral do Sistema de Arquivos do IOS

Os roteadores e os *switches* da Cisco são computadores com finalidade específica e, por esse motivo, contém *hardware* e *software* para sua correta operação.

Em se tratando de *software*, o mais importante seria o Sistema Operacional e o arquivo da configuração que, como o nome indica, carrega as configurações desse dispositivo.

O Sistema Operacional de Rede, utilizado em quase todos os dispositivos de Rede da Cisco é o IOS – Cisco Internet Operating System (IOS), que é o *software* que permite que o *hardware* do equipamento funcione como um *switch* e como um roteador, ou seja, com as funções de comutação/chaveamento de quadros ou pacotes (CISCO NETACAD, 2014).

Um dos componentes de *software* mais importantes para o bom funcionamento do Sistema Operacional é o arquivo de instruções, conhecido como arquivo de configuração ou apenas como arquivo de config que, como o nome diz, contém as “instruções” que definem como o dispositivo de Rede irá rotear ou comutar os dados a serem enviados para um determinado destinatário.

Esse arquivo é criado pelo administrador Rede que define a funcionalidade desejada do dispositivo Cisco nesse caso. Algumas das funções que podem ser especificadas nesse arquivo de configuração são: os endereços IP aplicados nas interfaces, as senhas de acesso ao dispositivo, os Protocolos de roteamento utilizados e as Redes que devem ser anunciadas na *internetworking*.

Esse arquivo de configuração, normalmente, tem entre algumas centenas e milhares de bytes (nada muito grande) e pode ser copiado e armazenado até mesmo num antigo disquete para uma cópia de *backup*.

Num dispositivo da Cisco, tanto o Sistema Operacional IOS como o arquivo de configuração estão armazenados em memórias diferentes; isso ocorre para termos maior segurança caso alguma memória dessas falhe e, assim, não coloquemos tudo a perder (CISCO NETACAD, 2014).

O Sistema Operacional IOS é armazenado numa área de memória chamada

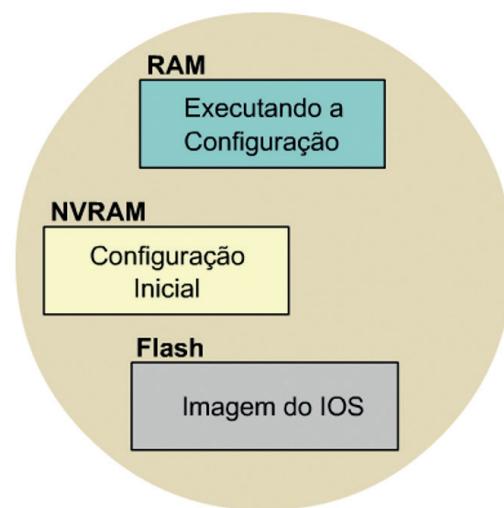


Figura 5 – Sistemas de Arquivos do IOS  
 Fonte: Acervo do artista

*flash* ou memória *flash* somente, que fornece armazenamento não volátil e possibilita o armazenamento de várias imagens de Sistema Operacional.

Após ligar o dispositivo e os processos de checagem e carregamento, o IOS é copiado e carregado na memória de acesso aleatório (RAM) que, apesar de ser uma memória volátil, é muito rápida e, por isso, seu custo é um pouco mais alto se comparado ao de outras memórias.

Uma cópia do arquivo de configuração é armazenada na memória NVRAM – RAM não volátil para utilização como configuração durante a inicialização, também conhecida como cópia de *backup*.

Essa configuração é conhecida pelo Sistema Operacional como “***startup-config***” e, depois de ser localizada, é copiada na RAM durante a inicialização do roteador.

Essa configuração, agora mantida na memória RAM, é utilizada para que se opere o dispositivo de Rede ou roteador, nesse exemplo.

Essa configuração que está carregada em memória RAM é conhecida como “***running-config***” ou arquivo ativo de configuração. Iniciando na versão 12 do IOS, é fornecida uma interface única para todos os Sistemas de arquivos utilizados pelo roteador.

Tal Sistema é chamado de Cisco IOS File System (IFS), e fornece um método único para realizar todo o Gerenciamento do Sistema de Arquivos utilizados pelo roteador. Isso inclui os Sistemas de Arquivos da memória *flash*, os Sistemas de Arquivos de Rede (TFTP, FTP e RCP) e a gravação e leitura das informações (como o *startup-configuration* em NVRAM, a *running-configuration* em RAM, *bootstrap* ou *Mini IOS* na ROM). Por esse motivo, o IFS utiliza um conjunto comum de prefixos para especificar os dispositivos do Sistema de Arquivos (CISCO NETACAD, 2014).

## Nomenclatura do Nome do IOS da Cisco

A Cisco, como uma Empresa que monta dissipativos de Redes, também desenvolve muitas versões diferentes do Sistema Operacional IOS. Isso ocorre porque ele pode suportar várias plataformas de *hardware* de vários equipamentos, e uma série de recursos (*features*) e características próprias, o que é realizado continuamente conforme a evolução da tecnologia e dos dispositivos.

Para que possamos identificar as diferentes versões existentes, a Cisco tem uma convenção de atribuição de nomes para arquivos do Sistema Operacional IOS.

Essa convenção de atribuição utiliza diferentes campos do nome indicado. Entre esses campos, estão: a identificação da plataforma de *hardware*, a identificação de recursos disponíveis (*features*) e a versão numérica (*release*) do Sistema Operacional (CISCO NETACAD, 2014).



Figura 6 – Nova Nomenclatura do Cisco IOS

Analizando a nomenclatura de nome, indicamos, na primeira parte, à esquerda, o nome do arquivo do Sistema Operacional Cisco IOS que também identifica a plataforma de *hardware* para a qual essa imagem foi desenvolvida.

A segunda parte define e identifica os vários recursos ou funcionalidades (*features*) contidos nesse arquivo de SOR. Com isso, é possível notar que existem diversos recursos que podem ser escolhidos por um determinado cliente ou administrador de Rede, por causa da gama e funcionalidade dos dispositivos de Rede.

Esses recursos são empacotados em diferentes “imagens do IOS” e cada conjunto de recursos contém um subconjunto específico de todos os recursos disponibilizados.

Como exemplos de categorias que incorporam conjuntos de recursos (*features*), temos:

- **Básico** – Um conjunto de recursos básicos para uma Plataforma de *hardware*, como, por exemplo, IP e IP/FW;
- **Plus** – Um conjunto de recursos básicos acrescido de recursos adicionais, tais como IP Plus, IP/FW Plus e Enterprise Plus;
- **Criptografia** – A adição de recursos de criptografia de dados de 56 bits, como na versão Plus 56, as versões básico ou plus, como, por exemplo, o IP/ATM Plus IPSEC 56 ou o Enterprise Plus 56. Do Cisco IOS versão 12.2 em diante, os designadores de criptografia são k8/k9:
  - » **k8** – Criptografia igual ou inferior a 64 bits no IOS versão 12.2 e superiores;
  - » **k9** – Criptografia superior a 64 bits (em 12.2 e superiores).

A terceira parte do nome do arquivo indica o seu formato, ou seja, especifica se o IOS está armazenado na memória *flash* em formato compactado ou se ele é realocável, pois, se a imagem do IOS estiver na *flash*, de uma forma compactada, o IOS deverá ser expandido durante a inicialização à medida que o Sistema Operacional for copiado para a memória RAM.

Uma imagem realocável é copiada da memória *flash* para a memória RAM, diretamente para ser executada.

A quarta parte do nome do arquivo identifica a versão do IOS (*release*), que identifica as novas versões do IOS desenvolvidas. O número da versão numérica geralmente aumenta com novas versões criadas de um mesmo Sistema Operacional (CISCO NETACAD, 2014).

Para dispositivos de Redes mais novos, a Cisco, geralmente, embarca nesse equipamento um Sistema Operacional completo (todas as funções possíveis que um Sistema Operacional da Cisco possa conter); porém, dependendo da forma como foi adquirido, nem todas essas funções são ativadas por padrão.

Nesse caso, o Administrador de Rede necessita comprar uma chave de liberação para os recursos que necessita e, depois disso, precisa aplicar tal chave para permitir a utilização desse recurso desejado.

## Registrador de Configuração

A ordem em que o roteador procura informações de *bootstrap* (inicialização) do Sistema depende muito da definição do campo de inicialização (*boot-field*), que é definida no *configuration register*.

Essa definição padrão do *configuration register* pode ser devidamente alterada, caso seja necessário, com o comando **config-register** do modo configuração global do IOS, acompanhada de um valor hexadecimal como argumento para esse comando.

O *configuration register* nada mais é do que um registrador de 16 bits armazenado em memória NVRAM. Os quatro *bits* inferiores do *configuration register* identificam o campo de inicialização (*boot field*).

Para que se possa identificar esses valores do registro de configuração, basta aplicar o comando **show version**. Caso deseje alterar o registro de configuração (apesar de não ser o recomendado nesse momento, pois é um processo que altera as sequências de *boot* do equipamento), utilize o comando **config-register**.

Não iremos tratar de todas as funções que o registro de configuração pode suportar; porém, é importante se lembrar de que o número padrão do *configuration register* é 0x2142, que faz com que o equipamento faça o *boot* corretamente e que vá buscar o arquivo de configuração do equipamento em memória NVRAM, primeiramente (CISCO NETACAD, 2014).

# Material Complementar

## Indicações para saber mais sobre os assuntos abordados nesta Unidade:

### Livros

#### **Redes de Computadores e a Internet**

STALLINGS, W. e ROSS K. – **Redes de Computadores e a Internet** 5.ed. Pearson, 2010.

#### **Redes de Computadores**

TANENBAUM, A. S. **Redes de Computadores** – 5.ed. Pearson, 2011.

### Leitura

#### **Curso Web – Conceitos Básicos de Roteadores – Módulo 4: Aprendendo sobre dispositivos**

CISCO NETACAD. **Módulo de Roteamento e Switching** – CCNA2 – Conceitos Básicos de Roteadores – Módulo 4 – Aprendendo sobre dispositivos, Versão 3.0, EUA, 2014.

#### **Curso Web – Conceitos Básicos de Roteadores – Módulo 5: Conhecimentos do Software Cisco IOS**

CISCO NETACAD. **CCNA2** – Conceitos Básicos de Roteadores. Módulo 5. Conhecimentos do Software Cisco IOS. Versão 3.0, EUA, 2014.

# Referências

CISCO NETACAD. **Módulo de Roteamento e Switching:** Conceitos Essenciais (CCNA2) – 6<sup>a</sup> Versão, Cisco Systems, 2017 (Material *on-line*).

STALLINGS; ROSS. **Redes de Computadores e a Internet.** 5.ed. Pearson, 2010.

TANENBAUM, A. S. **Redes de Computadores.** 5.edPearson, 2011.





**Cruzeiro do Sul**  
Educacional

# Tecnologias de Roteamento



Cruzeiro do Sul Virtual  
Educação a distância



# Material Teórico



**Tipos de Redes, Protocolos de Rede e Modelo de Referência**

**Responsável pelo Conteúdo:**

Prof. Esp. Antonio Eduardo Marques da Silva

**Revisão Textual:**

Prof. Esp. Claudio Pereira do Nascimento



# UNIDADE

## Tipos de Redes, Protocolos de Rede e Modelo de Referência



- Introdução;
- Componentes de Rede;
- Protocolos e Padrões de Redes;
- Modelo de Referência em Camadas;
- Endereços Públicos e Privados do IPv4.



### OBJETIVO DE APRENDIZADO

- Compreender e abordar os tipos de redes existentes (LANs, MANs e WANs), protocolos de redes e os modelos de referência OSI/ISO e TCP/IP.





# Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:



## Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu “momento do estudo”;
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

# Introdução

Quando acessamos a Internet a fim de utilizar algum recurso de rede, como, por exemplo, o envio de um *e-mail*, um *download* de um arquivo ou até mesmo um simples acesso a um portal WEB para leremos uma notícia, vários processos são realizados no computador e na rede para que você possa acessar esses recursos de forma confiável e com boa qualidade.

Nesta unidade vamos tratar dos componentes e tipos de redes existentes, bem como conhecer um pouco sobre a importância dos protocolos de comunicação e identificar os modelos de referência de redes mais utilizados, como por exemplo o modelo OSI/ISO e o modelo TCP/IP.

## Componentes de Rede

O caminho que uma mensagem enviada em uma rede percorre da máquina origem à máquina destino pode ser tão simples quanto um único cabo conectando ponto a ponto ou tão complexo quanto uma rede de abrangência geográfica global. Essa infraestrutura de rede é o alicerce que dá suporte à rede. Ela tem o intuito de fornecer um canal estável e confiável sobre a qual nossas comunicações podem ocorrer.

Uma infraestrutura de rede contém três categorias básicas de componentes de rede, são elas:

- dispositivos de rede (*Hosts*);
- meio físico (Cabo Coaxial, Cabo de Par trançado, Fibra Óptica);
- serviços de rede.

Dispositivos de rede e meio físico de rede são os elementos físicos (*hardware* da rede). O *hardware* de rede geralmente define os componentes visíveis da plataforma de rede, tais como um Servidor, um PC, um *Switch*, um Roteador, um Ponto de Acesso sem Fio ou os cabos de conexão utilizados para conectar os dispositivos. No caso de meio físico sem fio, as mensagens são transmitidas pelo próprio ar através da utilização de frequência de rádio invisível ou de ondas infravermelhas.

### Dispositivos finais de rede

Os dispositivos de rede que os usuários estão mais familiarizados são conhecidos como dispositivos finais de rede ou *hosts*. Esses *hosts* formam a interface entre os clientes e a rede de comunicação.

Alguns exemplos de dispositivos finais de rede (*hosts*) seriam:

- computadores (estações de trabalho, laptops e servidores);
- impressoras de rede;

- telefones VoIP;
- terminal de telepresença;
- câmeras de vídeo e segurança;
- dispositivos móveis (*smartphones, tablets, PDAs e scanners*).

Um *host* pode ser a origem ou o destino de uma mensagem transmitida através da rede. Para distinguir um *host* de outro, cada *host* em uma rede é identificado utilizando um endereço. Quando um *host* inicia a comunicação da informação, ele utiliza o endereço do *host* de destino para especificar para onde a mensagem deveria ser transmitida (STALLINGS, W. e ROSS K., 2010).

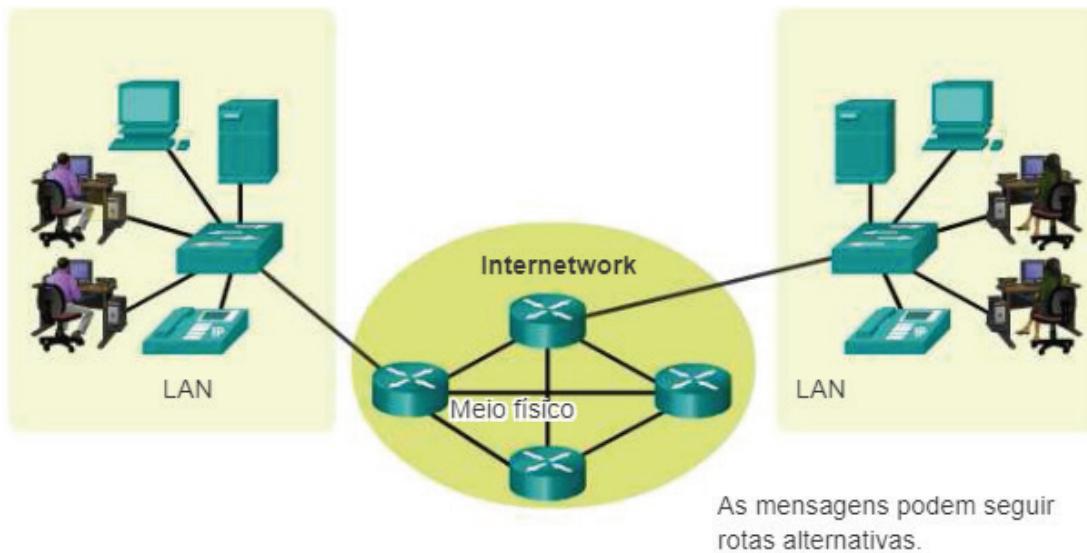


Figura 1 – Dispositivos Finais de Rede

Fonte: CISCO NETACAD (2017)

## Dispositivos intermediários de rede

Os dispositivos intermediários de rede se interconectam a dispositivos finais e possuem o objetivo de definir os limites da rede. Esses dispositivos fornecem conectividade e funcionam em segundo plano para garantir que os dados sejam transmitidos através da rede. Esses dispositivos se conectam aos hosts individuais à rede e podem se conectar em várias redes individuais para formar uma rede interconectada.

Exemplos de alguns dispositivos intermediários de rede seriam:

- acesso à rede (*switches* e pontos de acesso sem fio);
- interconexão (roteadores);
- segurança (*firewalls*).

O gerenciamento dos dados é feito à medida em que eles fluem pela rede que é uma das funções dos dispositivos intermediários. Eles utilizam o endereço do *host* destino, em conjunto com as informações sobre as interconexões de rede, a fim de determinar o caminho que as mensagens devem percorrer na rede em questão.

Os processos em execução dos dispositivos de rede intermediários desempenham as seguintes funções:

- regenerar e retransmitir sinais de dados;
- manter informações sobre quais caminhos existem na rede;
- notificar outros dispositivos de erros e falhas de comunicação;
- direcionar dados por caminhos alternativos quando houver uma falha de conexão;
- classificar e direcionar mensagens de acordo com prioridades de Qualidade de Serviços (QoS) aplicada na rede;
- permitir ou negar o fluxo de dados, com base em configurações de segurança limítrofe.

## Tipos de redes de comunicação

---

Uma Infraestruturas de rede pode variar muito em relação aos seguintes itens, por exemplo:

- tamanho da área de cobertura da rede;
- número de usuários conectados à rede;
- número e tipos de serviços disponíveis aos usuários.

Os tipos mais comuns de infraestruturas de rede:

- **Rede de Área Local (LAN):** uma infraestrutura de rede que fornece acesso a usuários e dispositivos finais em uma área geograficamente limitada, como por exemplo um andar de um edifício ou uma sala;
- **Rede de Longa Distância (WAN):** uma infraestrutura de rede que fornece acesso a outras redes dentro de uma grande área geograficamente ilimitada. A Internet seria o melhor exemplo de uma rede desse tipo;
- **Rede Metropolitana (MAN):** uma infraestrutura de rede que abrange uma área física geograficamente maior que uma LAN, porém menor que uma WAN com uma abrangência de uma cidade, por exemplo. As MANs são operadas normalmente por uma entidade pública, ou uma grande organização privada;
- **Rede de Área Local sem Fio (WLAN):** semelhante a uma LAN cabeada, mas interconecta sem a conectividade de cabos dentro de uma área geográfica pequena e limitada;
- **Rede de Armazenamento (SAN):** uma infraestrutura de rede projetada para suportar servidores de rede e fornecer armazenamento, recuperação e replicação de dados. Envolve servidores de alto desempenho, vários conjuntos de discos (chamados blocos) e tecnologia de interconexão *Fibre Channel*.

# Protocolos e Padrões de Redes

Os diversos protocolos de rede de comunicação devem ser capazes de interagir e trabalhar em conjunto para que a comunicação de rede seja bem-sucedida e realize corretamente suas funções. Conjuntos de protocolos são implementados por hosts e dispositivos de rede no software, no hardware ou em ambas as partes. Uma das melhores maneiras de visualizar como os protocolos dentro de um conjunto interagem é verificar a interação como uma pilha de protocolos.

Uma pilha de protocolos mostra como os protocolos individuais dentro de um conjunto são devidamente implementados. Estes são visualizados em camadas, com cada serviço de nível superior, dependendo da funcionalidade definida pelos protocolos mostrados nos níveis inferiores. As camadas inferiores da pilha estão relacionadas com a movimentação de dados pela rede e o fornecimento de serviços às camadas superiores, que se concentram no conteúdo da mensagem que está sendo enviada (CISCO NETACAD, 2017).

Podemos usar várias camadas para poder descrever as atividades que ocorrem em nosso exemplo de comunicação presencial. Na camada inferior, a camada física, temos duas pessoas, cada uma com um tom de voz que pode pronunciar palavras em voz alta. Na segunda camada, a camada das regras, temos um acordo para falar em um determinado idioma em comum. Na camada superior, a camada de conteúdo, existem palavras que são realmente faladas e possuem o conteúdo da comunicação e um entendimento lógico daquilo que é transmitido (STALLINGS, W. e ROSS K., 2010).

## Protocolos de redes

---

Para que os dispositivos de rede se comuniquem com sucesso, um conjunto de protocolos de rede devem descrever exigências mínimas de funcionamento e interações precisas. Os protocolos de comunicação de rede definem um formato e um conjunto de padrões de regras comuns para a troca de mensagens entre dispositivos de rede. Alguns protocolos de rede comuns do conjunto de protocolos IPv4 são o IP, HTTP e DHCP.

Os protocolos de rede descrevem os seguintes processos:

- como a mensagem está formatada ou estruturada para ser enviada na rede de comunicação;
- o processo pelo qual os dispositivos de rede compartilham informações sobre caminhos com outras redes;

- quando e como as mensagens de erro do sistema são transmitidas entre os dispositivos;
- a configuração e o término de sessões das transferências de dados a serem realizadas.

Por exemplo, o IP define como um pacote de dados é entregue dentro de uma rede local (LAN) ou para uma rede remota (WAN). As informações do protocolo IPv4 são transmitidas em um formato específico para que o receptor possa interpretá-las corretamente e que os dados sejam enviados para um destinatário corretamente. As informações devem obedecer a um determinado formato ou padrão para que tal informação seja transportada.

## Interação de protocolos de rede

---

Os diferentes protocolos de comunicação trabalham em conjunto para garantir que as mensagens sejam recebidas e entendidas por ambas as partes e que as aplicações possam interagir, como, por exemplo, um servidor Web e um cliente Web. Exemplos desses protocolos seriam:

- **Protocolo de Aplicação:** o protocolo HTTP é um protocolo que rege a forma de interação entre um servidor e um cliente Web. O HTTP define o conteúdo e formatação das solicitações e respostas trocadas entre o cliente e o servidor. Tanto o software do cliente quanto o do servidor Web implementam HTTP como parte da aplicação. O HTTP conta com outros protocolos para reger o modo como as mensagens são transportadas entre cliente e servidor (CISCO NETACAD, 2017);
- **Protocolo de Transporte:** o protocolo TCP é o protocolo de transporte que gerencia as conversas individuais entre servidores e clientes Web. O TCP divide as mensagens HTTP em partes menores, chamadas de segmentos. Estes segmentos são enviados entre os processos do servidor e cliente Web em execução no host destino. O TCP também é responsável por controlar o tamanho e o ritmo em que as mensagens são trocadas entre o servidor e o cliente (CISCO NETACAD, 2017);
- **Protocolo de Internet:** o protocolo IP é responsável por retirar os segmentos formatados do TCP, encapsulá-los em pacotes, atribuindo a eles endereços apropriados, além de entregá-los através do melhor caminho de rede até o host destino. Este último processo de envio de dados através de um melhor caminho em base a uma métrica de envio é conhecido como protocolo de roteamento;
- **Protocolos de Acesso à Rede:** os protocolos de acesso à rede descrevem duas funções básicas, a comunicação por meio de um enlace de dados e a transmissão física de dados na mídia de rede. Os protocolos de gerenciamento de enlace de dados retiram os pacotes do IP e os formatam para serem trans-

mitidos pelo meio físico. Os padrões e protocolos para o meio físico regem como os sinais são enviados e como eles são interpretados pelos clientes receptores. Um exemplo de um protocolo de acesso à rede é a *Ethernet* (CISCO NETACAD, 2017).

## Conjunto de protocolos de rede

Um conjunto de protocolos de rede é um grupo de protocolos que funcionam em conjunto para fornecer serviços abrangentes de uma comunicação de rede, ele pode ser especificado por uma organização de padrões ou até mesmo ser desenvolvido por um fornecedor / fabricante no segmento de TIC.

Os protocolos IP, HTTP e DHCP são partes do conjunto de protocolos da Internet conhecido como TCP/IP - *Transmission Control Protocol / Internet Protocol*. Esse conjunto de protocolos é um padrão aberto por norma e significa que eles estão totalmente disponíveis ao público em geral e qualquer fornecedor pode implementá-los no *hardware* ou no *software* de suas aplicações proprietárias (TANENBAUM, A. S., 2011).

Um protocolo baseado em padrões é um processo ou protocolo que foi endossado pelo setor de rede e ratificado, ou aprovado, por uma organização de padrões. O uso de padrões no desenvolvimento e na implementação de protocolos assegura que produtos de diferentes fabricantes possam interoperar com êxito. Se um protocolo não for rigidamente observado por um fabricante específico, seu equipamento ou software pode não ser capaz de se comunicar com sucesso com produtos fabricados por outros fabricantes (CISCO NETACAD, 2017).

Na comunicação de dados, por exemplo, se uma extremidade da conversação estiver utilizando um protocolo a fim de poder se comunicar com um dispositivo que está utilizando um outro protocolo, provavelmente a comunicação não poderá ocorrer, pois tais dispositivos não ‘falam’ a mesma língua e por esse motivo não se entenderão na respectiva comunicação (TANENBAUM, A. S., 2011).

Alguns protocolos são proprietários e, neste contexto, significa que uma empresa ou um fornecedor controla a definição do protocolo, como ele funciona e como foi desenvolvido. Neste caso, as comunicações devem ser realizadas em redes que possuam também dispositivos e aplicações proprietárias desse fabricante, caso contrário, os dados não serão trocados em dispositivos de outras marcas e muito menos na Internet que é uma rede aberta. Podemos, por exemplo, citar os protocolos proprietários da *Apple* (*Appletalk*) e o da *Novell* (*Novell NetWare*).



Como funciona a Internet? Parte 1 – O protocolo IP: <https://youtu.be/HNQD0qJOTC4>

TCP/IP	ISO	AppleTalk	Novell Netware
HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Ethernet PPP Frame Relay ATM WLAN			

Figura 2 – Conjunto de Protocolos

Fonte: CISCO NETACAD (2017)

## Modelo de Referência em Camadas

Um modelo de referência em camadas, como o modelo OSI e o modelo TCP/IP, é muitas vezes utilizado para auxiliar na visualização e interação entre vários protocolos de rede. Um modelo de camadas tem como principal intuito representar a operação dos protocolos que ocorrem dentro de cada camada do modelo, bem como a interação dos protocolos com as camadas acima e abaixo da camada correspondente. Podemos descrever alguns benefícios na utilização dos modelos de referência em camadas, como segue:

- auxilia na compreensão de como é o funcionamento da rede como um todo, tanto em relação aos protocolos de cada camada como em relação aos dispositivos de rede a serem utilizados na topologia;
- estimula a competição e desenvolvimento dos protocolos, pois os produtos de diferentes fornecedores podem trabalhar em conjunto;
- impede que mudanças de tecnologia ou habilidade em uma camada afetem outras camadas acima e abaixo;
- auxilia na elaboração de um protocolo, pois sabendo onde um protocolo deverá operar, sabe-se as regras específicas de cada camada e como eles irão manipular informações e as interfaces com as camadas inferiores e superiores;

- fornece uma padronização comum para descrever funções e habilidades da rede de dados.

Existem dois tipos básicos de modelos de rede:

- **Modelo de Protocolo:** esse modelo corresponde muito bem à estrutura de um conjunto específico de protocolo. O conjunto hierárquico de protocolos relacionados em um conjunto geralmente representa toda a funcionalidade necessária para fazer a interface da rede humana com a rede de dados. O modelo TCP/IP é um modelo de protocolo, visto que descreve as funções que ocorrem em cada camada de protocolos dentro do conjunto TCP/IP (CISCO NETACAD, 2017);
- **Modelo de Referência:** como o nome indica, esse modelo oferece consistência em todos os tipos de protocolos e serviços de rede descrevendo como é realizado os processos e o que precisa ser feito em uma camada específica. O principal propósito desse modelo é o de auxiliar em um entendimento mais claro das funções e dos processos envolvidos na comunicação de dados, às vezes é conhecido como um protocolo de direito.

O modelo de referência OSI da ISO é o modelo de referência de rede mais amplamente conhecido pelo segmento de tecnologia de informação. Ele é utilizado para o entendimento e elaboração de *layouts* de rede de dados, especificações de operação e resolução de problemas em uma rede (TANENBAUM, A. S., 2011).

## O Modelo de referência OSI

---

Inicialmente, o modelo de referência OSI foi elaborado pela ISO para fornecer uma estrutura na qual fosse possível criar um conjunto de protocolos de sistemas abertos. A ideia da criação desse modelo seria o desenvolvimento de um conjunto de protocolos que pudesse ser utilizado em uma rede internacional independente de sistemas proprietários (STALLINGS, W. e ROSS K., 2010).

Em contrapartida, a velocidade na qual a Internet baseada no protocolo TCP/IP foi adotada e a frequência na qual se expandia causou atraso no desenvolvimento e na aceitação do conjunto de protocolos do OSI. Embora poucos protocolos desenvolvidos usando as especificações OSI sejam amplamente usados atualmente, o modelo OSI de sete camadas fez grandes contribuições ao desenvolvimento de outros protocolos e produtos para todos os tipos de novas redes. Esse modelo fornece uma lista extensiva de funções e serviços que podem ocorrer em cada camada. Ele também descreve a interação de cada camada com as camadas diretamente acima e abaixo dela (CISCO NETACAD, 2017).

As camadas do Modelo OSI são: Física, Enlace, Rede, Transporte, Sessão, Apresentação e Aplicação.

## O Modelo de fato TCP/IP

O modelo do conjunto de protocolos TCP/IP usado nas comunicações de rede foi criado no início dos anos 70 e costuma ser chamado de modelo de Internet, pois suas características e usabilidade foram implementadas nessa grande rede. É uma arquitetura que define quatro camadas de funções que devem ocorrer para que as comunicações sejam bem-sucedidas na rede. O modelo de protocolos TCP/IP é um padrão aberto, ou seja, não se tem uma empresa ou marca que controle seus recursos e qualquer usuário pode utilizá-lo livremente.

As definições do padrão e dos protocolos TCP/IP são discutidas em um fórum público e definidas em um conjunto publicamente disponível de RFCs, elas por sua vez contêm a especificação formal de protocolos de comunicação de dados e recursos que descrevem o uso dos protocolos a serem utilizados de forma aberta. Os RFCs também contêm documentos técnicos e organizacionais sobre a Internet, incluindo as especificações técnicas e os documentos de política produzidos pela IETF - Internet Engineering Task Force (CISCO NETACAD, 2017).

As camadas do modelo TCP/IP são: Acesso à Rede, Internet, Transporte e Aplicação.

## Comparação dos modelos OSI e TCP/IP

Os protocolos de rede que são descritos dentro do conjunto de protocolos da família TCP/IP podem ser comparados com a descrição em termos com o do modelo de referência OSI da ISO. No modelo OSI/ISO, as camadas física e de enlace de dados são representadas como a camada de acesso à rede do TCP/IP. As três camadas superiores que são a sessão, apresentação e aplicação do modelo OSI estão descritas na camada de aplicação do modelo TCP/IP respectivamente (TANENBAUM, A. S., 2011).

Na camada de acesso à rede, o conjunto de protocolos TCP/IP não especifica que protocolos utilizam para se transmitir sobre um meio físico; ele descreve somente a transmissão da camada de Internet aos protocolos da rede física. As Camadas 1 e 2 do modelo OSI identificam os procedimentos necessários de uma forma detalhada para se acessar o meio físico com o intuito de se enviar dados em uma rede de comunicação.

As analogias diretas entre os dois modelos de rede (TCP/IP e OSI) ocorrem nas Camadas 3 e 4 do modelo OSI. A Camada 3 do modelo OSI, que é a camada de rede, é utilizada quase que universalmente para descrever o intervalo dos processos que ocorrem em todas as redes de dados para que possam lidar com mensagens enviadas com o intuito de roteá-las pela rede. O IP é o protocolo que faz parte do conjunto TCP/IP e que inclui várias funcionalidades descritas detalhadamente na Camada 3 do modelo OSI Rede (TANENBAUM, A. S., 2011).

Já a camada 4 do modelo OSI, que seria a camada de transporte, descreve os vários serviços e funções gerais que fornecem uma entrega ordenada e confiável de dados transmitidos entre os dispositivos de origem e destino. Essas funções incluem reconhecimento, recuperação de erros e sequenciamento dos dados enviados. Nesta camada do conjunto de protocolos TCP/IP podemos citar dois protocolos, o protocolo TCP e o protocolo UDP, que podem fornecer funcionalidades necessárias para que o dado seja transmitido sem problemas (TANENBAUM, A. S., 2011)).

A camada de aplicação do conjunto de protocolos TCP/IP inclui uma série de protocolos que deve fornecer uma série de funcionalidade específicas a uma variedade de aplicações de usuário final. As Camadas 5, 6 e 7 do modelo OSI são usadas como referências para os desenvolvedores e fornecedores de software de aplicativo de usuário, para que possam produzir produtos funcionais que operem nas redes de comunicação de uma forma interoperável.



Figura 3 – Comparação entre OSI e TCP/IP

Fonte: CISCO NETACAD (2017)

## Camada de Enlace e Endereço MAC

O modelo de referência OSI descreve os processos de formatação, codificação, segmentação e encapsulamento dos dados para a transmissão pela rede. A camada de rede e a camada de *link* de dados são por sua vez responsáveis por fornecer os dados do *host* origem ou remetente para o *host* destino ou destinatário. Ambos os protocolos dessas duas camadas possuem os endereços de origem e destino dos dispositivos participantes da comunicação, mas esses endereços têm finalidades diferentes, como segue:

### Endereço de Enlace de Dados

O endereço de enlace de dados, ou Camada 2, é conhecido como endereço físico e desempenha um papel fundamentalmente diferente. A finalidade do endereço

de link de dados é fornecer o frame de enlace de dados de uma interface de rede para outra interface de rede na mesma rede local que estão. Para que um pacote IPv4 possa ser enviado pela rede cabeada ou sem fio, deve ser encapsulado em um frame de enlace de dados e que possa ser transmitido através do meio físico. As LANs baseadas no protocolo *Ethernet* cabeado e sem fios são dois exemplos de redes locais que possuem meios físicos diferentes, cada um com seu próprio tipo de protocolo de enlace de dados e características de interfaces próprias (STALLINGS, W. e ROSS K., 2010).

Na transmissão da rede, o pacote IP então é encapsulado em um quadro de enlace de dados para que possa ser entregue à rede destino na respectiva comunicação. Os endereços de enlace de dados dos hosts de origem e destino são então adicionados:

- **Endereço de Enlace de Dados Origem:** o endereço físico da interface do dispositivo que está enviando o quadro na transmissão. Inicialmente, essa é a placa de rede que é o dispositivo de origem do pacote IP;
- **Endereço de Enlace de Dados Destino:** o endereço físico da interface do dispositivo que irá receber a informação, ou do roteador do próximo salto, que tem como função fazer a interligação entre as redes locais e remotas para que o dado seja enviado até um determinado destino fora da rede local.

### **Redes *Ethernet* e Subcamadas LLC / MAC e endereço de Enlace**

O protocolo de rede local (LAN) *Ethernet* é atualmente a tecnologia mais utilizada na interconexão de hosts. Ela opera na camada de enlace de dados e na camada física em relação ao modelo de referência OSI/ISO. É um conjunto de tecnologias de redes de comutação definida nos padrões IEEE 802.2 (LLC) e IEEE 802.3 (*Ethernet* descrita no IEEE - *Institute of Electrical and Electronics Engineers*). Tal rede pode suportar algumas vazões de dados como segue:

- 10 Mb/s;
- 100 Mb/s;
- 1000 Mb/s (1 Gb/s);
- 10.000 Mb/s (10 Gb/s);
- 40.000 Mb/s (40 Gb/s);
- 100.000 Mb/s (100 Gb/s).

Os padrões de rede *ethernet* definem os protocolos de Camada 2 e as tecnologias físicas de Camada 1. Em relação ao protocolo de Camada 2 (enlace), a *ethernet*

nessa camada é dividida em duas subcamadas, a subcamada de controle lógico de link (LLC) e a subcamada de controle de acesso ao meio (MAC) (TANENBAUM, A. S., 2011).

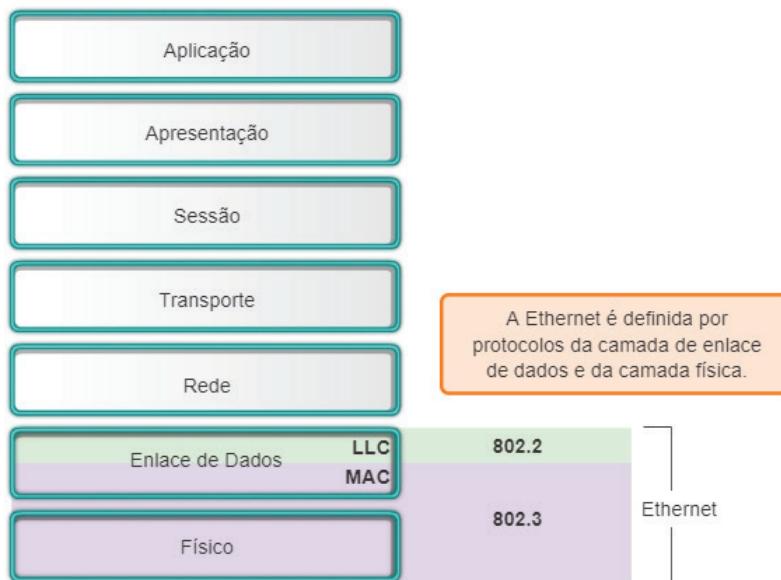


Figura 4 – Rede *Ethernet*

Fonte: CISCO NETACAD (2017)

## Estrutura do endereço MAC

Os endereços MAC devem ser globalmente exclusivos e seus valores são um resultado direto de regras impostas pelo IEEE a fornecedores para garantir endereços globalmente exclusivos que identifiquem dispositivos de rede na *Ethernet*. Tais regras estabelecidas pelo IEEE exigem que todos os fornecedores e fabricantes que vendam dispositivos de rede *Ethernet* sejam registrados no IEEE.

O IEEE atribui a cada fabricante / fornecedor um código de 3 bytes (24 bits) chamado Identificador organizacionalmente exclusivo (OUI), exigindo que siga duas regras simples:

- Todos os endereços MAC atribuídos a uma placa de rede de um dispositivo *Ethernet* devem usar os três primeiros bits para identificar o OUI atribuído ao fornecedor;
- Todos os endereços MAC com o mesmo OUI, ou seja, fabricados pelo mesmo fornecedor, devem receber um valor exclusivo (código do fornecedor ou número de série) nos últimos 3 bytes, que identifica características próprias de quem fabrica.

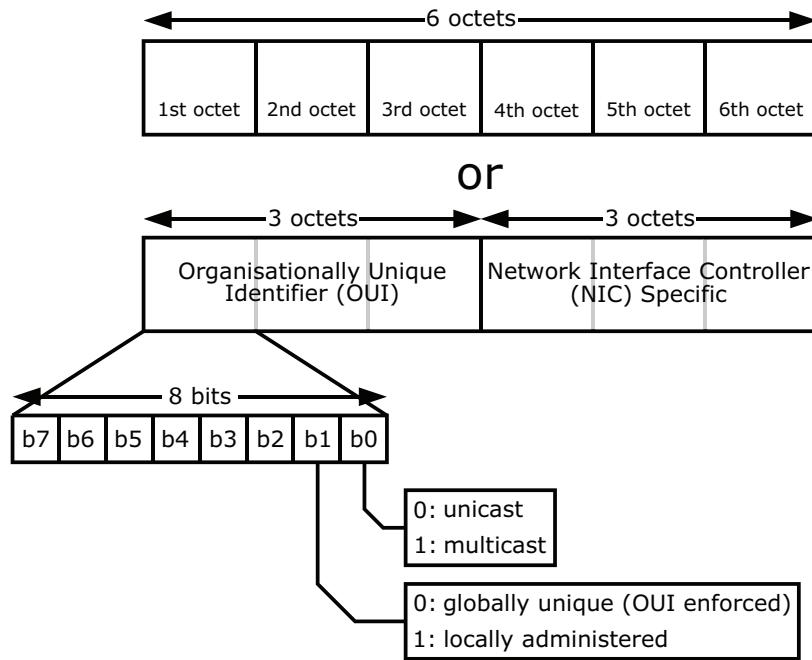


Figura 5 – Estrutura do Endereço MAC

Fonte: Wikimedia Commons

## Camada de rede e endereço IPv4

O endereço da camada de rede, ou Camada 3, é um endereço lógico e contém informações necessárias para que seja feita a entrega do pacote IP do *host* origem para o *host* destino. Um endereço IPv4, que é um endereço de camada de rede, tem duas partes, o prefixo que identifica a rede e a parte que identifica o *host* (REDE/HOST). O prefixo que identifica a porção rede do endereço é utilizada pelos roteadores para que possam encaminhar os pacotes de dados para uma rede apropriada em direção ao dispositivo de destino. Já a porção do *host* do endereço é utilizada pelo último roteador no caminho (roteador mais próximo ao *host* destino) para entregar o pacote ao dispositivo destino (STALLINGS, W. e ROSS K., 2010).

Um pacote IP possui dois endereços IPv4:

- **Endereço IPv4 Origem:** o endereço IPv4 que identifica o dispositivo emissor na transmissão de rede;
- **Endereço IPv4 Destino:** o endereço IPv4 que identifica o dispositivo receptor. O endereço IP destino é usado por roteadores da rede para encaminhar um pacote através dos possíveis caminhos até o seu destino da melhor forma possível (melhor métrica).

## Estrutura da Camada de Rede

---

A camada 3 do modelo OSI, ou camada de rede, pode fornecer serviços para que se possa permitir que dispositivos finais troquem dados através da rede. Para que ela possa fazer o transporte fim a fim, a camada de rede usa quatro processos básicos, que seriam:

- **Endereçamento:** da mesma maneira que um telefone convencional, que possui um identificador numérico exclusivo, dispositivos finais de rede precisam ser configurados com um endereço IP único que o identifica em uma rede. Tal dispositivo final de rede identificado com um endereço IP é conhecido como um *host*;
- **Encapsulamento:** em um processo chamado encapsulamento, a camada correspondente (ou de rede no exemplo) adiciona as informações do cabeçalho IP, como os endereços IP dos dispositivos origem e destino da transmissão e outros qualificadores de controle. Depois que as informações de cabeçalho são adicionadas à PDU (*Protocol Data Unit*) correspondente, ela é apelidada de vários nomes, como por exemplo: *Bit* para a camada física, quadro para a camada de enlace e pacote para a camada de rede;
- **Roteamento:** a camada de rede tem como função fornecer serviços para direcionar os pacotes a um dispositivo destino para uma mesma ou outra rede de uma melhor forma possível. Para que esse pacote seja encaminhado para o transporte de uma outra rede, ele deve ser processado por um dispositivo que faz roteamento (roteador). A função do roteador é fazer a escolha dos melhores caminhos para que os pacotes sejam direcionados aos *hosts* destino. Os pacotes enviados podem atravessar vários dispositivos intermediários de rede antes de alcançar o destino final. A cada rota que um pacote faz para chegar ao *host* destino é chamada de salto (*hops*);
- **Desencapsulamento:** quando um determinado pacote chega à camada de rede do equipamento destino, tal dispositivo examina o cabeçalho IP do pacote recebido. Se o endereço IP destino incluído no cabeçalho corresponde ao seu próprio endereço IP, o cabeçalho IP será removido do pacote com a finalidade de ler camadas mais internas desse invólucro. Tal processo de remover os cabeçalhos das camadas inferiores é conhecido como desencapsulamento de dados. Como exemplo: depois que o pacote (camada 3) for desencapsulado pela camada de rede, a PDU resultante da camada 4 (segmentos) é passada para a camada de transporte em um serviço apropriado.



Figura 6 – Protocolos da Camada de Rede

Fonte: CISCO NETACAD (2017).

## Endereços Públicos e Privados do IPv4

Quando o endereçamento IPv4 foi devidamente implementado na Internet, os endereços eram praticamente todos públicos, ou seja, endereços únicos na rede e entregues através dos provedores e órgãos de administração da Internet. Com o aumento de utilização da rede e o eventual esgotamento desses endereços, surge a necessidade da criação de blocos de endereços privados, ou seja, que possuem apenas significado local em uma rede e não são roteados na Internet, pois podem ser endereços repetidos em outras redes locais.

### Endereços Privados

Os endereços privativos são definidos pelo RFC 1918, conhecido como alocação de endereço de Internet privada, e algumas vezes chamados de endereços RFC 1918, apenas. Os blocos de endereço que identificam o espaço privado são apresentados abaixo. Foram extraídos e reservados com essa finalidade um bloco da classe A, da classe B e da classe C. Isso foi realizado porque, dependendo da classe que é utilizada, é possível identificar uma quantidade limitada de hosts dentro de uma rede. Por exemplo: se usarmos uma rede de classe C, com uma máscara de rede padrão (/24), podemos ter dentro dessa rede cerca de 254 hosts ativos. Quando usamos endereços privados em um host dentro de uma rede local, estes não são conhecidos pela Internet e por esse motivo necessitam a utilização de NAT (*Network Address Translation*) para que possam “sair” do ambiente local e podem ser identificados na rede mundial.

Os blocos de endereços particulares são:

- 10.0.0.0 a 10.255.255.255 (10.0.0.0/8);
- 172.16.0.0 a 172.31.255.255 (172.16.0.0/12);
- 192.168.0.0 a 192.168.255.255 (192.168.0.0/16).

No RFC 6598, o IANA (*Internet Assigned Numbers Authority*) também reservou outro grupo de endereços conhecidos como o espaço de endereço compartilhado. Semelhante ao espaço de endereço privado RFC 1918, os endereços de espaço de endereço compartilhado não são roteáveis globalmente. Entretanto, esses endereços são destinados somente para uso em redes de provedores de serviços. O bloco de endereços é compartilhado 100.64.0.0/10 (CISCO NETACAD, 2017).

## Endereços Públicos

A maioria dos endereços *unicast* do IPv4 são endereços públicos, eles foram desenvolvidos para serem utilizados de uma forma que possam ser acessíveis através da rede publicamente, ou seja, são considerados endereços válidos na Internet. Além desses endereços, existem muitos outros endereços que são atribuídos a outros fins especiais.

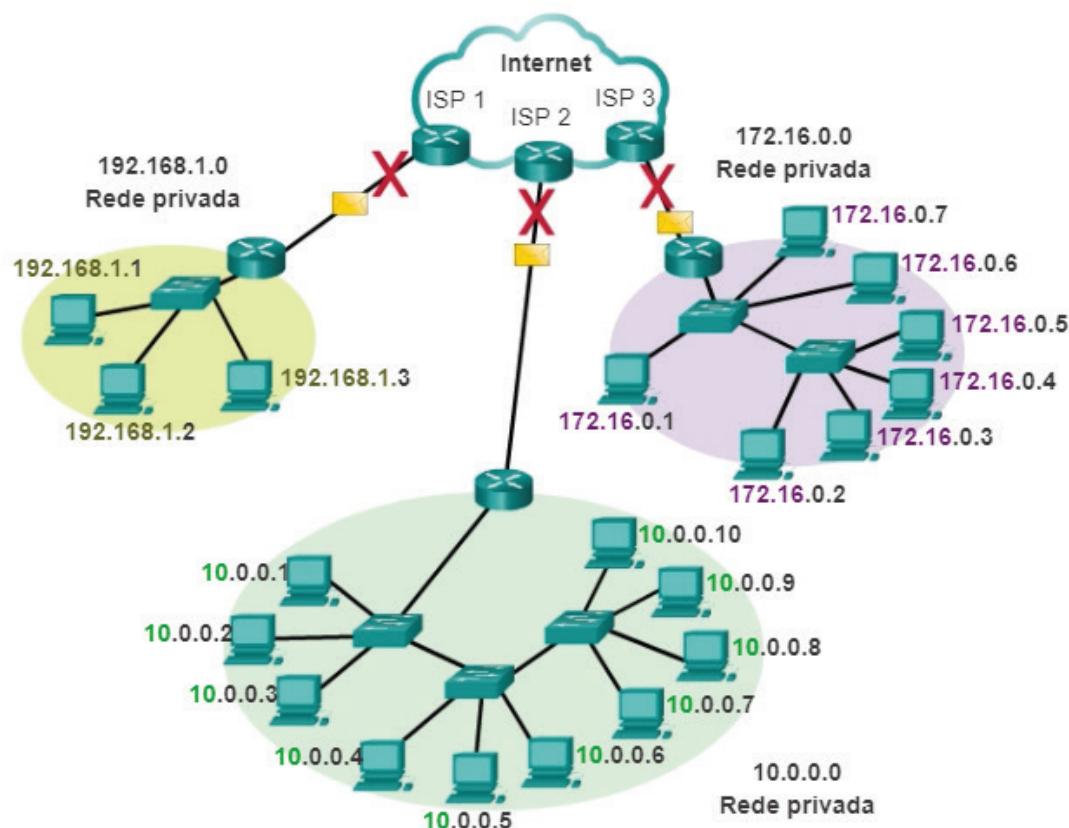


Figura 7 – Endereços Público e Privados do IPv4

Fonte: CISCO NETACAD (2017)

## Endereços ClassFull

No RFC1700, foram agrupados intervalos de endereços de *unicast* que definem tamanhos específicos da quantidade de *hosts* em uma rede através das classes A, classe B e classe C. Além dessas classes, possuem outras que definem endereços de *multicast*, que é definido pela classe D e a classe E, considerada uma classe experimental.

Classe	Primeiro octeto	Parte da rede ( <b>N</b> ) e parte para hosts ( <b>H</b> )	Máscara	Nº Redes / hosts por rede
<b>A</b>	1-127	<b>N.H.H.H</b>	255.0.0.0	<b>126</b> redes <b>16,777,214</b> hosts por rede ( $2^{24}-2$ )
<b>B</b>	128-191	<b>N.N.H.H</b>	255.255.0.0	<b>16,384</b> redes ( $2^{14}$ ) <b>65,534</b> hosts por rede ( $2^{16}-2$ )
<b>C</b>	192-223	<b>N.N.N.H</b>	255.255.255.0	<b>2,097,150</b> redes ( $2^{21}$ ) <b>254</b> hosts por rede ( $2^8-2$ )
<b>D</b>	224-239	Multicast	NA	NA
<b>E</b>	240-255	experimental	NA	NA

Figura 8 – Endereços ClassFull do IPv4

Fonte: CISCO NETACAD (2017)

- **Blocos de Classe A:** a classe A possui um bloco de endereços projetado para suportar redes grandiosas, com mais de 16 milhões de endereços reservados para dispositivos, esses endereços utilizavam um prefixo fixo /8 (ou 255.0.0.0) com o primeiro octeto para indicar os endereços na rede. Os três outros octetos à direita eram usados para os endereços mapear dispositivos de rede. Todos os endereços de classe A possuem um bit mais significativo à esquerda do primeiro octeto reservado como zero. Ou seja, podemos afirmar que havia apenas 128 redes possíveis de classe A, 0.0.0.0/8 a 127.255.255.255/8, sendo que o 127.0.0.0 apesar de ser uma classe A, também é reservado para a função de *loopback*.
- **Blocos de Classe B:** a classe B possui um bloco de endereços projetado para suportar redes de tamanho moderado com aproximadamente cerca de 65.000 dispositivos. Esse endereço usava dois octetos da esquerda para a direita para indicar o endereço de rede /16 (255.255.0.0), já os dois últimos octetos à direita especificavam os endereços de dispositivos. No caso de endereços classe B, os dois bits mais significativos do octeto de alta ordem eram 10 (lê-se um e zero), restringindo o bloco de endereços de 128.0.0.0/16 para 191.255.255.255/16, podendo suportar pelo menos cerca de 16.000 redes.
- **Blocos de Classe C:** a classe C possui um bloco de endereços projetado para suportar redes de tamanho pequeno com 254 dispositivos. Esses blocos de endereço usavam um prefixo /24 (255.255.255.0), ou seja, uma rede de classe C possui apenas o ultimo octeto para a criação de dispositivos e os três octetos de alta ordem eram usados para indicar o endereço da rede. Os blocos de endereço de classe C reservavam espaço de endereço usando um valor fixo de 110 (um, um, zero) para os três dígitos mais significativos do octeto de alta ordem, da esquerda para a direita. Isso restringia tal bloco de endereçamento de classe C entre 192.0.0.0/24 para 223.255.255.255/24. Mesmo ocupando apenas 12,5% do total de espaço de endereços IPv4, poderia fornecer endereços para 2 milhões de redes aproximadamente.

Os endereços IP não são todos iguais - parte 1: <https://youtu.be/jnuHODaLc08>

# Material Complementar

## Indicações para saber mais sobre os assuntos abordados nesta Unidade:

### Sites

#### **Módulo de Introdução a Redes – Capítulo 1: Explorando a Rede, Versão 6.0**

CISCO NETACAD. **Módulo de Introdução a Redes** – Capítulo 1: Explorando a Rede, Versão 6.0. EUA: Editora Cisco Systems/Site.

[www.netacad.com](http://www.netacad.com)

#### **Módulo de Introdução a Redes – Capítulo 2: Explorando a Rede, Versão 6.0**

CISCO NETACAD. **Módulo de Introdução a Redes** – Capítulo 2: Explorando a Rede, Versão 6.0. EUA: Editora Cisco Systems/Site.

[www.netacad.com](http://www.netacad.com)

### Livros

#### **Redes de Computadores e a Internet**

STALLINGS, W. e ROSS K. **Redes de Computadores e a Internet**. 5. ed. São Paulo: Editora Pearson, 2010.

#### **Redes de Computadores**

TANENBAUM, A. S; WETHERALL, D. **Redes de Computadores**. 5. ed. Rio de Janeiro: Editora Campus, 2011.

# Referências

CISCO NETACAD. **Módulo de Introdução a Redes (CCNA1)**. 6. v. Cisco Systems, 2017 (Material *on-line*). Disponível em: <[www.netacad.com](http://www.netacad.com)>. Acesso em: 20/10/2018.

STALLINGS, W. e ROSS K. **Redes de Computadores e a Internet**. 5. ed. São Paulo: Editora Pearson, 2010.

TANENBAUM, A. S; WETHERALL, D. **Redes de Computadores**. 5. ed. Rio de Janeiro: Editora Campus, 2011.





**Cruzeiro do Sul**  
Educacional

# Tecnologias de Roteamento



Cruzeiro do Sul Virtual  
Educação a distância



# Material Teórico



**Camadas de Transporte/Aplicação e Sistema  
Operacional de Rede (SOR) da Cisco**

**Responsável pelo Conteúdo:**

Prof. Esp. Antonio Eduardo Marques da Silva

**Revisão Textual:**

Prof. Me. Luciano Vieira Francisco



# UNIDADE

## Camadas de Transporte/Aplicação e Sistema Operacional de Rede (SOR) da Cisco



- Introdução;
- Camada de Transporte;
- Camada de Apresentação;
- Sistema Operacional de Rede (SOR);
- Proteção ao Dispositivo.



### OBJETIVO DE APRENDIZADO

- Compreender as camadas superiores do modelo de referência de rede OSI como, por exemplo, as camadas de transporte, sessão, apresentação e aplicação;
- Obter conhecimentos fundamentais do Sistema Operacional de Rede (SOR) da Cisco.





# Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:



## Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu “momento do estudo”;
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

# Introdução

Quando acessamos a Internet a fim de utilizar algum recurso como, por exemplo, o envio de e-mail, *download* de arquivo ou até mesmo o simples acesso a um portal *web* para leremos uma notícia, vários processos são realizados no computador e na rede para que você possa acessar esses recursos de forma confiável e com boa qualidade.

Assim, nesta Unidade você conhecerá as funções das camadas de transporte, sessão, apresentação e aplicação e seus protocolos mais importantes. Igualmente de uma forma simples, veremos o funcionamento do Sistema Operacional de Rede (SOR) da Cisco, assim como comandos básicos e onde é devidamente armazenado e manipulado em um dispositivo intermediário de rede.

## Camada de Transporte

A camada de transporte tem como função estabelecer uma sessão de comunicação temporária entre dois hosts finais, permitindo que os dados sejam transmitidos corretamente. Essa camada pode fornecer um método de distribuição de dados em toda a rede de uma maneira a assegurar que sejam devidamente colocados de uma forma ordenada para que o receptor opere sem problemas; proporciona também a segmentação dos dados em pedaços menores e controla o fluxo desses segmentos para que sejam reagrupados no destinatário.

No TCP/IP, os processos de segmentação dos dados e reagrupamento das informações no destinatário podem ser obtidos por meio de dois protocolos da camada de transporte: *Transmission Control Protocol* (TCP) e *User Datagram Protocol* (UDP).

As principais responsabilidades dos protocolos de camada de transporte são:

- Rastrear a comunicação de uma forma individual entre as aplicações nos dispositivos de origem e destino;
- Segmentar os dados para que possam ser gerenciados a fim de que sejam remontados nos dispositivos de destino;
- Identificar a aplicação adequada e controlar o seu fluxo no processo de comunicação.

## Confiabilidade da Camada de Transporte

Tal como comentamos, a camada de transporte também tem como atividade gerenciar os requisitos para que a comunicação seja confiável, pois diferentes aplicações de rede possuem distintas características e necessidades de confiabilidade para o seu pleno funcionamento.

A camada de rede que possui o protocolo IP está preocupada apenas com o endereçamento, a estrutura de encapsulamento dos pacotes e com o processo de roteamento. Dito de outra forma, o protocolo IP não especifica como os pacotes serão transportados ou entregues em um receptor.

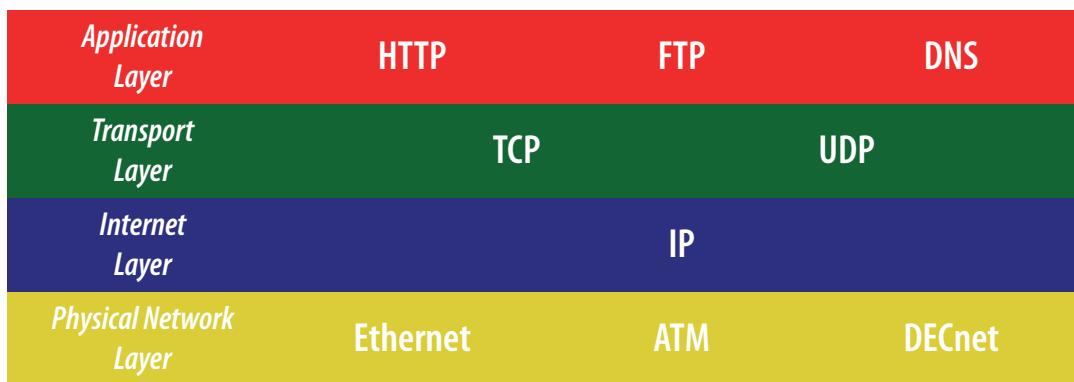


Figura 1 – Confiabilidade do Transporte

Nesse contexto, os protocolos de transporte definem e especificam como as informações devem ser transmitidas entre dispositivos de rede. O IP utiliza os protocolos de transporte TCP ou UDP para que os hosts sejam ativados e que possam transferir os dados.

O protocolo de transporte TCP é considerado confiável, completo, garantidor de que todos os segmentos de dados cheguem ao destino. Ao contrário, o protocolo UDP tem um cabeçalho simples e que praticamente não fornece confiabilidade alguma na transmissão, porém, por ser um protocolo enxuto, possui maior flexibilidade e rapidez quando transportado na rede.

## ***Transmission Control Protocol (TCP)***

---

No conjunto de protocolos TCP/IP, o protocolo de transporte TCP é a camada intermediária entre o IP abaixo desta e uma aplicação acima. Usando o TCP, as aplicações em hosts em rede podem estabelecer conexões confiáveis entre si. Ademais, esse protocolo garante, de forma confiável, a entrega em ordem de dados a partir do emissor ao receptor.

## **Operação Básica do Protocolo**

---

TCP é orientado à conexão, ou seja, os dados do usuário não são trocados entre os pontos TCP até que uma conexão seja estabelecida entre os dois pontos finais. Tal ligação é realizada durante toda a transmissão de dados entre os nós. Conexões TCP têm três fases:

- 1º Estabelecimento de conexão;
- 2º Transferência de dados;
- 3º Término de conexão.

## Cabeçalho do Protocolo TCP

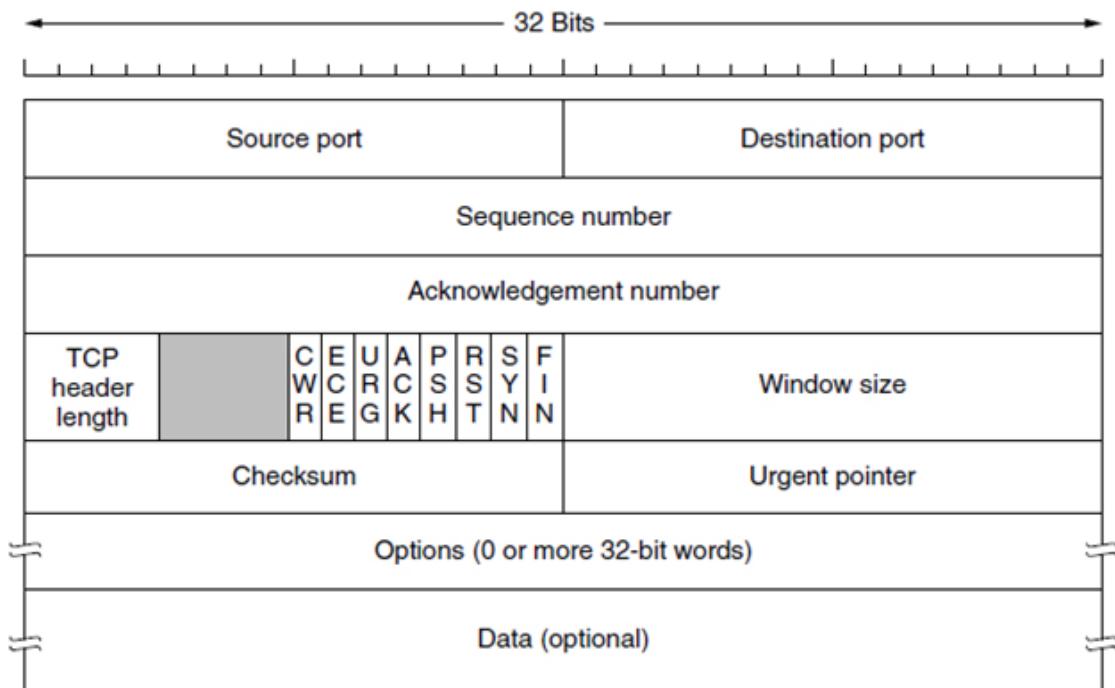


Figura 2 – Cabeçalho do segmento TCP

Fonte: Wikimedia Commons

## User Datagram Protocol (UDP)

Descrito no RFC 768, o UDP é simples e seu PDU é chamado de datagrama, este considerado não confiável, pois não garante que o dado será reconstruído se não for recebido em ordem correta. Se for necessário termos confiabilidade nas informações transmitidas, o protocolo de transporte UDP e as aplicações que o utilizam por natureza não devem ser empregados.

Enquanto UDP não é confiável, as ausências de verificação e correção de erros fazem com que esse protocolo seja muito rápido e eficiente para diversas aplicações de dados intensivos ou menos sensíveis ao tempo como, por exemplo, o *Domain Name Service (DNS)*, *Simple Network Management Protocol (SNMP)*, *Dynamic Host Configuration Protocol (DHCP)* e *Routing Information Protocol (RIP)* – este último considerado um protocolo de roteamento. Ademais, a utilização do protocolo de transporte UDP também é adequada para streaming de vídeo.

Eis alguns recursos que descrevem o datagrama UDP:

- **Sem orientação à conexão:** não possui um mecanismo de estabelecimento de conexão entre os dispositivos na comunicação, antes que os dados sejam transmitidos;
- **Entrega não confiável:** não fornece mecanismos de confiabilidade para que os dados possam ser enviados de uma forma segura; além disso, não possui processos de retransmissão de dados perdidos ou corrompidos;
- **Sem reconstrução ordenada:** os dados são transmitidos em sequência e devem ser recebidos nessa mesma ordem, pois o UDP não possui técnicas de remontagem e reagrupamento dos datagramas enviados;
- **Sem controle de fluxo:** não possui um mecanismo de controle e gerenciamento da qualidade na transmissão dos dados. Se a origem transmitir os dados e os recursos de rede ficarem sobrecarregados, o host de destino provavelmente descartará os dados até que os recursos possam se tornar disponíveis novamente; além disso, não possui um mecanismo de reenvio de dados descartados ou corrompidos.

## Cabeçalho do Protocolo UDP

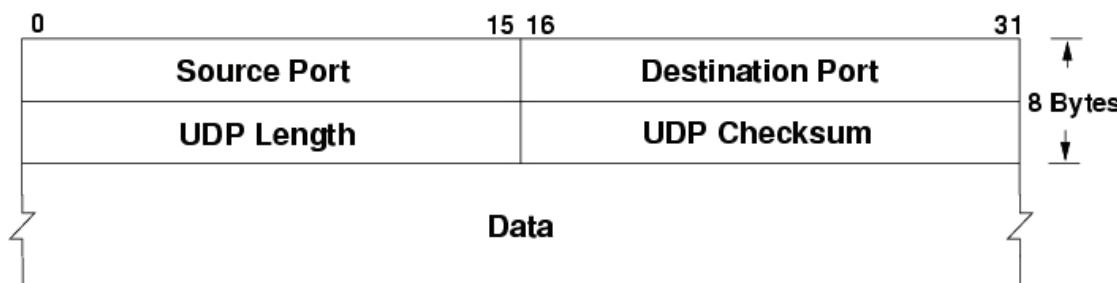


Figura 3 – Cabeçalho do datagrama UDP

Fonte: Wikimedia Commons



Veja como a internet funciona, no tocante aos sistemas autônomos, BGP e PTT, no vídeo disponível em: [https://youtu.be/C5qNAT\\_j63M](https://youtu.be/C5qNAT_j63M)

## Camada de Apresentação

A camada de apresentação tem três funções principais:

1. Codificação e conversão de dados de camada de aplicação para assegurar que os dados a partir da fonte possam ser interpretados pela aplicação apropriada no dispositivo de destino;

2. Compressão dos dados de forma que possam ser descompactados pelo dispositivo de destino;
3. Criptografia dos dados para transmissão e descriptografia após o recebimento pelo destino.

Implementações da camada de apresentação não estão tipicamente associadas a uma pilha de protocolo particular – os padrões para vídeos e gráficos são exemplos. Alguns padrões conhecidos para vídeos incluem *QuickTime* e *Motion Picture Experts Group* (MPEG) – *QuickTime* é uma especificação Apple Computer para vídeo e áudio e MPEG é um padrão para compressão de vídeo e codificação.

Entre os formatos de imagem gráfica conhecidos figuram os seguintes: *Graphics Interchange Format* (GIF), *Joint Photographic Experts Group* (JPEG) e *Tagged Image File Format* (TIFF) – GIF e JPEG correspondem à compressão de padrões de codificação para imagens gráficas, enquanto TIFF é um formato de codificação padrão para imagens gráficas.

Lembre-se de que ao comparar o modelo de referência OSI ao TCP/IP, a camada de sessão do modelo OSI figurará contida na camada de aplicação do TCP/IP em conjunto com as camadas de apresentação e aplicação do modelo OSI.

## Camada de Sessão

---

Funções na camada de sessão devem criar e manter diálogos entre a origem e o destino das aplicações utilizadas na transmissão dos dados. A camada de sessão lida com a troca de informações para iniciar diálogos e mantê-los ativos, assim como para reiniciar as sessões que são interrompidas ou estão ociosas por um longo intervalo de tempo.

## Camada de Aplicação

---

O mundo experimenta a internet por meio do uso dos programas de compartilhamento de arquivos *world wide web*, e-mail etc. Tais aplicações, bem como outros recursos, fornecem a interface humana para a rede subjacente, o que permite enviar e receber informações com relativa facilidade. A maioria das aplicações é intuitiva, possibilitando acesso e uso sem a necessidade de saber como funcionam.

### Alguns Protocolos da Camada de Aplicação do TCP/IP

Os protocolos da camada de aplicação do TCP/IP mais amplamente conhecidos são aqueles que fornecem a troca de informações do usuário. Podem ainda especificar o formato e controlar informações necessárias para muitas das funções de comunicação da internet. Entre tais protocolos de aplicação do TCP/IP podemos citar os seguintes:

- *Domain Name System (DNS)*: utilizado para resolver nomes da internet em endereços IP;
- *Hypertext Transfer Protocol (HTTP)*: empregado para transferir arquivos que compõem as páginas do *world wide web*.
- *Simple Mail Transfer Protocol (SMTP)*: usado para a transferência de mensagens de correio e anexos;
- *File Transfer Protocol (FTP)*: utilizado para a transferência interativa de arquivos entre sistemas;
- *Telnet*: um protocolo de emulação de terminal, usado para fornecer acesso remoto a servidores e dispositivos de rede.

Os protocolos do conjunto TCP/IP são comumente definidos pelas RFC. O *Internet Engineering Task Force* (IETF) mantém as RFC, que são as normas para o conjunto de protocolos do TCP/IP.



Os endereços IP não são todos iguais - parte 2 – <https://youtu.be/5hDZbroaQDc>

Veja porque os endereços IP não são todos iguais.

## Sistema Operacional de Rede (SOR)

Todos os dispositivos finais e os de rede conectados à internet exigem um SOR para auxiliar na execução de uma função.

Quando um computador é conectado em uma rede, carrega o sistema operacional que comumente está instalado em uma unidade de disco, SSD ou *flash* na memória de trabalho ou RAM. A parte do código do sistema operacional que interage diretamente com o hardware é conhecida como *kernel* e a que faz a interface com os aplicativos e o usuário final é conhecida como *shell*. O usuário pode interagir com o uso do *shell* na Interface de Linha de Comando (CLI) ou na Interface Gráfica de Usuário (GUI), significativamente utilizada em ambientes gráficos, tal como o sistema operacional *Windows* (CISCO NETACAD, 2017).

Ao usar a CLI, o usuário interage diretamente com o sistema operacional em um ambiente baseado em texto ao inserir comandos no teclado digitados a frente de um prompt de comando. O sistema executa o comando, geralmente fornecendo uma saída textual. Já a interface GUI permite que o usuário interaja com o sistema operacional em um ambiente que utilize imagens gráficas, multimídia e textos. As ações são realizadas pela interação com as imagens na tela graficamente. A GUI é mais fácil de usar e requer menos conhecimento do operador na estrutura do comando para se utilizar o sistema. Por esse motivo, muitas pessoas

confiam em ambientes de GUI. A maioria dos sistemas operacionais do dispositivo final é acessada usando a GUI, incluindo o *MS Windows*, *MAC OS X*, *Linux*, *Apple iOS*, *Android* e muito mais.

Os dispositivos de rede de infraestrutura também utilizam um SOR. O sistema operacional de rede empregado em dispositivos da Cisco é chamado de *Internetwork Operating System (IOS)* – Cisco IOS é um termo genérico dos sistemas operacionais de rede empregados em dispositivos de rede da Cisco como, por exemplo, *switches* e roteadores que independem do tamanho ou tipo do dispositivo. O método mais comum de acessar esses dispositivos por meio do IOS é usando uma CLI.

## Finalidade do Sistema Operacional

---

Sistemas operacionais de rede são, de várias formas, semelhantes aos sistemas operacionais de computadores pessoais. Ademais, um sistema operacional executa várias funções técnicas internas, permitindo que um usuário:

- Possa usar um *mouse*;
- Exiba a saída de informações em um monitor;
- Insira comandos de texto na prompt de comando;
- Selecione opções dentro de uma janela da caixa de diálogo.

As funções internas de *switches* e roteadores são muito parecidas, pois fornecem uma interface ao administrador de rede, quem pode inserir comandos para configurar ou programar o dispositivo para realizar várias tarefas de rede. Os detalhes operacionais do IOS variam entre os dispositivos de redes interconectadas, dependendo do propósito e recursos suportados pelos quais.

Cisco IOS é um termo que abrange diversos sistemas operacionais diferentes em execução para vários dispositivos de rede. Existem muitas variações distintas do Cisco IOS, por exemplo:

- IOS para *switches*, roteadores e outros dispositivos de rede da Cisco;
- Versões numeradas de IOS para determinado dispositivo de rede da Cisco;
- Recurso IOS define o fornecimento de pacotes diferentes de recursos e serviços.

## Localização do IOS nos Equipamentos

---

Em muitos dispositivos Cisco, o IOS é copiado na memória flash e depois carregado na memória de acesso aleatório (RAM), conhecida também como memória de trabalho, quando o dispositivo é iniciado. O IOS é, então, carregado e executado na RAM quando o dispositivo está em funcionamento, atividade que possui muitas funções – tais como armazenar dados que serão utilizados pelo dispositivo para dar suporte a operações de rede.

Executar o IOS na RAM aumenta o desempenho do dispositivo, pois essa memória é rápida; no entanto, a RAM é considerada uma memória volátil porque os dados são perdidos caso o dispositivo deixe de ser alimentado pela energia elétrica – **ciclo de energia**.

A  
Z

Um **ciclo de energia** ocorre quando um dispositivo é desligado propositalmente ou por acidente e, então, religado.

## Funções do IOS

Roteadores, *switches* e pontos de acesso da Cisco que utilizam o IOS executam funções esperadas pelos administradores de rede – depois de corretamente configuradas – a fim de funcionarem conforme o esperado. As principais funções executadas ou habilitadas pelos roteadores, *switches* e pontos de acesso da Cisco incluem:

- Oferecer segurança de rede limítrofe e dos dispositivos;
- Endereçamento IP de interfaces físicas e virtuais;
- Permitir configurações específicas à interface com o objetivo de otimizar a conectividade do respectivo meio físico;
- Fazer corretamente o roteamento – encaminhamento de pacotes por meio do melhor caminho – dos dados de rede;
- Habilitar tecnologias de Qualidade de serviço (QoS);
- Suportar tecnologias de gerenciamento de rede.

Cada recurso ou serviço de rede possui uma coleção de comandos associados de configuração, os quais permitem que um administrador de rede possa implementá-los.

Ademais, os serviços fornecidos pelo sistema operacional Cisco IOS são comumente acessados usando uma Interface de Linha de Comando (CLI), comandos os quais aplicados em uma prompt de execução.

## Métodos de Acesso do IOS

Existem várias maneiras de acessar o ambiente de CLI da Cisco IOS, sendo as mais comuns:

- Porta denominada *Console* – a primeira forma de acesso;
- Porta denominada *AUX* – porta auxiliar em que se pode conectar um modem;
- Conexão *Telnet* ou *SSH*.

Figura 4 – Porta *Console*

## Programas de Emulação de Terminal

Há vários e excelentes programas de emulação de terminal disponíveis para conectar um dispositivo de rede por meio serial de comunicação sobre uma porta de console ou conexão *Telnet/SSH*; vejamos as seguintes aplicações:

- PuTTY;
- *Tera Term*;
- SecureCRT;
- *HyperTerminal*.

Essas aplicações de emulação de terminal permitem que o administrador de rede aumente a sua produtividade ajustando tamanhos de janela, alterando tamanhos de fonte e esquemas de cores.

Para que possamos, então, acessar um roteador ou *switch* da Cisco – pela primeira vez – é necessário conectar o cabo console – cabo específico de configuração – na porta *Console* do dispositivo e rodar uma aplicação de emulação de terminal para acessar o CLI do dispositivo que deve ser configurado.

## Navegação no Sistema Operacional Cisco IOS

Depois que um administrador de rede estiver conectado a um dispositivo de rede, será possível configura-lo por meio da navegação de vários modos de configuração do IOS. Tais modos são semelhantes em *switches*, roteadores e pontos de acesso – o CLI utiliza uma estrutura hierárquica para que esses modos possam ser acessados.

Utilizando essa hierarquia dos padrões do Cisco IOS, podemos definir os seguintes modos mais clássicos e utilizados:

- De execução do usuário – EXEC usuário;
- De execução privilegiada – EXEC privilegiado;
- De configuração global;

Outros modos específicos de configuração, tais como de interface, de *line*, de roteamento, de protocolo etc.

Cada modo possui um prompt específico que é utilizado para realizar determinadas tarefas por meio de um conjunto de comandos disponíveis somente para aquele padrão de configuração. Por exemplo, o modo de configuração global permite que um administrador defina as configurações que afetam o dispositivo como um todo, tal como especificar um nome para esse dispositivo – comando `hostname`. No entanto, um modo diferente é necessário se o administrador de rede desejar definir configurações de segurança para uma porta específica em um *switch*. Nesse caso, deve acessar o modo de configuração de interface – `config-if` – dessa porta – todos os padrões inseridos no modo de configuração de interface se aplicam apenas a essa porta.

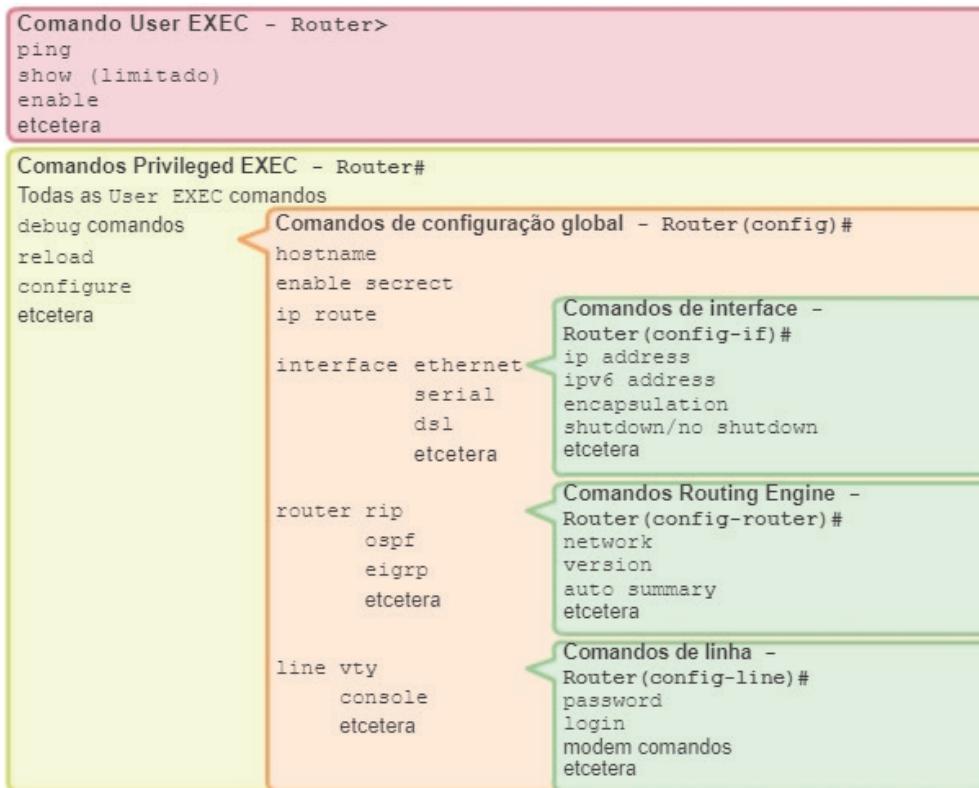


Figura 5 – Estrutura hierárquica do IOS

## Modos Primários de Configuração

Os dois modos primários de operação são o EXEC usuário e EXEC privilegiado. Como um recurso de segurança, o software Cisco IOS separa as sessões EXEC em dois níveis de acesso (Figura 6). O modo EXEC privilegiado possui um nível superior de autoridade e prerrogativa, no qual permite que o usuário possa fazer um todo no equipamento.

## Modo EXEC Usuário

O modo EXEC usuário tem recursos limitados e com poucos privilégios, mas é útil para algumas operações básicas no equipamento. Está no nível mais básico da estrutura hierárquica dos modos de configuração, sendo o primeiro modo executado na entrada do CLI de um dispositivo IOS, logo que tal equipamento é inicializado.

O modo EXEC usuário permite uma quantidade limitada de comandos básicos de monitoramento como, por exemplo, de verificação, além de alguns comandos *show*, *ping* e *tracert*. Ademais, o nível EXEC usuário não permite a execução de quaisquer comandos que poderiam alterar a configuração do dispositivo como um todo, muito menos comandos que possam apagar arquivos de configuração e resetar o respectivo dispositivo.

Por padrão, não há autenticação exigida para acessar o modo EXEC usuário por meio da conexão console. Contudo, essa é uma boa prática para garantir que a autenticação seja estabelecida durante a configuração inicial (CISCO NETACAD, 2017).

O modo EXEC usuário é identificado pelo prompt do CLI que termina com o símbolo >. Eis um exemplo que mostra o símbolo > no prompt: *Router>*

## Modo EXEC Privilegiado

A execução de comandos de configuração e gerenciamento exige que o administrador de rede use o modo EXEC privilegiado ou um mais específico na hierarquia. Significa que um usuário deve, inicialmente, entrar no modo EXEC usuário e, de lá, acessar o modo EXEC privilegiado (CISCO NETACAD, 2017).

O modo EXEC privilegiado pode ser identificado pelo prompt terminado com o símbolo #, por exemplo: *Router#*

Por padrão, o modo EXEC privilegiado não requer autenticação; contudo, é uma boa prática garantir que a autenticação seja configurada.

Ademais, o modo de configuração global e outros padrões como, por exemplo, o de configuração de interface, podem ser alcançados apenas a partir do modo EXEC privilegiado.

## Modo de Configuração Global

---

O modo de configuração global, ou *config. global*, afeta a operação no dispositivo como um todo – eis o motivo do nome. Tal modo de configuração é acessado antes dos modos específicos de configuração, tais como os de interface e roteamento.

O comando CLI a seguir é usado para tirar o dispositivo do modo EXEC privilegiado e acessar o de configuração global, a fim de permitir a entrada de comandos de configuração por meio de uma conexão de terminal.

*Router# configure terminal*

Depois que tal comando for executado, o prompt é alterado para mostrar que o *switch* está no modo de configuração global: *Router(config)#*

## Modos Específicos de Configuração

---

No modo de configuração global, o usuário pode inserir diferentes modos de sub-configuração, cada um permitindo a configuração de uma parte específica ou função do dispositivo de IOS, casos exemplares dos modos de:

- *Interface*: para configurar uma das interfaces de rede – Fa0/0, S0/0/0;
- Linha: para configurar uma das linhas físicas ou virtuais – console, AUX, VTY.

Para sair de um modo específico de configuração e voltar ao modo global para tal, insira o comando *exit* em um prompt do sistema operacional. Para deixar por completo o modo de configuração e voltar ao padrão EXEC privilegiado, insira o comando *end* ou use a sequência de teclas <Ctrl-Z>.

## Prompts de Comando

---

Ao usar a CLI, o modo é identificado pelo prompt da linha de comando que é único para aquele modo. Por padrão, todo prompt começa com o nome do dispositivo como, por exemplo, *router* ou *switch*.

Após o nome, o restante do prompt indica o modo em que está. Outro exemplo, o prompt padrão do modo de configuração global em um *switch* seria *Router(config)#*

## Navegar entre os Modos do IOS

Os comandos enable e disable são empregados para alterar a CLI entre os modos EXEC usuário e privilegiado, respectivamente.

Do padrão usuário para acessar o modo EXEC privilegiado, use o comando *enable* – algumas vezes o modo EXEC privilegiado é chamado de modo habilitar –; o comando *disable* é utilizado para retornar do padrão privilegiado ao modo usuário. O comando *exit* no modo privilegiado termina toda a sessão com o dispositivo; ou seja:

```
Router>  
Router> enable  
Router#  
Router# disable  
Router>  
Router> exit
```

## Ajuda Contextual ou Help

Cisco IOS possui várias formas de ajuda – *help* – disponíveis, por exemplo:

- Ajuda contextual;
- Verificação de sintaxe de comando;
- Teclas de acesso e atalhos.

A ajuda contextual fornece uma lista de comandos e os argumentos associados a esses comandos dentro do contexto do modo atual. Logo, para acessar a ajuda contextual, insira uma interrogação (?) em qualquer *prompt*. Há uma resposta imediata – sem a necessidade de usar a tecla <Enter> para executá-lo.

## Comandos de Monitoramento

Com o intuito de verificar e solucionar eventuais problemas na operação da rede, devemos checar a operação dos dispositivos de rede. O comando básico de monitoramento é *debug* ou *show* – existem muitas variações e qualificadores diferentes para esses comandos.

À medida que você desenvolve mais habilidades com Cisco IOS, aprenderá a melhor forma de usar e interpretar os resultados desses comandos – por exemplo, teste o comando *show?* para obter uma lista de subcomandos disponíveis em determinado contexto ou modo a ser aplicado.

Ainda sobre o comando *show*, pode fornecer várias informações acerca da configuração, operação e do status de partes de um *switch* ou roteador da Cisco – podemos verificar alguns dos comandos mais comuns em Cisco IOS.

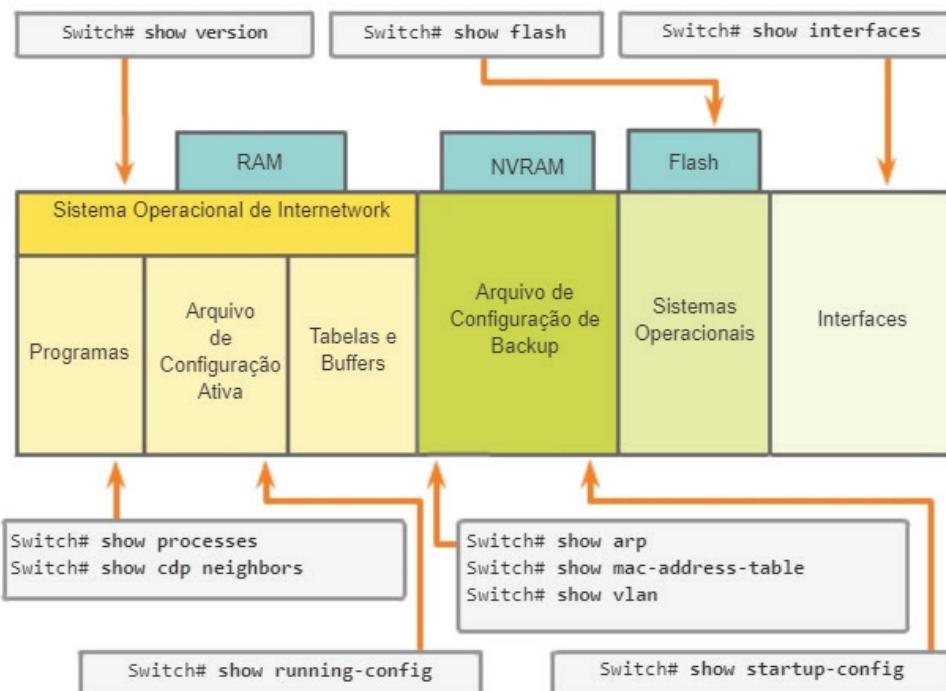


Figura 6 – Comandos de exames

## Proteção ao Dispositivo

Limitar fisicamente o acesso a dispositivos de rede, colocando-os em racks fechados ou abertos – o que seria uma boa prática de segurança física –; no entanto, senhas são as principais defesas contra o acesso não autorizado a esses dispositivos de rede. Cada dispositivo, até mesmo o trivial roteador doméstico, deve ter senhas configuradas localmente para limitar o acesso (CISCO NETACAD, 2017).

Cisco IOS utiliza modos hierárquicos de configuração para auxiliar na segurança do dispositivo em questão, fazendo parte desse reforço de segurança lógica do equipamento. O sistema operacional pode aceitar várias senhas para determinar e permitir distintos privilégios de acesso ao equipamento.

Ademais, as senhas aqui apresentadas são as seguintes:

- **Habilitar Senha:** limita o acesso ao modo EXEC privilegiado, isto com senha em texto claro;
- **Habilitar Senha Secreta:** limita o acesso ao modo EXEC privilegiado, com senha criptografada em MD5;
- **Senha do Console:** limita o acesso via conexão console ao dispositivo a ser utilizado;
- **Senha VTY:** limita o acesso ao dispositivo com conexão de sessão *Telnet*.

```
Router> enable
Router#
Router# configure terminal
Router(config)# enable secret class
Router(config)# exit
Router#
Router# disable
Router> enable
Password: class
Router#
```

## Arquivo de Configuração

---

O arquivo de configuração em execução na memória RAM reflete a configuração atual aplicada a um dispositivo Cisco. Contém comandos utilizados para determinar como o dispositivo deve operar na rede. Assim, modificar uma configuração em execução afeta imediatamente a operação de um dispositivo Cisco (CISCO NETACAD, 2017).

O arquivo de configuração de execução – *running-configuration* – é armazenado na memória de operação/trabalho do dispositivo ou de acesso aleatório (RAM). Significa que o arquivo de configuração de execução está temporariamente ativo enquanto o dispositivo Cisco é executado – ligado – e energizado. Entretanto, se a energia do dispositivo for cessada, ou se o equipamento for reiniciado, todas as mudanças na configuração serão perdidas a menos que tenham sido salvas, pois a memória RAM é volátil.

Depois de fazer alterações em um arquivo de configuração em execução, considere estas opções distintas:

- Retorne o dispositivo à sua configuração original;
- Remova todas as configurações do dispositivo;
- Torne a configuração alterada a nova para inicialização.

O arquivo de configuração de inicialização – *startup-configuration* – reflete a configuração que será utilizada pelo dispositivo na reinicialização, arquivo que está armazenado na NVRAM, esta que é uma memória rápida e não volátil. Quando um dispositivo de rede for configurado e a configuração em execução tiver sido modificada, será importante salvar essas alterações no arquivo de configuração de inicialização – impedindo, portanto, que as alterações sejam perdidas devido à falha de energia ou reinicialização intencional (CISCO NETACAD, 2017).

Antes de se comprometer com as alterações, use os comandos *show* adequados para verificar a operação do dispositivo. O comando *show running-config* pode ser empregado para verificar um arquivo de configuração em execução. Quando as

alterações forem certificadas como corretas, use o comando `copy running-config startup-config` no prompt do modo EXEC privilegiado. Por sua vez, o comando para salvar a configuração em execução ao arquivo de configuração de inicialização é `Router# copy running-config startup-config`

Depois de ser executado, o arquivo de configuração em execução atualizará o arquivo de configuração de inicialização (CISCO NETACAD, 2017).

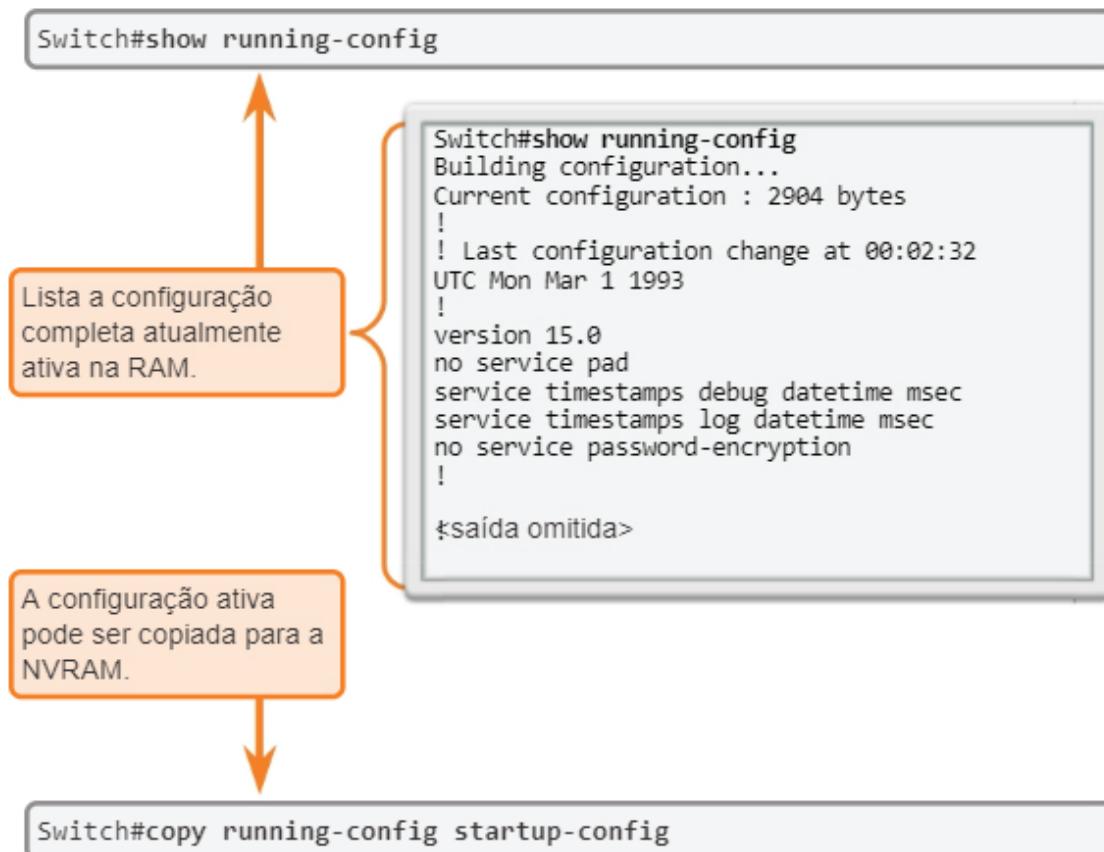


Figura 7 – Arquivos de configuração

Se as alterações realizadas à configuração de execução não tiverem o efeito desejado, pode ser necessário restaurar o dispositivo à sua condição anterior. Considerando que não sobrescrevemos a configuração de inicialização com as alterações, podemos substituir a configuração em execução pela de inicialização – o que é melhor realizado ao reiniciar o dispositivo usando o comando `reload` no prompt do modo EXEC privilegiado (CISCO NETACAD, 2017).

Ao iniciar uma recarga, o IOS detectará que o running config tem alterações que não foram salvas na configuração de inicialização. Um prompt aparecerá para perguntar se será necessário salvar as alterações realizadas. Já para descartar tais alterações, insira `n` ou `no` (CISCO NETACAD, 2017). Outro prompt aparecerá para confirmar a recarga; assim, pressione Enter – pressionar qualquer outra tecla abortará o processo.

# Material Complementar

## Indicações para saber mais sobre os assuntos abordados nesta Unidade:

### Sites

#### **Módulo de Introdução a Redes – capítulo 1: explorando a rede, versão 6.0**

CISCO NETACAD. **Módulo de Introdução a Redes** – Capítulo 1: Explorando a Rede, versão 6.0. Estados Unidos: Cisco Systems, 2017a. Disponível em:

<https://goo.gl/lNdwR>

#### **Módulo de Introdução a Redes – Capítulo 2: Explorando a Rede, versão 6.0**

\_\_\_\_\_. Módulo de Introdução a Redes – Capítulo 2: Explorando a Rede, versão 6.0. Estados Unidos: Cisco Systems, 2017b.

<https://goo.gl/lNdwR>

### Livros

#### **Redes de Computadores e a Internet**

STALLINGS, W.; ROSS K. **Redes de computadores e a internet**. 5. ed. São Paulo: Pearson, 2010.

#### **Redes de Computadores**

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores**. 5. ed. Rio de Janeiro: Campus, 2011.

# Referências

CISCO NETACAD. **Módulo de Introdução a Redes (CCNA1)**. 6. ver. Estados Unidos: Cisco Systems, 2017. Disponível em: <<http://www.netacad.com>>. Acesso em: 20 out. 2018.

STALLINGS, W.; ROSS K. **Redes de Computadores e a Internet**. 5. ed. São Paulo: Pearson, 2010.

TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores**. 5. ed. Rio de Janeiro: Campus, 2011.



**Cruzeiro do Sul**  
Educacional